GALOIS MODULE STRUCTURE OF THE SQUARE ROOT OF THE INVERSE DIFFERENT IN EVEN DEGREE TAME EXTENSIONS OF NUMBER FIELDS

LUCA CAPUTO AND STÉPHANE VINATIER

Abstract. Let $G$ be a finite group and let $N/E$ be a tamely ramified $G$-Galois extension of number fields whose inverse different $\mathcal{C}_{N/E}$ is a square. Let $\mathcal{A}_{N/E}$ denote the square root of $\mathcal{C}_{N/E}$. Then $\mathcal{A}_{N/E}$ is a locally free $\mathbb{Z}[G]$-module, which is in fact free provided $N/E$ has odd order, as shown by Erez. Using M. Taylor’s theorem, we can rephrase this result by saying that, when $N/E$ has odd degree, the classes of $\mathcal{A}_{N/E}$ and $\mathcal{O}_N$ (the ring of integers of $N$) in $\text{Cl}(\mathbb{Z}[G])$ are equal (and in fact both trivial). We show that the above equality of classes still holds when $N/E$ has even order, assuming that $N/E$ is locally abelian. This result is obtained through the study of the Fröhlich representatives of the classes of some torsion modules, which are independently introduced in the setting of cyclotomic number fields. Jacobi sums, together with the Hasse-Davenport formula, are involved in this study. Finally, when $G$ is the binary tetrahedral group, we use our result in conjunction with Taylor’s theorem to exhibit a tame $G$-Galois extension whose square root of the inverse different has nontrivial class in $\text{Cl}(\mathbb{Z}[G])$.

1. Introduction

Let $G$ be a finite group and let $N/E$ be a Galois extension of number fields with Galois group $G$. Let $\mathcal{O}_N$ and $\mathcal{O}_E$ denote the rings of integers of $N$ and $E$, respectively; then $\mathcal{O}_N$ is an $\mathcal{O}_E[G]$-module, and in particular a $\mathbb{Z}[G]$-module, whose structure has long been studied. In the case where $N/E$ is a tame extension, $\mathcal{O}_N$ is known to be locally free by Noether’s theorem and the investigation of its Galois module structure culminated with M. Taylor’s theorem [31] expressing the class $(\mathcal{O}_N)$ defined by $\mathcal{O}_N$ in the class group of locally free $\mathbb{Z}[G]$-modules $\text{Cl}(\mathbb{Z}[G])$ in terms of Artin root numbers (see Theorem 5.1).

Other $\mathcal{O}_E[G]$-modules which appear naturally in our context have also been studied, among which the inverse different $\mathcal{C}_{N/E}$ of the extension and, when it exists, its square root $\mathcal{A}_{N/E}$. The existence of $\mathcal{A}_{N/E}$ is of course equivalent to $\mathcal{C}_{N/E}$ being a square, a condition which can be tested using Hilbert’s valuation formula [25, IV, Proposition 4]. In particular, when $N/E$ is tame, $\mathcal{A}_{N/E}$ exists if and only if the inertia group of every prime of $\mathcal{O}_E$ in $N/E$ has odd order (which is the case for example if the degree $[N : E]$ is odd). In the tame case, both these modules are locally free $\mathbb{Z}[G]$-modules by a result of S. Ullom in [33] (applying to any $G$-stable fractional ideal of $N$).


Key words and phrases. Tamely ramified extensions, square root of the inverse different, Fröhlich Group Determinants, Stickelberger theorem, Hasse-Davenport theorem, root numbers, binary tetrahedral Galois extension.
The modules $\mathcal{O}_N$ and $\mathcal{C}_{N/E}$ are related by duality. For a fractional ideal $I$ of $\mathcal{O}_N$, the dual of $I$ with respect to the trace $\text{Tr}_{N/E}$ from $N$ to $E$ is the fractional ideal

$$I^\# = \{ x \in N \mid \text{Tr}_{N/E}(xI) \subseteq \mathcal{O}_E \}.$$ 

Then $I^\#$ is $G$-isomorphic to the $\mathcal{O}_E$-dual of $I$, namely $I^\# \cong \text{Hom}_{\mathcal{O}_E}(I, \mathcal{O}_E)$, and by definition one has $\mathcal{C}_{N/E} = \mathcal{O}_N^\#$, namely $\mathcal{O}_N$ and $\mathcal{C}_{N/E}$ are dual of each other. It can be shown that, for any fractional ideal $I$ of $\mathcal{O}_N$, one has $I^\# = \mathcal{C}_{N/E}I^{-1}$, which implies that $\mathcal{A}_{N/E}$, when it exists, is the only self-dual fractional ideal of $\mathcal{O}_E$.

