ANNALES

DE

L'INSTITUT FOURIER

Nigel P. BYOTT & Bouchaïb SODAÏGUI

Realizable Galois module classes over the group ring for non abelian extensions

Tome 63, nº 1 (2013), p. 303-371.

<http://aif.cedram.org/item?id=AIF_2013___63_1_303_0>

Ann. Inst. Fourier, Grenoble
63, 1 (2013) 303-371

REALIZABLE GALOIS MODULE CLASSES OVER THE GROUP RING FOR NON ABELIAN EXTENSIONS

by Nigel P. BYOTT & Bouchaïb SODAÏGUI

ABSTRACT. — Given an algebraic number field k and a finite group Γ, we write $\mathcal{R}(O_k[\Gamma])$ for the subset of the locally free classgroup $\mathrm{Cl}(O_k[\Gamma])$ consisting of the classes of rings of integers O_N in tame Galois extensions N/k with $\mathrm{Gal}(N/k) \cong \Gamma$. We determine $\mathcal{R}(O_k[\Gamma])$, and show it is a subgroup of $\mathrm{Cl}(O_k[\Gamma])$ by means of a description using a Stickelberger ideal and properties of some cyclic codes, when k contains a root of unity of prime order p and $\Gamma = V \rtimes C$, where V is an elementary abelian group of order p^r and C is a cyclic group of order $m > 1$ acting faithfully on V and making V into an irreducible $\mathbb{F}_p[C]$-module. This extends and refines results of Byott, Greither and Sodaïgui for $p = 2$ in Crelle, respectively of Bruche and Sodaïgui for $p > 2$ in J. Number Theory, which cover only the case $m = p^r - 1$ and determine only the image $\mathcal{R}(\mathcal{M})$ of $\mathcal{R}(O_k[\Gamma])$ under extension of scalars from $O_k[\Gamma]$ to a maximal order $\mathcal{M} \supset O_k[\Gamma]$ in $k[\Gamma]$. The main result here thus generalizes the calculation of $\mathcal{R}(O_k[A_4])$ for the alternating group A_4 of degree 4 (the case $p = r = 2$) given by Byott and Sodaïgui in Compositio.

RÉSUMÉ. — Étant donné un corps de nombres k et un groupe fini Γ, on note $\mathcal{R}(O_k[\Gamma])$ le sous-ensemble du groupe de classes localement libre $\mathrm{Cl}(O_k[\Gamma])$ formé par les classes d'anneaux d'entiers O_N d'extensions galoisiennes modérées N/k avec $\mathrm{Gal}(N/k) \cong \Gamma$. Nous déterminons $\mathcal{R}(O_k[\Gamma])$, et montrons que c'est un sous-groupe de $\mathrm{Cl}(O_k[\Gamma])$, au moyen d'une description utilisant un idéal de Stickelberger et des propriétés de certains codes cycliques, lorsque k contient une racine de l'unité d'ordre premier p et $\Gamma = V \rtimes C$, où V est un groupe élémentaire abélien d'ordre p^r et C est un groupe cyclique d'ordre $m > 1$ agissant fidèlement sur V et rendant V un $\mathbb{F}_p[C]$-module irréductible. Ceci généralise et raffine des résultats de Byott, Greither et Sodaïgui pour $p = 2$ dans Crelle, respectivement de Bruche et Sodaïgui pour $p > 2$ dans J. Number Theory, lesquels couvrent seulement le cas $m = p^r - 1$ et déterminent seulement l'image $\mathcal{R}(\mathcal{M})$ de $\mathcal{R}(O_k[\Gamma])$ sous l'extension des scalaires de $O_k[\Gamma]$ à un ordre maximal $\mathcal{M} \supset O_k[\Gamma]$ dans $k[\Gamma]$. Le résultat principal ici généralise donc le calcul de $\mathcal{R}(O_k[A_4])$ pour le groupe alterné A_4 de degré 4 (le cas $p = r = 2$) donné par Byott et Sodaïgui dans Compositio.

Keywords: Galois module structure; Rings of algebraic integers; Locally free classgroup; Fröhlich-Lagrange resolvent; Realizable classes; Embedding problem; Stickelberger ideal; Cyclic codes.
Math. classification: 11R33.

1. Introduction

For any number field k, we write O_k for the ring of algebraic integers of k, k^c for an algebraic closure of k, and $\Omega_k = \mathrm{Gal}(k^c/k)$ for the absolute Galois group of k. We say that an extension of number fields is tame if it is at most tamely ramified. Given a finite group Γ, we will say N is a Γ-extension of k if N/k is a Galois extension of fields equipped with an isomorphism $\mathrm{Gal}(N/k) \longrightarrow \Gamma$. We write ξ_n for a primitive nth root of unity in k^c.

If N is a tame Γ-extension of k then O_N is a locally free module of rank 1 over the group ring $O_k[\Gamma]$, and its structure as such is determined up to stable isomorphism by its class $(O_N)_{O_k[\Gamma]}$ in the locally free class group $\mathrm{Cl}(O_k[\Gamma])$. We define the set $\mathcal{R}(O_k[\Gamma])$ of *realizable classes* in $\mathrm{Cl}(O_k[\Gamma])$ to be the subset of $\mathrm{Cl}(O_k[\Gamma])$ consisting of the classes $(O_N)_{O_k[\Gamma]}$ as N runs through all tame Γ-extensions of k. It is expected that $\mathcal{R}(O_k[\Gamma])$ is always a subgroup of $\mathrm{Cl}(O_k[\Gamma])$, but this is not known in general; indeed, a proof even that $\mathcal{R}(O_k[\Gamma])$ is nonempty would solve the inverse Galois problem for Γ over k.

In this paper we will determine $\mathcal{R}(O_k[\Gamma])$ for certain metabelian groups Γ under a mild restriction on k. In particular, our results will show that $\mathcal{R}(O_k[\Gamma])$ is indeed a subgroup of $\mathrm{Cl}(O_k[\Gamma])$ in the cases we consider.

We first explain the background to this work. For tame extensions N of $\mathbb{Q}$, the situation is well understood. The theorem of Taylor [27], previously conjectured by Fröhlich, shows how the Galois module class in $\mathrm{Cl}(\mathbb{Z}[\Gamma])$ of the ring of integers O_N of a tame Γ-extension of a number field k is related to the symplectic root numbers of the extension. In particular, taking $k = \mathbb{Q}$, it follows that any class in $\mathcal{R}(\mathbb{Z}[\Gamma])$ has order at most 2, and if Γ has no irreducible symplectic characters (e.g., if Γ is abelian or of odd order) then $\mathcal{R}(\mathbb{Z}[\Gamma])$ is the trivial subgroup of $\mathrm{Cl}(\mathbb{Z}[\Gamma])$, provided only that tame Γ-extensions of $\mathbb{Q}$ exist at all.

For abelian groups Γ, realizable classes over more general base fields have been thoroughly investigated by McCulloh [17, 18, 19]. A homomorphism $\phi\colon G \longrightarrow H$ of finite groups induces a homomorphism of classgroups $\phi_*\colon \mathrm{Cl}(O_k[G]) \longrightarrow \mathrm{Cl}(O_k[H])$ (see [13, §II.3] or §2.1 below). The subset $\mathcal{R}(O_k[\Gamma])$ is stable under the automorphisms δ_* of $\mathrm{Cl}(O_k[\Gamma])$ induced by $\delta \in \mathrm{Aut}(\Gamma)$ since we may "twist" a Γ-extension N by composing the given isomorphism $\mathrm{Gal}(N/k) \cong \Gamma$ with δ. In [17], McCulloh gave an explicit description of $\mathcal{R}(O_k[C_p])$ for the cyclic group C_p of prime order p, under the assumption $\xi_p \in k$, in terms of the action on $\mathrm{Cl}(O_k[C_p])$ of the Stickelberger ideal in $\mathbb{Z}[\mathrm{Aut}(C_p)]$. This was generalized in [18] to describe $\mathcal{R}(O_k[V])$ for

an elementary abelian group V of order p^r (and without the hypothesis $\xi_p \in k$). In this case, V can be identified with the additive group of the finite field $\mathbb{F}_{p^r}$ of order p^r. Let C_0 be the cyclic subgroup of $\mathrm{Aut}(V)$ of order $p^r - 1$ given by multiplication by elements of $\mathbb{F}_{p^r}^{\times}$. Then there is a Stickelberger ideal $\mathcal{J} \subseteq \mathbb{Z}[C_0]$. (We recall its definition in §3.4 below.) The trivial group homomorphism $\epsilon\colon V \longrightarrow \{1\}$ induces a homomorphism $\epsilon_*\colon \mathrm{Cl}(O_k[V]) \longrightarrow \mathrm{Cl}(O_k)$, where $\mathrm{Cl}(O_k)$ is the ideal classgroup of O_k. The main result of [18] can then be stated in the following form:

$$\mathcal{R}(O_k[V]) = \mathcal{J} \cdot \ker(\epsilon_*), \tag{1}$$

where the right-hand side denotes the subgroup of $\ker(\epsilon_*)$ generated by all elements $j \cdot a$ with $j \in \mathcal{J}$ and $a \in \ker(\epsilon_*)$. McCulloh further treated the case of an arbitrary finite abelian group Γ in [19], where he characterized $\mathcal{R}(O_k[\Gamma])$ in terms of Fröhlich's idèlic Hom-Description of $\mathrm{Cl}(O_k[\Gamma])$ (cf. [13]). In this case, the Stickelberger ideal is replaced by a Stickelberger map, and the resulting description of $\mathcal{R}(O_k[\Gamma])$ is less explicit than (1) but again shows that $\mathcal{R}(O_k[\Gamma])$ is a subgroup of $\mathrm{Cl}(O_k[\Gamma])$. We shall therefore regard $\mathcal{R}(O_k[\Gamma])$ as being in principle known for any finite abelian group Γ and any number field k. Much of McCulloh's approach can be extended to certain wildly ramified extensions (and even to certain non-Galois extensions) by replacing the group ring $O_k[\Gamma]$ with a commutative Hopf order: see [2, 3].

For nonabelian groups, much less is known. A fruitful approach is to extend scalars from $O_k[\Gamma]$ to a maximal order $\mathcal{M} \supset O_k[\Gamma]$ in $k[\Gamma]$, and then to investigate the image $\mathcal{R}(\mathcal{M})$ of $\mathcal{R}(O_k[\Gamma])$ in $\mathrm{Cl}(\mathcal{M})$. This has been done in a number of cases [1, 4, 15, 22, 23, 24, 25, 26]. In particular, nonabelian groups Γ of order lq, with $l > q$ both prime, were considered in [23] under the assumption that $k \cap \mathbb{Q}(\xi_{lq}) = \mathbb{Q}$. This was generalized in [22] to groups Γ of order lm, with m an arbitrary divisor of $l - 1$, under the weaker assumption $k \cap \mathbb{Q}(\xi_l) = \mathbb{Q}$. In both these papers, what is actually characterized is the subset $\mathcal{R}_1(\mathcal{M})$ of $\mathcal{R}(\mathcal{M})$ consisting of the classes realized by tame Γ-extensions N of k with $N \cap k(\xi_l) = k$. (See [22, p. 1820] for a correction to [23]). A different family of metabelian groups was treated in [4], where $\mathcal{R}(\mathcal{M})$ was determined when $\Gamma = V \rtimes C$ is a group of order $2^r(2^r - 1)$ for $r \geqslant 2$, constructed as the semidirect product of an elementary abelian group V of order 2^r by a cyclic group C of order $2^r - 1$ acting faithfully on V. When $r = 2$, Γ is the alternating group A_4 and the result in this case was previously given in [15] under some assumptions on the base field. An analogous result to that of [4] for the corresponding metabelian groups of order $p^r(p^r - 1)$ (where p is an odd

prime) was given in [1] under the hypothesis $\xi_p \in k$. In both [1] and [4] we drew on the language of coding theory: the construction of Γ-extensions can be conveniently described in terms of a certain cyclic code of length $p^r - 1$ (for $p = 2$ and $p > 2$ respectively) over the field $\mathbb{F}_p$.

Our goal in this paper is to improve on the results in [1] and [4] in two directions, treating the cases $p = 2$ and $p > 2$ simultaneously. We again assume that $\xi_p \in k$. The first improvement is that we will work over the group ring $O_k[\Gamma]$ rather than over a maximal order $\mathcal{M}$, so that we obtain a description of $\mathcal{R}(O_k[\Gamma])$ itself and not just of its image $\mathcal{R}(\mathcal{M})$. To do this we extend the techniques of [5] and [6], where we considered realizable classes over the group ring for, respectively, the dihedral group of order 8 and the alternating group A_4. (The main result of [6] is therefore covered here as a special case; see after Corollary 7.3.2 below.) The second improvement is that we allow a somewhat more general family of metabelian groups Γ: we now take Γ to be the semidirect product $V \rtimes C$ of an elementary abelian group V of order p^r by any cyclic group C of order $m > 1$ which acts faithfully on V and makes V into an irreducible $\mathbb{F}_p[C]$-module. We will show in Proposition 4.1.1 that this can occur if and only if m is a divisor of $p^r - 1$ which does not divide $p^s - 1$ for any $s < r$. Moreover, Γ is then a normal subgroup in a group $\Gamma_0 = V \rtimes C_0$, where C_0 is cyclic of order $p^r - 1$; in the case $m = p^r - 1$ we have $\Gamma = \Gamma_0$, and Γ is the group considered in [1] (for $p > 2$) or [4] (for $p = 2$). For our groups Γ, therefore, $\mathrm{Cl}(O_k[\Gamma])$ is a $\mathbb{Z}[C_0]$-module, where the action of C_0 on $\mathrm{Cl}(O_k[\Gamma])$ is induced by its action on Γ via conjugation inside Γ_0. In fact C_0 is related to V in the same way as in McCulloh's result (1). If D is any C_0-stable subgroup of $\mathrm{Cl}(O_k[\Gamma])$, we can therefore form its image $\mathcal{J} \cdot D \subseteq D$ under the Stickelberger ideal $\mathcal{J} \subseteq \mathbb{Z}[C_0]$.

To state our main results, we require some further notation. Viewing C and V as subgroups of Γ, we have the inclusion homomorphisms

$$\iota^C : C \longrightarrow \Gamma, \qquad \iota^V : V \longrightarrow \Gamma.$$

Viewing C as a quotient of Γ, we also have the canonical surjection

$$\pi : \Gamma \longrightarrow C = \Gamma/V.$$

These induce homomorphisms of classgroups

$$\iota^C_* : \mathrm{Cl}(O_k[C]) \longrightarrow \mathrm{Cl}(O_k[\Gamma]), \qquad \iota^V_* : \mathrm{Cl}(O_k[V]) \longrightarrow \mathrm{Cl}(O_k[\Gamma]),$$

$$\pi_* : \mathrm{Cl}(O_k[\Gamma]) \longrightarrow \mathrm{Cl}(O_k[C]).$$

Using McCulloh's result that the realizable classes form a group in the abelian case, we therefore have subgroups $\iota^C_* \mathcal{R}(O_k[C])$ and $\iota^V_* \mathcal{R}(O_k[V])$ of

$\mathcal{R}(O_k[\Gamma])$. Also, $\ker(\pi_*)$ is stable under C_0 because V is normal in Γ_0, so we can form the subgroup $\mathcal{J}\cdot\ker(\pi_*)$ of $\mathrm{Cl}(O_k[\Gamma])$.

The first of our main results gives two characterizations of the set $\mathcal{R}(O_k[\Gamma])$ of realizable classes in $\mathrm{Cl}(O_k[\Gamma])$.

THEOREM 1. — *Let p be a prime number, and let $\Gamma = V \rtimes C$ be a metabelian group of order $p^r m$ as above. Let k be any number field containing a primitive pth root of unity ξ_p. Then*

$$\mathcal{R}(O_k[\Gamma]) = (\iota_*^C\mathcal{R}(O_k[C]))\,(\iota_*^V\mathcal{R}(O_k[V])) = (\iota_*^C\mathcal{R}(O_k[C]))(\mathcal{J}\cdot\ker(\pi_*)).$$

Moreover, given any finite set S of finite places of k and any class $\mathcal{A}\in\mathcal{R}(O_k[\Gamma])$, there are infinitely many tame Γ-extensions N of k with $(O_N)_{O_k[\Gamma]} = \mathcal{A}$, and N can be chosen to satisfy the following properties: N/k is unramified at all places in S, and every intermediate field $F\neq k$ of N/k is ramified at some finite place of k.

It is immediate from Theorem 1 that $\mathcal{R}(O_k[\Gamma])$ is a subgroup of $\mathrm{Cl}(O_k[\Gamma])$ under our hypotheses on Γ and k.

We reformulate this result in a more concrete form, allowing easier comparison with [1] and [4], at the end of this paper (see Theorem 7.3.1).

The proof of Theorem 1 proceeds via a relative version (see Theorem 2 below). Given a tame C-extension E of k, we say that N is a Γ-extension of k *relative to* E if $E\subset N$ and the isomorphism $\mathrm{Gal}(N/k)\longrightarrow\Gamma$ associated to N induces the given isomorphism $\mathrm{Gal}(E/k)\longrightarrow C=\Gamma/V$. We write $\mathcal{R}(O_k[\Gamma],E)\subseteq\mathrm{Cl}(O_k[\Gamma])$ for the set of classes $(O_N)_{O_k[\Gamma]}$ where N runs through all tame Γ-extensions of k relative to E. For each finite group G, there is a Fröhlich norm homomorphism (see §2.1 below)

$$\mathcal{N}_{E/k}\colon \mathrm{Cl}(O_E[G])\longrightarrow\mathrm{Cl}(O_k[G]).$$

THEOREM 2. — *Under the hypotheses of Theorem 1, for each tame C-extension E of k we have*

$$\mathcal{R}(O_k[\Gamma],E) = (\iota_*^C(O_E)_{O_k[C]})(\iota_*^V\mathcal{N}_{E/k}(\mathcal{R}(O_E[V]))).$$

Moreover, given any finite set S_E of finite places of E and any class $\mathcal{A}\in\mathcal{R}(O_k[\Gamma],E)$, there are infinitely many tame Γ-extensions N of k relative to E with $(O_N)_{O_k[\Gamma]}=\mathcal{A}$, and N can be chosen to satisfy the following properties: N/E is unramified at all places in S_E, and every intermediate field $F\neq E$ of N/E is ramified at some finite place of E.

We are not able to resolve completely the question of how the class $(O_N)_{O_k[\Gamma]}$ is related to the classes $(O_E)_{O_k[C]}$ and $(O_N)_{O_E[V]}$ associated to the intermediate extensions E/k and N/E of N/k. The following result

provides a partial answer in terms of the extension-of-scalars homomorphism $\mathbf{i}_{E/k}\colon \mathrm{Cl}(O_k[G]) \longrightarrow \mathrm{Cl}(O_E[G])$ induced by the inclusion $k \hookrightarrow E$ (again, see §2.1 below).

THEOREM 3. — *Let N be a tame Γ-extension of k relative to E, and suppose that either $r = 1$ or that all the places of E above p split completely in N. Then the class $(O_N)_{O_k[\Gamma]}$ in $\mathrm{Cl}(O_k[\Gamma])$ factorizes as*

$$(O_N)_{O_k[\Gamma]} = (\iota_*^C(O_E)_{O_k[C]})\mathcal{X},$$

where the class $\mathcal{X} \in \mathrm{Cl}(O_k[\Gamma])$ satisfies

$$\mathbf{i}_{E/k}(\mathcal{X}) = \iota_*^V((O_N)_{O_E[V]}) \text{ in } \mathrm{Cl}(O_E[\Gamma]).$$

(We do not know whether Theorem 3 holds for $r \geqslant 2$ without the hypothesis on places above p, but the analogous result does always hold over a maximal order $\mathcal{M} \supset O_k[\Gamma]$ in $k[\Gamma]$; see Theorem 7.1.3.)

In the excluded case $m = 1$, the assertions of Theorems 2 and 3 and the first equality of Theorem 1 are trivially true and the second equality of Theorem 1 reduces to McCulloh's result (1).

The proof of the above results will occupy most of the paper (§§2–6), and draws quite heavily on the methods of [1] and [4]. In particular, we shall again use the language of cyclic codes. After developing some general tools for working with locally free classgroups in §2, we give various results on cyclic codes in §3. We will in fact need to consider codes both of length m and of length $p^r - 1$, corresponding to the two groups C and C_0. We will also explain how McCulloh's Stickelberger ideal is related to these codes. In §4, we consider the group $\Gamma = V \rtimes C$ occurring in our main results, and describe various subgroups of $\mathrm{Cl}(O_k[\Gamma])$. The key steps in the proofs of our main results occur in §5, where we explicitly construct all tame Γ-extensions of k relative to a given C-extension E, obtain factorisations for the corresponding Galois module classes, and determine a number of properties of the factors. Our strategy here is somewhat different to that in [1, 4], where we were working over a maximal order $\mathcal{M}$ in $k[\Gamma]$. The class $(O_N)_{\mathcal{M}} \in \mathrm{Cl}(\mathcal{M})$ corresponding to N is determined by the Steinitz classes associated to N/k and its various subextensions, and we characterised the realizable Galois module classes over $\mathcal{M}$ by first finding the realizable Steinitz classes. Over the group ring $O_k[\Gamma]$, however, the Steinitz classes no longer suffice to describe $(O_N)_{O_k[\Gamma]}$, so we are forced to work directly with local normal integral bases of our extensions. Thus in §5 we need to specify suitable local normal integral bases and obtain precise information on their resolvents. We put all the pieces together to complete the proof of Theorems 1–3 in §6.

In the final section of the paper (§7), we relate our main results to earlier work. Functorial properties of the classgroups will allow us to read off both the realizable Galois module classes in $\mathrm{Cl}(\mathcal{M})$, and the realizable Steinitz classes in $\mathrm{Cl}(O_k)$. Thus the main results of [1] and [4] will turn out to be corollaries (in the case $m = p^r - 1$) of Theorems 1 and 2 (see Theorem 7.2.3 and Corollary 7.3.2).

We do not attempt here to remove the hypothesis $\xi_p \in k$, but we hope to return to this problem in a future publication. There are several possible approaches to this. The most direct would be to use Kummer descent arguments, adapting the methods used in the unpublished thesis of Endo [10]. (A summary of Endo's results is given in the Appendix of [7].) Alternatively, one could try to use the resolvend machinery developed by McCulloh in [18, 19]; this essentially gives a version of Kummer theory in which the pth roots of unity are replaced by the nontrivial elements of V. A third possibility would be to use the techniques recently introduced by Cobbe [8] to study realizable Steinitz classes, where the relevant extensions are constructed directly from class field theory without recourse to Kummer theory. It would be interesting to see whether Cobbe's methods can be adapted to give information on realizable Galois module classes.

2. Preliminaries on locally free classgroups

In this section we recall Fröhlich's Hom-Description of the locally free classgroup and set out, in a form convenient for our purposes, some tools for working with it. We also briefly describe the formalism of Galois algebras, which enables us to understand the behaviour of rings of algebraic integers as Galois modules on passing to completions of number fields. The techniques described in this section were applied in a somewhat ad-hoc fashion in our earlier papers [5, 6], but we present them here in a more general context.

2.1. The Hom-Description

We briefly recall some standard facts about Fröhlich's idèlic Hom-Description of the locally free classgroup $\mathrm{Cl}(O_k[G])$ for an arbitrary finite group G and an arbitrary number field k (see [13]). In contrast to [13], we take Galois groups to act on the left (although for notational convenience we shall often write the action exponentially on the right).

The Fröhlich Hom-Description consists of an isomorphism

$$\mathrm{Cl}(O_k[G]) \cong \frac{\mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))}{\mathrm{Hom}_{\Omega_k}(R_G, k^{c\times})\mathrm{Det}(\mathbb{U}(O_k[G]))}, \tag{2}$$

where the notation is as follows: k^c is an algebraic closure of k, $\Omega_k = \mathrm{Gal}(k^c/k)$ is the absolute Galois group of k, R_G is the group of virtual characters of G, $\mathbb{J}(k^c)$ is the idèle group of k^c (that is, the limit of the idèle groups $\mathbb{J}(L)$ as L runs over all finite extensions of k), $\mathbb{U}(O_k[G])$ is the group of unit idèles of $O_k[G]$, and $\mathrm{Det}\colon \mathbb{U}(O_k[G]) \longrightarrow \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$ is the determinant map given by $\mathrm{Det}(\alpha)(\chi) = \det(T_\chi(\alpha))$ for any representation T_χ affording the character χ.

For later use, we give a generalization of this Det map. For an invertible matrix $\alpha = (\alpha_{ij}) \in \mathrm{GL}_m(\mathbb{A}(k[G]))$ over the adèle ring $\mathbb{A}(k[G])$ of $k[G]$, we define $\mathrm{Det}_\chi(\alpha) = \mathrm{Det}(\alpha)(\chi)$ to be the determinant over $\mathbb{A}(k)$ of the block matrix whose entry in row i and column j is the matrix $T_\chi(\alpha_{ij})$.

Now let N be a tame G-extension of k. Then O_N is a locally free $O_k[G]$-module of rank 1. We recall how to construct a character homomorphism $h \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$ representing the class $(O_N)_{O_k[G]}$ under (2).

Let $\mathfrak{p}$ be any place of k. We write $O_{k,\mathfrak{p}}$ for the completion of O_k at $\mathfrak{p}$, with the usual convention that $O_{k,\mathfrak{p}} = \mathbb{R}$ (respectively $\mathbb{C}$) for a real (respectively complex) place $\mathfrak{p}$. If $\mathfrak{p}$ is a finite place, we also write $\mathfrak{p}$ for the corresponding prime ideal of O_k.

By the Normal Basis Theorem, N is a free $k[G]$-module of rank 1, with generator α, say. We will refer to α as a normal basis for N/k. For each place $\mathfrak{p}$, let $\alpha_\mathfrak{p}$ be a generator of the free rank 1 $O_{k,\mathfrak{p}}[G]$-module $O_{N,\mathfrak{p}} = O_N \otimes_{O_k} O_{k,\mathfrak{p}}$. We will refer to $\alpha_\mathfrak{p}$ as a local normal integral basis for N/K at $\mathfrak{p}$. By the Weak Approximation Theorem, we can choose α so that it is also a local normal integral basis at any given finite set of places. It is convenient to consider α and the $\alpha_\mathfrak{p}$ as a single entity, so we define

$$\boldsymbol{\alpha} = (\alpha, (\alpha_\mathfrak{p})_\mathfrak{p}) \in N \times \prod_\mathfrak{p} O_{N,\mathfrak{p}}$$

(where the product is over all places $\mathfrak{p}$ of k) to be a *normal basis system* for N/k if α is a normal basis for N/k and $\alpha_\mathfrak{p}$ is a local normal integral basis for N/k at each $\mathfrak{p}$. Given a normal basis system $\boldsymbol{\alpha}$ for N/k and an intermediate field E of N/k, we define

$$\mathrm{Tr}_{N/E}(\boldsymbol{\alpha}) = (\mathrm{Tr}_{N/E}(\alpha), (\mathrm{Tr}_{N_\mathfrak{p}/E_\mathfrak{p}}(\alpha_\mathfrak{p}))_\mathfrak{p}).$$

If E/k is Galois then $\mathrm{Tr}_{N/E}(\boldsymbol{\alpha})$ is a normal basis system for E/k.

For each character χ of G we form the Fröhlich-Lagrange resolvent

$$\langle \alpha, \chi \rangle_{N/k} = \det \left(\sum_{g \in G} g(\alpha) T_\chi(g^{-1}) \right) \in k^c,$$

and similarly we form the local resolvents $\langle \alpha_\mathfrak{p}, \chi \rangle_{N/k} \in O_{k,\mathfrak{p}}^c$ for each $\mathfrak{p}$. From [13, Theorem 4, p. 30] we then have

LEMMA 2.1.1. — *Let $\boldsymbol{\alpha} = (\alpha, (\alpha_\mathfrak{p})_\mathfrak{p})$ be a normal basis system for N/k and let $h_{\boldsymbol{\alpha}} \in \mathrm{Hom}(R_G, \mathbb{J}(k^c))$ be the character homomorphism defined by*

$$h_{\boldsymbol{\alpha}}(\chi) = \left(\frac{\langle \alpha_\mathfrak{p}, \chi \rangle_{N/k}}{\langle \alpha, \chi \rangle_{N/k}} \right)_\mathfrak{p} \quad \textit{for each character } \chi \textit{ of } G.$$

Then $h_\alpha \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$, and its class under (2) represents $(O_N)_{O_k[G]}$.

We next consider the functorial behaviour of locally free classgroups under change of group and change of base field: see [13, §II.3]. A homomorphism $\phi\colon G \longrightarrow H$ of finite groups induces a homomorphism of classgroups $\phi_*\colon \mathrm{Cl}(O_k[G]) \longrightarrow \mathrm{Cl}(O_k[H])$, given at the level of character homomorphisms by $\phi_*\colon \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c)) \longrightarrow \mathrm{Hom}_{\Omega_k}(R_H, \mathbb{J}(k^c))$ with

$$(\phi_* h)(\chi) = h(\chi \circ \phi) \text{ for } h \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c)) \text{ and } \chi \in R_H.$$

In particular, if $\iota\colon F \longrightarrow G$ is the inclusion of a subgroup F in G then $(\iota_* h)(\chi) = h(\mathrm{Res}_F^G \chi)$ for $\chi \in R_G$, where Res denotes restriction of characters. Similarly, if Q is a quotient of G and $\pi\colon G \longrightarrow Q$ is the canonical surjection, then $(\pi_* h)(\chi) = h(\mathrm{Inf}_Q^G \chi)$ for $\chi \in R_Q$, where Inf denotes inflation of characters. (Thus, in the notation of [13], we have $\iota_* = \mathrm{Ind}_F^G$ and $\pi_* = \mathrm{Coinf}_Q^G$.)