The duality relation between $\mathcal{C}_{N/E}$ and $\mathcal{O}_N$ accounts for comparing their $\mathbb{Z}[G]$-module structures. In the tame case, this essentially amounts to comparing their classes $\mathcal{C}_{N/E}$ and $\mathcal{O}_N$ in $\text{Cl}(\mathbb{Z}[G])$, and A. Fröhlich conjectured that $\mathcal{O}_N$ is stably self-dual, namely that

$$\mathcal{O}_N = \mathcal{C}_{N/E}.$$ 

This equality was later proved by Taylor [30] under slightly stronger hypotheses and by S. Chase [7] in full generality. Taylor’s proof uses Fröhlich’s Hom-description of $\text{Cl}(\mathbb{Z}[G])$, while Chase examines the torsion module

$$\mathcal{T}_{N/E} = \mathcal{C}_{N/E}/\mathcal{O}_N.$$ 

It is worth noting that both proofs make crucial use of the stable freeness of the Swan modules of cyclic groups, a result due to R. Swan [28]. At the same time, Equality (1) has also been considered in the wildly ramified case by Cassou-Noguès and Queyrut who proved that an analogous statement holds in the Grothendieck group of $\mathbb{Z}[G]$-locally free modules outside a set of places [6, Corollaire 6.3].

The study of the Galois module structure of $\mathcal{A}_{N/E}$ was initiated by B. Erez, who proved in particular that, when $N/E$ is tamely ramified and of odd degree, the class $\mathcal{A}_{N/E}$ defined in $\text{Cl}(\mathbb{Z}[G])$ is trivial, see [16]. His proof follows the same strategy as that of Taylor in [31], using in particular Fröhlich’s Hom-description of $\text{Cl}(\mathbb{Z}[G])$. Since Taylor’s theorem implies the triviality of $\mathcal{O}_N$ when $N/E$ is of odd degree, we get:

$$\text{if } [N : E] \text{ is odd, then } (\mathcal{O}_N) = (\mathcal{A}_{N/E})$$

and both classes are in fact trivial. Note incidentally that it seems unlikely that Erez’s techniques can be easily generalized to the even degree case. This is mainly because the second Adams operation, which lies at the core of Erez’s proof, does not behave well with respect to induction for groups of even order.

In fact, it is interesting to observe that so far the class of $\mathcal{A}_{N/E}$ has only been studied when $N/E$ has odd degree (except for a short local study, due to Burns and Erez, in the absolute, abelian and very wildly ramified case, see [17, §3]). In particular, to our knowledge, the following question has not been answered yet.

**Question 1.** Is $(\mathcal{A}_{N/E})$ trivial for every tame Galois extension $N/E$ (whose inverse different is a square)?

In this paper, we consider a tame $G$-Galois extension $N/E$ such that the square root of the inverse different $\mathcal{A}_{N/E}$ exists. We introduce the torsion module

$$\mathcal{S}_{N/E} = \mathcal{A}_{N/E}/\mathcal{O}_N,$$

check it to be $G$-cohomologically trivial, hence to define a class in $\text{Cl}(\mathbb{Z}[G])$, and show that this class is trivial, yielding a new proof of Equality (2) without any
assumption on the degree of the extension (see Theorem 2). Nevertheless we need to assume that $N/E$ is locally abelian, namely that the decomposition group of every prime ideal of $\mathcal{O}_F$ is abelian (of course, this condition is restrictive only for ramified primes). The generalization of Equality (2) to locally abelian even degree extensions has a perhaps surprising consequence, namely a negative answer to the above Question (see Theorem 3).