Finally there are two homomorphisms of classgroups associated to each extension F/k of number fields. Firstly, the Fröhlich norm

$$\mathcal{N}_{F/k}\colon \mathrm{Cl}(O_F[G]) \longrightarrow \mathrm{Cl}(O_k[G]),$$

(see [13, §II.3, Theorem 13]) is induced by the map of character homomorphisms

$$\mathcal{N}_{F/k}\colon \mathrm{Hom}_{\Omega_F}(R_G, \mathbb{J}(k^c)) \longrightarrow \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$$

defined as follows: let X be a fixed left transversal of Ω_F in Ω_k, and for $h \in \mathrm{Hom}_{\Omega_F}(R_G, \mathbb{J}(k^c))$ set

$$(\mathcal{N}_{F/k} h)(\chi) = \prod_{\omega \in X} h(\chi^{\omega^{-1}})^\omega.$$

Secondly, the extension-of-scalars homomorphism $\mathbf{i}_{F/k}\colon \mathrm{Cl}(O_k[G]) \longrightarrow \mathrm{Cl}(O_F[G])$ is induced by the inclusion

$$\mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c)) \hookrightarrow \mathrm{Hom}_{\Omega_F}(R_G, \mathbb{J}(k^c)).$$

For a locally free $O_k[G]$-module M we have $\mathbf{i}_{F/k}((M)_{O_k[G]}) = (M \otimes_{O_k} O_F)_{O_F[G]}$ (see [12, p. 186]).

2.2. Congruences on character homomorphisms

Given a finite group G and a number field k, let us fix once and for all a system of orbit representatives $\chi_1, \ldots, \chi_t$ of the absolutely irreducible characters of G under the action of Ω_k. Then a character homomorphism $h \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$ is determined by its values on the χ_i, and each $h(\chi_i)$ can be chosen arbitrarily in the idèle group $\mathbb{J}(k_i)$ of the field $k_i = k(\chi_i)$ obtained by adjoining the values of χ_i to k. Our choice of orbit representatives therefore allows us to make the identification

$$\mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c)) = \prod_{i=1}^{t} \mathbb{J}(k_i), \tag{3}$$

where h corresponds to its t-tuple of values $(h(\chi_1), \ldots, h(\chi_t))$. Similarly,

$$\mathrm{Hom}_{\Omega_k}(R_G, k^{c\times}) = \prod_{i=1}^{t} k_i^{\times}. \tag{4}$$

The factors in these decompositions correspond to the Wedderburn components of the group algebra $k[G]$: we have

$$k[G] = \prod_{i=1}^{t} A_i,$$

where A_i is a simple algebra with center k_i, and χ_i is an absolutely irreducible constituent of the character of G afforded by A_i. The dimension of A_i over k_i is a square, say

$$\dim_{k_i}(A_i) = n_i^2, \tag{5}$$

where $\chi_i(1)/n_i$ is the Schur index of χ_i relative to k. The map

$$\mathrm{Det}\colon k[G]^{\times} = \prod_{i=1}^{t} A_i^{\times} \longrightarrow \prod_{i=1}^{t} k_i^{\times}$$

coincides with $\prod_{i=1}^{t} \mathrm{nr}_i$, where $\mathrm{nr}_i = \mathrm{nr}_{A_i/k_i}$ is the reduced norm in the ith component.

We shall use the identifications (3) and (4) to bound the denominator in the Hom-Description (2). We first introduce some more notation.

For $1 \leqslant i \leqslant t$, let $\mathfrak{f}_i$ be an integral ideal of O_{k_i}, and let $\mathbb{U}_{\mathfrak{f}_i}(k_i, \chi_i)^+$ be the subgroup of $\mathbb{U}(O_{k_i})$ consisting of unit idèles $(u_{\mathfrak{P}})_{\mathfrak{P}}$ such that:

(i) if $\mathfrak{P}$ is a finite place of k_i, then $u_{\mathfrak{P}} \equiv 1 \pmod{\mathfrak{f}_i O_{k_i,\mathfrak{P}}}$;

(ii) if $\mathfrak{P}$ is a real place of k_i and χ_i is symplectic, then $u_{\mathfrak{P}} > 0$.

Then let

$$\mathrm{Cl}_{\mathfrak{f}_i}(k_i, \chi_i)^+ = \frac{\mathbb{J}(k_i)}{k_i^\times \mathbb{U}_{\mathfrak{f}_i}(k_i, \chi_i)^+}.$$

Thus if the irreducible character χ_i is not symplectic, then $\mathrm{Cl}_{\mathfrak{f}_i}(k_i, \chi_i)$ is the ray classgroup $\mathrm{Cl}_{\mathfrak{f}_i}(O_{k_i})$ of O_{k_i} with conductor $\mathfrak{f}_i$, while if χ is symplectic then $\mathrm{Cl}_{\mathfrak{f}}(k_i, \chi_i)$ is the ray classgroup $\mathrm{Cl}_{\mathfrak{f}_i \cdot \infty}(O_{k_i})$ whose conductor is the formal product of $\mathfrak{f}_i$ and all real places of k_i.

LEMMA 2.2.1. — *For each i, let $\mathfrak{f}_i$ be an O_{k_i}-ideal divisible by $|G|/n_i$. Let $h \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$ and suppose that*

$$h(\chi_i) \in k_i^\times \mathbb{U}_{\mathfrak{f}_i}(k_i, \chi_i)^+ \text{ for } 1 \leqslant i \leqslant t.$$

Then h represents the trivial class in $\mathrm{Cl}(O_k[G])$.

Equivalently, the canonical surjection $\mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c)) \longrightarrow \mathrm{Cl}(O_k[G])$ factors through

$$\prod_{i=1}^{t} \mathrm{Cl}_{\mathfrak{f}_i}(k_i, \chi_i)^+.$$

Proof. — With the identification (3), it is clear from (2) that both assertions are equivalent to

$$\prod_{i=1}^{t} \mathbb{U}_{\mathfrak{f}_i}(k, \chi_i)^+ \subseteq \mathrm{Det}(\mathbb{U}(O_k[G])). \tag{6}$$

We will verify the corresponding inclusion at each place $\mathfrak{p}$ of k.

Let $\mathcal{M}$ be a maximal order in $k[G]$ such that $\mathcal{M} \supseteq O_k[G]$. Then

$$\mathcal{M} = \prod_{i=1}^{t} \mathcal{M}_i,$$

where $\mathcal{M}_i$ is a maximal O_{k_i}-order in A_i. By Jacobinski's formula [20, (41.3)] for the conductor of $O_k[G]$ into $\mathcal{M}$, we have

$$\prod_{i=1}^{t} \mathfrak{f}_i \mathcal{M}_i \subset O_k[G]. \tag{7}$$

If $\mathfrak{p}$ is an infinite place then, by [9, p. 337], $\mathrm{Det}(O_{k,\mathfrak{p}}[G]^\times) = \mathrm{Det}(\mathcal{M}_{\mathfrak{p}}^\times)$ consists of the character homomorphisms h with $h(\chi_i)_{\mathfrak{P}}$ real and positive

whenever χ_i is symplectic and $\mathfrak{P}$ is a place of k^c above a real place of k. Since the values of a symplectic character χ_i are real, the places of $k(\chi_i)$ above real places of k are precisely the real places of $k(\chi_i)$. Thus the components at an infinite place $\mathfrak{p}$ on the two sides of (6) agree.

Now let $\mathfrak{p}$ be a finite place of k. Given $(a_1,\dots,a_t) \in \prod_i O_{k_i,\mathfrak{p}}^\times$ with $a_i \equiv 1 \pmod{\mathfrak{f}_i O_{k_i,\mathfrak{p}}}$ for each i, we claim that there exist α_i for $1 \leqslant i \leqslant t$ with $\alpha_i \in \mathcal{M}_{i,\mathfrak{p}}^\times$ and $\alpha_i \equiv 1 \pmod{\mathfrak{f}_i \mathcal{M}_{i,\mathfrak{p}}}$ and $\mathrm{nr}_i(\alpha_i) = a_i$. This will give the required inclusion for the components at $\mathfrak{p}$ in (6), since $(\alpha_1,\dots,\alpha_t) \in O_{k,\mathfrak{p}}[G]^\times$ by (7) and $\mathrm{Det}((\alpha_1,\dots,\alpha_t)) = (\mathrm{nr}_1(\alpha_1),\dots,\mathrm{nr}_t(\alpha_t)) = (a_1,\dots,a_t)$. Moreover, we have

$$\mathcal{M}_{i,\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{M}_{i,\mathfrak{P}}, \tag{8}$$

where the product is over the places $\mathfrak{P}$ of k_i above $\mathfrak{p}$. It will therefore suffice to find for each i an element $\beta_i \in (1+\mathfrak{f}_i\mathcal{M}_{i,\mathfrak{P}}) \cap \mathcal{M}_{i,\mathfrak{P}}^\times$ with $\mathrm{nr}_i(\beta_i) = a_i$ for *one* place $\mathfrak{P}$ of k_i above $\mathfrak{p}$, since we can then take $\alpha_i = (\beta_i, 1, \dots, 1)$ in the product (8), where the first entry corresponds to the place $\mathfrak{P}$. But $A_{i,\mathfrak{P}} = M_s(D)$ for some $s \geqslant 1$ and some division algebra D with center $k_{i,\mathfrak{P}}$. Replacing $\mathcal{M}_i$ by a conjugate, we may assume that $\mathcal{M}_{i,\mathfrak{P}} = M_s(\Lambda)$ where Λ is the unique maximal order in D. We can also assume that $s = 1$, since if $\beta_i \in \Lambda$ has reduced norm a_i in $k_{i,\mathfrak{P}}$, then so does the diagonal matrix with diagonal entries $\beta_i, 1, \dots, 1$. But when $s = 1$ we have the explicit description of D, and hence of Λ, given in the proof of [20, (14.6)] (see in particular equation (14.7)). A simple induction then shows that the reduced norm (determinant) induces surjections

$$\frac{\Lambda^\times}{1+\mathfrak{P}\Lambda} \twoheadrightarrow \frac{O_{k_i,\mathfrak{P}}^\times}{1+\mathfrak{P}}, \qquad \frac{1+\mathfrak{P}^j\Lambda}{1+\mathfrak{P}^{j+1}\Lambda} \twoheadrightarrow \frac{1+\mathfrak{P}^j}{1+\mathfrak{P}^{j+1}} \text{ for } j \geqslant 1.$$

By completeness, we then have

$$\mathrm{nr}(\Lambda^\times) = {O_{k_i,\mathfrak{P}}}^\times, \qquad \mathrm{nr}(1+\mathfrak{P}^j\Lambda) = 1+\mathfrak{P}^j \text{ for } j \geqslant 1,$$

so that $a_i = \mathrm{nr}(\beta_i)$ for some $\beta_i \in (1+\mathfrak{f}_i\Lambda) \cap \Lambda^\times$ as required. □

2.3. Quotient groups

Let N be a normal subgroup of the finite group G, with quotient $Q = G/N$. In this subsection we examine the homomorphism $\pi_* \colon \mathrm{Cl}(O_k[G]) \to \mathrm{Cl}(O_k[Q])$ induced by the canonical surjection $\pi \colon G \to Q$.

Any character χ of G which is trivial on N induces a character $\overline{\chi}$ on Q such that $\overline{\chi} \circ \pi = \chi$. Thus $\chi = \mathrm{Inf}_Q^G \overline{\chi}$. All characters of Q arise in this way,

and $\overline{\chi}$ is irreducible if and only if χ is. Thus if $\mathcal{A} \in \mathrm{Cl}(O_k[G])$ is represented by $h \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$ then $\pi_*(\mathcal{A})$ is represented by the character homomorphism $\pi_* h \in \mathrm{Hom}_{\Omega_k}(R_Q, \mathbb{J}(k^c))$ determined by $(\pi_* h)(\overline{\chi}) = h(\chi)$ for each character χ of G trivial on N.

LEMMA 2.3.1. — *Suppose that the surjection $\pi\colon G \to Q$ splits. Then, for a class $\mathcal{A} \in \mathrm{Cl}(O_k[G])$, the following are equivalent:*

(i) $\mathcal{A} \in \ker \pi_*$;
(ii) *$\mathcal{A}$ is represented by some $h' \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$ with $h'(\chi) = 1$ for all characters χ of G trivial on N.*

Proof. — The implication (ii)⇒(i) is immediate from the above discussion. For the converse, suppose that $h \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$ represents $\mathcal{A}$. Then, by (2) for Q, we have $\pi_* h = \kappa \,\mathrm{Det}(u)$ for some $\kappa \in \mathrm{Hom}_{\Omega_k}(R_Q, k^{c\times})$ and $u \in \mathbb{U}(O_k[Q]))$. Define $\widetilde{\kappa} \in \mathrm{Hom}_{\Omega_k}(R_G, k^{c\times})$ by

$$\widetilde{\kappa}(\chi) = \begin{cases} \kappa(\overline{\chi}) & \text{if } \chi \text{ is trivial on } N; \\ 1 & \text{if } \chi \text{ is nontrivial on } N. \end{cases}$$

Since π splits, there is an injective group homomorphism $Q \hookrightarrow G$. This induces an inclusion $\mathbb{U}(O_k[Q])) \hookrightarrow \mathbb{U}(O_k[G]))$. We write $\widetilde{u} \in \mathbb{U}(O_k[G]))$ for the image of u under this inclusion. Then $h' = (\widetilde{\kappa}\,\mathrm{Det}(\widetilde{u}))^{-1} h$ has the required properties. □

2.4. Fröhlich's Induction Formula

We next give a result, due to Fröhlich ([11, Theorem 7] or [12, Theorem 12]) on resolvents for induced characters. As we will require more precise information on the local units than is given in these references, we include a more detailed proof than the sketch provided in [11].

LEMMA 2.4.1. — *Let N be a tame G-extension of k, let H be a subgroup of G (not necessarily normal) of index m, and fix an ordered left transversal X of H in G. Let $F = N^H$. Let $\boldsymbol{\alpha} = (\alpha, (\alpha_\mathfrak{p})_\mathfrak{p})$ and $\boldsymbol{\eta} = (\eta, (\eta_\mathfrak{p})_\mathfrak{p})$ be normal basis systems for N/k and N/F respectively. Let $(\beta_i)_{1\leqslant i\leqslant m}$ be a k-basis for F, and for each place $\mathfrak{p}$ of k let $(\beta_{\mathfrak{p},i})_{1\leqslant i\leqslant m}$ be an $O_{k,\mathfrak{p}}$-basis for $O_{F,\mathfrak{p}}$. Let ψ be a character of H and let $\chi = \mathrm{Ind}_H^G \psi$ be the character of G induced from ψ. Define a matrix $\lambda = (\lambda_{ig}) \in \mathrm{GL}_m(k[H])$ by*

$$\beta_i \eta = \sum_{g\in X} \lambda_{ig} g^{-1}(\alpha). \tag{9}$$

Let R_η be the map taking each character ψ' of H to the resolvent $\langle \eta, \psi' \rangle_{N/F}$. Then

$$\langle \alpha, \chi \rangle_{N/k} \mathrm{Det}_\psi(\lambda) = e(F/k)^{\deg(\psi)} (\mathcal{N}_{F/k} R_\eta)(\psi), \tag{10}$$

where

$$e(F/k) = \det(g(\beta_i))_{g \in X, 1 \leqslant i \leqslant m}. \tag{11}$$

For each place $\mathfrak{p}$ of k we likewise have

$$\langle \alpha_\mathfrak{p}, \chi \rangle_{N/k} \mathrm{Det}_\psi(\lambda_\mathfrak{p}) = e_\mathfrak{p}(F/k)^{\deg(\psi)} (\mathcal{N}_{F/k} R_{\eta_\mathfrak{p}})(\psi), \tag{12}$$

with analogous definitions of $R_{\eta_\mathfrak{p}}$, $\lambda_\mathfrak{p}$ and $e_\mathfrak{p}(F/k)$.

Proof. — We fix a representation $T_\psi \colon H \longrightarrow M_s(k^c)$ affording the character ψ. We will prove the identity (10), the proof of (12) being similar.

For any $k[H]$-basis $\mathcal{A} = \{a_1, \ldots, a_m\}$ of N we define $R_\psi(\mathcal{A}) = (R_\psi(\mathcal{A})_{ig})$ to be the block matrix, with rows indexed by $i \in \{1, \ldots, m\}$ and columns indexed by $g \in X$, whose entry in row i and column g is the matrix

$$R_\psi(\mathcal{A})_{ig} = \sum_{h \in H} gh(a_i) T_\psi(h^{-1}) \in M_s(k^c).$$

We then define $\mathrm{Det}_\psi(\mathcal{A})$ to be the determinant of $R_\psi(\mathcal{A})$, regarded as an $ms \times ms$ matrix over k^c. (One can check that $\mathrm{Det}_\psi(\mathcal{A})$ is in fact independent of the choice of T_ψ).

Now suppose that $\mathcal{B} = \{b_1, \ldots, b_m\}$ is another $k[H]$-basis for N, satisfying

$$b_i = \sum_{j=1}^{m} \lambda_{ij} a_j \tag{13}$$

with $\lambda = (\lambda_{ij}) \in \mathrm{GL}_m(k[H])$. For each pair i, j, we write

$$\lambda_{ij} = \sum_{h_1 \in H} \lambda_{ijh_1} h_1, \quad \lambda_{ijh_1} \in k.$$

Then we calculate

$$\begin{aligned} R_\psi(\mathcal{B})_{ig} &= \sum_{h\in H} gh\left(\sum_j \lambda_{ij}a_j\right) T_\psi(h^{-1}) \\ &= \sum_j \sum_{h_1} \lambda_{ijh_1} \sum_h ghh_1(a_j) T_\psi(h^{-1}) \\ &= \sum_j \sum_{h_1} \lambda_{ijh_1} \sum_{h_2} gh_2(a_j) T_\psi(h_1 h_2^{-1}) \\ &= \sum_j \left(\sum_{h_1} \lambda_{ijh_1} T_\psi(h_1)\right)\left(\sum_{h_2} gh_2(a_j) T_\psi(h_2^{-1})\right) \\ &= \sum_j \Lambda_{ij} R_\psi(\mathcal{A})_{jg}, \end{aligned}$$

where $\Lambda = (\Lambda_{ij})$ is the block matrix whose determinant defines $\mathrm{Det}_\psi(\lambda)$. Thus we have the equation

$$R_\psi(\mathcal{B}) = \Lambda R_\psi(\mathcal{A})$$

in $M_{ms}(k^c)$, and taking determinants yields

$$\mathrm{Det}_\psi(\mathcal{B}) = \mathrm{Det}_\psi(\lambda)\mathrm{Det}_\psi(\mathcal{A}). \tag{14}$$

The induced character $\chi = \mathrm{Ind}_H^G \psi$ is afforded by the representation T_χ constructed as follows: $T_\chi(g)$ for $g \in G$ is the block matrix, with rows and columns indexed by X, whose entry in row g_1 and column g_2 is $T_\psi(g_2^{-1} g g_1)$, where we adopt the convention $T_\psi(g') = 0$ if $g' \notin H$. The resolvent $\langle \alpha, \chi\rangle_{N/k}$ is therefore the determinant of the block matrix $\sum_{z\in G} z^{-1}(\alpha) T_\chi(z)$ whose entry in row g_1 and column g_2 (for $g_1, g_2 \in X$) is the matrix

$$\sum_{z\in G} z^{-1}(\alpha) T_\psi(g_2^{-1} z g_1) = \sum_{g\in X, h\in H} h^{-1}g^{-1}(\alpha) T_\psi(g_2^{-1} g h g_1).$$

We consider this entry for fixed g_1, $g_2 \in X$. For each $\hat{h} \in H$, there are unique elements $g \in X$ and $h \in H$ with $g_2^{-1} g h g_1 = \hat{h}$, and it is readily checked that the function $\hat{h} \mapsto h$ is a permutation of H. We may therefore write the above sum as

$$\sum_{\hat{h}\in H} g_1 \hat{h}^{-1} g_2^{-1}(\alpha) T_\psi(\hat{h}) = \sum_{h\in H} g_1 h(g_2^{-1}(\alpha)) T_\psi(h^{-1}).$$

But this is just the entry in row g_1 and column g_2 in the block matrix $R_\psi(\mathcal{A})$, where $\mathcal{A}$ is the $k[H]$-basis $\{g_2^{-1}(\alpha)\}_{g_2\in X}$ of N. Taking determinants, we then have

$$\langle \alpha, \chi\rangle_{N/k} = \mathrm{Det}_\psi(\mathcal{A}).$$

Now let $\mathcal{B}$ be the basis $\{\beta_i\eta\}_{1\leqslant i\leqslant m}$. Then (13) holds for the matrix $\lambda \in \mathrm{GL}_m(k[H])$ of (9), and $\mathrm{Det}_\psi(\mathcal{B})$ is the determinant of the block matrix $R_\psi(\mathcal{B})$ whose entry in row i and column g is

$$\begin{aligned} R_\psi(\mathcal{B})_{ig} &= \sum_{h\in H} gh(\beta_i\eta)T_\psi(h^{-1}) \\ &= g(\beta_i)\left(\sum_h h(\eta)T_\psi^{g^{-1}}(h^{-1})\right)^g. \end{aligned}$$

Thus $R_\psi(\mathcal{B})$ is the product of two block matrices, the first of which has in row i and column g the matrix $g(\beta_i)I_s$ (where I_s is the identity matrix of size $s = \deg(\psi)$), while the second is block diagonal and has as its diagonal entries the matrices whose determinants define $\langle \eta, \psi^{g^{-1}}\rangle_{N/F}^g$ for $g \in X$. These two block matrices have determinants $e(F/k)^{\deg(\psi)}$ and $(\mathcal{N}_{F/k}R_\eta)(\psi)$ respectively, where $\mathcal{N}_{F/k}$ is evaluated using the transversal X. Thus

$$\mathrm{Det}_\psi(\mathcal{B}) = e(F/k)^{\deg(\psi)}(\mathcal{N}_{F/k}R_\eta)(\psi),$$

and (10) follows from (14). □

Remark 2.4.2. — The element $e(F/k)^2$ is the discriminant of the basis β_i of F/k, and $e(F/k)_\mathfrak{p}^2 O_{k,\mathfrak{p}} = \Delta(F/k)O_{k,\mathfrak{p}}$, where $\Delta(F/k)$ is the relative discriminant of F/k. Equivalently, $e(F/k)_\mathfrak{p}^2 O_{k,\mathfrak{p}}$ is the discriminant of the semilocal $O_{k,\mathfrak{p}}$-algebra $O_{F,\mathfrak{p}}$.

Corollary 2.4.3. — *Suppose that N/k is tame. Let $h_{\boldsymbol{\alpha}} \in \mathrm{Hom}_{\Omega_k}(R_G, \mathbb{J}(k^c))$ and $h_{\boldsymbol{\eta}} \in \mathrm{Hom}_{\Omega_F}(R_H, \mathbb{J}(k^c))$ be the character homomorphisms constructed from $\boldsymbol{\alpha}$ and $\boldsymbol{\eta}$ as in Lemma 2.1.1. Then*

$$h_{\boldsymbol{\alpha}}(\chi) = \left(\frac{\mathrm{Det}_\psi(\lambda_\mathfrak{p})}{\mathrm{Det}_\psi(\lambda)}\right)_\mathfrak{p}^{-1}\left(\frac{e_\mathfrak{p}(F/k)}{e(F/k)}\right)_\mathfrak{p}^{\deg\psi}(\mathcal{N}_{F/k}h_{\boldsymbol{\eta}})(\psi).$$

We now see how Lemma 2.4.1 can be simplified in special cases.

Proposition 2.4.4. — *Suppose that H is normal in G, and that $F = N^H$ is tame over k. Let $Q = G/H$, and pick a normal basis system $\boldsymbol{\beta} = (\beta, (\beta_\mathfrak{p})_\mathfrak{p})$ for F/k over $k[Q]$. Fix an ordered* **right** *transversal $\sigma_1, \ldots, \sigma_m$ of H in G. Then in Lemma 2.4.1 we may take λ to be the matrix (λ_{ij})*

defined by

$$\sigma_i(\beta)\eta = \sum_{j=1}^{m} \lambda_{ij}\sigma_j(\alpha), \tag{15}$$

and $e(F/k)$ *to be defined by*

$$e(F/k) = \det(\sigma_i^{-1}\sigma_j(\beta))_{1\leqslant i,j\leqslant m}, \tag{16}$$

with similar statements for the $\lambda_{\mathfrak{p}}$ *and* $e_{\mathfrak{p}}(F/k)$.

Moreover, suppose that Q *is abelian and that we choose* $\boldsymbol{\beta} = \mathrm{Tr}_{N/F}(\boldsymbol{\alpha})$. *Then*

$$\left(\frac{e_{\mathfrak{p}}(F/k)}{e(F/k)}\right)_{\mathfrak{p}} = h_{\boldsymbol{\alpha}}(\mathrm{Inf}_Q^G r_Q),$$

where r_Q *is the regular representation of* Q.

Proof. — Take the left transversal X to be $\sigma_1^{-1}, \ldots, \sigma_m^{-1}$, and take $\beta_i = \sigma_i(\beta)$ and $\beta_{\mathfrak{p},i} = \sigma_i(\beta_{\mathfrak{p}})$ for each $\mathfrak{p}$. Then (9), (11) and their analogues at $\mathfrak{p}$ reduce to (15), (16) and their analogues at $\mathfrak{p}$.

Now suppose that Q is abelian and $\boldsymbol{\beta} = \mathrm{Tr}_{N/F}(\boldsymbol{\alpha})$. The characters ϕ of G which are trivial on H are in bijection with the characters $\overline{\phi}$ of Q via $\phi = \mathrm{Inf}_Q^G\overline{\phi}$. We have

$$\langle \alpha, \phi\rangle_{N/k} = \langle \beta, \overline{\phi}\rangle_{F/k}$$

and similarly at each place $\mathfrak{p}$.

Since $r_Q = \sum_{\overline{\phi}\in Q^\dagger} \overline{\phi}$, where $Q^\dagger$ is the group of 1-dimensional characters of Q, we therefore have

$$h_{\boldsymbol{\alpha}}(\mathrm{Inf}_Q^G r_Q) = \prod_{\overline{\phi}\in Q^\dagger} \left(\frac{\langle \alpha_{\mathfrak{p}}, \phi\rangle_{N/k}}{\langle \alpha, \phi\rangle_{N/k}}\right)_{\mathfrak{p}} = \prod_{\overline{\phi}\in Q^\dagger} \left(\frac{\langle \beta_{\mathfrak{p}}, \overline{\phi}\rangle_{F/k}}{\langle \beta, \overline{\phi}\rangle_{F/k}}\right)_{\mathfrak{p}}.$$

Now

$$\prod_{\overline{\phi}\in Q^\dagger} \langle \beta, \overline{\phi}\rangle_{F/k} = \det(\sigma_i^{-1}\sigma_j(\beta))_{0\leqslant i,j\leqslant m-1} = e(F/k)$$

by a well-known determinantal formula (see [14, (A14)]), and similarly

$$\prod_{\overline{\phi}\in Q^\dagger} \langle \beta_{\mathfrak{p}}, \overline{\phi}\rangle_{F/k} = e_{\mathfrak{p}}(F/k)$$

for each place $\mathfrak{p}$. The result follows. □

2.5. Galois algebras and completions

It will be convenient to formulate part of our argument (see §§5.5, 5.6) in the language of Galois algebras, as developed in [19, §1]. In this section, we briefly review that language.

Let K be an arbitrary field, with absolute Galois group Ω_K, and let G be a finite group. Any homomorphism $\varpi\colon \Omega_K \longrightarrow G$ determines a G-Galois algebra

$$K_\varpi = \mathrm{Map}_{\Omega_K}({}^{\varpi}G, K^c)$$

whose elements are the functions $h\colon G \longrightarrow K^c$ with $h(\varpi(\tau)g) = \tau(h(g))$ for all $\tau \in \Omega_K$ and $g \in G$. The action of G (from the left) on K_ϖ is given by

$$(g' \cdot h)(g) = h(gg') \text{ for } g, g' \in G.$$

The values of the functions $h \in K_\varpi$ lie in the field $N = (K^c)^{\ker(\varpi)}$. Choosing a system of coset representatives for $\varpi(\Omega_K)\backslash G$, we obtain an isomorphism of K-algebras between K_ϖ and a product of $[G : \varpi(\Omega_K)]$ copies of N. In particular, if ϖ is surjective, we can identify K_ϖ with N by choosing the identity element as our representative of the single coset. We write $[n]\colon G \longrightarrow K^c$ for $n \in N$ considered as element of K_ϖ. Thus $[n](g) = g(n)$ for all $g \in G$. In this case, ϖ induces an isomorphism $\mathrm{Gal}(N/K) = \Omega_K/\ker(\varpi) \longrightarrow G$, so that N becomes a G-extension of K. Conversely, any G-extension N of K is a Galois algebra $\mathrm{Map}_{\Omega_K}({}^{\varpi}G, K^c)$ for some surjective homomorphism $\varpi\colon \Omega_K \longrightarrow G$. Abusing notation, we write $\mathrm{Map}_G(G, N)$ for N regarded as a Galois algebra in this fashion.

We next consider the behaviour of Galois algebras under completion. Let now k be a number field, and let N be a G-Galois algebra over k. The semilocal completion $N_\mathfrak{p} = N \otimes_k k_\mathfrak{p}$ is then identified with the G-Galois algebra $\mathrm{Map}_{\Omega_k}(G, k^c \otimes_k k_\mathfrak{p})$ over $k_\mathfrak{p}$. If N is a field, $N_\mathfrak{p}$ need not be a field. Indeed, as $k_\mathfrak{p}$-algebras, we have the well-known decomposition

$$N_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} N_\mathfrak{P},$$

where the product is over all places $\mathfrak{P}$ of O_N above $\mathfrak{p}$. The Galois algebra formalism enables us to keep track of the action of G on this product. Fix one place $\mathfrak{P}$ of O_N above $\mathfrak{p}$, let $i\colon N \longrightarrow N_\mathfrak{P}$ be the corresponding inclusion, and let $D \subseteq G$ be the decomposition group of $\mathfrak{P}$. Then the identification $N = \mathrm{Map}_G(G, N)$ induces an isomorphism

$$N_\mathfrak{p} \cong \mathrm{Map}_D(G, N_\mathfrak{P}),$$

where, explicitly, $n \otimes x$ corresponds to the map $g \mapsto i(g(n))x$. The semilocal completion $O_{N,\mathfrak{p}} = O_N \otimes_{O_k} O_{k,\mathfrak{p}}$ of O_N at $\mathfrak{p}$ then corresponds to the maximal $O_{k,\mathfrak{p}}$-order $\mathrm{Map}_D(G, O_{N,\mathfrak{P}})$ in $\mathrm{Map}_D(G, N_{\mathfrak{P}})$.

3. Codes and Stickelberger Ideals

For the rest of the paper, we fix the prime number p. As in [1, 4], it is convenient to work in terms of certain cyclic codes over $\mathbb{F}_p$. Whereas in these earlier papers we only required codes of length $p^r - 1$, here we will need codes both of length m and of length $p^r - 1$. In this section, we explain how these two codes are related, and we interpret McCulloh's Stickelberger ideal in terms of these codes.

3.1. Generalities on cyclic codes

In this subsection, we set out the terminology and notation needed in our discussion of cyclic codes, and we recall some elementary results. A more detailed account of most of this material can be found, for example, in [21].

A linear code $\mathcal{C}$ of length m and dimension d over $\mathbb{F}_p$ is simply a d-dimensional subspace of the $\mathbb{F}_p$-vector space $\mathbb{F}_p^m$. The reverse code $\hat{\mathcal{C}}$ of $\mathcal{C}$ is obtained by reversing the order of the components in $\mathbb{F}_p^m$:

$$\hat{\mathcal{C}} = \{(a_{m-1}, a_{m-2}, \ldots, a_0) \mid (a_0, a_1, \ldots, a_{m-1}) \in \mathcal{C}\}.$$

The code $\mathcal{C}$ is *cyclic* if it is stable under the shift operator

$$(a_0, a_1, \ldots, a_{m-1}) \mapsto (a_{m-1}, a_0, \ldots, a_{m-2}). \tag{17}$$

Thus a cyclic code $\mathcal{C}$ is a module over the group algebra $\mathbb{F}_p[C]$, where $C = \langle\sigma\rangle$ is a cyclic group of order m whose generator σ acts as the shift operator (17). Indeed, if we identify $\mathbb{F}_p^m$ with $\mathbb{F}_p[C]$ by making the vector $(a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_p^m$ correspond to $\sum_{i=0}^{m-1} a_i\sigma^i$, then a linear code $\mathcal{C} \subseteq \mathbb{F}_p[C]$ is cyclic if and only if it is an ideal of $\mathbb{F}_p[C]$. We shall always regard cyclic codes as ideals of group algebras in this way.

Now $\mathbb{F}_p[C]$ is the image of the polynomial algebra $\mathbb{F}_p[X]$ under the ring homomophism taking the indeterminate X to σ: we have

$$\mathbb{F}_p[C] \cong \mathbb{F}_p[X]/(X^m - 1).$$

For any polynomial $h \neq 0$ in $\mathbb{F}_p[X]$, we write $\hat{h}$ for its reciprocal polynomial:

$$\hat{h}(X) = X^{\deg g} h(X^{-1}).$$

As $\mathbb{F}_p[X]$ is a principal ideal domain, every cyclic code $\mathcal{C}$ in $\mathbb{F}_p[C]$ has the form $(g(\sigma)) = g(\sigma)\mathbb{F}_p[C]$ for a unique monic divisor $g(X)$ of $X^m - 1$ in $\mathbb{F}_p[X]$. We call $g(X)$ the generator of $\mathcal{C}$. The reverse code $\hat{\mathcal{C}}$ of $\mathcal{C}$ is then the ideal $(\hat{g}(\sigma))$, and $\hat{\mathcal{C}}$ has generator $g(0)^{-1}\hat{g}(X)$.

Let $f \in \mathbb{F}_p[X]$ be the polynomial such that

$$f(X)g(X) = X^m - 1 \text{ in } \mathbb{F}_p[X]. \tag{18}$$

Then the dimension of the code $(g(\sigma))$ is $\deg f$, and the following result is immediate.

PROPOSITION 3.1.1. — *Let $g(X)$ be a monic divisor of $X^m - 1$ in $\mathbb{F}_p[X]$. Let $\mathcal{C} = (g(\sigma)) \subseteq \mathbb{F}_p[C]$ be the corresponding cyclic code of length m, and let f be as in (18). Let $\hat{f}$ be the reciprocal polynomial of f . Then, for any $h(\sigma) \in \mathbb{F}_p[C]$ we have*

$$h(\sigma) \in \mathcal{C} \Leftrightarrow h(\sigma)f(\sigma) = 0 \text{ in } \mathbb{F}_p[C]$$

and

$$h(\sigma) \in \hat{\mathcal{C}} \Leftrightarrow h(\sigma)\hat{f}(\sigma) = 0 \text{ in } \mathbb{F}_p[C].$$

□

This says that we may interpret f as a parity check polynomial for $\mathcal{C}$. Then $(\hat{f}(\sigma))$ is the dual code of $\mathcal{C}$ (cf. [21, Theorem 7.4.4, p. 325]).

3.2. Lifting and integral weights

We shall often need to consider preimages in $\mathbb{Z}[C]$ of elements of $\mathbb{F}_p[C]$. We shall always choose the preimage for which each coefficient lies in $\{0, \ldots, p-1\}$. For an element

$$\alpha = \sum_{i=0}^{m-1} a_i \sigma^i \in \mathbb{F}_p[C],$$

we will frequently abuse notation by also writing α for the corresponding element of $\mathbb{Z}[C]$:

$$\alpha = \sum_{i=0}^{m-1} A_i \sigma^i \in \mathbb{Z}[C]$$

where $A_i \in \{0, \ldots, p-1\}$ has image a_i in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We will then refer $\sum_{i=0}^{m-1} A_i\sigma^i$ as α **considered as an element of** $\mathbb{Z}[C]$. Where there is any possibility of confusion, we will indicate explicitly whether equations are to be understood as holding in $\mathbb{F}_p[C]$ or in $\mathbb{Z}[C]$.

We define the integral weight of $\alpha \in \mathbb{F}_p[C]$ to be the sum of the coefficients in α, considered as an element of $\mathbb{Z}[C]$:

$$w_{int}(\alpha) = \sum_i A_i \in \mathbb{Z}.$$

Note that this is **not** the same as the Hamming weight (i.e., the number of coefficients $\neq 0$ in $\mathbb{F}_p$) except in the case $p = 2$.

In a similar fashion, **we will consider polynomials in $\mathbb{F}_p[X]$ as elements of $\mathbb{Z}[X]$ by lifting each coefficient in $\mathbb{F}_p$ to its preimage in $\{0, \dots, p-1\} \subset \mathbb{Z}$.**

3.3. The codes $\mathcal{C}$ and $\mathcal{C}_0$

We now introduce the cyclic codes needed to prove our main result.

We fix an integer $r \geqslant 1$, and a monic irreducible polynomial $f(X) \neq X-1$ or X of degree r in $\mathbb{F}_p[X]$. (Thus $r \geqslant 2$ if $p = 2$.) Let ω be a root of f in $\mathbb{F}_{p^r}$, and let $m > 1$ be the order of ω in $\mathbb{F}_{p^r}^\times$. Then $\mathbb{F}_p(\omega) = \mathbb{F}_{p^r}$, so m divides $p^r - 1$ but does not divide $p^s - 1$ for $s < r$.

We set $d = (p^r - 1)/m$. Then $\omega = \omega_0^d$ for some generator ω_0 of $\mathbb{F}_{p^r}^\times$. Let f_0 be the minimal polynomial of ω_0. Since $\omega^m = \omega_0^{p^r-1} = 1$, there are polynomials g, $g_0 \in \mathbb{F}_p[X]$ with

$$f(X)g(X) = X^m - 1; \quad f_0(X)g_0(X) = X^{p^r-1} - 1 \text{ in } \mathbb{F}_p[X]. \tag{19}$$

Then

$$\deg f = \deg f_0 = r; \quad \deg g = m - r; \quad \deg g_0 = p^r - 1 - r.$$

The polynomials $X^{p^r-1} - 1$ and $X^m - 1$ are separable over $\mathbb{F}_p$, so f_0 and g_0 are coprime, as are f and g. In particular, we have

$$g_0(\omega_0) \neq 0 \text{ in } \mathbb{F}_{p^r}. \tag{20}$$

Moreover, since $p^r - 1 \geqslant m > 1$, we have

$$f(1) \neq 0, \quad f_0(1) \neq 0, \quad g(1) = g_0(1) = 0 \text{ in } \mathbb{F}_p, \tag{21}$$

and as $f(\omega_0^d) = f(\omega) = 0$, we have

$$f_0(X) \text{ divides } f(X^d) \text{ in } \mathbb{F}_p[X]. \tag{22}$$

Now let $C = \langle\sigma\rangle \subseteq C_0 = \langle\sigma_0\rangle$ be cyclic groups of order m, $p^r - 1$ respectively, with generators related by $\sigma = \sigma_0^d$. The codes we shall consider are $\mathcal{C} = (g(\sigma)) \subseteq \mathbb{F}_p[C]$ of length m and dimension r, and $\mathcal{C}_0 = (g_0(\sigma_0)) \subseteq \mathbb{F}_p[C_0]$ of length $p^r - 1$ and dimension r, together with their reverse codes $\hat{\mathcal{C}} = (\hat{g}(\sigma))$ and $\hat{\mathcal{C}}_0 = (\hat{g}_0(\sigma_0))$.

DEFINITION 3.3.1. — *Let P denote the set of polynomials over $\mathbb{F}_p$ of degree at most $r-1$:*

$$P = \{a_0 + a_1 X + \ldots + a_{r-1}X^{r-1} \mid a_0, \ldots, a_{r-1} \in \mathbb{F}_p\}.$$

Then each element of $\mathcal{C}$ (respectively $\mathcal{C}_0$, respectively $\mathbb{F}_{p^r}$) can be written $a(\sigma)g(\sigma)$ (respectively $a(\sigma_0)g_0(\sigma_0)$, respectively $a(\omega)$) for a unique $a \in P$.

DEFINITION 3.3.2. — *For all $j \in \mathbb{Z}$, let $c^{(j)}$ be the unique element of P with*

$$c^{(j)}(\omega) = \omega_0^j \text{ in } \mathbb{F}_{p^r}.$$

We then set

$$g^{(j)}(\sigma) = c^{(j)}(\sigma)g(\sigma) \in \mathbb{F}_p[C],$$
$$\mathcal{C}^{(j)} = \{\sigma^h g^{(j)}(\sigma) \mid 0 \leqslant h \leqslant m-1\},$$

and

$$w_j = w_{int}(g^{(j)}(\sigma)).$$

LEMMA 3.3.3. — *The code $\mathcal{C}$ is the disjoint union of $\{0\}, \mathcal{C}^{(0)}, \ldots, \mathcal{C}^{(d-1)}$. For all i, $j \in \mathbb{Z}$ we have*

$$\sigma\mathcal{C}^{(j)} = \mathcal{C}^{(j)} = \mathcal{C}^{(j+d)} \text{ and } c^{(i)}(\sigma)\mathcal{C}^{(j)} = \mathcal{C}^{(i+j)} \tag{23}$$

Moreover, for each j, the codewords in $\mathcal{C}^{(j)}$ all have integral weight w_j, and w_j is divisible by p.

Proof. — We have an isomorphism of $\mathbb{F}_p[C]$-modules

$$\mathcal{C} \longrightarrow \mathbb{F}_p[C]/(f(\sigma))$$

induced by $a(\sigma)g(\sigma) \mapsto a(\sigma)$ for any $a \in \mathbb{F}_p[X]$. On the other hand, we have isomorphisms of finite fields

$$\mathbb{F}_p[C]/(f(\sigma)) \cong \mathbb{F}_{p^r}$$

induced by $\sigma \mapsto \omega$. Composing these, we obtain an $\mathbb{F}_p$-linear bijection between $\mathcal{C}$ and $\mathbb{F}_{p^r}$, in which $a(\sigma)g(\sigma)$ corresponds to $a(\omega)$, and each element of $\mathcal{C}$ (respectively $\mathbb{F}_{p^r}$) occurs exactly once as a runs through P.

Each element of $\mathbb{F}_{p^r}^\times$ can be written in the form $\omega_0^{hd+j} = \omega^h c^{(j)}(\omega)$ (with $h \in \mathbb{Z}$) for a unique $j \in \{0, \ldots, d-1\}$. It follows that each nonzero codeword in $\mathcal{C}$ can be written in the form $\sigma^h c^{(j)}(\sigma)g(\sigma) = \sigma^h g^{(j)}(\sigma) \in \mathcal{C}^{(j)}$ for a unique $j \in \{0, \ldots, d-1\}$. As $\mathcal{C}^{(j)}$ clearly consists of nonzero codewords, $\mathcal{C}$ is the disjoint union of $\{0\}$ and the $\mathcal{C}^{(j)}$. Then (23) follows immediately from the definitions.

Since all the codewords in $\mathcal{C}^{(j)}$ are obtained by repeatedly shifting $g^{(j)}(\sigma)$, they all have the same integral weight: this is just $w_j = g^{(j)}(1)$ where

$g^{(j)}(X)$ is now considered as an element of $\mathbb{Z}[X]$. But in $\mathbb{F}_p$ we have $g^{(j)}(1) = c^{(j)}(1)g(1) = 0$ by (21), so w_j is divisible by p. □

Remark 3.3.4. — In the case $m = p^r - 1$ we have $\mathcal{C}_0 = \mathcal{C}$, and Lemma 3.3.3 says that all the nonzero codewords have the same integral weight. In fact, they all have integral weight $p^r(p-1)/2$ and Hamming weight $p^{r-1}(p-1)$ (see [1, Proposition 2.6] and [4, Lemme 3.6] for the corresponding statements for $\hat{\mathcal{C}}$; the argument is the same for $\mathcal{C}$). For $m < p^r - 1$, neither the integral weights nor the Hamming weights need be the same for all nonzero codewords.

LEMMA 3.3.5. — *In $\mathbb{F}_p[C_0]$, we can write $g_0(\sigma_0)$ uniquely in the form*

$$g_0(\sigma_0) = \sum_{j=0}^{d-1} r_j(\sigma)\sigma_0^j \tag{24}$$

where $r_j(\sigma) \in \mathcal{C}$ for each j. Moreover, there exists $n \in \{0, \dots, d-1\}$ such that

$$r_i(\sigma) \in \mathcal{C}^{(n-i)}$$

for each i.

Proof. — Since $\sigma = \sigma_0^d$, it is clear that we can write $g_0(\sigma_0)$ uniquely in the form (24) for some $r_j(\sigma) \in \mathbb{F}_p[C]$. We must show that the $r_j(\sigma)$ lie in $\mathcal{C}$.

By (22) we have $f(X^d) = h(X)f_0(X)$ for some $h \in \mathbb{F}_p[X]$, so

$$f(\sigma)g_0(\sigma_0) = f(\sigma_0^d)g_0(\sigma_0) = h(\sigma_0)f_0(\sigma_0)g_0(\sigma_0) = 0 \text{ in } \mathbb{F}_p[C_0],$$

since $f_0(\sigma_0)g_0(\sigma_0) = \sigma_0^{p^r-1} - 1 = 0$. But

$$f(\sigma)g_0(\sigma_0) = \sum_{j=0}^{d-1} \big(f(\sigma)r_j(\sigma)\big)\sigma_0^j,$$

so $f(\sigma)r_j(\sigma) = 0$ for each j. By Proposition 3.1.1, we conclude that $r_j(\sigma) \in \mathcal{C}$ for each j.

Since $c^{(i)}(\omega_0^d) = c^{(i)}(\omega) = \omega_0^i$, the minimal polynomial f_0 of ω_0 divides $c^{(i)}(X^d) - X^i$, so by Proposition 3.1.1 again we have $c^{(i)}(\sigma)g_0(\sigma_0) = \sigma_0^i g_0(\sigma_0)$. Hence

$$\sum_{j=0}^{d-1}(c^{(i)}(\sigma)r_j(\sigma))\sigma_0^j = c^{(i)}(\sigma)g_0(\sigma_0) = \sigma_0^i g_0(\sigma_0) = \sum_{h=0}^{d-1} r_h(\sigma)\sigma_0^{i+h}.$$

It follows from the uniqueness in (24) that, for $0 \leqslant i,\, j \leqslant d-1$,

$$c^{(i)}(\sigma)r_j(\sigma) = \begin{cases} r_{j-i}(\sigma) & \text{if } j-i \geqslant 0; \\ \sigma r_{d-i+j}(\sigma) & \text{if } j-i < 0. \end{cases} \tag{25}$$

Since $g_0(\sigma_0) \neq 0$, we see from (24) that $r_j(\sigma) \neq 0$ for all j. But $r_0(\sigma) \in \mathcal{C}$, so $r_0(\sigma) \in \mathcal{C}^{(n)}$ for some n. By (25) we then have $c^{(d-i)}(\sigma)r_0(\sigma) = \sigma r_i(\sigma)$ for $1 \leqslant i \leqslant d-1$, so that $r_i(\sigma) \in \mathcal{C}^{(n-i)}$ for all i, by (23). □

We now consider the reverse code $\hat{\mathcal{C}} = (\hat{g}(\sigma)) \subseteq \mathbb{F}_p[C]$. For any polynomial $q(X) \in \mathbb{F}_p[X]$ we have

$$\hat{q}(\sigma) \in \hat{\mathcal{C}} \Leftrightarrow q(\sigma) \in \mathcal{C}.$$

We define

$$\hat{\mathcal{C}}^{(j)} = \{\hat{q}(\sigma) \mid q(\sigma) \in \mathcal{C}^{(j)}\} = \{\sigma^i \hat{g}^{(j)}(\sigma) \mid i \in \mathbb{Z}\}.$$

The next result is then immediate from Lemma 3.3.3.

Lemma 3.3.6. — *The code $\hat{\mathcal{C}}$ is the disjoint union of $\{0\}$ and the $\hat{\mathcal{C}}^{(j)}$ for $0 \leqslant j \leqslant d-1$. Also,*

$$\sigma\hat{\mathcal{C}}^{(j)} = \hat{\mathcal{C}}^{(j)} = \hat{\mathcal{C}}^{(j+d)} \text{ and } \hat{c}^{(i)}(\sigma)\hat{\mathcal{C}}^{(j)} = \hat{\mathcal{C}}^{(i+j)}.$$

for all i, j. Each codeword in $\hat{\mathcal{C}}^{(j)}$ has integral weight w_j. □

The last two results of this subsection relate to the code $\hat{\mathcal{C}}$. The first requires some more notation.

Definition 3.3.7. — *For $0 \leqslant j < d$, let*

$$P^{(j)} = \{a \in P \mid a(\sigma)\hat{g}(\sigma) \in \hat{\mathcal{C}}^{(j)}\},$$

and, regarding the elements of $P^{(j)}$ as elements of $\mathbb{Z}[X]$, we set

$$\Pi^{(j)}(X) = \sum_{a \in P^{(j)}} a(X) \in \mathbb{Z}[X].$$

(Thus $\Pi^{(j)}(X)$ is a polynomial of degree at most $r-1$.)

Lemma 3.3.8. — *There are integers $t(0), \ldots, t(r-1)$ such that*

$$\Pi^{(j)}(X) = \sum_{v=0}^{r-1} w_{t(v)+j} X^v \text{ for all } j.$$

Proof. — For $0 \leqslant j < d$ and for all $i \in \mathbb{Z}$, write

$$c^{(i,j)}(X) = \sum_{v=0}^{r-1} c_v^{(i,j)} X^v$$

for the unique element of $P^{(j)}$ with $c^{(i,j)}(\sigma)\hat{g}(\sigma) = \sigma^i \hat{g}^{(j)}(\sigma)$ in $\mathbb{F}_p[C]$. Also, let

$$C_v^{(j)}(X) = \sum_{i=0}^{m-1} c_v^{(i,j)} X^{m-1-i} \in \mathbb{Z}[X]. \tag{26}$$

Then

$$\Pi^{(j)}(X) = \sum_{i=0}^{m-1} c^{(i,j)}(X) = \sum_{v=0}^{r-1}\sum_{i=0}^{m-1} c_v^{(i,j)} X^v = \sum_{v=0}^{r-1} C_v^{(j)}(1) X^v. \tag{27}$$

We write

$$\hat{g}^{(j)}(\sigma) = \sum_{u=0}^{m-1} \hat{g}_u^{(j)} \sigma^u,$$

and define $\hat{g}_u^{(j)}$ for all $u \in \mathbb{Z}$ by reading the subscripts modulo m. Recall that $g^{(0)} = g$ is monic of degree $m-r$ with $g(0) \neq 0$. It follows that $\hat{g}^{(0)} = \hat{g}$ has degree $m-r$, so that in particular $\hat{g}_{m-r}^{(0)} \neq 0$ in $\mathbb{F}_p$. Now

$$\sigma^i \hat{g}^{(j)}(\sigma) = c^{(i,j)}(\sigma)\hat{g}(\sigma) = \sum_{v=0}^{r-1}\sum_{u=0}^{m-r} c_v^{(i,j)} \hat{g}_u^{(0)} \sigma^{v+u}$$

in $\mathbb{F}_p[C]$. Thus, for $0 \leqslant h \leqslant r-1$, we may equate coefficients of σ^{m-1-h} to obtain

$$\hat{g}_{m-1-h-i}^{(j)} = \sum_{k=0}^{h} c_{r-1-h+k}^{(i,j)} \hat{g}_{m-r-k}^{(0)}.$$

Multiplying by σ^{m-1-i} and summing over $0 \leqslant i \leqslant m-1$ yields

$$\sigma^h \hat{g}^{(j)}(\sigma) = \sum_{k=0}^{h} \hat{g}_{m-r-k}^{(0)} \sum_{i=0}^{m-1} c_{r-1-h+k}^{(i,j)} \sigma^{m-1-i}.$$

Using (26), we may rewrite this as

$$\sigma^h \hat{g}^{(j)}(\sigma) = \hat{g}_{m-r}^{(0)} C_{r-1-h}^{(j)}(\sigma) + \sum_{k=1}^{h} \hat{g}_{m-r-k}^{(0)} C_{r-1-h+k}^{(j)}(\sigma). \tag{28}$$

We now claim that for $0 \leqslant v \leqslant r-1$ there exist $\tau_v(\sigma) \in \mathbb{F}_p[C]$ (independent of j) such that

$$\hat{g}_{m-r}^{(0)} C_v^{(j)}(\sigma) = \tau_v(\sigma)\hat{g}^{(j)}(\sigma) \text{ for all } j. \tag{29}$$

We show this by decreasing induction on v. By (28) for $h = 0$ we have

$$\hat{g}_{m-r}^{(0)} C_{r-1}^{(j)}(\sigma) = \hat{g}^{(j)}(\sigma),$$

so we may take $\tau_{r-1}(\sigma)=1$. Assuming now that $\tau_{r-1}(\sigma),\tau_{r-2}(\sigma),\dots,\tau_{v+1}(\sigma)$ have already been found, we set $h=r-1-v$ in (28) to obtain

$$\hat{g}^{(0)}_{m-r}C^{(j)}_v(\sigma)=\sigma^{r-1-v}\hat{g}^{(j)}(\sigma)-\sum_{k=1}^{r-1-v}\hat{g}^{(0)}_{m-r-k}C^{(j)}_{v+k}(\sigma).$$

Letting $a\in\mathbb{F}_p$ satisfy $\hat{g}^{(0)}_{m-r}a=1$, we may therefore take

$$\tau_v(\sigma)=\sigma^{r-1-v}-\sum_{k=1}^{r-1-v}a\hat{g}^{(0)}_{m-r-k}\tau_{v+k}(\sigma).$$

This completes the proof of (29).

Now let $t(v)$ be such that $a\tau_v(\sigma)\hat{g}(\sigma)\in\hat{\mathcal{C}}^{(t(v))}$. Then by (29) and Lemma 3.3.6 we have $C^{(j)}_v(\sigma)\in\hat{\mathcal{C}}^{(j+t(v))}$, so that $C^{(j)}_v(1)=w_{j+t(v)}$, and the result follows from (27). □

LEMMA 3.3.9. — *There exist $\nu(\sigma)$, $\nu'(\sigma)\in\mathbb{F}_p[C]$ satisfying the properties:*

(i) $\nu(\sigma)\hat{g}(\sigma)=\nu'(\sigma)\hat{g}(\sigma)\neq 0$ *in* $\mathbb{F}_p[C]$;

(ii) *given any $\mathbb{Z}[C]$-module M (written multiplicatively) and any elements y, $z\in M$, there exist a, $b\in M$ such that*

$$a^{\nu(\sigma)}b^{\nu'(\sigma)}=y,\qquad ab^{\sigma}=z, \tag{30}$$

where $\nu(\sigma)$, $\nu'(\sigma)$ are now considered as elements of $\mathbb{Z}[C]$.

Proof. — By (21) we have $\hat{f}(1)\neq 0$ in $\mathbb{F}_p$. Thus there exist s, $t\in\mathbb{F}_p[X]$ such that

$$\hat{f}(X)s(X)+(X-1)t(X)=1 \text{ in } \mathbb{F}_p[X].$$

Substituting $X=\sigma$, multiplying by $\hat{g}(\sigma)$, and observing that $\hat{f}(\sigma)\hat{g}(\sigma)=0$, we obtain

$$(\sigma-1)t(\sigma)\hat{g}(\sigma)=\hat{g}(\sigma) \text{ in } \mathbb{F}_p[C].$$

In particular, $t(\sigma)\hat{g}(\sigma)\neq 0$ in $\mathbb{F}_p[C]$. We now consider $t(\sigma)$ as an element of $\mathbb{Z}[C]$, and in $\mathbb{Z}[C]$ we define

$$\nu(\sigma)=t(\sigma)+1,\qquad \nu'(\sigma)=\sigma t(\sigma).$$

Then in $\mathbb{F}_p[C]$ we have $\nu(\sigma)\hat{g}(\sigma)=\nu'(\sigma)\hat{g}(\sigma)\neq 0$ and given y, $z\in M$, the equations (30) are satisfied by

$$a=yz^{-t(\sigma)},\qquad b=(za^{-1})^{\sigma^{-1}}.$$

□

3.4. Stickelberger ideals

As in the proof of Lemma 3.3.3, we may identify the group C_0 with $\mathbb{F}_{p^r}^\times$ so that σ_0^i corresponds to ω_0^i for all i. Writing V for the additive group of $\mathbb{F}_{p^r}$, we now have the situation in McCulloh's result (1). The Stickelberger ideal $\mathcal{J} \subseteq \mathbb{Z}[C_0]$ occurring in that result is defined using the trace $\mathrm{Tr}_{\mathbb{F}_{p^r}/\mathbb{F}_p}$ from $\mathbb{F}_{p^r}$ to $\mathbb{F}_p$. We now recall this definition, and relate $\mathcal{J}$ to our codes.

We first set

$$\theta = \sum_{i=0}^{p^r-2} \mathrm{Tr}_{\mathbb{F}_{p^r}/\mathbb{F}_p}(\omega_0^i)\sigma_0^{-i} \in \mathbb{F}_p[C_0],$$

and then consider θ as an element of $\mathbb{Z}[C_0]$, as explained in §3.2. The Stickelberger ideal itself is then defined as

$$\mathcal{J} = \mathbb{Z}[C_0] \cap \mathbb{Z}[C_0](p^{-1}\theta).$$

The connection with our codes is given by the following result.