1.1. Our results. We now explain our strategy more in detail. In Section 2 we follow Chase’s approach: we reduce the study of the $\mathbb{Z}[G]$-module $S_{N/E}$ to that of its totally and tamely ramified local analogue $S_{K/F}$, where $K/F$ is a cyclic totally ramified tame $p$-adic extension with Galois group $\Delta$ of odd order $e$ (prime to $p$). As mentioned earlier, the ramification index $e$ needs to be odd so that the inverse different of $K/F$ exists. Up to this point, the only difference with Chase’s study of $T_{N/E}$ is that we need $N/E$ to be locally abelian when dealing with $S_{N/E}$.

The key ingredient in Chase’s proof of the triviality of $T_{N/E}$ is the link he establishes between the local torsion module $T_{K/F}$ and the Swan module $\Sigma_\Delta(p) = p\mathbb{Z}[\Delta] + \text{Tr}_\Delta\mathbb{Z}[\Delta]$ (here $\text{Tr}_\Delta = \sum_{\delta \in \Delta} \delta \in \mathbb{Z}[\Delta]$). Consider the torsion module $T(p, \mathbb{Z}[\Delta]) = \mathbb{Z}[\Delta]/\Sigma_\Delta(p)$ associated to the Swan module, then

$$T_{K/F} \cong T(p, \mathbb{Z}[\Delta])^{\text{f}}$$

as $\mathbb{Z}[\Delta]$-modules, where $f$ is the inertia degree of $F/\mathbb{Q}_p$.

To deal with $S_{K/F}$, we need to enlarge the coefficient ring of the group algebra of $\Delta$. Let $\mu_e$ denote the group of $e$th roots of unity in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let $\mathfrak{o}$ denote the ring of integers of the cyclotomic field $\mathbb{Q}(\mu_e)$. We introduce a new torsion $\mathbb{Z}[\Delta]$-module $S_{\chi}(\mathfrak{p}, \mathfrak{o}[\Delta])$, which depends on a character $\chi : \Delta \to \mu_e$ and a prime $\mathfrak{p}$ of $\mathfrak{o}$ not dividing $e$. It may be considered as an analogue of $T(p, \mathbb{Z}[\Delta])$ in the sense that, for an appropriate choice of $\chi$ and $\mathfrak{p}$ (in particular $\mathfrak{p} \mid p$, the residual characteristic of $K/F$), we have

$$S_{K/F} \cong S_{\chi}(\mathfrak{p}, \mathfrak{o}[\Delta])^{\text{f}/\mathfrak{f}}$$

as $\mathbb{Z}[\Delta]$-modules, where $f$ is the inertia degree of $\mathfrak{p}$ in $\mathbb{Q}(\mu_e)/\mathbb{Q}$. These constructions are described in Section 2.2. Furthermore it is easy to see that $S_{\chi}(\mathfrak{p}, \mathfrak{o}[\Delta])$ is a cohomologically trivial $\mathbb{Z}[\Delta]$-module, hence it defines a class in $\text{Cl}(\mathbb{Z}[\Delta])$, see Section 2.3.

Now let $\chi : \Delta \to \mu_e$ be any injective character and $\mathfrak{p}$ be a prime of $\mathfrak{o}$ not dividing $e$ and set $S = S_{\chi}(\mathfrak{p}, \mathfrak{o}[\Delta])$. The central part of this paper is devoted to the study of the class $(S)$ in $\text{Cl}(\mathbb{Z}[\Delta])$. In Section 3, we find an equivariant morphism $s$ from the group of virtual characters of $\Delta$ to the idèles of $\mathbb{Q}(\mu_e)$, representing $(S)$ in Fröhlich’s Hom-description of $\text{Cl}(\mathbb{Z}[\Delta])$. In Section 4, we note that the content of the values of $s$ is a principal ideal: this follows from Stickelberger’s theorem, which also gives an explicit generator of this ideal in terms of Jacobi sums. Dividing $s$ by this suitably modified generator $c_e$ yields a morphism with unit idelic values. With the help of the Hasse-Davenport formula we express the resulting morphism $sc_e^{-1}$ as a Fröhlich generalized Determinant of some unit idèle of $\mathbb{Z}[\Delta]$, showing that it lies in the denominator of the Hom-description, namely that $(S)$ is trivial.