LEMMA 3.4.1. — *As an element of $\mathbb{F}_p[C_0]$, the Stickelberger element θ is a nonzero codeword of $\mathcal{C}_0 = (g_0(\sigma_0)) \subseteq \mathbb{F}_p[C_0]$. Thus $\theta = \sigma_0^h g_0(\sigma_0)$ for some h. The Stickelberger ideal $\mathcal{J} \subseteq \mathbb{Z}[C_0]$ is generated over $\mathbb{Z}[C_0]$ by the two elements*

$$p^{-1}f_0(\sigma_0)g_0(\sigma_0), \qquad g_0(\sigma_0).$$

Proof. — By the nondegeneracy of the trace map, $\theta \neq 0$ in $\mathbb{F}_p[C_0]$. In the action of C_0 on V, the minimal polynomial of σ_0 is f_0. Thus the annihilator in $\mathbb{Z}[C_0]$ of V contains $f_0(\sigma_0)$ (considered as an element of $\mathbb{Z}[C_0]$). By [18, Prop. 3.10(b)] we therefore have

$$f_0(\sigma_0)(p^{-1}\theta) \in \mathbb{Z}[C_0].$$

Thus in $\mathbb{F}_p[C_0]$ we have $f_0(\sigma_0)\theta = 0$. It follows from Proposition 3.1.1 (applied to the code $\mathcal{C}_0$) that $\theta \in \mathcal{C}_0$, so $\theta = \sigma_0^h g_0(\sigma_0)$ for some h by Lemma 3.3.3 (applied to $\mathcal{C}_0$). Now

$$\begin{aligned}\mathcal{J} &= \mathbb{Z}[C_0] \cap \big(\mathbb{Z}[C_0] \cdot \big(p^{-1}\theta\big)\big) \\ &= \mathbb{Z}[C_0] \cap \big(\mathbb{Z}[C_0] \cdot \big(p^{-1}g_0(\sigma_0)\big)\big) \\ &= \big\{p^{-1}a(\sigma_0)g_0(\sigma_0) \mid a(\sigma_0) \in \mathbb{Z}[C_0],\, a(\sigma_0)g_0(\sigma_0) \in p\mathbb{Z}[C_0]\big\}\end{aligned}$$

But

$$\begin{aligned}a(\sigma_0)g_0(\sigma_0) \in p\mathbb{Z}[C_0] &\Leftrightarrow a(\sigma_0)g_0(\sigma_0) = 0 \text{ in } \mathbb{F}_p[C_0] \\ &\Leftrightarrow a(\sigma_0) \in (f_0(\sigma_0)) \text{ in } \mathbb{F}_p[C_0] \\ &\Leftrightarrow a(\sigma_0) \in f_0(\sigma_0)\mathbb{Z}[C_0] + p\mathbb{Z}[C_0],\end{aligned}$$

where the second equivalence comes from Proposition 3.1.1 applied to $(f_0(\sigma_0))$. Hence $\mathcal{J}$ is generated by the two elements stated. □

Now let $\overline{C}$ denote the quotient group C_0/C, so that $\overline{C}$ is cyclic of order d, generated by the image $\overline{\sigma}_0$ of σ_0. Recall from Lemma 3.3.3 that the weights w_j of nonzero codewords in $\mathcal{C}$ are divisible by p. We now define a reduced Stickelberger element T in $\mathbb{Z}[\overline{C}]$.

Definition 3.4.2. — *Let $b_j = w_j/p$ for all $j \in \mathbb{Z}$, and set*

$$T = \sum_{j=0}^{d-1} b_j \, (\overline{\sigma}_0)^{-j} \in \mathbb{Z}[\overline{C}].$$

Lemma 3.4.3. — *The image $\overline{\mathcal{J}}$ in $\mathbb{Z}[\overline{C}]$ of the Stickelberger ideal $\mathcal{J} \subseteq \mathbb{Z}[C_0]$ is $\mathbb{Z}[\overline{C}] \cdot T$.*

Proof. — By Lemma 3.4.1, $\overline{\mathcal{J}}$ is generated by the images of $p^{-1} f_0(\sigma_0) g_0(\sigma_0)$ and $g_0(\sigma_0)$. By Lemma 3.3.5 (and using the notation of that Lemma), the image of $g_0(\sigma_0)$ in $\mathbb{Z}[\overline{C}]$ can be calculated as

$$\sum_{i=0}^{d-1} r_i(1) \overline{\sigma}_0^i = \sum_{i=0}^{d-1} w_{n-i} \overline{\sigma}_0^i = \sum_{j=0}^{d-1} w_j \overline{\sigma}_0^{n-j} = \overline{\sigma}_0^n p T.$$

Hence $\overline{\mathcal{J}}$ is generated by $f_0(\overline{\sigma}_0)T$ and pT. It therefore remains to show that

$$\mathbb{Z}[\overline{C}] \cdot f_0(\overline{\sigma}_0) + p\mathbb{Z}[\overline{C}] = \mathbb{Z}[\overline{C}],$$

or equivalently, that $f_0(\overline{\sigma}_0)$ is invertible as an element of $\mathbb{F}_p[\overline{C}] \cong \mathbb{F}_p[X]/(X^d - 1)$. But this follows from the fact that the roots of f_0 all have order $p^r - 1 > d$, so that $f_0(X)$ and $X^d - 1$ are relatively prime in $\mathbb{F}_p[X]$. □

4. The group Γ

We now fix, once and for all, a number field k containing ξ_p, a primitive pth root of unity. In this section, we examine the group Γ which occurs in our main results and we determine its absolutely irreducible characters. We then investigate the locally free classgroup $\mathrm{Cl}(O_k[\Gamma])$, and describe the effect of the Stickelberger ideal on this classgroup.

4.1. Construction of Γ and Γ_0

Let V be an elementary abelian group of order p^r, where $r \geqslant 1$. Let C be a cyclic group of order m, acting on V. Viewing V as an $\mathbb{F}_p$-vector space of dimension r, we then have an $\mathbb{F}_p$-linear representation

$$\rho\colon C \longrightarrow \mathrm{Aut}(V) = \mathrm{Aut}_{\mathbb{F}_p}(V). \tag{31}$$

We form the semidirect product

$$\Gamma = V \rtimes_\rho C.$$

To simplify notation, we identify V and C with subgroups of Γ; the multiplication in Γ is then determined by

$$\sigma v \sigma^{-1} = \rho(\sigma)(v) \text{ for } \sigma \in C,\ v \in V.$$

PROPOSITION 4.1.1. — *If the representation ρ is irreducible and faithful, then m divides p^r-1 but does not divide p^s-1 for any s with $1 \leqslant s < r$. Conversely, if m satisfies these conditions, then there is a faithful action of C on V for which the corresponding representation ρ is irreducible.*

Proof. — First suppose that ρ is irreducible. Let σ be a generator of C, and let $f \in \mathbb{F}_p[X]$ be the minimal polynomial of $\rho(\sigma)$ on V. Then f is an irreducible factor of $X^m - 1$ in $\mathbb{F}_p[X]$ and $\deg f = \dim_{\mathbb{F}_p} V = r$. We therefore have isomorphisms of $\mathbb{F}_p$-algebras

$$\frac{\mathbb{F}_p[X]}{(f(X))} \cong \frac{\mathbb{F}_p[C]}{(f(\sigma))} \cong \mathbb{F}_{p^r},$$

where the first isomorphism is induced by $X \mapsto \sigma$, and the second by $\sigma \mapsto \omega$ with $\omega \in \mathbb{F}_{p^r}^\times$ of order m. Then ρ induces on V the structure of a 1-dimensional $\mathbb{F}_{p^r}$-vector space, with σ acting as multiplication by ω. Hence m divides $|\mathbb{F}_{p^r}^\times| = p^r-1$. For any $v \neq 0$ in V, we have $V = \mathbb{F}_p[C]\cdot v = \mathbb{F}_p(\omega)\cdot v$ since V is irreducible. Hence $\mathbb{F}_p(\omega) = \mathbb{F}_{p^r}$. For $s < r$, we therefore have $\omega \notin \mathbb{F}_{p^s}$, so m does not divide $p^s - 1$.

Conversely, suppose that m divides $p^r - 1$ but does not divide $p^s - 1$ for any $1 \leqslant s < r$. Then there is some $\omega \in \mathbb{F}_{p^r}^\times$ of order m, and $\mathbb{F}_p(\omega) = \mathbb{F}_{p^r}$. Identify V with the additive subgroup of $\mathbb{F}_{p^r}$, and let the cyclic group C of order m act on V so that the generator σ corresponds to multiplication by ω. This makes V into a faithful, irreducible $\mathbb{F}_p[C]$-module. □

Remark 4.1.2. — It is not hard to see that if the action of C on V is faithful and irreducible, then the resulting group Γ is determined up to isomorphism by p^r and m.

Remark 4.1.3. — If m satisfies the conditions in Proposition 4.1.1, then there may be other actions of C on V which are faithful but not irreducible. For example, if $p = 2$, $r = 6$ and $m = 21$, then we have shown that C can have a faithful and irreducible action on V which arises by identifying V with a 1-dimensional $\mathbb{F}_{2^6}$-vector space. However, C has another faithful action on V, inducing a decomposition $V \cong \mathbb{F}_{2^3} \times \mathbb{F}_{2^2} \times \mathbb{F}_2$ where the generator σ of C acts on the three factors as multiplication by elements of order 7, 3, 1 respectively. In the case $m = p^r - 1$, any faithful action of C on V will necessarily be irreducible [1, Proposition 2.3], [4, Proposition 2.3]. The same is true if m divides $p^r - 1$ and has a prime factor not dividing $p^s - 1$ for any $s < r$.

For the rest of the paper, we take $\Gamma = V \rtimes_\rho C$ where C acts on V via a faithful, irreducible representation ρ. Thus m will always satisfy the conditions in Proposition 4.1.1. Moreover we assume $m > 1$ (so the metabelian group Γ is not abelian.) We fix a generator σ of C, and let f be the minimal polynomial of $\rho(\sigma)$ on V.

We set

$$d = \frac{p^r - 1}{m}.$$

We fix a root ω of f in $\mathbb{F}_{p^r}^\times$. Then ω has minimal polynomial f. Now fix an element $\omega_0 \in \mathbb{F}_{p^r}$ with $\omega_0^d = \omega$. Let f_0 be the minimal polynomial of ω_0.

We embed C in a cyclic group $C_0 = \langle \sigma_0 \rangle$ of order $p^r - 1$, with $\sigma_0^d = \sigma$.

We fix an element $v \neq 0$ in V. This determines an isomorphism between V and the additive group of $\mathbb{F}_{p^r}$, in which 1 corresponds to v and σ acts as multiplication by ω. We may extend the given representation

$$\rho \colon C \longrightarrow \mathrm{Aut}(V)$$

to a faithful irreducible representation

$$\rho_0 \colon C_0 \longrightarrow \mathrm{Aut}(V),$$

where σ_0 acts as multiplication by ω_0. Then ρ_0 is independent of the choice of v. We form the semidirect product

$$\Gamma_0 = V \rtimes_{\rho_0} C_0.$$

Then Γ is a normal subgroup of index d in Γ_0.

We are now in the situation of §3.3, and associated to the groups Γ, Γ_0 we have cyclic codes $\mathcal{C}$, $\mathcal{C}_0$ and their dual codes $\hat{\mathcal{C}}$, $\hat{\mathcal{C}}_0$ as constructed there.

Our chosen element $v \in V$ generates V as an $\mathbb{F}_p[C]$-module:

$$V = \{v^{a(\sigma)} \mid a \in P\}.$$

4.2. The characters of V, C and Γ

In this subsection we describe the absolutely irreducible characters of Γ and of its subgroups V and C.

We first consider the group $V^\dagger$ of irreducible characters of the elementary abelian group V. These characters take values in k since $\xi_p \in k$. There is a natural action of C_0 on $V^\dagger$, contragredient to its action on V, so that

$$(\sigma_0^j \cdot \psi)(u) = \psi(\sigma_0^{-j} \cdot u) \text{ for all } u \in V, \psi \in V^\dagger.$$

This restricts to an action of C. The minimal polynomial over $\mathbb{F}_p$ of σ_0 (respectively σ) on $V^\dagger$ is therefore $f_0(0)^{-1}\hat{f}_0$ (respectively $f(0)^{-1}\hat{f}$).

We define an $\mathbb{F}_p$-bilinear pairing

$$[\,\cdot\,,\,\cdot\,] : \mathbb{F}_p[C] \times \mathbb{F}_p[C] \longrightarrow \mathbb{F}_p$$

by

$$[a(\sigma), b(\sigma)] = \mathrm{Tr}_{\mathbb{F}_{p^r}/\mathbb{F}_p}(a(\omega)b(\omega^{-1})). \tag{32}$$

We therefore have

$$[c(\sigma)a(\sigma), b(\sigma)] = [a(\sigma), c(\sigma)^{-1}b(\sigma)] \tag{33}$$

for any $a(\sigma)$, $b(\sigma)$, $c(\sigma) \in \mathbb{F}_p[C]$. This pairing induces a perfect C-invariant $\mathbb{F}_p$-bilinear pairing (for which we use the same notation)

$$[\,\cdot\,,\,\cdot\,] : \frac{\mathbb{F}_p[C]}{(f(\sigma))} \times \frac{\mathbb{F}_p[C]}{(\hat{f}(\sigma))} \longrightarrow \mathbb{F}_p.$$

We now fix a character $\psi \in V^\dagger$ by specifying (with a slight abuse of notation)

$$\psi(v^{a(\sigma)}) = \xi_p^{[a(\sigma),1]}. \tag{34}$$

For arbitrary $a(\sigma)$, $b(\sigma) \in \mathbb{F}_p[C]$ we have

$$\psi^{b(\sigma)}(v^{a(\sigma)}) = \psi(v^{b(\sigma^{-1})a(\sigma)}) = \xi_p^{[a(\sigma),b(\sigma)]}. \tag{35}$$

Thus ψ generates $V^\dagger$ as an $\mathbb{F}_p[C]$-module.

For later use, we record that to each character $\psi^{b(\sigma)}$ is associated the primitive idempotent

$$e_{b(\sigma)} = \frac{1}{p^r} \sum_{a \in P} \psi^{b(\sigma)}(v^{a(\sigma)}) v^{-a(\sigma)} \in k[V]. \tag{36}$$

We then have

$$e_{\sigma b(\sigma)} = \sigma e_{b(\sigma)} \sigma^{-1}, \tag{37}$$

where the multiplication takes place in $k[\Gamma]$.

The irreducible characters of C are ϕ_i for $0 \leqslant i \leqslant m-1$, where $\phi_i(\sigma) = \xi_m^i$. (Recall that ξ_m denotes a primitive mth root of unity.)

We now turn to the characters of Γ. We view the characters ϕ_i of C also as irreducible characters of Γ by inflation from $C = \Gamma/V$. We will show that the remaining irreducible characters of Γ are induced from V. Now C_0 acts transitively on the nontrivial characters on V, and C has d orbits on these characters. The characters $\psi_j = \sigma_0^j \cdot \psi$ for $0 \leqslant j \leqslant d-1$ therefore form a system of orbit representatives. We set

$$\chi_j = \mathrm{Ind}_V^\Gamma \psi_j.$$

Explicitly, the values of these characters are as follows:

$$\begin{aligned}
\chi_j(1) &= m; \\
\chi_j(u) &= \sum_{h=0}^{m-1} \psi_j((\sigma^h)^{-1} \cdot u) = \sum_{h=0}^{m-1} \psi((\sigma_0^j \sigma^h)^{-1} \cdot u) \quad \text{for } u \in V; \\
\chi_j(\sigma^k u) &= 0 \quad \text{for } u \in V \text{ and } 1 \leqslant k \leqslant m-1.
\end{aligned}$$

LEMMA 4.2.1. — *The absolutely irreducible characters of the group Γ are precisely the ϕ_i for $0 \leqslant i \leqslant m-1$ and the χ_j for $0 \leqslant j \leqslant d-1$.*

Proof. — Since

$$\sum_{i=0}^{m-1} \phi_i(1)^2 + \sum_{j=0}^{d-1} \chi_j(1)^2 = m + dm^2 = |\Gamma|,$$

it suffices to show that the characters χ_j, $0 \leqslant j \leqslant d-1$ are irreducible and distinct. This will follow if the character $X = \sum_{j=0}^{d-1} \chi_j$ satisfies $\langle X, X \rangle = d$, where $\langle\, .\, ,\, . \,\rangle$ denotes the usual inner product of class functions on Γ. Now for $1 \neq u \in V$ we have

$$X(u) = \sum_{j=0}^{d-1} \sum_{h=0}^{m-1} \psi((\sigma_0^j \sigma^h)^{-1} \cdot u) = \sum_{1 \neq u' \in V} \psi(u') = -1,$$

while $X(\sigma^h u) = 0$ for $1 \leqslant h \leqslant m-1$. Thus we have

$$\begin{aligned}
|\Gamma| \langle X, X \rangle &= \sum_{\gamma \in \Gamma} |X(\gamma)|^2 \\
&= X(1)^2 + \sum_{1 \neq w \in V} (-1)^2 + \sum_{\gamma \in \Gamma \setminus V} 0^2 \\
&= (dm)^2 + (p^r - 1) + 0 \\
&= p^r (p^r - 1) \\
&= d|\Gamma|,
\end{aligned}$$

so that $\langle X, X \rangle = d$, as required. □

LEMMA 4.2.2. — *None of the irreducible characters of* Γ *are symplectic.*

Proof. — The ϕ_h are not symplectic, since they factor through the abelian group C. For the χ_j, we use the fact that an irreducible character χ is symplectic if and only if its Frobenius-Schur indicator $c(\chi)$ is -1 ([9, (73.13)]). Indeed, a simple calculation yields

$$c(\chi_j) = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\chi_j(\gamma^2) = \begin{cases} 1 & \text{if } p=2, \text{ or } p\geqslant 3 \text{ and } m \text{ is even;} \\ 0 & \text{if } p\geqslant 3 \text{ and } m \text{ is odd.} \end{cases}$$

□

DEFINITION 4.2.3. — *For all* $j\in\mathbb{Z}$ *we define* $\overline{c}^{(j)}$ *to be the unique element of* P *with*

$$\psi_j = \psi^{\overline{c}^{(j)}(\sigma)}.$$

LEMMA 4.2.4. — *For all* $j\in\mathbb{Z}$ *we have* $\overline{c}^{(j)}(\sigma) = c^{(-j)}(\sigma^{-1})$. *Thus* $\overline{c}^{(j)}(\sigma)\hat{g}(\sigma)\in\hat{\mathcal{C}}^{(-j)}$ *and* $\sigma\overline{c}^{(j)}(\sigma)\hat{g}(\sigma) = \overline{c}^{(j+d)}(\sigma)\hat{g}(\sigma)$.

Proof. — For any $a\in P$ we have

$$\begin{aligned} \xi_p^{[a(\sigma),\overline{c}^{(j)}(\sigma)]} &= \psi_j(v^{a(\sigma)}) \\ &= \psi(\sigma_0^{-j}\cdot v^{a(\sigma)}) \\ &= \psi(c^{(-j)}(\sigma)\cdot v^{a(\sigma)}) \\ &= \xi_p^{[c^{(-j)}(\sigma)a(\sigma),1]} \\ &= \xi_p^{[a(\sigma),c^{(-j)}(\sigma^{-1})]}. \end{aligned}$$

Hence $\overline{c}^{(j)}(\sigma) = c^{(-j)}(\sigma^{-1})$. Writing D for the degree of the polynomial $c^{(-j)}$, we then have

$$\overline{c}^{(j)}(\sigma)\hat{g}(\sigma) = \sigma^{-D}\hat{c}^{(-j)}(\sigma)\hat{g}(\sigma)\in\hat{\mathcal{C}}^{(-j)}$$

by Lemma 3.3.6. Finally, since $\sigma^{-1}c^{(-j)}(\sigma)g(\sigma) = c^{(-j-d)}(\sigma)g(\sigma)$, we have

$$\sigma c^{(-j)}(\sigma^{-1})\hat{g}(\sigma) = c^{(-j-d)}(\sigma^{-1})\hat{g}(\sigma),$$

which is equivalent to the final assertion. □

4.3. Locally free classgroups

In this subsection, we apply Lemma 2.2.1 to the group Γ of §4.1 and its quotient C, taking k to be a number field containing ξ_p. We also give explicit descriptions of the various homomorphisms between classgroups that occur in our main results.

Let $(\Phi_i)_{1\leqslant i\leqslant s}$ be a system of orbit representatives under $\mathrm{Gal}(k(\xi_m)/k)$ of the 1-dimensional characters ϕ_q, $0 \leqslant q \leqslant m-1$, of Γ. For each i, set $k_i = k(\Phi_i)$. The values of the m-dimensional irreducible characters χ_j already lie in k. Thus $h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ is determined by its values $h(\Phi_i) \in \mathbb{J}(k_i)$ for $1 \leqslant i \leqslant s$ and $h(\chi_j) \in \mathbb{J}(k)$ for $0 \leqslant j \leqslant d-1$.

The next result is immediate from Lemmas 2.2.1 and 4.2.2:

LEMMA 4.3.1. — *A character homomorphism $h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ represents the trivial class in $\mathrm{Cl}(O_k[\Gamma])$ if*

$$h(\Phi_i) \in k_i^\times \mathbb{U}_{mp^r}(k_i) \text{ for } 1 \leqslant i \leqslant s; \qquad h(\chi_j) \in k^\times \mathbb{U}_{p^r}(k) \text{ for } 0 \leqslant j \leqslant d-1.$$

Thus the canonical surjection $\mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c)) \longrightarrow \mathrm{Cl}(O_k[\Gamma])$ factors through

$$\prod_{i=1}^{s} \mathrm{Cl}_{mp^r}(k_i) \times \prod_{j=0}^{d-1} \mathrm{Cl}_{p^r}(k).$$

We of course have a similar result for $\mathrm{Cl}(O_k[C])$: a character homomorphism $h' \in \mathrm{Hom}_{\Omega_k}(R_C, \mathbb{J}(k^c))$ represents the trivial class in $\mathrm{Cl}(O_k[C])$ if

$$h'(\overline{\Phi}_i) \in k_i^\times \mathbb{U}_m(k_i) \text{ for } 1 \leqslant i \leqslant s.$$

We now consider the homomorphism of classgroups induced by the inclusion $\iota^C : C \longrightarrow \Gamma$.

LEMMA 4.3.2. — *If a class $\mathcal{A} \in \mathrm{Cl}(O_k[C])$ is represented by $h' \in \mathrm{Hom}_{\Omega_k}(R_C, \mathbb{J}(k^c))$, then the character homomorphism $h = \iota^C_* h' \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ representing the class $\iota^C_*(\mathcal{A}) \in \mathrm{Cl}(O_k[\Gamma])$ is given by*

$$h(\Phi_i) = h'(\overline{\Phi}_i) \text{ for } 1 \leqslant i \leqslant s; \qquad h(\chi_j) = h'(r_C) \text{ for } 1 \leqslant j \leqslant d,$$

where r_C is the regular character of C. Moreover, writing $x_i = h'(\overline{\Phi}_i)$ for $1 \leqslant i \leqslant s$, we have

$$h'(r_C) = \prod_{i=1}^{s} N_{k_i/k}(x_i).$$

Proof. — We have $h(\alpha) = h'(\alpha \circ \iota^C) = h'(\mathrm{Res}^\Gamma_C \alpha)$ for each character α of Γ. Thus $h(\Phi_i) = h'(\mathrm{Res}^\Gamma_C \Phi_i) = h'(\overline{\Phi}_i)$ for $1 \leqslant i \leqslant s$ and $h(\chi_j) = h'(\mathrm{Res}^\Gamma_C \chi_j)$ for $1 \leqslant j \leqslant d$. Now $\chi_j(1) = m$, and $\chi_j(\sigma^t) = 0$ for $1 \leqslant t \leqslant m-1$, so $\mathrm{Res}^\Gamma_C \chi_j$ is the regular character $r_C = \sum_{q=0}^{m-1} \phi_q$ of C, whence $h(\chi_j) = h'(r_C)$. But the characters ϕ_q for $0 \leqslant q \leqslant m-1$ are precisely the Φ_i^τ as i runs through $\{1, \ldots, s\}$ and τ runs through $\mathrm{Gal}(k_i/k)$ for each i. Thus

$$h'(r_C) = \prod_{q=0}^{m-1} h'(\phi_q) = \prod_{i=1}^{s} \left(\prod_{\tau \in \mathrm{Gal}(k_i/k)} x_i^\tau \right) = \prod_{i=1}^{s} N_{k_i/k}(x_i). \qquad \square$$

We now turn to the map $\iota_*^V\colon \mathrm{Cl}(O_k[V]) \longrightarrow \mathrm{Cl}(O_k[\Gamma])$. As $\xi_p \in k$ we have

$$\mathrm{Hom}_{\Omega_k}(R_V, \mathbb{J}(k^c)) = \mathrm{Hom}(R_V, \mathbb{J}(k)) \cong \prod_{\psi' \in V^\dagger} \mathbb{J}(k).$$

LEMMA 4.3.3. — *Let $h \in \mathrm{Hom}_{\Omega_k}(R_V, \mathbb{J}(k^c))$ represent the class $\mathcal{A} \in \mathrm{Cl}(O_k[V])$. Then the character homomorphism $\iota_*^V h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ representing $\iota_*^V(\mathcal{A}) \in \mathrm{Cl}(O_k[\Gamma])$ is given by*

$$\iota_*^V h(\Phi_i) = h(\epsilon) \text{ for } 1 \leqslant i \leqslant s;$$

$$\iota_*^V h(\chi_j) = \prod_{\lambda=0}^{m-1} h(\psi_{j+d\lambda}) \text{ for } 0 \leqslant j \leqslant d-1;$$

where ϵ is the trivial character of V.

Proof. — By definition $\iota_*^V h(\alpha) = h(\mathrm{Res}_V^\Gamma(\alpha))$ for any character α of Γ, and we have $\mathrm{Res}_V^\Gamma(\Phi_i) = \epsilon$ and $\mathrm{Res}_V^\Gamma(\chi_j) = \sum_{\lambda=0}^{m-1} \psi_{j+d\lambda}$. □

Recall that $\epsilon_*\colon \mathrm{Cl}(O_k[V]) \longrightarrow \mathrm{Cl}(O_k)$ is induced by the trivial homomorphism on V. From Lemma 4.3.3 and Lemma 2.3.1, we immediately deduce the next result:

COROLLARY 4.3.4. — *The subgroup $\iota_*^V(\ker \epsilon_*)$ of $\mathrm{Cl}(O_k[\Gamma])$ consists of all classes represented by character homomorphisms $h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ with $h(\Phi_i) = 1$ for $1 \leqslant i \leqslant s$ (and $h(\chi_j) \in \mathbb{J}(k)$ arbitrary for $0 \leqslant j \leqslant d-1$). Thus $\iota_*^V(\ker \epsilon_*) = \ker \pi_*$.*

We next describe the effect of the Stickelberger ideal $\mathcal{J}$ on $\ker(\pi_*)$.

LEMMA 4.3.5. — *Let $b_i = w_i/p$, as in Definition 3.4.2. Then $\mathcal{J} \cdot \ker(\pi_*)$ consists of those classes in $\mathrm{Cl}(O_k[\Gamma])$ represented by character homomorphisms $h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ with*

$$h(\Phi_i) = 1 \text{ for } 1 \leqslant i \leqslant s;$$

$$h(\chi_j) = \prod_{\lambda=0}^{d-1} \omega_\lambda^{b_{\lambda-j}} \text{ for } 0 \leqslant j \leqslant d-1$$

for some $\omega_0, \ldots, \omega_{d-1} \in \mathbb{J}(k)$, the subscripts on the b_λ being read modulo d.

Proof. — Recall that Γ is a normal subgroup of Γ_0, and we have an action of C_0 on $\mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ induced by the action of C_0 on Γ given by conjugation inside Γ_0. Writing $\hat{\sigma}_0\colon \Gamma \longrightarrow \Gamma$ for the map $\gamma \mapsto \sigma_0 \gamma \sigma_0^{-1}$, we have for $h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ that $(\sigma_0 \cdot h)(\Phi_i) = h(\Phi_i \circ \hat{\sigma}_0) = h(\Phi_i)$ and

$$(\sigma_0 \cdot h)(\chi_j) = h(\chi_j \circ \hat{\sigma}_0) = h(\sigma_0^{-1} \cdot \chi_j) = h(\chi_{j-1}),$$

since $\sigma_0^t \cdot \chi_j = \chi_{t+j}$ (with the subscripts on the χ_j read modulo d). Thus the action of C_0 on $\mathrm{Cl}(O_k[\Gamma])$ factors through $\overline{C} = C_0/C$, and by Lemma 3.4.3 we have

$$\mathcal{J} \cdot \ker(\pi_*) = \overline{\mathcal{J}} \cdot \ker(\pi_*) = T \cdot \ker(\pi_*).$$

By Lemma 2.3.1, $\ker(\pi_*)$ consists of the classes represented by character homomorphisms $h' \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ with $h'(\Phi_i) = 1$ for $1 \leqslant i \leqslant s$. Let

$$\omega_j = h'(\chi_j) \in \mathbb{J}(k) \text{ for } 0 \leqslant j \leqslant d-1.$$

Then

$$\begin{aligned}(T \cdot h')(\chi_j) &= \left(\sum_{\lambda=0}^{d-1} b_\lambda (\overline{\sigma}_0)^{-\lambda} \cdot h' \right)(\chi_j) \\ &= \prod_{\lambda=0}^{d-1} h'(\chi_{\lambda+j})^{b_\lambda} \\ &= \prod_{\lambda=0}^{d-1} \omega_{\lambda+j}^{b_\lambda} \\ &= \prod_{\lambda=0}^{d-1} \omega_\lambda^{b_{\lambda-j}}.\end{aligned}$$

□

Now let F be any finite extension of k. Since $\xi_p \in k$, the Fröhlich norm $\mathcal{N}_{F/k} \colon \mathrm{Cl}(O_F[V]) \longrightarrow \mathrm{Cl}(O_k[V])$ is induced by the usual idèle norm $N_{F/k} \colon \mathbb{J}(F) \longrightarrow \mathbb{J}(k)$.

LEMMA 4.3.6. — *The group $\iota_*^V \mathcal{N}_{F/k}(\mathcal{R}(O_F[V]))$ consists of those classes in $\mathrm{Cl}(O_k[\Gamma])$ represented by character homomorphisms $h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ with*

$$h(\Phi_i) = 1 \text{ for } 1 \leqslant i \leqslant s;$$

$$h(\chi_j) = \prod_{\lambda=0}^{d-1} N_{F/k}(\omega_\lambda)^{b_{\lambda-j}} \text{ for } 0 \leqslant j \leqslant d-1$$

for some $\omega_0, \ldots, \omega_{d-1} \in \mathbb{J}(F)$. Also $\iota_*^V(\mathcal{R}(O_k[V])) = \mathcal{J} \cdot \ker(\pi_*)$, and

$$\iota_*^V \mathcal{N}_{F/k}(\mathcal{R}(O_F[V])) \subseteq \iota_*^V(\mathcal{R}(O_k[V])),$$

with equality if every intermediate field $L \neq k$ of F/k is ramified over k at some place not above p.

Proof. — First note that $\mathcal{R}(O_F[V])) = \mathcal{J} \cdot \ker(\epsilon_{*F})$ by McCulloh's result (1) for elementary abelian groups, where the homomorphism $\epsilon_{*F} \colon \mathrm{Cl}(O_F[V]) \longrightarrow \mathrm{Cl}(O_F)$ is induced by $\epsilon \colon V \longrightarrow \{1\}$. Now ι_*^V commutes with the Fröhlich norm and with the elements of $\mathcal{J}$. Thus, using Corollary 4.3.4 (with F in place of k), we have

$$\begin{aligned}\iota_*^V \mathcal{N}_{F/k}(\mathcal{R}(O_F[V])) &= \iota_*^V(\mathcal{N}_{F/k}(\mathcal{J} \cdot \ker \epsilon_{*F})) \\ &= \mathcal{N}_{F/k}(\mathcal{J} \cdot \iota_*^V \ker \epsilon_{*F}) \\ &= \mathcal{N}_{F/k}(\mathcal{J} \cdot \ker \pi_{*F}),\end{aligned}$$

where $\pi_{*F} \colon \mathrm{Cl}(O_F[\Gamma]) \longrightarrow \mathrm{Cl}(O_F[C])$ is the homomorphism induced by π.

By Lemma 4.3.5 (with F in place of k), $\mathcal{J} \cdot \ker \pi_{*F}$ consists of those classes in $\mathrm{Cl}(O_F[\Gamma])$ represented by character homomorphisms $h' \in \mathrm{Hom}_{\Omega_F}(R_\Gamma, \mathbb{J}(k^c))$ with $h'(\phi) = 1$ for each character ϕ of Γ which factors through C and

$$h'(\chi_j) = \prod_{\lambda=0}^{d-1} \omega_\lambda^{b_{\lambda-j}} \text{ for } 0 \leqslant j \leqslant d-1$$

for arbitrary $\omega_0, \ldots, \omega_{d-1} \in \mathbb{J}(F)$. Thus $\mathcal{N}_{F/k}(\mathcal{J} \cdot \ker \pi_{*F})$ is represented by the character homomorphisms $h = \mathcal{N}_{F/k}(h') \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ with $h(\Phi_i) = 1$ for $1 \leqslant i \leqslant s$ and

$$h(\chi_j) = N_{F/k}(h'(\chi_j)) = \prod_{\lambda=0}^{d-1} N_{F/k}(\omega_\lambda)^{b_{\lambda-j}} \text{ for } 0 \leqslant j \leqslant d-1.$$

This proves the first assertion.

Taking $F = k$ shows that $\iota_*^V(\mathcal{R}(O_k[V]))$ consists of classes represented by character homomorphisms h as in Lemma 4.3.5, whence $\iota_*^V(\mathcal{R}(O_k[V])) = \mathcal{J} \cdot \ker(\pi_*)$ and $\iota_*^V \mathcal{N}_{F/k}(\mathcal{R}(O_F[V])) \subseteq \iota_*^V(\mathcal{R}(O_k[V]))$. By Lemma 4.3.1, the last inclusion will be an equality if the norm $N_{F/k} \colon \mathrm{Cl}_{p^r}(O_F) \longrightarrow \mathrm{Cl}_{p^r}(O_k)$ on ray classgroups is surjective. A slight generalization of [28, Theorem 10.1] shows that this condition is satisfied if F/k has no intermediate extension $L \neq k$ which is unramified outside p. □

5. Γ-extensions

Recall that k is a number field containing ξ_p. Let E be a tame C-extension of k; we identify $\mathrm{Gal}(E/k)$ with C via the associated isomorphism. In this section we describe all tame Γ-extensions N of k, and we show how to find the class $(O_N)_{O_k[\Gamma]}$ of O_N in $\mathrm{Cl}(O_k[\Gamma])$.

5.1. An Embedding Problem

By Kummer theory, finite elementary abelian p-extensions of E correspond to finite-dimensional subspaces of the $\mathbb{F}_p$-vector space $E^\times/E^{\times p}$. We will determine when such extensions are Galois over k. The content of this subsection recalls and extends part of [1, §2] and [4, §2].

For $w \in E^\times$ we write $[w]$ for the class of w in $E^\times/E^{\times p}$, and denote by $\sqrt[p]{w}$ a fixed choice of pth root of w. For notational convenience, we will often write the $\mathbb{F}_p[C]$-module $E^\times/E^{\times p}$ and the $\mathbb{Z}[C]$-module $E^\times$ additively, so that for instance the notations $\hat{g}(\sigma)\cdot y$ and $y^{\hat{g}(\sigma)}$ will be used interchangeably.

LEMMA 5.1.1. — *Let $L = E(\sqrt[p]{w})$ be a cyclic extension of E of degree p. Let N be its Galois closure over k, and let $V = \mathrm{Gal}(N/E)$. Let $W = \mathbb{F}_p[C]\cdot[w]$ be the cyclic $\mathbb{F}_p[C]$-submodule of $E^\times/E^{\times p}$ generated by $[w]$, let $r = \dim_{\mathbb{F}_p}(W)$, and let $\rho_1 \colon C \to \mathrm{Aut}_{\mathbb{F}_p}(W)$ be the representation of C afforded by W. Then $N = E(\sqrt[p]{\sigma^i(w)} \mid 0 \leqslant i \leqslant r-1)$, $|V| = p^r$, and $\mathrm{Gal}(N/k) = V \rtimes_{\rho_2} C$, where the representation $\rho_2 \colon C \to \mathrm{Aut}_{\mathbb{F}_p}(V)$ is contragredient to ρ_1.*

Proof. — The conjugates of L over k are $E(\sqrt[p]{\sigma^i(w)})$ for $0 \leqslant i \leqslant m-1$, and clearly N is the compositum of these. Hence $V = \mathrm{Gal}(N/E)$ is elementary abelian, and N corresponds by Kummer theory to the subspace $W = \mathbb{F}_p[C]\cdot[w]$ of $E^\times/E^{\times p}$. But W is spanned by $[w], \ldots, [\sigma^{r-1}(w)]$, so it suffices to take $0 \leqslant i \leqslant r-1$.

We have the Kummer pairing

$$\langle\ ,\ \rangle \colon V \times W \longrightarrow \mathbb{F}_p$$

defined by

$$\xi_p^{\langle v,[w]\rangle} = v(\sqrt[p]{w})/\sqrt[p]{w}.$$

(This is independent of the choice of representative w of $[w]$, and of the pth root $\sqrt[p]{w}$.) The Kummer pairing is perfect, so that in particular $|V| = |W| = p^r$.

Now $\mathrm{Gal}(N/k)$ fits into an exact sequence

$$1 \longrightarrow V \longrightarrow \mathrm{Gal}(N/k) \longrightarrow C \longrightarrow 1.$$

This extension splits since V, C have coprime orders, so we may lift the generator σ of $C = \mathrm{Gal}(E/k)$ to an automorphism of N of order m. Denoting this automorphism again by σ, we have $\Gamma = V \rtimes_{\rho_2} C$ where ρ_2 is the representation of C on V given by conjugation inside Γ, i.e., $\rho_2(\sigma)(v) = \sigma v \sigma^{-1}$.

A simple calculation (analogous to that in [4, Proposition 2.1]) shows that

$$\langle \rho_2(\sigma)v, \rho_1(\sigma)[w]\rangle = \langle v, [w]\rangle \text{ for all } v \in V, [w] \in W,$$

so ρ_2 is the contragredient representation to ρ_1. □

Now let ρ and $\Gamma = V \rtimes_\rho C$ be as in §4.1. Recall that f is the minimal polynomial of $\rho(\sigma)$, and that g is defined by $fg = X^m - 1$.

LEMMA 5.1.2. — *Let $y \in E^\times$, with $[\hat{g}(\sigma)\cdot y] \neq 0$ in $E^\times/E^{\times p}$. Let N be the Galois closure over k of the field*

$$L = E(\sqrt[p]{\hat{g}(\sigma)\cdot y}).$$

Then N is a Γ-extension of k relative to E.

Conversely, if N is a Γ-extension of k relative to E then N is the Galois closure of $E(\sqrt[p]{\hat{g}(\sigma)\cdot y})$ for some $y \in E^\times$ with $[\hat{g}(\sigma)\cdot y] \neq 0$ in $E^\times/E^{\times p}$.

Proof. — Apply Lemma 5.1.1 to $w = \hat{g}(\sigma)\cdot y$. Then $W = \mathbb{F}_p[C]\cdot[w] \neq 0$ but $\hat{f}(\sigma)\cdot W = 0$ in $E^\times/E^{\times p}$, since $\hat{f}(\sigma)\hat{g}(\sigma) = \sigma^m - 1 = 0$ in $\mathbb{F}_p[C]$. Thus W is a cyclic $\mathbb{F}_p[C]$-module of dimension r over $\mathbb{F}_p$ annihilated by $\hat{f}(\sigma)$. Hence $V_* = \mathrm{Gal}(N/E)$ is elementary abelian of order p^r, and $\mathrm{Gal}(N/k) = V_* \rtimes_{\rho_*} C$ where ρ_* is a representation of degree r in which σ has minimal polynomial f. Thus we may identify V_* with V and ρ_* with the given representation ρ, making N into a Γ-extension of k relative to E.

Conversely, let N be a Γ-extension of k relative to E. Let $L = E(\sqrt[p]{w})$ be a subfield of N of degree p over E. Let $U = \mathrm{Gal}(N/L)$. Then $\cap_{i=0}^{m-1}\sigma^i U\sigma^{-i} = \{1\}$, so N is the Galois closure of L over k, and by Lemma 5.1.1, ρ is the contragredient of the representation ρ_1 of C on $W = \mathbb{F}_p[C]\cdot w$. Hence $\dim_{\mathbb{F}_p}(W) = r$ and W is annihilated by $\hat{f}(\sigma)$. Since $\hat{f}(X)$ and $\hat{g}(X)$ are relatively prime in $\mathbb{F}_p[X]$ with $\hat{f}(\sigma)\hat{g}(\sigma) = 0$ in $\mathbb{F}_p[C]$, it follows that $[w] = [\hat{g}(\sigma)\cdot y]$ for some $y \in E^\times$. Clearly $[y] \neq 0$ in $E^\times/E^{\times p}$. □

We now restrict our attention to tame extensions N/k. We begin by examining the behaviour of primes above p in N/k.

LEMMA 5.1.3. — *Let N be a tame Γ-extension of k relative to E. Let $\mathfrak{p}$ be a prime of k above p. Then either*

(i) *every prime of E above $\mathfrak{p}$ splits completely in N/E, or*
(ii) *$\mathfrak{p}$ splits completely in E/k, and every prime of N above $\mathfrak{p}$ has inertia degree p in N/E (and hence also in N/k).*

Proof. — Let $\tilde{\mathfrak{P}}$ be a prime of N above $\mathfrak{p}$, let $\Delta \subseteq \Gamma$ be the decomposition group of $\tilde{\mathfrak{P}}$ in N/k, and let $I \subseteq \Delta$ be its inertia group. As N/k is tame, I is a cyclic normal subgroup of Δ of order prime to p, and Δ/I is cyclic, its order being the inertia degree of $\tilde{\mathfrak{P}}$ in N/k.

Now Δ is a semidirect product $V' \rtimes C'$, where $V' = \Delta \cap V$ is a normal subgroup of Δ of order $p^{r'}$ with $0 \leqslant r' \leqslant r$, and $C' = \Delta/V'$ is cyclic of order m' for some divisor m' of m. If $V' = \{1\}$, then Δ has order prime to $|V|$, and the prime $\mathfrak{P}$ of E below $\tilde{\mathfrak{P}}$ splits completely in N/E. Since E/k is Galois, this means that (i) holds. If on the other hand $V' \neq \{1\}$, the only cyclic normal subgroups of Δ are subgroups of V', so $I = \{1\}$. Then Δ/I cannot be cyclic unless $C' = \{1\}$. So $\Delta = V'$ and this group is cyclic of order p. Thus the inertia degree of $\tilde{\mathfrak{P}}$ in N/k is p, giving (ii). □

Definition 5.1.4. — *Let S^p_{split} (respectively S^p_{nonsplit}) be the set of places of k above p satisfying condition (i) (respectively (ii)) in Lemma 5.1.3.*

We now show how we can choose y in Lemma 5.1.2 to have a convenient form. We write mod^* for the usual generalized congruence relation of class field theory.

Lemma 5.1.5. — *Let E/k be as above. If N/k is a tame Γ-extension of k relative to E then N is the Galois closure over k of the field $L = E(\sqrt[p]{\hat{g}(\sigma)\cdot y})$ for some $y \in E^\times$ satisfying the following conditions:*

(i) $\hat{g}(\sigma)\cdot y \notin E^{\times p}$;
(ii) $y \equiv 1 \pmod^* (\xi_p - 1)^p O_E)$;
(iii) $y \equiv 1 \pmod{p^{2r+1} O_{E,\mathfrak{p}}}$ *for each* $\mathfrak{p} \in S^p_{\mathrm{split}}$;
(iv) *the fractional ideal yO_E factorizes as*

$$yO_E = \prod_{i=1}^{n} \mathfrak{Q}_i^{e_i(\sigma)} \tag{38}$$

for some $n \geqslant 0$, some $e_i(\sigma) \in \mathbb{Z}[C]$, and some prime ideals $\mathfrak{Q}_i$ of O_E which lie above distinct prime ideals $\mathfrak{q}_i$ of O_k which split completely in E/k and do not contain p.

Conversely, given y satisfying these conditions, the Galois closure over k of $E(\sqrt[p]{\hat{g}(\sigma)\cdot y})$ is a tame Γ-extension of k relative to E.

Proof. — Since E/k is tame, any Γ-extension N of k relative to E will be tame if and only if N/E is tame, and this holds if and only if any (and hence all) of the subextensions L/E of degree p are tame. But it is well-known from Kummer theory that $L = E(\sqrt[p]{w})$ is tame over E if and only if there is some $x \in E^\times$ with

$$x^p w \equiv 1 \pmod^* (\xi_p - 1)^p O_E) \tag{39}$$

(see for instance [16, §39]). Thus, if y satisfies (i) and (ii), it follows from Lemma 5.1.2 that the Galois closure N over k of $L = E(\sqrt[p]{\hat{g}(\sigma)\cdot y})$ is a

tame Γ-extension of k relative to E. This proves the "converse" part of the Lemma.

Now let N be any tame Γ-extension of k relative to E. By Lemma 5.1.2, N is the Galois closure over k of $L = E(\sqrt[p]{w})$, where $w = \hat{g}(\sigma) \cdot y$ for some $y \in E^\times$ satisfying (i). Since L/E is tame, (39) holds for some $x \in E$. We need to show that we can adjust y (without changing N) so that (ii), (iii) and (iv) hold.

If $\mathfrak{P}$ is a place of E above a place of k in S^p_{split}, then $w = a^p_{\mathfrak{P}}$ for some $a_{\mathfrak{P}} \in E^\times_{\mathfrak{P}}$. By the Weak Approximation Theorem, we may choose $x_1 \in E$ satisfying the following conditions:

$$x_1 \equiv a_{\mathfrak{P}}^{-1} \pmod{p^{2r} O_{E,\mathfrak{P}}} \quad \text{for all } \mathfrak{P} \text{ above places in } S^p_{\text{split}}.$$
$$x_1 \equiv x \pmod{(\xi_p - 1) O_{E,\mathfrak{P}}} \quad \text{for all } \mathfrak{P} \text{ above places in } S^p_{\text{nonsplit}}.$$

Then we have

$$x_1^p w \equiv 1 \pmod{p^{2r+1} O_{E,\mathfrak{P}}} \quad \text{for all } \mathfrak{P} \text{ above places in } S^p_{\text{split}}.$$
$$x_1^p w \equiv 1 \pmod{(\xi_p - 1)^p O_{E,\mathfrak{P}}} \quad \text{for all } \mathfrak{P} \text{ above places in } S^p_{\text{nonsplit}}.$$

In particular, $x_1^p w \equiv 1 \pmod^* (\xi_p - 1)^p O_E)$.

Since $\hat{f}$ and $\hat{g}$ are coprime in $\mathbb{F}_p[X]$, there exist $l(X)$, $l'(X) \in \mathbb{Z}[X]$ so that $1 = \hat{g}(X)l(X) + \hat{f}(X)l'(X)$ in $\mathbb{F}_p[X]$. Let $y_1 = l(\sigma) \cdot (x_1^p w)$, so y_1 satisfies (ii) and (iii). Then in $E^\times / E^{\times p}$ we have

$$\begin{aligned}[y] &= [\hat{g}(\sigma) l(\sigma) \cdot y] + [\hat{f}(\sigma) l'(\sigma) \cdot y] \\ &= [l(\sigma) \cdot w] + [\hat{f}(\sigma) l'(\sigma) \cdot y] \\ &= [y_1] + [\hat{f}(\sigma) l'(\sigma) \cdot y],\end{aligned}$$

so that

$$[w] = [\hat{g}(\sigma) \cdot y] = [\hat{g}(\sigma) \cdot y_1] + [\hat{g}(\sigma) \hat{f}(\sigma) l'(\sigma) \cdot y] = [\hat{g}(\sigma) \cdot y_1].$$

We can therefore replace y by y_1 without changing N. Hence we may choose y to satisfy (ii) and (iii).

We now turn to condition (iv). We can certainly factorize yO_E in the form

$$yO_E = \prod_{i=1}^{n} \mathfrak{Q}_i^{e_i(\sigma)},$$

where the $\mathfrak{Q}_i$ lie above distinct prime ideals $\mathfrak{q}_i$ of k. By (ii) and (iii), none of the $\mathfrak{q}_i$ can contain p. To obtain (iv) it remains to show that y can be further adjusted so that the $\mathfrak{Q}_i$ all have degree 1 over k (whence $N_{E/k}(\mathfrak{Q}_i) = \mathfrak{q}_i$).

We may write

$$y^{\hat{g}(\sigma)}O_E = \prod_{i=1}^{n} \mathfrak{Q}_i^{e_i(\sigma)\hat{g}(\sigma)} = \prod_{i=1}^{n} \mathfrak{Q}_i^{pq_i(\sigma)+r_i(\sigma)},$$

where the $q_i(\sigma)$, $r_i(\sigma) \in \mathbb{Z}[C]$ and the $\mathfrak{Q}_i^{r_i(\sigma)}$ are integral p-power-free ideals of O_E (so $\prod_{i=1}^{n} \mathfrak{Q}_i^{q_i(\sigma)}$ is the "p-part" of $y^{\hat{g}(\sigma)}O_E$). Renumbering the $\mathfrak{Q}_i$, we can suppose that $\mathfrak{Q}_i^{r_i(\sigma)} \neq O_E$ if and only if $i \leqslant t$, say. Then

$$y^{\hat{g}(\sigma)}O_E = \prod_{i=1}^{t} \mathfrak{Q}_i^{pq_i(\sigma)+r_i(\sigma)} \left(\prod_{i=t+1}^{n} \mathfrak{Q}_i^{q_i(\sigma)} \right)^p.$$

Now suppose some $\mathfrak{q}_i$ does not split completely in E/k. Then $\mathfrak{Q}_i$ is fixed by σ^h for some divisor $h < m$ of m. But $\sigma^h - 1$ divides $\hat{g}(\sigma)$ in $\mathbb{F}_p[C]$, so $\mathfrak{Q}_i^{e_i(\sigma)\hat{g}(\sigma)}$ is a pth power, and hence $i > t$. This shows that $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_t$ split completely in E/k, and therefore have degree 1 over k.

By the Tchebotarev density theorem, we may choose a prime $\mathfrak{Q}$ of O_E, of degree 1 over k, not above p or any of the $\mathfrak{q}_i$, and with the same class in $\mathrm{Cl}_{p^{2r+1}}(O_E)$ as $\prod_{i=t+1}^{n} \mathfrak{Q}_i^{q_i(\sigma)}$. Thus, for some $u \in E$ with $u \equiv 1 \pmod^{*} p^{2r+1}O_E$, we have

$$u^p y^{\hat{g}(\sigma)}O_E = \left(\prod_{i=1}^{t} \mathfrak{Q}_i^{pq_i(\sigma)+r_i(\sigma)} \right) \mathfrak{Q}^p.$$

We have just seen that the $\mathfrak{Q}_i$ for $i \leqslant t$ have degree 1 over k. Arguing as above, we may replace y by $l(\sigma) \cdot (u^p y^{\hat{g}(\sigma)})$. Then condition (iv) is satisfied; (ii) and (iii) still hold by the congruence condition on u. □

Remark 5.1.6. — By Kummer theory, the ramified primes in N/E are precisely the conjugates of the $\mathfrak{Q}_i$ with $\mathfrak{Q}_i^{r_i(\sigma)} \neq O_E$. The proof of Lemma 5.1.5 therefore shows that if some (and hence every) prime $\mathfrak{Q}$ of E above a prime $\mathfrak{q}$ of k ramifies in N/E, then $\mathfrak{q}$ splits completely in E/k. Moreover, the ramification groups in N/E must be cyclic as N/E is tame, so each $\mathfrak{Q}_i$ has ramification index p in N/k.

5.2. Local Normal Integral Bases for N/E

Let N be as in Lemma 5.1.5. In this subsection we describe the action of Γ on N somewhat more explicitly, and construct a normal basis system $\boldsymbol{\eta} = (\eta, (\eta_{\mathfrak{P}})_{\mathfrak{P}})$ for N/E. We shall in fact choose the $\eta_{\mathfrak{P}}$ so that $\eta_{\mathfrak{P}} = \eta_{\mathfrak{P}'}$ whenever the places $\mathfrak{P}$, $\mathfrak{P}'$ of E lie over the same place $\mathfrak{p}$ of k, and we

denote this common value by $\eta_{\mathfrak{p}}$. Thus we shall write $\boldsymbol{\eta} = (\eta, (\eta_{\mathfrak{p}})_{\mathfrak{p}})$, with components $\eta_{\mathfrak{p}}$ indexed by places $\mathfrak{p}$ of k.

We know that N is the Galois closure over k of $L = E(\sqrt[p]{\hat{g}(\sigma)\cdot y})$ for some $y \in E^{\times}$ satisfying conditions (i)–(iv) of Lemma 5.1.5. Fix $z \in N$ satisfying

$$z^p = \hat{g}(\sigma)\cdot y.$$

Then $N = E(z, \widetilde{\sigma}(z), \ldots, \widetilde{\sigma}^{r-1}(z))$, where $\widetilde{\sigma} \in \mathrm{Gal}(N/k) = \Gamma$ is any preimage of the generator σ of $C = \mathrm{Gal}(E/k)$. There are p^r possible choices for $\widetilde{\sigma}$, all of order m, corresponding to the p choices for each $\widetilde{\sigma}^i(z)$, $1 \leqslant i \leqslant r$, subject to the conditions

$$(\widetilde{\sigma}^i(z))^p = \sigma^i \hat{g}(\sigma)\cdot y \text{ for } 1 \leqslant i \leqslant r-1; \qquad (\hat{f}(\widetilde{\sigma})\cdot z)^p = \hat{f}(\sigma)\hat{g}(\sigma)\cdot y. \quad (40)$$

We make a convenient choice of $\widetilde{\sigma}$ as follows. In $\mathbb{Z}[C]$ we have

$$\hat{f}(X)\hat{g}(X) = (1 - X^m) + pc(X) \quad (41)$$

for some $c(X) \in \mathbb{Z}[X]$. Thus the last equation of (40) becomes

$$(\hat{f}(\widetilde{\sigma})\cdot z)^p = (c(\sigma)\cdot y)^p.$$

We then choose one of the p^{r-1} possibilities for $\widetilde{\sigma}$ such that

$$\hat{f}(\widetilde{\sigma})\cdot z = c(\sigma)\cdot y.$$

To ease notation, we from now on write σ in place of $\widetilde{\sigma}$.

We note a consequence of our choice of σ.

PROPOSITION 5.2.1. — *For $\sigma \in \mathrm{Gal}(N/k)$ as above, we have*

$$(1 + \sigma + \cdots + \sigma^{m-1})\cdot z = N_{E/k}(y)^{b_0}$$

where b_0 is as in Definition 3.4.2.

Proof. — First observe that

$$\begin{aligned}\big((1 + \sigma + \cdots + \sigma^{m-1})\cdot z\big)^p &= N_{E/k}(z^p)\\ &= N_{E/k}(y^{\hat{g}(\sigma)})\\ &= N_{E/k}(y)^{\hat{g}(1)}\\ &= N_{E/k}(y)^{pb_0},\end{aligned}$$

so that

$$(1 + \sigma + \cdots + \sigma^{m-1})\cdot z = \xi_p^e N_{E/k}(y)^{b_0}$$

for some e. Now in $\mathbb{F}_p[X]$ we have

$$(1 + X + \cdots + X^{m-1})(1 - X) = 1 - X^m = \hat{f}(X)\hat{g}(X)$$

with $\hat{f}(1) \neq 0$, so $\hat{f}(X)$ divides $1 + X + \cdots + X^{m-1}$. Thus in $\mathbb{Z}[X]$ we have

$$1 + X + \cdots + X^{m-1} = \hat{f}(X)h(X) + pd(X)$$

for some $h(X)$ and $d(X)$. Since $\hat{f}(\sigma) \cdot z \in \mathbb{Z}[C] \cdot y$ by choice of σ, and $z^p = \hat{g}(\sigma) \cdot y \in \mathbb{Z}[C] \cdot y$, it follows that $(1 + \sigma + \cdots + \sigma^{m-1}) \cdot z \in \mathbb{Z}[C] \cdot y$. Since clearly also $N_{E/k}(y) \in \mathbb{Z}[C] \cdot y$, we must have $\xi_p^e \in \mathbb{Z}[C] \cdot y$, so $\xi_p^e = 1$ by condition (ii) of Lemma 5.1.5. □

We next consider the Galois group $V = \mathrm{Gal}(N/E)$. This is an $\mathbb{F}_p[C]$-module dual to the submodule of $E^\times/E^{\times p}$ generated by $\hat{g}(\sigma) \cdot y$. Now N has a basis over E consisting of the p^r elements $z^{a(\sigma)}$ as a runs through the set P (see Definition 3.3.1), and we fix a nontrivial element $v \in V$ by setting

$$v(z^{a(\sigma)}) = \xi_p^{[1,a(\sigma)]} z^{a(\sigma)} \text{ for all } a \in P,$$

where $[\,\cdot\,,\,\cdot\,]$ is the pairing (32). Then $V = \mathbb{F}_p[C] \cdot v$, and we have

$$v^{c(\sigma)}(z^{a(\sigma)}) = \xi_p^{[c(\sigma),a(\sigma)]} z^{a(\sigma)} \text{ for all } a,\, c \in P.$$

For the idempotents $e_{b(\sigma)}$ of (36) we have

$$\begin{aligned}
e_{b(\sigma)} \cdot z^{a(\sigma)} &= \frac{1}{p^r} \sum_{c \in P} \psi^{b(\sigma)}(v^{c(\sigma)})\, v^{-c(\sigma)}(z^{a(\sigma)}) \\
&= \frac{1}{p^r} \sum_{c \in P} \xi_p^{[c(\sigma),b(\sigma)]} \xi_p^{-[c(\sigma),a(\sigma)]} z^{a(\sigma)} \\
&= \frac{1}{p^r} \left(\sum_{c \in P} \xi_p^{[c(\sigma),b(\sigma)-a(\sigma)]} \right) z^{a(\sigma)} \\
&= \frac{1}{p^r} \left(\sum_{c \in P} \psi^{b(\sigma)-a(\sigma)}(v^{c(\sigma)}) \right) z^{a(\sigma)} \\
&= \begin{cases} z^{a(\sigma)} & \text{if } b(\sigma) = a(\sigma) \\ 0 & \text{otherwise,} \end{cases}
\end{aligned}$$

since $\sum_{u \in V} \psi'(u) = 0$ for any nontrivial $\psi' \in V^\dagger$.

Now define

$$\eta = \frac{1}{p^r} \sum_{a \in P} z^{a(\sigma)}. \tag{42}$$

For each $a \in P$ we have

$$e_{a(\sigma)} \cdot \eta = \frac{1}{p^r} z^{a(\sigma)} \neq 0, \tag{43}$$

so η is a normal basis for N/E.