More precisely, let $J$ denote the Jacobi sum defined by

$$J = \sum_{x \in \mathfrak{o}/\mathfrak{p}} \left(\frac{x}{\mathfrak{p}}\right)^{-1} \left(\frac{1-x}{\mathfrak{p}}\right)^{-1}.$$
where \( \left( \frac{\cdot}{p} \right) \) is the \( e \)th power residue symbol. Then \( J \) belongs to \( \mathfrak{o} \). Let \( \delta \) be a fixed generator of \( \Delta \). In Section 4 we define \( n_i \in \mathbb{Z} \) for \( i = 0, \ldots, e - 1 \) such that

\[
J = \sum_{i=0}^{e-1} n_i \chi(\delta)^i.
\]

We can now formulate the main result of this paper, in terms of Fröhlich’s Hom-description of the class group (see Section 3.1 for more details).

**Theorem 1.** The class \((S)\) is trivial in \( \text{Cl}(\mathbb{Z}[\Delta]) \). More precisely it is represented in \( \text{Hom}_{\Omega_q}(\mathbb{R}, J(\mathbb{Q}(\mu_e))) \) by the morphism with \( q \)-components equal to 1 at places \( q \) of \( \mathbb{Q}(\mu_e) \) such that \( q \nmid e \), and to \( \text{Det}(u^{-1}) \), at prime ideals \( q \) of \( \mathfrak{o} \) such that \( q \mid e \), where \( u_s \in \mathbb{Z}[\Delta] \) is defined by

\[
u_s = \sum_{i=0}^{e-1} n_i \delta^i,
\]

and is a unit of \( \mathbb{Z}_q[\Delta] \), for any rational prime \( q \) such that \( q \mid e \).

The proof will follow from the results of Sections 3 and 4 (see Theorem 4.3 and its proof). Of course the fact that \((S)\) is trivial yields that it is represented by any homomorphism belonging to the denominator of the Hom-description. The representative given in Theorem 1 makes apparent the link between the \( \Delta \)-module \( S \) and the Jacobi sum and is the one we use to show the triviality of \((S)\).

Using the reduction results of Section 2, we deduce the following consequence.

**Theorem 2.** Let \( N/E \) be a \( G \)-Galois tamely ramified extension of number fields. Assume further that \( N/E \) is locally abelian. Then the class of \( S_{N/E} \) is trivial in \( \text{Cl}(\mathbb{Z}[G]) \). In particular we have

\[
(\mathcal{O}_N) = (A_{N/E}) \in \text{Cl}(\mathbb{Z}[G]).
\]

In Section 5 we use this result to answer negatively to Question 1. When \( N/E \) is locally abelian and tame, Theorem 2 together with Taylor’s theorem reduces the question to the study of the triviality of the image of the root number class in \( \text{Cl}(\mathbb{Z}[G]) \) (see Corollary 5.2). This immediately gives that \( (A_{N/E}) = 1 \) if \( N/E \) is abelian or has odd order (thus recovering Erez’s result in the locally abelian case). Computing the appropriate root numbers, we show next that \( (A_{N/E}) = 1 \) if \( N/E \) is locally abelian and no real place of \( E \) becomes complex in \( N \). However the class of the square root of the inverse different is not trivial in general, in other words we have the following result.

**Theorem 3.** There exists a tame Galois extension \( N/Q \) of even degree such that \( C_{N/Q} \) is a square and the class of \( A_{N/Q} \) is nontrivial in \( \text{Cl}(\mathbb{Z}[\text{Gal}(N/Q)]) \).