LEMMA 5.2.2. — *For each place $\mathfrak{p} \neq \mathfrak{q}_1, \ldots, \mathfrak{q}_n$ of k (see Lemma 5.1.5), we have*

$$O_{N,\mathfrak{p}} = O_{E,\mathfrak{p}}[V] \cdot \eta.$$

Proof. — This is clear for the infinite places $\mathfrak{p}$. We next deal with the places above p. Since $z^p \equiv 1 \pmod^* (\xi_p - 1)^p)$, it is well-known that the element

$$\eta_L = \frac{1}{p} \sum_{h=0}^{p-1} z^h$$

is a local normal integral basis at p for L/E (see e.g. [17, proof of Theorem (3.2.2)]). Hence $\sigma^i(\eta_L)$ is a local normal integral basis at p for $\sigma^i(L)/E$. Since $N = \otimes_{i=0}^{r-1} \sigma^i(L)$ (tensor product over E) and the $\sigma^i(L)/E$ are all unramified over p, it follows that $\eta = \prod \sigma^i(\eta_L)$ is a local normal integral basis for N/E at p.

Finally, let $\mathfrak{p}$ be a finite place of E distinct from $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ and not above p. Then p is invertible in $O_{E,\mathfrak{p}}$, and the idempotents $e_{a(\sigma)}$ form an $O_{E,\mathfrak{p}}$-basis of $O_{E,\mathfrak{p}}[V]$. Since the prime factorizations of the ideals $(z^{a(\sigma)})^p O_E = y^{a(\sigma)\hat{g}(\sigma)} O_E$ do not involve primes above $\mathfrak{p}$, it follows that the $z^{a(\sigma)}$ form an $O_{E,\mathfrak{p}}$-basis of $O_{N,\mathfrak{p}}$. Hence, by (43), η is a local normal integral basis generator at $\mathfrak{p}$. □

For each place $\mathfrak{p} \neq \mathfrak{q}_1, \ldots, \mathfrak{q}_n$ of k, we set

$$\eta_{\mathfrak{p}} = \eta.$$

We now construct local normal integral basis generators $\eta_{\mathfrak{q}_i}$ at the places $\mathfrak{q}_i$ for $1 \leqslant i \leqslant n$. For each i, choose $\mu_i \in E$ so that μ_i has valuation 1 at $\mathfrak{Q}_i$ and valuation 0 at $\sigma^j(\mathfrak{Q}_i)$ for $1 \leqslant j \leqslant m-1$, and also μ_i has valuation 0 at $\sigma^j(\mathfrak{Q}_h)$ for all $h \neq i$ and all j. Let $\pi_i = N_{E/k}(\mu_i)$. Then π_i has valuation 1 at $\mathfrak{q}_i$ and valuation 0 at $\mathfrak{q}_h$ for $h \neq i$.

For each i and each $a \in P$, set

$$r_i(\sigma; a) = a(\sigma) e_i(\sigma) \hat{g}(\sigma) \in \mathbb{F}_p[C].$$

Viewing $r_i(\sigma; a)$ as an element of $\mathbb{Z}[C]$, we then have

$$a(\sigma) e_i(\sigma) \hat{g}(\sigma) = p q_i(\sigma; a) + r_i(\sigma; a) \tag{44}$$

for some $q_i(\sigma; a) \in \mathbb{Z}[C]$. Since the $\mathfrak{q}_i$ split completely in E/k,

$$\left(\mu_i^{-q_i(\sigma;a)} z^{a(\sigma)}\right)^p O_{E,\mathfrak{q}_i} = \mathfrak{Q}_i^{r_i(\sigma;a)} O_{E,\mathfrak{q}_i}$$

is then a p-power-free integral ideal in the semilocal ring $O_{E,\mathfrak{q}_i}$. Define

$$\eta_{\mathfrak{q}_i} = \frac{1}{p^r} \sum_{a \in P} \mu_i^{-q_i(\sigma;a)} z^{a(\sigma)}.$$

Then $\eta_{\mathfrak{q}_i}$ is a local normal integral basis generator for N/E at all places of E above $\mathfrak{q}_i$.

Taking $a(\sigma) = \overline{c}^{(j)}(\sigma)$ in (44), and noting that $\sigma\overline{c}^{(j)}(\sigma)\hat{g}(\sigma) = \overline{c}^{(j+d)}(\sigma)\hat{g}(\sigma)$ by Lemma 4.2.4, we have

$$pq_i(\sigma;\overline{c}^{(j+d)}) + r_i(\sigma;\overline{c}^{(j+d)}) = \sigma pq_i(\sigma;\overline{c}^{(j)}) + \sigma r_i(\sigma;\overline{c}^{(j)}),$$

and hence

$$q_i(\sigma;\overline{c}^{(j+d)}) = \sigma q_i(\sigma;\overline{c}^{(j)}). \tag{45}$$

5.3. Resolvents for N/E

We now have a normal basis system $\boldsymbol{\eta} = (\eta, (\eta_{\mathfrak{p}})_{\mathfrak{p}})$ for N/E. An easy calculation gives the corresponding Fröhlich-Lagrange resolvents: for each $a \in P$ we find

$$\langle \eta, \psi^{a(\sigma)} \rangle_{N/E} = z^{a(\sigma)};$$

$$\langle \eta_{\mathfrak{p}}, \psi^{a(\sigma)} \rangle_{N/E} = z^{a(\sigma)} \text{ if } \mathfrak{p} \neq \mathfrak{q}_1, \ldots, \mathfrak{q}_n;$$

$$\langle \eta_{\mathfrak{q}_i}, \psi^{a(\sigma)} \rangle_{N/E} = \mu_i^{-q_i(\sigma;a)} z^{a(\sigma)} \text{ for } 1 \leqslant i \leqslant n.$$

In the next subsection, we will apply Fröhlich's induction formula in the form of Corollary 2.4.3 to the induced characters $\chi_j = \mathrm{Ind}_V^{\Gamma}\psi_j$ of Γ. With this in mind, we make the following definition:

Definition 5.3.1. — *The element $\mathcal{X}$ of $\mathrm{Cl}(O_k[\Gamma])$ is the class represented by the character homomorphism $h_{\mathcal{X}} \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ with*

$$h_{\mathcal{X}}(\Phi_i) = 1 \text{ for } 1 \leqslant i \leqslant s; \quad h_{\mathcal{X}}(\chi_j) = (\mathcal{N}_{E/k} h_{\boldsymbol{\eta}})(\psi_j) \text{ for } 0 \leqslant j \leqslant d-1,$$

where $h_{\boldsymbol{\eta}}$ is as in Lemma 2.1.1:

$$h_{\boldsymbol{\eta}}(\psi') = \left(\frac{\langle \eta_{\mathfrak{p}}, \psi' \rangle_{N/E}}{\langle \eta, \psi' \rangle_{N/E}} \right)_{\mathfrak{p}} \text{ for all } \psi' \in R_V.$$

Since $\xi_p \in k$, the Fröhlich norm $\mathcal{N}_{E/k}$ is induced by the usual idèle norm $N_{E/k}$. In particular, for $1 \leqslant i \leqslant n$, the component at the place $\mathfrak{q}_i$ of $h_{\mathcal{X}}(\chi_j)$ is given by

$$h_{\mathcal{X}}(\chi_j)_{\mathfrak{q}_i} = N_{E/k}(\mu_i^{-q_i(\sigma;\overline{c}^{(j)})}) = \pi_i^{-q_i(1;\overline{c}^{(j)})},$$

with $h_{\mathcal{X}}(\chi_j)_{\mathfrak{p}} = 1$ at all other places $\mathfrak{p}$.

Lemma 5.3.2. — *In $\mathrm{Cl}(O_E[\Gamma])$ we have $\mathbf{i}_{E/k}(\mathcal{X}) = \iota_*^V((O_N)_{O_E[V]})$.*

Proof. — The class $(O_N)_{O_E[V]}$ is represented by

$$h_{\boldsymbol{\eta}} \in \mathrm{Hom}_{\Omega_E}(R_V, \mathbb{J}(k^c)).$$

We have $h_{\boldsymbol{\eta}}(\epsilon) = 1$ and

$$h_{\boldsymbol{\eta}}(\psi_j) = \left(\frac{\langle \eta_{\mathfrak{p}}, \psi^{\overline{c}^{(j)}(\sigma)} \rangle_{N/E}}{\langle \eta, \psi^{\overline{c}^{(j)}(\sigma)} \rangle_{N/E}} \right)_{\mathfrak{p}} \text{ for } 0 \leqslant j \leqslant p^r - 2,$$

so that

$$h_{\boldsymbol{\eta}}(\psi_j)_{\mathfrak{p}} = \begin{cases} \mu_i^{-q_i(\sigma;\overline{c}^{(j)})} & \text{if } \mathfrak{p} = \mathfrak{q}_i \text{ with } 1 \leqslant i \leqslant n; \\ 1 & \text{otherwise.} \end{cases}$$

By Lemma 4.3.3 (applied to E in place of k), the class $\iota_*^V((O_N)_{O_E[V]}) \in \mathrm{Cl}(O_E[\Gamma])$ is represented by $\iota_*^V h_{\boldsymbol{\eta}} \in \mathrm{Hom}_{\Omega_E}(R_\Gamma, \mathbb{J}(k^c))$ where

$$\iota_*^V h_{\boldsymbol{\eta}}(\phi) = 1 \text{ for all characters } \phi \text{ of } \Gamma \text{ trivial on } V;$$

$$\iota_*^V h_{\boldsymbol{\eta}}(\chi_j) = \prod_{\lambda=0}^{m-1} h_{\boldsymbol{\eta}}(\psi_{j+\lambda d}) \text{ for } 0 \leqslant j \leqslant d-1.$$

Thus $\iota_*^V h_{\boldsymbol{\eta}}(\chi_j)_{\mathfrak{p}} = 1$ unless $\mathfrak{p} \in \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$, while

$$\iota_*^V h_{\boldsymbol{\eta}}(\chi_j)_{\mathfrak{q}_i} = \mu_i^{-Q_{i,j}},$$

where

$$Q_{i,j} = \sum_{\lambda=0}^{m-1} q_i(\sigma; \overline{c}^{(j+\lambda d)}).$$

Using (45), we then have

$$Q_{i,j} = \left(\sum_{\lambda=0}^{m-1} \sigma^\lambda \right) q_i(\sigma; \overline{c}^{(j)}).$$

Hence $\iota_*^V h_{\boldsymbol{\eta}}(\chi_j) \in \mathbb{J}(E)$ has components

$$\iota_*^V h_{\boldsymbol{\eta}}(\chi_j)_{\mathfrak{q}_i} = N_{E/k}(\mu_i^{-q_i(\sigma;\overline{c}^{(j)})}) = h_{\mathcal{X}}(\chi_j)_{\mathfrak{q}_i} \text{ for } 1 \leqslant i \leqslant n,$$

and $\iota_*^V h_{\boldsymbol{\eta}}(\chi_j)_{\mathfrak{p}} = 1$ if $\mathfrak{p} \notin \{\mathfrak{q}_1, \dots, \mathfrak{q}_t\}$. Thus $\iota_*^V h_{\boldsymbol{\eta}} = \mathfrak{i}_{E/k} h_{\mathcal{X}}$, and the result follows. □

For each $i \in \{1, \dots, n\}$, either $e_i(\sigma)\hat{g}(\sigma) \in \hat{\mathcal{C}}^{(t)}$ for some $t \in \{1, \dots, d\}$ or $e_i(\sigma)\hat{g}(\sigma) = 0$ in $\mathbb{F}_p[C]$. For each t, let $S_t \subseteq \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ consist of those places $\mathfrak{q}_i$ with $e_i(\sigma)\hat{g}(\sigma) \in \hat{\mathcal{C}}^{(t)}$, and let S' be the set of places $\mathfrak{q}_i$ with $e_i(\sigma)\hat{g}(\sigma) = 0$. If $\mathfrak{q}_i \in S_t$, it follows from (44) and Lemma 4.2.4 that $r_i(\sigma; \overline{c}^{(j)}) \in \hat{\mathcal{C}}^{(t-j)}$ and hence

$$pq_i(1; \overline{c}^{(j)}) + w_{t-j} = \overline{c}^{(j)}(1) e_i(1) w_0.$$

Since $w_{t-j} = pb_{t-j}$ and $w_0 = pt_0$, we then have

$$q_i(1;\overline{c}^{(j)}) = \overline{c}^{(j)}(1)e_i(1)b_0 - b_{t-j}.$$

If $\mathfrak{q}_i \in S'$ then $r_i(\sigma;\overline{c}^{(j)}) = 0$ for all j, so

$$q_i(1;\overline{c}^{(j)}) = \overline{c}^{(j)}(1)e_i(1)b_0.$$

Hence the idèle $h_{\mathcal{X}}(\chi_j) \in \mathbb{J}(k)$ has components

$$h_{\mathcal{X}}(\chi_j)_{\mathfrak{p}} = \begin{cases} \pi_i^{-\overline{c}^{(j)}(1)e_i(1)b_0+b_{t-j}} & \text{if } \mathfrak{p} \in S_t \text{ for some } t; \\ \pi_i^{-\overline{c}^{(j)}(1)e_i(1)b_0} & \text{if } \mathfrak{p} \in S'; \\ 1 & \text{otherwise.} \end{cases} \tag{46}$$

We now define character homomorphisms $g_1 \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ and $g_2 \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, k^{c\times})$ by

$$g_1(\Phi_i) = g_2(\Phi_i) = 1 \text{ for } 1 \leqslant i \leqslant m;$$

$$g_1(\chi_j)_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p} \in S^p_{\mathrm{nonsplit}}; \\ \left(N_{E/k}(y)^{-1}\pi_i^{e_i(1)}\right)^{\overline{c}^{(j)}(1)b_0} & \text{if } \mathfrak{p} = \mathfrak{q}_i \text{ with } 1 \leqslant i \leqslant n; \\ N_{E/k}(y)^{-\overline{c}^{(j)}(1)b_0} & \text{otherwise;} \end{cases}$$

$$g_2(\chi_j) = N_{E/k}(y)^{\overline{c}^{(j)}(1)b_0}.$$

Now

$$N_{E/k}(y)O_k = N_{E/k}\left(\prod_{i=1}^n \mathfrak{Q}_i^{e_i(\sigma)}\right) = \prod_{i=1}^n \mathfrak{q}_i^{e_i(1)}.$$

Thus $g_1(\chi_j)_{\mathfrak{p}} \in O_{k,\mathfrak{p}}^\times$ for all places $\mathfrak{p}$ of k not dividing p. Also, $g_1(\chi_j)_{\mathfrak{p}} \equiv 1 \pmod{p^r O_{k,\mathfrak{p}}}$ for all $\mathfrak{p} \in S^p_{\mathrm{split}}$ by condition (iii) of Lemma 5.1.5, and the same congruence certainly holds for $\mathfrak{p} \in S^p_{\mathrm{nonsplit}}$. Hence $g_1(\chi_j) \in \mathbb{U}_{p^r}(k)$. It follows from Lemma 4.3.1 that g_1 and g_2 both represent the trivial class in $\mathrm{Cl}(O_k[\Gamma])$, so that $\mathcal{X}$ is represented by $g_1 g_2 h_{\mathcal{X}}$. Separating the parts of this character homomorphism supported above the $\mathfrak{q}_i$ and above p, we therefore obtain the following result.

LEMMA 5.3.3. — *The class $\mathcal{X}$ factorizes as $\mathcal{X} = \mathcal{X}'\mathcal{X}''$, where $\mathcal{X}'$, $\mathcal{X}''$ are represented by the character homomorphisms $h_{\mathcal{X}'}$, $h_{\mathcal{X}''}$ defined as follows:*

$$h_{\mathcal{X}'}(\Phi_i) = h_{\mathcal{X}''}(\Phi_i) = 1 \text{ for } 1 \leqslant i \leqslant m;$$

$$h_{\mathcal{X}'}(\chi_j)_{\mathfrak{p}} = \begin{cases} \pi_i^{b_{t-j}} & \text{if } \mathfrak{p} = \mathfrak{q}_i \text{ with } \mathfrak{q}_i \in S_t \text{ for some } t; \\ 1 & \text{otherwise.} \end{cases}$$

$$h_{\mathcal{X}''}(\chi_j)_{\mathfrak{p}} = \begin{cases} N_{E/k}(y)^{\overline{c}^{(j)}(1)b_0} & \text{if } \mathfrak{p} \in S^p_{\text{nonsplit}}; \\ 1 & \text{otherwise.} \end{cases}$$

PROPOSITION 5.3.4. — *The class $\mathcal{X}'$ satisfies $\mathcal{X}' \in \iota_*^V \mathcal{N}_{E/k}(\mathcal{R}(O_E[V]))$.*

Proof. — This follows from Lemma 4.3.6 on taking the $\omega_\lambda \in \mathbb{J}(E)$ to be the idèles with components

$$\omega_{\lambda,\mathfrak{P}} = \begin{cases} \mu_i & \text{if } \mathfrak{P} = \mathfrak{Q}_i \text{ with } \mathfrak{q}_i \in S_\lambda; \\ 1 & \text{otherwise.} \end{cases}$$

□

5.4. The class of O_N

We now apply the general machinery described in §2 to determine $(O_N)_{O_k[\Gamma]}$.

Let $\boldsymbol{\alpha} = (\alpha, (\alpha_{\mathfrak{p}})_{\mathfrak{p}})$ be a normal basis system for N/k. The normal basis α and local normal integral bases $\alpha_{\mathfrak{p}}$ for $\mathfrak{p}$ not above p may be chosen arbitrarily. We will specify the choice of $\alpha_{\mathfrak{p}}$ for $\mathfrak{p}$ above p later, distinguishing the cases $\mathfrak{p} \in S^p_{\text{split}}$ and $\mathfrak{p} \in S^p_{\text{nonsplit}}$.

The class $(O_N)_{O_k[\Gamma]}$ is represented by the character homomorphism $h_{\boldsymbol{\alpha}}$ constructed as in Lemma 2.1.1. We set

$$x_i = h_{\boldsymbol{\alpha}}(\Phi_i) = \left(\frac{\langle \alpha_{\mathfrak{p}}, \Phi_i \rangle_{N/k}}{\langle \alpha, \Phi_i \rangle_{N/k}} \right)_{\mathfrak{p}} \in \mathbb{J}(k_i) \text{ for } 1 \leqslant i \leqslant s;$$

and

$$y_j = h_{\boldsymbol{\alpha}}(\chi_j) = \left(\frac{\langle \alpha_{\mathfrak{p}}, \chi_j \rangle_{N/k}}{\langle \alpha, \chi_j \rangle_{N/k}} \right)_{\mathfrak{p}} \in \mathbb{J}(k) \text{ for } 0 \leqslant j \leqslant d-1.$$

Let $\boldsymbol{\beta} = (\beta, (\beta_{\mathfrak{p}})_{\mathfrak{p}}) = \mathrm{Tr}_{N/E}(\boldsymbol{\alpha})$ so that $\boldsymbol{\beta}$ is a normal basis system for E/k. For $1 \leqslant i \leqslant s$ we have

$$\langle \alpha, \Phi_i \rangle_{N/k} = \langle \beta, \overline{\Phi}_i \rangle_{E/k}, \qquad \langle \alpha_{\mathfrak{p}}, \Phi_i \rangle_{N/k} = \langle \beta_{\mathfrak{p}}, \overline{\Phi}_i \rangle_{E/k} \text{ for each } \mathfrak{p},$$

where $\overline{\Phi}_i$ is the character of $C = \Gamma/V$ induced by Φ_i. Thus $(O_E)_{O_k[C]}$ is represented by $\overline{h} \in \mathrm{Hom}_{\Omega_k}(R_C, \mathbb{J}(k^c))$ where $\overline{h}(\overline{\Phi}_i) = x_i$ for $1 \leqslant i \leqslant s$.

We now evaluate the y_j using Corollary 2.4.3 and Proposition 2.4.4 with $\sigma_i = \sigma^i$. (Thus the σ_i form both a left and right transversal.). We then obtain

$$y_j = \left(\frac{\mathrm{Det}_{\psi_j}(\lambda_{\mathfrak{p}})}{\mathrm{Det}_{\psi_j}(\lambda)} \right)_{\mathfrak{p}}^{-1} h_{\boldsymbol{\alpha}}(\mathrm{Inf}_C^\Gamma r_C) \mathcal{N}_{E/k} h_{\boldsymbol{\eta}}(\psi_j), \tag{47}$$

where $\lambda = (\lambda_{ij})$ is the matrix over $k[V]$ given by

$$\sigma^i(\beta)\eta = \sum_{j=0}^{m-1} \lambda_{ij}\sigma^j(\alpha), \tag{48}$$

and $\lambda_{\mathfrak{p}}$ is defined analogously.

The character ψ_j has degree 1, so it extends to a k-algebra homomorphism $k[V] \longrightarrow k$, and to an $O_{k,\mathfrak{p}}$-algebra homomorphism $O_{k,\mathfrak{p}}[V] \longrightarrow O_{k,\mathfrak{p}}$ for each place $\mathfrak{p}$ of k. Denoting all these homomorphisms again by ψ_j, we have $\mathrm{Det}_{\psi_j}(\lambda) = \psi_j(\det(\lambda))$ and $\mathrm{Det}_{\psi_j}(\lambda_{\mathfrak{p}}) = \psi_j(\det(\lambda_{\mathfrak{p}}))$ for each $\mathfrak{p}$.

LEMMA 5.4.1. — *The class $(O_N)_{O_k[\Gamma]}$ factorizes as $(\iota_*^C(O_E)_{O_k[C]})\mathcal{X}\mathcal{Y}$ where $\mathcal{X}$ is given by Definition 5.3.1, and where $\mathcal{Y}$ is represented by the character homomorphism $h_{\mathcal{Y}}$ with*

$$h_{\mathcal{Y}}(\Phi_i) = 1 \text{ for } 1 \leqslant i \leqslant m;$$

$$h_{\mathcal{Y}}(\chi_j)_{\mathfrak{p}} = \begin{cases} \psi_j(\det(\lambda_{\mathfrak{p}}))^{-1} & \text{if } \mathfrak{p} \text{ is above } p; \\ 1 & \text{otherwise.} \end{cases}$$

Proof. — We may write $h_{\boldsymbol{\alpha}} = h_1 h_2 h_{\mathcal{X}}$, where $h_{\mathcal{X}}$ is defined in Definition 5.3.1 and represents the class $\mathcal{X}$, and where h_1, h_2 are determined by

$$h_1(\Phi_i) = 1, \quad h_2(\Phi_i) = x_i \text{ for } 1 \leqslant i \leqslant s;$$

$$h_1(\chi_j) = \left(\frac{\psi_j(\det(\lambda_{\mathfrak{p}}))}{\psi_j(\det(\lambda))}\right)_{\mathfrak{p}}^{-1}, \quad h_2(\chi_j) = h_{\boldsymbol{\alpha}}(\mathrm{Inf}_C^{\Gamma} r_C) \text{ for } 0 \leqslant j \leqslant d-1.$$

Using Lemma 4.3.1, we may replace h_1 by $h_{\mathcal{Y}}$ since, on the one hand, the factors $\psi_j(\det(\lambda))$ lie in $k^\times$, and, on the other hand, the idèle $u_j = (u_{j,\mathfrak{p}}) \in \mathbb{J}(k)$ with components

$$u_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ is above } p, \\ \psi_j(\det(\lambda_{\mathfrak{p}})) & \text{otherwise,} \end{cases}$$

lies in $\mathbb{U}_{p^r}(k)$ because $\psi_j(\det(\lambda_{\mathfrak{p}})) \in O_{k,\mathfrak{p}}^\times$ for all places $\mathfrak{p}$. Finally, h_2 represents the class $(\iota_*^C(O_E)_{O_k[C]})$ by Lemma 4.3.2. □

Remark 5.4.2. — The classes $\mathcal{X}$ and $\iota_*^C(O_E)_{O_k[C]}$ do not depend on the choice of $\boldsymbol{\alpha}$. Hence neither does $\mathcal{Y}$, although its representing character homomorphism $h_{\mathcal{Y}}$ may depend on $\boldsymbol{\alpha}$.

5.5. Local units at places in S^p_{split}

It remains to specify a convenient choice of local normal integral basis $\alpha_{\mathfrak{p}}$ for each place $\mathfrak{p}$ of k above p, allowing us to determine the local units $\psi_j(\det(\lambda_{\mathfrak{p}}))$ and hence investigate the class $\mathcal{Y}$. We treat the easier case $\mathfrak{p} \in S^p_{\text{split}}$ in this subsection, and the harder case $\mathfrak{p} \in S^p_{\text{nonsplit}}$ in the next.

Let $\mathfrak{p} \in S^p_{\text{split}}$ and fix a place $\mathfrak{P}$ of E above $\mathfrak{p}$. Let $D \subseteq C$ be the decomposition group of $\mathfrak{P}$ in E/k.

Now $N = E(z_0, \dots, z_{r-1})$, where $z_i = \sigma^i(z)$ satisfies

$$z_i^p = y^{\sigma^i \hat{g}(\sigma)} \equiv 1 \pmod{p^{2r+1} O_{E,\mathfrak{p}}}$$

by Lemma 5.1.5. (This congruence takes place in the ring $O_{E,\mathfrak{p}}$, which is in general a product of copies of the integral domain $O_{E,\mathfrak{P}}$.) Thus z_i^p is a pth power in $O_{E,\mathfrak{P}}$. Let z_{i*} be the unique element of $O_{E,\mathfrak{P}}$ satisfying

$$z_{i*}^p = y^{\sigma^i \hat{g}(\sigma)}, \qquad z_{i*} \equiv 1 \pmod{p^{2r} O_{E,\mathfrak{p}}}. \tag{49}$$

The p^r places of O_N above $\mathfrak{P}$ correspond to the assignments $z_i \mapsto \xi_p^{e_i} z_{i*} \in E_{\mathfrak{P}}$ for all possible $e_0, \dots, e_{r-1} \in \{0, \dots, p-1\}$. Let $\tilde{\mathfrak{P}}$ be the place of N determined by $z_i \mapsto z_{i*}$ for all i, and let $i_{\tilde{\mathfrak{P}}} \colon N \longrightarrow E_{\mathfrak{P}}$ be the corresponding inclusion. It follows that, for all $\gamma \in \Gamma$, we have

$$i_{\tilde{\mathfrak{P}}}(\gamma(z_i)) \equiv 1 \pmod{p^{2r} O_{E,\mathfrak{p}}} \text{ for all } i \Leftrightarrow \gamma \in C,$$

so the decomposition group of $\tilde{\mathfrak{P}}$ in Γ is contained in the subgroup C of Γ. This decomposition group is therefore D (now viewed as a subgroup of Γ). We identify $N_{\mathfrak{p}}$ with the Galois algebra $\mathrm{Map}_D(\Gamma, N_{\tilde{\mathfrak{P}}})$, and $O_{N,\mathfrak{p}}$ with $\mathrm{Map}_D(\Gamma, O_{N,\tilde{\mathfrak{P}}})$, as explained in §2.5. Recall that we then write $[x]$ for the function on Γ corresponding to $x \in N$. We similarly identify $E_{\mathfrak{p}}$ (respectively $O_{E,\mathfrak{p}}$) with $\mathrm{Map}_D(C, E_{\mathfrak{P}})$ (respectively $\mathrm{Map}_D(C, O_{E,\mathfrak{P}})$).

Now fix a local normal integral basis generator $\nu_{\mathfrak{p}}$ of E/E^D, and define $\alpha_{\mathfrak{p}} \in O_{N,\mathfrak{p}}$ so that the corresponding function $[\alpha_{\mathfrak{p}}] \in \mathrm{Map}_D(\Gamma, O_{N,\tilde{\mathfrak{P}}})$ is given by

$$[\alpha_{\mathfrak{p}}](\gamma) = \begin{cases} \gamma(\nu_{\mathfrak{p}}) & \text{if } \gamma \in D, \\ 0 & \text{otherwise.} \end{cases}$$

To determine its translate $\gamma' \cdot [\alpha_\mathfrak{p}] = [\gamma' \cdot \alpha_\mathfrak{p}]$ by an arbitrary element $\gamma' = v^{a(\sigma)}\sigma^j$ of Γ, we evaluate this function at an arbitrary $\gamma = \sigma^t v^{b(\sigma)} \in \Gamma$:

$$\begin{aligned}[\gamma' \cdot \alpha_\mathfrak{p}](\gamma) &= [\alpha_\mathfrak{p}](\gamma\gamma') \\ &= [\alpha_\mathfrak{p}](\sigma^t v^{b(\sigma)+a(\sigma)}\sigma^j) \\ &= \begin{cases} \sigma^{t+i}(\nu_\mathfrak{p}) & \text{if } b(\sigma)+a(\sigma) = 0 \text{ in } \mathbb{F}_p[C] \text{ and } \sigma^{t+i} \in D; \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{50}$$

Thus $[\gamma' \cdot \alpha_\mathfrak{p}]$ vanishes on all right cosets of D in Γ except for $D\sigma^{-j}v^{-a(\sigma)}$. By varying γ', we can arrange for any chosen coset to be the one on which $[\gamma' \cdot \alpha_\mathfrak{p}]$ does not vanish. Moreover, we can select γ' so that $[\gamma' \cdot \alpha_\mathfrak{p}]$ takes a fixed element of this coset to any of the basis elements $\delta(\nu_\mathfrak{p})$, $\delta \in D$ of $O_{N,\tilde{\mathfrak{P}}}$ over $O_{k,\mathfrak{p}}$. Hence $O_{k,\mathfrak{p}}[\Gamma] \cdot [\alpha_\mathfrak{p}] = \mathrm{Map}_D(\Gamma, O_{N,\tilde{\mathfrak{P}}}) = O_{N,\mathfrak{p}}$, so that $\alpha_\mathfrak{p}$ is a local normal integral basis for N/k at $\mathfrak{p}$.

LEMMA 5.5.1. — *For $\mathfrak{p} \in S^p_{\mathrm{split}}$ and $\alpha_\mathfrak{p}$ as above, we have $h_\mathcal{Y}(\chi_j)_\mathfrak{p} \equiv 1 \pmod{p^r O_{k,\mathfrak{p}}}$.*

Proof. — It will suffice to show that

$$\det(\lambda_\mathfrak{p}) \equiv 1 \pmod{p^r O_{k,\mathfrak{p}}}. \tag{51}$$

Now $\eta \in N$ corresponds to the map $[\eta]$ taking an arbitrary element $\sigma^t v^{b(\sigma)}$ of Γ (where $0 \leqslant t \leqslant m-1$ and $b \in P$) to

$$\begin{aligned}[\eta](\sigma^t v^{b(\sigma)}) &= \frac{1}{p^r} \sum_{a \in P} i_{\tilde{\mathfrak{P}}}(\sigma^t v^{b(\sigma)}(z^{a(\sigma)})) \\ &= \frac{1}{p^r} \sum_{a \in P} \xi_p^{[b(\sigma),a(\sigma)]} z_*^{\sigma^t a(\sigma)} \\ &\equiv \frac{1}{p^r} \sum_{a \in P} \xi_p^{[b(\sigma),a(\sigma)]} \pmod{p^r O_{N,\tilde{\mathfrak{P}}}} \\ &= \begin{cases} 1 & \text{if } b = 0 \\ 0 & \text{otherwise,} \end{cases} \end{aligned}$$

where the congruence comes from (49).

Recall that $\beta_\mathfrak{p} = \mathrm{Tr}_{N/E}(\alpha_\mathfrak{p})$ is a local normal integral basis for E/k at $\mathfrak{p}$. The corresponding function $[\beta_\mathfrak{p}] \in \mathrm{Map}_D(\Gamma, O_{N,\tilde{\mathfrak{P}}})$ is determined by

$$[\beta_\mathfrak{p}](\sigma^t v^{b(\sigma)}) = \begin{cases} \sigma^t(\nu_\mathfrak{p}) & \text{if } \sigma^t \in D, \\ 0 & \text{otherwise.} \end{cases} \tag{52}$$

We compare the two bases $(\sigma^i \cdot \alpha_\mathfrak{p})_{0 \leqslant i \leqslant m-1}$ and $(\sigma^i(\beta_\mathfrak{p})\eta)_{0 \leqslant i \leqslant m-1}$ for the $O_{k,\mathfrak{p}}[V]$-module $O_{N,\mathfrak{p}}$. Viewing these basis elements as elements in

$\mathrm{Map}_D(\Gamma, O_{N,\tilde{\mathfrak{P}}})$, we have, on the one hand

$$[\sigma^i \cdot \alpha_{\mathfrak{p}}](\sigma^t v^{b(\sigma)}) = \begin{cases} \sigma^{t+i}(\nu_{\mathfrak{p}}) & \text{if } b(\sigma) = 0 \text{ and } \sigma^{t+i} \in D; \\ 0 & \text{otherwise;} \end{cases}$$

by (50). On the other hand,

$$[\sigma^i(\beta_{\mathfrak{p}})\eta](\sigma^t v^{b(\sigma)}) = [\beta_{\mathfrak{p}}](\sigma^t v^{b(\sigma)}\sigma^i)[\eta](\sigma^t v^{b(\sigma)}).$$

If $b(\sigma) \neq 0$ then $[\eta](\sigma^t v^{b(\sigma)}) \equiv 0 \pmod{p^r O_{N,\tilde{\mathfrak{P}}}}$. If $b(\sigma) = 0$ then $[\eta](\sigma^t v^{b(\sigma)}) \equiv 1 \pmod{p^r O_{N,\tilde{\mathfrak{P}}}}$. Hence, using (52), we have the congruence mod $p^r O_{N,\mathfrak{P}}$:

$$[\sigma^i(\beta_{\mathfrak{p}})\eta](\sigma^t v^{b(\sigma)}) \equiv \begin{cases} \sigma^{t+i}(\nu_{\mathfrak{p}}) & \text{if } b(\sigma) = 0 \text{ and } \sigma^{t+i} \in D; \\ 0 & \text{otherwise.} \end{cases}$$

We have therefore shown that, for each i,

$$\sigma^i \cdot \alpha_{\mathfrak{p}} \equiv \sigma^i(\beta_{\mathfrak{p}})\eta \pmod{p^r O_{N,\mathfrak{p}}}.$$

It follows that if $\lambda_{\mathfrak{p}} = (\lambda_{\mathfrak{p},i,j})$ is the matrix over $O_{k,\mathfrak{p}}[V]$ such that

$$\sigma^i(\beta_{\mathfrak{p}})\eta = \sum_{j=0}^{m-1} \lambda_{\mathfrak{p},i,j}\sigma^j \cdot \alpha_{\mathfrak{p}} \text{ for } 0 \leqslant i \leqslant m-1,$$

then $\lambda_{\mathfrak{p}}$ is congruent to the identity matrix mod $p^r O_{k,\mathfrak{p}}[V]$, so certainly $\lambda_{\mathfrak{p}}$ satisfies (51). □

5.6. Local units at places in S^p_{nonsplit}

Now let $\mathfrak{p} \in S^p_{\mathrm{nonsplit}}$, so by Lemma 5.1.3, $\mathfrak{p}$ splits completely in E/k. Let $\mathfrak{P}$ be a place of E above $\mathfrak{p}$, and let $\tilde{\mathfrak{P}}$ be a place of N above $\mathfrak{P}$. Then the decomposition group D of $\tilde{\mathfrak{P}}$ in Γ has order p, so that in particular $D \subseteq V$, and we have $E_{\mathfrak{P}} \cong k_{\mathfrak{p}}$. Let $i_{\tilde{\mathfrak{P}}} \colon N \longrightarrow N_{\tilde{\mathfrak{P}}}$ be the embedding determined by $\tilde{\mathfrak{P}}$.

Recall that η is a local normal integral basis for N/E at all places above p. We view $N_{\mathfrak{p}}$ as the $k_{\mathfrak{p}}$-Galois algebra $\mathrm{Map}_D(\Gamma, N_{\tilde{\mathfrak{P}}})$. Let $\alpha_{\mathfrak{p}} \in N_{\mathfrak{p}}$ correspond to the function $[\alpha_{\mathfrak{p}}] \colon \Gamma \longrightarrow N_{\tilde{\mathfrak{P}}}$ defined by

$$[\alpha_{\mathfrak{p}}](\sigma^t v^{b(\sigma)}) = \begin{cases} i_{\tilde{\mathfrak{P}}}(v^{b(\sigma)}(\eta)) & \text{if } t \equiv 0 \pmod{m}, \\ 0 & \text{otherwise.} \end{cases} \tag{53}$$

We verify that $[\alpha_{\mathfrak{p}}]$ satisfies the required equivariance property

$$[\alpha_{\mathfrak{p}}](\delta\gamma) = [\alpha_{\mathfrak{p}}](\gamma)^{\delta} \text{ for all } \delta \in D,\ \gamma \in \Gamma :$$

if $\gamma \notin V$ then $\delta\gamma \notin V$ so both sides are 0, while if $\gamma \in V$ we have

$$[\alpha_{\mathfrak{p}}](\delta\gamma) = i_{\tilde{\mathfrak{P}}}(\delta\gamma(\eta)) = i_{\tilde{\mathfrak{P}}}(\gamma(\eta))^{\delta} = [\alpha_{\mathfrak{p}}](\gamma)^{\delta}.$$

As η is a local normal integral basis for N/E at $\mathfrak{P}$, it follows that $O_{k,\mathfrak{p}}[V]\cdot\alpha_{\mathfrak{p}} = O_{N,\mathfrak{P}} = \mathrm{Map}_D(V, O_{N,\tilde{\mathfrak{P}}})$. We may decompose the $O_{k,\mathfrak{p}}[V]$-module $\mathrm{Map}_D(\Gamma, O_{N,\tilde{\mathfrak{P}}}) \cong O_{N,\mathfrak{p}}$ as

$$\mathrm{Map}_D(\Gamma, O_{N,\tilde{\mathfrak{P}}}) = \bigoplus_{i=0}^{m-1} \mathrm{Map}_D(V\sigma^{-i}, O_{N,\tilde{\mathfrak{P}}}),$$

and $\sigma^i\cdot[\alpha_{\mathfrak{p}}]$ is an $O_{k,\mathfrak{p}}[V]$-basis for the ith summand. Thus $\alpha_{\mathfrak{p}}$ is a generator for the free $O_{k,\mathfrak{p}}[\Gamma]$-module $O_{N,\mathfrak{p}}$. We choose $\alpha_{\mathfrak{p}}$ as our local normal integral basis for N/k at $\mathfrak{p}$. Explicitly, we have

$$(\sigma^i\cdot[\alpha_{\mathfrak{p}}])\gamma = \begin{cases} i_{\tilde{\mathfrak{P}}}(\gamma\sigma^i(\eta)) & \text{if } \gamma \in V\sigma^{-i}; \\ 0 & \text{otherwise.} \end{cases} \tag{54}$$

We now identify $O_{N,\mathfrak{p}}$ with $\mathrm{Map}_D(\Gamma, O_{N,\mathfrak{P}})$ as before. Recall that $\beta_{\mathfrak{p}} = \mathrm{Tr}_{N/E}(\alpha_{\mathfrak{p}})$. For $\gamma \in \Gamma$ we have

$$[\beta_{\mathfrak{p}}](\gamma) = \sum_{a\in P} [\alpha_{\mathfrak{p}}](\gamma v^{a(\sigma)}) = \begin{cases} 1 & \text{if } \gamma \in V, \\ 0 & \text{otherwise;} \end{cases}$$

and therefore

$$[\sigma^i(\beta_{\mathfrak{p}})](\gamma) = \begin{cases} 1 & \text{if } \gamma \in V\sigma^{-i}, \\ 0 & \text{otherwise.} \end{cases}$$

For each i, the product $[\sigma^i(\beta_{\mathfrak{p}})][\eta]$ is then the map taking γ to

$$\begin{cases} i_{\tilde{\mathfrak{P}}}(\gamma(\eta)) & \text{if } \gamma \in V\sigma^{-i}; \\ 0 & \text{otherwise.} \end{cases}$$

We want to determine

$$\Lambda_i = \sum_{s\in P} \lambda_{i,s} v^{s(\sigma)} \in O_{k,\mathfrak{p}}[V]^{\times}$$

such that

$$\sigma^i(\beta_{\mathfrak{p}})\eta = \Lambda_i \sigma^i(\alpha_{\mathfrak{p}}).$$

Evaluating at $v^{b(\sigma)}\sigma^{-i}$ (and suppressing $i_{\tilde{\mathfrak{P}}}$) this means that, for each $b \in P$, we have

$$[\eta](v^{b(\sigma)}\sigma^{-i}) = \sum_{s\in P} \lambda_{i,s}[\eta](v^{b(\sigma)}\sigma^{-i}v^{s(\sigma)}\sigma^i) = \sum_{s\in P} \lambda_{i,s}[\eta](v^{b(\sigma)+\sigma^{-i}s(\sigma)}) \tag{55}$$

in $N_{\tilde{\mathfrak{P}}}$.

For each $h(\sigma) \in \mathbb{F}_p[C]$, let $\langle h(\sigma)\rangle$ denote $e(\sigma) \in \mathbb{F}_p[C]$, where $e(X)$ is the unique element of P with $h(\sigma)\hat{g}(\sigma) = e(\sigma)\hat{g}(\sigma)$. Thus, for each $i \in \mathbb{Z}$ and each $a \in P$, we have

$$\sigma^{-i}(z^{a(\sigma)}) = \kappa_{i,a} z^{\langle \sigma^{-i} a(\sigma)\rangle}$$

for some $\kappa_{i,a} \in E^\times$; in additive notation,

$$\kappa_{i,a} = (\sigma^{-i} a(\sigma) - \langle \sigma^{-i} a(\sigma)\rangle) \cdot z. \tag{56}$$

We now evaluate the coefficients $\lambda_{i,s}$ in terms of the $\kappa_{i,a}$.

LEMMA 5.6.1. —

$$\lambda_{i,s} = \frac{1}{p^r} \sum_{a \in P} \kappa_{i,a} \xi_p^{[-s(\sigma), a(\sigma)]}.$$

(These coefficients lie in $E_{\mathfrak{P}} \cong k_{\mathfrak{p}}$.)

Proof. — We expand both sides of (55). Firstly,

$$\begin{aligned}
[\eta](v^{b(\sigma)}\sigma^{-i}) &= \frac{1}{p^r} \sum_{a \in P} v^{b(\sigma)} \sigma^{-i} \left(z^{a(\sigma)} \right) \\
&= \frac{1}{p^r} \sum_{a} v^{b(\sigma)} \left(\kappa_{i,a} z^{\langle \sigma^{-i} a(\sigma)\rangle} \right) \\
&= \frac{1}{p^r} \sum_{a} \xi_p^{[b(\sigma), \sigma^{-i} a(\sigma)]} \kappa_{i,a} z^{\langle \sigma^{-i} a(\sigma)\rangle} \\
&= \frac{1}{p^r} \sum_{a} \xi_p^{[b(\sigma), a(\sigma)]} \kappa_{i, \langle \sigma^i a\rangle} z^{a(\sigma)}.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\sum_{s \in P} \lambda_{i,s} [\eta](v^{b(\sigma) + \sigma^{-i} s(\sigma)}) &= \sum_{s \in P} \lambda_{i,s} \left(\frac{1}{p^r} \sum_{a \in P} \xi_p^{[b(\sigma) + \sigma^{-i} s(\sigma), a(\sigma)]} z^{a(\sigma)} \right) \\
&= \frac{1}{p^r} \sum_{a} \xi_p^{[b(\sigma), a(\sigma)]} z^{a(\sigma)} \sum_{s} \lambda_{i,s} \xi_p^{[\sigma^{-i} s(\sigma), a(\sigma)]} \\
&= \frac{1}{p^r} \sum_{a} \xi_p^{[b(\sigma), a(\sigma)]} z^{a(\sigma)} \sum_{s} \lambda_{i,s} \xi_p^{[s(\sigma), \sigma^i a(\sigma)]}.
\end{aligned}$$

As this holds for all b, it follows that

$$\kappa_{i, \langle \sigma^i a\rangle} = \sum_{s} \lambda_{i,s} \xi_p^{[s(\sigma), \sigma^i a(\sigma)]}$$

for each a, so that

$$\kappa_{i,a} = \sum_s \lambda_{i,s} \xi_p^{[s(\sigma),a(\sigma)]},$$

from which we obtain the formula stated. □

The matrix $\lambda_{\mathfrak{p}}$ whose determinant occurs in the Fröhlich induction formula is the diagonal matrix over $O_{k,\mathfrak{p}}[V]$ whose diagonal entries are the Λ_i. Thus for $0 \leqslant j \leqslant d-1$ we have

$$\begin{aligned}
\psi_j(\det(\lambda_{\mathfrak{p}})) &= \psi^{\overline{c}^{(j)}(\sigma)} \left(\prod_{i=0}^{m-1} \Lambda_i \right) \\
&= \psi^{\overline{c}^{(j)}(\sigma)} \left(\prod_{i=0}^{m-1} \sum_{s \in P} \lambda_{i,s} v^{s(\sigma)} \right) \\
&= \prod_{i=0}^{m-1} \sum_{s \in P} \lambda_{i,s} \xi_p^{[s(\sigma),\overline{c}^{(j)}(\sigma)]} \\
&= \prod_{i=0}^{m-1} \sum_{s \in P} \xi_p^{[s(\sigma),\overline{c}^{(j)}(\sigma)]} \left(\frac{1}{p^r} \sum_a \kappa_{i,a} \xi_p^{[-s(\sigma),a(\sigma)]} \right) \\
&= \prod_{i=0}^{m-1} \kappa_{i,\overline{c}^{(j)}}.
\end{aligned}$$

From (56) we then have

$$\psi_j(\det(\lambda_{\mathfrak{p}})) = \left(\sum_i \left(\sigma^{-i} \overline{c}^{(j)}(\sigma) - \langle \sigma^{-i} \overline{c}^{(j)}(\sigma) \rangle \right) \right) \cdot z. \tag{57}$$

We evaluate this in two pieces. Firstly,

$$\sum_i \sigma^{-i} \overline{c}^{(j)}(\sigma) = \overline{c}^{(j)}(1) \sum_i \sigma^{-i},$$

so by Proposition 5.2.1

$$\left(\sum_i \sigma^{-i} \overline{c}^{(j)}(\sigma) \right) \cdot z = N_{E/k}(y)^{b_0 \overline{c}^{(j)}(1)}.$$

Secondly, we have $\overline{c}^{(j)}(\sigma) \hat{g}(\sigma) \in \hat{\mathcal{C}}^{(-j)}$ by Lemma 4.2.4. Thus we have

$$\Pi^{(-j)}(\sigma) = \sum_i \langle \sigma^{-i} \overline{c}^{(j)}(\sigma) \rangle = \sum_{a \in P^{(-j)}} a(\sigma),$$

where $\Pi^{(-j)}(X)$ and $P^{(-j)}$ are as in Definition 3.3.7. By Lemma 3.3.8 we then have

$$\Pi^{(-j)}(\sigma) = \sum_{v=0}^{r-1} w_{t(v)-j} \sigma^v = \sum_{v=0}^{r-1} p b_{t(v)-j} \sigma^v$$

for some integers $t(v)$. Hence

$$\left(\sum_i \langle \sigma^{-i}\overline{c}^{(j)}(\sigma)\rangle\right)\cdot z = \prod_{v=0}^{r-1}(\sigma^v\cdot z^p)^{b_{t(v)-j}} = \prod_{v=0}^{r-1}(\sigma^v\hat{g}(\sigma)\cdot y)^{b_{t(v)-j}}.$$

Thus (57) becomes

$$\psi_j(\det(\lambda_{\mathfrak{p}})) = N_{E/k}(y)^{\overline{c}^{(j)}(1)b_0}\prod_{v=0}^{r-1}(\sigma^v\hat{g}(\sigma)\cdot y)^{-b_{t(v)-j}}. \tag{58}$$

LEMMA 5.6.2. — *Let the local normal integral bases $\alpha_{\mathfrak{p}}$ for all $\mathfrak{p}\in S^p_{\text{nonsplit}}$ be chosen as in (53). Then there exist elements $U_\lambda\in E$ for $0\leqslant\lambda\leqslant d-1$, satisfying $U_\lambda\equiv 1 \pmod^*(\xi_p-1)^pO_E)$ such that*

$$h_{\mathcal{Y}}(\chi_j)_{\mathfrak{p}} = N_{E/k}(y)^{-\overline{c}^{(j)}(1)b_0}\prod_{\lambda=0}^{d-1}U_\lambda^{b_{\lambda-j}} \text{ for } 0\leqslant j\leqslant d-1.$$

Proof. — Define

$$U_\lambda = \prod_{t(v)=\lambda}(\sigma^v\hat{g}(\sigma)\cdot y)\in E,$$

where the product is over those $v\in\{0,\dots,r-1\}$ with $t(v)=\lambda$. Then $U_\lambda\equiv 1 \pmod^*(\xi_p-1)^pO_E)$ by the choice of y in Lemma 5.1.5. The formula for $h_{\mathcal{Y}}(\chi_j)_{\mathfrak{p}}$ then follows from (58) and the definition of $h_{\mathcal{Y}}$ in Lemma 5.4.1. □

COROLLARY 5.6.3. — $h_{\mathcal{Y}}(\chi_j)\in\mathbb{U}_p(k)$.

Proof. — Recall that $pO_k=(\xi_p-1)^{p-1}O_k$. We therefore have $N_{E/k}(y)\equiv 1 \pmod^* pO_k)$ by condition (ii) of Lemma 5.1.5. Thus, from Lemma 5.5.1 and Lemma 5.6.2 we have

$$h_{\mathcal{Y}}(\chi_j)_{\mathfrak{p}}\equiv 1 \pmod{pO_{k,\mathfrak{p}}}$$

for all places $\mathfrak{p}$ of k above p. Since by definition $h_{\mathcal{Y}}(\chi_j)_{\mathfrak{p}}=1$ at places not above p, the result follows. □

6. Conclusion of the proofs

In this section, we complete the proofs of Theorems 1–3 in reverse order.

6.1. Proof of Theorem 3

By Lemma 5.3.2 and Lemma 5.4.1, it suffices to show that $\mathcal{Y}$ is trivial. If $r = 1$ this is clear from Corollary 5.6.3 and Lemma 4.3.1. If all places of E above p split completely in N, then S^p_{nonsplit} is empty and the result follows from Lemma 5.5.1 together with Lemma 4.3.1.

6.2. Proof of Theorem 2

Let E be a tame C-extension of k. We first show the inclusion

$$\mathcal{R}(O_k[\Gamma], E) \subseteq (\iota_*^C(O_E)_{O_k[C]})(\iota_*^V \mathcal{N}_{E/k}(\mathcal{R}(O_E[V]))). \tag{59}$$

After Lemma 5.4.1, Lemma 5.3.3 and Proposition 5.3.4, this amounts to showing that the class $\mathcal{X}''\mathcal{Y}$, represented by $h_{\mathcal{X}''}h_{\mathcal{Y}}$, belongs to $\iota_*^V \mathcal{N}_{E/k}(\mathcal{R}(O_E[V]))$. Now $h_{\mathcal{X}''}h_{\mathcal{Y}}(\Phi_i) = 1$ for $1 \leqslant i \leqslant s$ and, by Lemma 5.5.1 and Lemma 5.6.2,

$$h_{\mathcal{X}''}h_{\mathcal{Y}}(\chi_j)_{\mathfrak{p}} \begin{cases} \equiv 1 \pmod{p^r O_{k,\mathfrak{p}}} & \text{if } \mathfrak{p} \in S^p_{\mathrm{split}}, \\ = \displaystyle\prod_{\lambda=0}^{d-1} U_\lambda^{b_{\lambda-j}} & \text{if } \mathfrak{p} \in S^p_{\mathrm{nonsplit}}, \\ = 1 & \text{otherwise,} \end{cases}$$

for $0 \leqslant j \leqslant d-1$. Here the $U_\lambda \in E$ are as in Lemma 5.6.2. Now if $\mathfrak{p} \in S^p_{\mathrm{nonsplit}}$ then $\mathfrak{p}$ splits completely in E/k. Thus for any place $\mathfrak{P}$ of E above $\mathfrak{p}$ we have $E_{\mathfrak{P}} = k_{\mathfrak{p}}$ and hence $U_\lambda \in k_{\mathfrak{p}} = N_{E_{\mathfrak{p}}/k_{\mathfrak{p}}}(E_{\mathfrak{p}})$. We can therefore define idèles $w_\lambda \in \mathbb{J}(k)$ by

$$w_{\lambda,\mathfrak{p}} = \begin{cases} U_\lambda & \text{if } \mathfrak{p} \in S^p_{\mathrm{nonsplit}}; \\ 1 & \text{otherwise,} \end{cases}$$

and we have $w_\lambda = N_{E/k}(\omega_\lambda)$ for some $\omega_\lambda \in \mathbb{J}(E)$. It then follows from Lemma 4.3.1 and Lemma 4.3.6 that $\mathcal{X}''\mathcal{Y} \in \iota_*^V \mathcal{N}_{E/k}(\mathcal{R}(O_E[V]))$. Thus (59) holds.

It remains to show that, given a finite set S_E of places of E and a class $\mathcal{Z} \in \iota_*^V \mathcal{N}_{E/k}(\mathcal{R}(O_E[V]))$, there exists a tame Γ-extension N of k relative to E with $(O_N)_{O_k[\Gamma]} = (\iota_*^C((O_E)_{O_k[C]}))\mathcal{Z}$ such that N satisfies the additional conditions in the statement of Theorem 2. This will show that there are infinitely many such N, since we may enlarge S_E to include the places of E ramified in N and then repeat the construction. We shall construct N so that the class $\mathcal{X}'$ in Lemma 5.3.3 coincides with $\mathcal{Z}$ and S^p_{nonsplit} is empty. The latter condition ensures that the class $\mathcal{X}''$ in Lemma 5.3.3 and (by Lemma 5.5.1 and Lemma 4.3.1) the class $\mathcal{Y}$ in Lemma 5.4.1 are both trivial, so that $(O_N)_{O_k[\Gamma]}$ will be as required.

By Lemma 4.3.6, $\mathcal{Z}$ is represented by some $h_{\mathcal{Z}} \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ with

$$h_{\mathcal{Z}}(\Phi_i) = 1 \text{ for } 1 \leqslant i \leqslant s,$$

$$h_{\mathcal{Z}}(\chi_j) = \prod_{\lambda=0}^{d-1} N_{E/k}(\omega_\lambda)^{b_{\lambda-j}} \text{ for } 0 \leqslant j \leqslant d-1,$$

where $\omega_0, \ldots, \omega_{d-1} \in \mathbb{J}(E)$. To construct N, we will find an element $y \in E$ so that yO_E has a factorisation as in Lemma 5.1.5(iv) in which $n = d+1$, and the classes of the $\mathfrak{Q}_i$ in $\mathrm{Cl}_{p^{2r+1}}(O_E)$, together with the exponents $e_i(\sigma)$, are as prescribed below. We stipulate in addition that the $\mathfrak{Q}_i$ must lie above distinct prime ideals $\mathfrak{q}_i$ of O_k, none of which lies above p or below a place in S_E, and that the $\mathfrak{Q}_i$ must split completely in E/k. This means in particular that $N_{E/k}(\mathfrak{Q}_i) = \mathfrak{q}_i$. Such a choice is possible by the Tchebotarev density theorem.

Let $\nu(\sigma)$, $\nu'(\sigma)$ be as in Lemma 3.3.9. Then there is some $\kappa \in \{0, \ldots, d-1\}$ such that $\nu(\sigma)\hat{g}(\sigma) = \nu'(\sigma)\hat{g}(\sigma) \in \hat{\mathcal{C}}^{(d-\kappa)}$. For $0 \leqslant j \leqslant d-1$ with $j \neq \kappa$, take $\mathfrak{Q}_{d-j}$ to have the class in $\mathrm{Cl}_{p^{2r+1}}(O_E)$ determined by ω_{d-j}, and set $e_{d-j}(\sigma) = \overline{c}^{(j)}(\sigma)$. Applying Lemma 3.3.9 to the $\mathbb{Z}[C]$-module $\mathrm{Cl}_{p^{2r+1}}(O_E)$, we can find classes A, B in $\mathrm{Cl}_{p^{2r+1}}(O_E)$ so that $A^{\nu(\sigma)}B^{\nu'(\sigma)}$ is the class of $\left(\prod_{j\neq\kappa} \mathfrak{Q}_{d-j}^{\overline{c}^{(j)}(\sigma)}\right)^{-1}$ (where the product is over $\{0, \ldots, d-1\}\backslash\{\kappa\}$), and AB^σ is the class determined by $\omega_{d-\kappa}$. Let $\mathfrak{Q}_{d-\kappa}$, $\mathfrak{Q}_{d+1}$ be prime ideals of E in the classes A, B respectively, and let $e_{d-\kappa}(\sigma) = \nu(\sigma)$, $e_{d+1}(\sigma) = \nu'(\sigma)$. By construction, we then have

$$\prod_{i=1}^{d+1} \mathfrak{Q}_i^{e_i(\sigma)} = yO_E$$

for some $y \in E$ with $y \equiv 1 \pmod^* p^{2r+1}O_E$. We then take N to be the field constructed from y in Lemma 5.1.5. The congruence on y ensures that each prime $\mathfrak{p}$ of E above p splits completely in each of the fields $E(\sqrt[p]{\sigma^j(y)})$ for $0 \leqslant j \leqslant d-1$ (see e.g. [16, Theorem 119]), and therefore splits completely in the compositum N of these fields. Thus S^p_{nonsplit} is indeed empty.

For $i \neq d-\kappa,\, d+1$ we have

$$e_i(\sigma)\hat{g}(\sigma) = \overline{c}^{(d-i)}(\sigma)\hat{g}(\sigma) \in \hat{\mathcal{C}}^{(i)}$$

by Lemma 4.2.4. For $i = d-\kappa$ we have

$$e_i(\sigma)\hat{g}(\sigma) = \nu(\sigma)\hat{g}(\sigma) \in \hat{\mathcal{C}}^{(d-\kappa)},$$

and similarly for $i = d+1$ we have $e_i(\sigma)\hat{g}(\sigma) \in \hat{\mathcal{C}}^{(d-\kappa)}$. Thus the sets $S_1, \ldots, S_d$ occurring in Lemma 5.3.3 are as follows:

$$S_t = \begin{cases} \{t\} & \text{if } t \neq d-\kappa; \\ \{d-\kappa, d+1\} & \text{if } t = d-\kappa. \end{cases}$$

From the definition of $h_{\mathcal{X}'}$ in Lemma 5.3.3, we then see that, for each j, the content of the idèle $h_{\mathcal{X}'}(\chi_j)$ is the O_k-ideal

$$\prod_{t=1}^{d} \prod_{\mathfrak{q}_i \in S_t} \mathfrak{q}_i^{b_{t-j}} = \left(\prod_{t \neq d-\kappa} \mathfrak{q}_t^{b_{t-j}} \right) (\mathfrak{q}_{d-\kappa}\mathfrak{q}_{d+1})^{b_{d-\kappa-j}}.$$

Now the ideal $\mathfrak{q}_{d-\kappa}\mathfrak{q}_{d+1} = N_{E/k}(\mathfrak{Q}_{d-\kappa}\mathfrak{Q}^{\sigma}_{d+1})$ lies in the class of $\mathrm{Cl}_{p^{2r+1}}(O_k)$ determined by $N_{E/k}(\omega_{d-\kappa})$, and for $t \neq d-\kappa$ the ideal $\mathfrak{q}_t$ lies in the class determined by $N_{E/k}(\omega_t)$. Thus $h_{\mathcal{X}'}(\chi_j)h_{\mathcal{Z}}(\chi_j)^{-1} \in k^{\times}\mathbb{U}_{p^r}(O_k)$. By Lemma 4.3.1, we then have $\mathcal{X}' = \mathcal{Z}$ as required.

The places of E ramified in N are precisely the conjugates of the $\mathfrak{Q}_i$. The choice of the $\mathfrak{Q}_i$ ensures that none of these belongs to S_E. Moreover, for each i, we have $e_i(\sigma)\hat{g}(\sigma) \neq 0$ in $\mathbb{F}_p[C]$, so that at least one of the conjugates over k of $\mathfrak{Q}_i$ ramifies in the extension $L = E(\sqrt[p]{\hat{g}(\sigma)\cdot y})$ of E. Any field F with $E \subsetneq F \subseteq N$ contains some conjugate of L, and is therefore ramified in at least one place of E above $\mathfrak{q}_i$. Hence we have constructed a Γ-extension N relative to E with all the properties stated.

6.3. Proof of Theorem 1

The second equality follows from Lemma 4.3.6. Clearly

$$\mathcal{R}(O_k[\Gamma]) = \bigcup_E \mathcal{R}(O_k[\Gamma], E),$$

where the union is over all tame C-extensions E of k. Theorem 2 and Lemma 4.3.6 then give one inclusion of the first equality of Theorem 1:

$$\begin{aligned}\mathcal{R}(O_k[\Gamma]) &= \bigcup_E (\iota_*^C(O_E)_{O_k[C]})(\iota_*^V \mathcal{N}_{E/k}(\mathcal{R}(O_E[V]))) \\ &\subseteq (\iota_*^C \mathcal{R}(O_k[C]))\,(\iota_*^V \mathcal{R}(O_k[V])).\end{aligned}$$

We now show the reverse inclusion. For each class $\mathcal{B} \in \mathcal{R}(O_k[C])$, it follows from [19, Theorem (6.17)], that there is a tame C-extension E of k, unramified at any given finite set S of places of k and above p, and with the property that no intermediate field of E/k (except k itself) is unramified. Then $\mathcal{N}_{E/k}(\mathcal{R}(O_E[V]))) = \mathcal{R}(O_k[V])$ by Lemma 4.3.6, and it follows from Theorem 2 that $\iota_*^C(\mathcal{B})\,(\iota_*^V \mathcal{R}(O_k[V])) \subseteq \mathcal{R}(O_k[\Gamma])$. Moreover, each class in this subset is realized by infinitely many Γ-extensions N relative to E with the following properties: N/E is unramified at all places of E above those in S and those ramified in E/k, but every intermediate extension of N/E (except E itself) is ramified at some finite place. It then follows that N/k is unramified at all places in S, but every intermediate extension $F \neq k$ of N/k is ramified at some finite place. To see the last condition, suppose that F/k is unramified. Then $F \cap E = k$ by the choice of E. The extension FE/E is unramified because E/k and F/k are arithmetically disjoint. Therefore $FE = E$ by the choice of N, whence $F = k$. This completes the proof of Theorem 1.

7. Consequences and special cases

7.1. Realizable classes over the maximal order

For any finite group G, let $\mathcal{M}_G$ denote a maximal order in $k[G]$ containing $O_k[G]$. Then the classgroup $\mathrm{Cl}(\mathcal{M}_G)$ of locally free $\mathcal{M}_G$-modules admits a Hom-Description analogous to (2):

$$\mathrm{Cl}(\mathcal{M}_G) \cong \frac{\mathrm{Hom}_{\Omega_K}(R_G, \mathbb{J}(k^c))}{\mathrm{Hom}_{\Omega_K}(R_G, k^{c\times})\mathrm{Det}(\mathbb{U}(\mathcal{M}_G))}. \tag{60}$$

This is independent of the choice of maximal order $\mathcal{M}_G$. Since $\mathrm{Det}(\mathbb{U}(O_k[G])) \subseteq \mathrm{Det}(\mathbb{U}(\mathcal{M}_G))$, there is a natural surjection

$$\mathrm{Ex}\colon \mathrm{Cl}(O_k[G]) \twoheadrightarrow \mathrm{Cl}(\mathcal{M}_G).$$

This corresponds to extension of scalars:

$$\mathrm{Ex}((M)_{O_k[G]}) = (\mathcal{M}_G \otimes_{O_k[G]} M)_{\mathcal{M}_G}$$

for a locally free $O_k[G]$-module M. Also, each group homomorphism $\alpha\colon G \to H$ induces a homomorphism $\alpha_*\colon \mathrm{Cl}(\mathcal{M}_G) \longrightarrow \mathrm{Cl}(\mathcal{M}_H)$. Explicitly, if $h \in \mathrm{Hom}_{\Omega_K}(R_G, \mathbb{J}(k^c))$ represents a class $A \in \mathrm{Cl}(\mathcal{M}_G)$, then the class $\alpha_*(A) \in \mathrm{Cl}(\mathcal{M}_H)$ is represented by the character homomorphism taking each character χ of H to $h(\chi \circ \alpha)$. Thus the diagram

$$\begin{array}{ccc} \mathrm{Cl}(O_k[G]) & \longrightarrow & \mathrm{Cl}(O_k[H]) \\ \downarrow & & \downarrow \\ \mathrm{Cl}(\mathcal{M}_G) & \longrightarrow & \mathrm{Cl}(\mathcal{M}_H) \end{array}$$

commutes. We write $\mathcal{R}(\mathcal{M}_G)$ for the image in $\mathrm{Cl}(\mathcal{M}_G)$ of the realizable classes $\mathcal{R}(O_k[G])$.

Taking $G = \Gamma$, and writing $\mathcal{R}(\mathcal{M}_\Gamma, E)$ for the image in $\mathrm{Cl}(\mathcal{M}_\Gamma)$ of $\mathcal{R}(O_k[\Gamma], E)$, we can now read off from Theorems 1 and 2 analogous results over $\mathcal{M}_\Gamma$.

THEOREM 7.1.1. — *Under the hypotheses of Theorem 1, $\mathcal{R}(\mathcal{M}_\Gamma)$ is the following subgroup of $\mathrm{Cl}(\mathcal{M}_\Gamma)$:*

$$\mathcal{R}(\mathcal{M}_\Gamma) = (\iota_*^C \mathcal{R}(\mathcal{M}_C))\,(\iota_*^V \mathcal{R}(\mathcal{M}_V)) = (\iota_*^C \mathcal{R}(\mathcal{M}_C))(\mathcal{J} \cdot \ker(\pi_*)),$$

where π_* now denotes the natural map $\mathrm{Cl}(\mathcal{M}_\Gamma) \longrightarrow \mathrm{Cl}(\mathcal{M}_C)$.

Moreover, given any finite set S of places of k and any class $\mathcal{A} \in \mathcal{R}(\mathcal{M}_\Gamma)$, there are infinitely many tame Γ-extensions N of k with $(O_N)_{\mathcal{M}_\Gamma} = \mathcal{A}$, and N can be chosen to satisfy the following properties: N/k is unramified at all places in S, and every intermediate field $F \neq k$ of N/k is ramified at some finite place of k.

THEOREM 7.1.2. — *Under the hypotheses of Theorem 1, for each tame C-extension E of k we have*

$$\mathcal{R}(\mathcal{M}_\Gamma, E) = (\iota_*^C (O_E)_{\mathcal{M}_C})(\iota_*^V \mathcal{N}_{E/k}(\mathcal{R}(\mathcal{M}_V))).$$

Moreover, given any finite set S_E of places of E and any class $\mathcal{A} \in \mathcal{R}(\mathcal{M}_\Gamma, E)$, there are infinitely many tame Γ-extensions N of k relative to E with $(O_N)_{\mathcal{M}_\Gamma} = \mathcal{A}$, and N can be chosen to satisfy the following properties: N/E is unramified at all places in S_E, and every intermediate field $F \neq E$ of N/E is ramified at some finite place of E.

Over a maximal order, we have a more satisfactory version of Theorem 3:

THEOREM 7.1.3. — *Let N be any tame Γ-extension of k relative to E. Then the class $(O_N)_{\mathcal{M}_\Gamma}$ in $\mathrm{Cl}(\mathcal{M}_\Gamma)$ factorizes as*

$$(O_N)_{\mathcal{M}_\Gamma} = (\iota_*^C(O_E)_{\mathcal{M}_C})\mathcal{X}$$

where the class $\mathcal{X} \in \mathrm{Cl}(\mathcal{M}_\Gamma)$ satisfies $\mathbf{i}_{E/k}(\mathcal{X}) = \iota_*^V((O_N)_{\mathcal{M}(E)_V})$ in $\mathrm{Cl}(\mathcal{M}(E)_\Gamma)$, where $\mathcal{M}(E)_V$ (respectively $\mathcal{M}(E)_\Gamma$) denotes a maximal order in $E[V]$ (respectively $E[\Gamma]$) containing $O_E[V]$ (respectively $O_E[\Gamma]$).

Proof. — From the proof of Theorem 3 (§6.1), it suffices to show that the class in $\mathrm{Cl}(\mathcal{M}_\Gamma)$ represented by $h_{\mathcal{Y}}$ in Lemma 5.4.1 is trivial in all cases. But this is clear since

$$h_{\mathcal{Y}} \in \mathrm{Hom}_{\Omega_K}(R_\Gamma, \mathbb{U}(k^c)),$$

and $\mathrm{Hom}_{\Omega_K}(R_\Gamma, \mathbb{U}(k^c)) = \mathrm{Det}(\mathbb{U}(\mathcal{M}_\Gamma))$ by [13, p. 23], since Γ has no irreducible symplectic characters by Lemma 4.2.2. □

7.2. Steinitz classes

Let $\iota\colon H \longrightarrow G$ be the inclusion of a subgroup H into a finite group G, and let K be any number field. In addition to the homomorphism $\iota_*\colon \mathrm{Cl}(O_K[H]) \longrightarrow \mathrm{Cl}(O_K[G])$ mentioned in the Introduction, there is a homomorphism $\iota^*\colon \mathrm{Cl}(O_K[G]) \longrightarrow \mathrm{Cl}(O_K[H])$ taking the class $(X)_{O_K[G]}$ of a locally free $O_K[G]$-module X to its class $(X)_{O_K[H]}$ when considered as a locally free $O_K[H]$-module. If $h \in \mathrm{Hom}_{\Omega_K}(R_G, \mathbb{J}(K^c))$ represents $(X)_{O_K[G]}$ in the Hom-Description, then the function $\chi \mapsto h(\mathrm{Ind}_H^G\chi)$ on R_H represents $(X)_{O_K[H]}$ (see [13, p. 62]). In particular, if $H = \{1\}$ is the trivial subgroup of G, then $\iota^*((X)_{O_K[G]}) \in \mathrm{Cl}(O_K[H]) = \mathrm{Cl}(O_K)$ is the Steinitz class $\mathrm{cl}(X)$ of the locally free O_K-module X. In this case, R_H is generated by the trivial character 1_H, and we may identify a homomorphism $f \in \mathrm{Hom}_{\Omega_K}(R_H, \mathbb{J}(K^c))$ with its value $f(1_H) \in \mathbb{J}(K)$ at 1_H. Since $\mathrm{Ind}_H^G 1_H = r_G$, the regular representation of G, it follows that $\mathrm{cl}(X)$ is the class in $\mathrm{Cl}(O_K)$ of the content of the idèle $h(r_G)$, where $h \in \mathrm{Hom}_{\Omega_K}(R_G, \mathbb{J}(K^c))$ represents $(X)_{O_K[G]}$. In the special case that $X = O_F$ is the ring of integers of a tame G-extension of K, the class $\mathrm{cl}(X)$ is the Steinitz class of the extension F/K.

We now apply this to determine the Steinitz classes realized by the tame Γ-extensions N of k in Theorem 1. By Lemma 4.2.1, we have

$$r_\Gamma = \sum_{i=0}^{m-1} \phi_i + m \sum_{j=0}^{d-1} \chi_j. \tag{61}$$

Following [1, 4], we denote by Σ the exact sequence of groups

$$\Sigma : \qquad \{1\} \longrightarrow V \longrightarrow \Gamma \longrightarrow C \longrightarrow \{1\}.$$

For a given tame C-extension E of k, we write $\mathcal{R}_t(E/k, \Sigma)$ (where the t stands for "tame") to denote the set of classes $c \in \mathrm{Cl}(O_k)$ for which there exists a tame Γ-extension N of k containing E, such that $\mathrm{cl}(O_N) = c$, and such that the isomorphism $\pi\colon \mathrm{Gal}(N/k) \longrightarrow \Gamma$ induces the given isomorphism $\mathrm{Gal}(E/k) \longrightarrow C$. We also write $\mathcal{R}_t(k, \Gamma)$ for the set of all classes $\mathrm{cl}(O_N)$ as N runs through tame Γ-extensions of k.

To determine $\mathcal{R}_t(E/k, \Sigma)$ and $\mathcal{R}_t(k, \Gamma)$ from Theorem 1, we require two preliminary results. Let $\alpha\colon \{1\} \longrightarrow \Gamma$ be the inclusion of the trivial subgroup in Γ.

Lemma 7.2.1. — *For any tame C-extension E of k we have*

$$\alpha^*(\iota_*^C(O_E)_{O_k[C]}) = \mathrm{cl}(O_E)^{p^r}.$$

Proof. — Let the class $(O_E)_{O_k[C]} \in \mathrm{Cl}(O_k[C])$ be represented by $h' \in \mathrm{Hom}_{\Omega_k}(R_C, \mathbb{J}(k^c))$ as in Lemma 4.3.2, and let $x_i = h'(\overline{\Phi}_i)$ for $1 \leqslant i \leqslant s$. Applying the discussion above to the extension E/k, we find that $\mathrm{cl}(O_E)$ is represented by $h'(r_C)$ with

$$h'(r_C) = \prod_{i=1}^{s} N_{k_i/k}(x_i),$$

Lemma 4.3.2 also tells us that $\iota_*^C(O_E)_{O_k[C]}$ is represented by $h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$, where $h(\phi_i) = h'(\phi_i)$ for all i and $h(\chi_j) = h'(r_C)$ for each j. Using (61), it follows that $\alpha^*(\iota_*^C(O_E)_{O_k[C]})$ is represented by

$$h(r_\Gamma) = \left(\prod_{i=0}^{m-1} h'(\phi_i)\right)\left(h'(r_C)\right)^d\Big)^m = h'(r_C)^{1+dm} = h'(r_C)^{p^r},$$

as required. □

Lemma 7.2.2. — *Let F be any finite extension of k. Then*

$$\alpha^*(\iota_*^V \mathcal{N}_{F/k}(\mathcal{R}(O_F[V]))) = N_{F/k}(\mathrm{Cl}(O_F))^{\frac{1}{2}mp^{r-1}(p-1)}.$$

Proof. — By Lemma 4.3.6, $\iota_*^V \mathcal{N}_{F/k}(\mathcal{R}(O_F[V]))$ consists of the classes in $\mathrm{Cl}(O_k[\Gamma])$ represented by character homomorphisms h with $h(\phi_i) = 1$ and $h(\chi_j) = \prod_{l=0}^{d-1} z_l^{b_{l-j}}$, where the z_i are arbitrary elements of $N_{F/k}(\mathbb{J}(F))$. But if $A \in \mathrm{Cl}(O_k[\Gamma])$ is the class represented by h, then, by (61), $\alpha^*(A)$ is

represented by

$$h(r_\Gamma) = \prod_{i=0}^{m-1} h(\phi_i) \prod_{j=0}^{d-1} \left(\prod_{l=0}^{d-1} z_l^{b_{l-j}} \right)^m$$
$$= \left(\prod_{l=0}^{d-1} \left(\prod_{t=0}^{d-1} z_l^{b_t} \right) \right)^m$$
$$= \left(\prod_{l=0}^{d-1} z_l \right)^{mb},$$

where $b = \sum_{t=0}^{d-1} b_t$. It follows that $\alpha^*(\iota_*^V \mathcal{N}_{F/k}(\mathcal{R}(O_F[V])))$ is the subset of $\mathrm{Cl}(O_k)$ represented by idèles belonging to $N_{F/k}(\mathrm{Cl}(O_F))^{mb}$, so that

$$\alpha^*(\iota_*^V \mathcal{N}_{F/k}(\mathcal{R}(O_F[V]))) = N_{F/k}(\mathrm{Cl}(O_F))^{mb}.$$

But, by Definitions 3.4.2 and 3.3.2 and Lemma 3.3.3, we have

$$pb = \sum_{j=0}^{d-1} w_j = g_0(1) = \hat{g}_0(1),$$

and we know from [1, Proposition 2.6] that $\hat{g}_0$ has integral weight $\hat{g}_0(1) = p^r(p-1)/2$. Hence $b = p^{r-1}(p-1)/2$, and the result follows. □

THEOREM 7.2.3. — *Let Γ and k be as in Theorem 1. Then*

(i) $\mathcal{R}_t(k,\Gamma) = \mathcal{R}_t(k,C)^{p^r}\mathrm{Cl}(O_k)^{\frac{1}{2}mp^{r-1}(p-1)}$. *In particular, $\mathcal{R}_t(k,\Gamma)$ is a subgroup of $\mathrm{Cl}(O_k)$.*

(ii) *for each tame C-extension E of k we have*

$$\mathcal{R}_t(E/k,\Sigma) = \mathrm{cl}(O_E)^{p^r} N_{E/k}(\mathrm{Cl}(O_E))^{\frac{1}{2}mp^{r-1}(p-1)}.$$

Proof. — The two equalities follow from Theorems 1 and 2, together with Lemmas 7.2.1 and 7.2.2. To see that $\mathcal{R}_t(k,\Gamma)$ is a subgroup of $\mathrm{Cl}(O_k)$, it suffices to observe that $\mathcal{R}_t(k,C)$ is a subgroup of $\mathrm{Cl}(O_k)$ since it is the image of $\mathcal{R}(O_k[C])$ under the homomorphism $\mathrm{Cl}(O_k[C]) \longrightarrow \mathrm{Cl}(O_k)$ induced by $\{1\} \longrightarrow C$, and $\mathcal{R}(O_k[C])$ is a subgroup of $\mathrm{Cl}(O_k[C])$ by [19, (6.20)]. □

In the case $m = p^r - 1$, Γ is the group considered in [4] for $p = 2$ (respectively [1] for $p > 2$), and Theorem 7.2.3 reduces to [1, Theorem 1.3] (respectively [4, Théorème 1.4]), except that the description of $\mathcal{R}_t(E/k,\Sigma)$ for $p > 2$ in [1] is obtained under the slightly weaker hypothesis $\xi_p \in E$ (rather than $\xi_p \in k$). As noted in [4, Théorème 1.4], the group $\mathcal{R}_t(k,C)$ when C is cyclic of odd order has a more explicit description due to Endo [10].

7.3. Reformulation in terms of ideal classes

In this final subsection, we restate Thereoms 1 and 2 in more concrete terms in order to deduce the Galois module class results in [1] and [4].

Recall from Lemma 4.3.1 that we have a surjection

$$\prod_{i=1}^{s} \mathrm{Cl}_{mp^r}(k_i) \times \prod_{j=0}^{d-1} \mathrm{Cl}_{p^r}(k) \twoheadrightarrow \mathrm{Cl}(O_k[\Gamma]). \tag{62}$$

Explicitly, the class in $\mathrm{Cl}(O_k[\Gamma])$ represented by $h \in \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{J}(k^c))$ is the image of the $(s+d)$-tuple $([h(\Phi_1)], \ldots, [h(\Phi_s)], [h(\chi_0)], \ldots, [h(\chi_{d-1})])$, where for an idèle x we write $[x]$ for the class of the content of x in the appropriate ray classgroup.

We have a similar description of $\mathrm{Cl}(\mathcal{M}_\Gamma)$, where $\mathcal{M}_\Gamma \supset O_k[\Gamma]$ is a maximal order in $k[\Gamma]$. As above, we have $\mathrm{Det}(\mathbb{U}(\mathcal{M}_\Gamma)) = \mathrm{Hom}_{\Omega_k}(R_\Gamma, \mathbb{U}(k^c))$. Arguing as in Lemma 4.3.1, we therefore obtain an *isomorphism*

$$\prod_{i=1}^{s} \mathrm{Cl}(k_i) \times \prod_{j=0}^{d-1} \mathrm{Cl}(k) \cong \mathrm{Cl}(\mathcal{M}_\Gamma). \tag{63}$$

Analogous statements hold for $\mathrm{Cl}(O_k[C])$ and $\mathrm{Cl}(\mathcal{M}_C)$, with the factors for $0 \leqslant j \leqslant d-1$ omitted.

Using Lemmas 4.3.2 and 4.3.6, we can therefore restate Theorems 1 and 2 as follows:

THEOREM 7.3.1. — *Let Γ and k be as in Theorem 1. Then*

(i) *$\mathcal{R}(O_k[\Gamma])$ (respectively $\mathcal{R}(\mathcal{M}_\Gamma)$) is represented under (62) (respectively (63)) by all $(s+d)$-tuples of the form*

$$(x_1, \ldots, x_s, x'y_0, \ldots, x'y_{d-1}),$$

where $(x_1, \ldots, x_s)$ represents a class in $\mathcal{R}(O_k[C])$ (respectively $\mathcal{R}(\mathcal{M}_C)$),

$$x' = \prod_{i=1}^{s} N_{k_i/k}(x_i),$$

and the y_j are given by

$$y_j = \prod_{\lambda=0}^{d-1} z_\lambda^{b_{\lambda-j}}$$

for some $z_0, \dots z_{d-1} \in \mathrm{Cl}_{p^r}(O_k)$ *(respectively* $\mathrm{Cl}(O_k)$*), the integers* $b_0, \dots, b_{d-1}$ *being those associated to the code attached to* Γ *as in Definition 3.4.2.*

(ii) *for each tame* C*-extension* E *of* k*, the group* $\mathcal{R}(O_k[\Gamma], E)$ *(respectively* $\mathcal{R}(\mathcal{M}_\Gamma, E)$*) is represented by all* $(s+d)$*-tuples as in (i), where also* $(x_1, \dots, x_s)$ *represents* $(O_E)_{O_k[C]}$ *(respectively* $(O_E)_{\mathcal{M}_C}$*) and the* z_j *lie in* $N_{E/k}(\mathrm{Cl}_{p^r}(O_k))$ *(respectively* $N_{E/k}(\mathrm{Cl}(O_k))$*).*

In the case $m = p^r - 1$ (so $d = 1$), we have $b_0 = \hat{g}(1)/p = p^{r-1}(p-1)/2$ (see Remark 3.3.4). Thus Theorem 7.3.1(i) simplifies to give the following result:

COROLLARY 7.3.2. — *Let* Γ *and* k *be as in Theorem 1, with* $m = p^r - 1$*. Then* $\mathcal{R}(O_k[\Gamma])$ *(respectively* $\mathcal{R}(\mathcal{M}_\Gamma)$*) is represented under (62) (respectively (63)) by all* $(s+1)$*-tuples of the form*

$$(x_1, \dots, x_s, x' z^{p^{r-1}(p-1)/2})$$

where $(x_1, \dots, x_s)$ *represents a class in* $\mathcal{R}(O_k[C])$ *(respectively* $\mathcal{R}(\mathcal{M}_C)$*),* x' *is as in Theorem 7.3.1, and* $z \in \mathrm{Cl}_{p^r}(O_k)$ *(respectively* $\mathrm{Cl}(O_k)$*).*

This description of $\mathcal{R}(\mathcal{M}_\Gamma)$ is precisely that given in [1, Theorem 1.1] (for $p > 2$) and [4, Théorème 1.1] (for $p = 2$), so we have shown how these results over the maximal order $\mathcal{M}_\Gamma$ lift to the group ring $O_k[\Gamma]$.

In particular, if $p = r = 2$ and $m = p^r - 1 = 3$, then Γ is the alternating group A_4 of degree 4. In this case C is cyclic of order 3, and $\mathcal{R}(O_k[C_3])$ is precisely the kernel $\mathrm{Cl}^0(O_k[C])$ of the homomorphism $\mathrm{Cl}(O_k[C]) \longrightarrow \mathrm{Cl}(O_k)$ induced by the augmentation. It follows that $\mathcal{R}(O_k[A_4])$ is the augmentation kernel $\mathrm{Cl}^0(O_k[A_4])$ for any number field k. This is precisely the main result of [6].

Acknowledgements. The authors thank the anonymous referee for his/her careful reading of the paper and numerous detailed comments.

N. Byott thanks the Mathematics Department at Valenciennes for its hospitality during several visits as invited professor.

B. Sodaïgui is very grateful to the CNRS which has granted him a delegation for the full academic year 2010-2011, and Max Planck Institute for Mathematics in Bonn for its generous hospitality during the two months October and November 2010.

BIBLIOGRAPHY

[1] C. Bruche & B. Sodaïgui, "On realizable Galois module classes and Steinitz classes of nonabelian extensions", *J. Number Theory* **128** (2008), p. 954-978.

[2] N. Byott, "Hopf orders and a generalization of a theorem of L.R. McCulloh", *J. Algebra* **177** (1995), p. 409-433.

[3] ———, "Tame realisable classes over Hopf orders", *J. Algebra* **201** (1998), p. 284-316.

[4] N. Byott, C. Greither & B. Sodaïgui, "Classes réalisables d'extensions non abéliennes", *J. reine angew. Math.* **601** (2006), p. 1-27.

[5] N. Byott & B. Sodaïgui, "Galois module structure for dihedral extensions of degree 8: realizable classes over the group ring", *J. Number Theory* **112** (2005), p. 1-19.

[6] ———, "Realizable Galois module classes for tetrahedal extensions", *Compositio Math.* **141** (2005), p. 573-282.

[7] J. Carter & B. Sodaïgui, "Classes de Steinitz d'extensions quaterniennes généralisées de degré $4p^r$", *J. London Math. Soc.* **76** (2007), p. 331-344.

[8] A. Cobbe, "Steinitz classes of tamely ramified Galois extensions of number fields", *J. Number Theory* **130** (2010), p. 1129-1154.

[9] C. W. Curtis & I. Reiner, *Methods of Representation Theory, Volume II*, Wiley, New York, 1994.

[10] L. P. Endo, "Steinitz Classes of Tamely Ramified Galois Extensions of Algebraic Number Fields", unpublished doctoral thesis, University of Illinois at Urbana-Champaign, 1975.

[11] A. Fröhlich, "Arithmetic and Galois module structure for tame extensions", *J. reine angew. Math.* **286/287** (1976), p. 380-440.

[12] ———, "Galois module structure", in *A. Fröhlich (ed.) "Algebraic Number Fields (L-functions and Galois properties)"*, Academic Press, London, 1977, p. 133-191.

[13] ———, *Galois Module Structure of Algebraic Integers*, Springer, Berlin, 1983.

[14] A. Fröhlich & M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1991.

[15] M. Godin & B. Sodaïgui, "Realizable classes of tetrahedral extensions", *J. Number Theory* **98** (2003), p. 320-328.

[16] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Graduate Texts in Math., vol. 77, Springer, New York, 1981.

[17] L. R. McCulloh, "A Stickelberger condition on Galois module structure for Kummer extensions of prime degree", in *A. Fröhlich (ed.), "Algebraic Number Fields (L-functions and Galois properties)"*, Academic Press, 1977.

[18] ———, "Galois module structure of elementary abelian extensions", *J. Algebra* **82** (1983), p. 102-134.

[19] ———, "Galois module structure of abelian extensions", *J. reine angew. Math.* **375/376** (1987), p. 259-306.

[20] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

[21] S. Roman, *Coding and Information Theory*, Graduate Texts in Mathematics, vol. 134, Springer, New York, 1992.

[22] F. Sbeity & B. Sodaïgui, "Classes réalisables d'extesnions métacycliques de degré lm", *J. Number Theory* **130** (2010), p. 1818-1834.

[23] B. Sodaïgui, "Classes réalisables par des extensions métacycliques non abéliennes et éléments de Stickelberger", *J. Number Theory* **65** (1997), p. 87-95.

[24] ———, ""Galois Module Structure" des extensions quaternioniennes de degré 8", *J. Algebra* **213** (1999), p. 549-556.

[25] ———, "Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8", *J. Algebra* **223** (2000), p. 367-378.

[26] ———, "Relative Galois module structure of octahedral extensions", *J. Algebra* **312** (2007), p. 590-601.

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

[28] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math., vol. 83, Springer, New York, 1996.

Manuscrit reçu le 3 juin 2011,
accepté le 15 mars 2012.

Nigel P. BYOTT
College of Engineering,
Mathematics and Physical Sciences,
University of Exeter,
Exeter, EX4 4QF,
UK
N.P.Byott@ex.ac.uk

Bouchaïb SODAÏGUI
Département de Mathématiques,
Université de Valenciennes,
Le Mont Houy,
59313 Valenciennes Cedex 9,
France
bouchaib.sodaigui@univ-valenciennes.fr