In fact, in Section 5.2 we will explicitly describe a tame locally abelian \( \tilde{A}_4 \)-Galois extension \( N/Q \), taken from [1], such that \( (A_{N/Q}) \neq 1 \) in \( \text{Cl}(\mathbb{Z}[\tilde{A}_4]) \), where \( \tilde{A}_4 \) is the binary tetrahedral group (which has order 24). We also show that this example is minimal in the sense that \( (A_{N/Q}) = 1 \) if \( N/Q \) is a tame locally abelian \( G \)-Galois extension with \( \#G \leq 24 \) and \( G \neq \tilde{A}_4 \).
1.2. Connections and generalizations. We end this introduction by making some remarks on connections and possible generalizations of our results.

The link we use in a crucial way between the Galois module structure of \(A_{N/E}\) and Jacobi sums is not new. In his early work [15] on the square root of the inverse different, Erez already establishes such a link in the case of a cyclic extension of \(K/Q\) of odd prime degree \(l\). Using a result of Ullom [35, Theorem 1], he shows that the class of \(A_{K/Q}\) in \(\text{Cl}(\mathbb{Z}[\text{Gal}(K/Q)])\) corresponds, through Rim’s isomorphism [13, (42.16)], to the class in \(\text{Cl}(\mathbb{Q}(\mu_l))\) of an ideal of \(\mathbb{Q}(\mu_l)\) which is defined by the action of some specific element of \(\mathbb{Z}[\text{Gal}(\mathbb{Q}(\mu_l))/\mathbb{Q}]\) on prime ideals. This group algebra element, which is pretty close to what ours, \(u_s\), would yield in the prime degree case, happens to be the exponent which appears in the factorization of the Jacobi sum, yielding the triviality of the class under study. The factorisation of Jacobi sums through Stickelberger’s theorem is also an essential step in our proof of the triviality of the class of \(S\) and therefore of that of \(S_{N/E}\).

In the introduction of his thesis [14], Erez gives other examples of results on the Galois module structure of rings of integers that are proved using Stickelberger elements ([20], [10]). In [7] Chase uses such elements to give, when \(N/E\) is cyclic or elementary abelian, the composition series of certain primary components of a certain \(\mathcal{O}_E[G]\)-module \(R_{N/E}\) related to the tensor product \(\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N\).

In fact the strategy described in the present paper also applies, without any restriction on the decomposition groups (i.e. the locally abelian hypothesis is not needed), to the torsion module \(T_{N/E}\) defined above as well as to \(R_{N/E}\). One can prove this way that both \(T_{N/E}\) and \(R_{N/E}\) define the trivial class in \(\text{Cl}(\mathbb{Z}[G])\), using cyclotomic units and (appropriate powers of) Gauss sums instead of Jacobi sums, respectively. This gives on the one hand another approach to the proof of Equality (1), and on the other hand, can be used to show that the \(\mathbb{Z}[G]\)-module \(\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N\) defines the trivial class in \(\text{Cl}(\mathbb{Z}[G])\). The latter result looked new to us at first sight, but in fact it is easily deduced from Taylor’s theorem, since one can show that \((\mathcal{O}_N \otimes_{\mathcal{O}_E} \mathcal{O}_N)^{[N:E]}\) in \(\text{Cl}(\mathbb{Z}[G])\).

As pointed out by Fröhlich in [18, Note 6 to Chapter III], Chase remarks that the character function associated to \(T_{N/E}\) (in the ideal-theoretic Hom-description) is the Artin conductor. Similarly, the character function associated to \(R_{N/E}\) (in the idèle-theoretic Hom-description) is closely related to a resolvent map (see [7, p. 210]). Fröhlich also wonders how his method, based on the comparison of Galois Gauss sums and resolvents, could be linked to Chase’s approach. The connection we make between \(R_{N/E}\) and Gauss sums might help answering this question.

It is also interesting to remark that \(S_{N/E}\) and \(T_{N/E}\) are particular instances of torsion modules arising from ideals, i.e. modules of the form \(\mathcal{O}_N/I\) or \(I^{-1}/\mathcal{O}_N\), where \(I\) is a \(G\)-stable ideal of \(\mathcal{O}_N\). In fact our techniques also extend to this more general framework and can be used to give a new proof of a result of Burns [4, Theorem 1.1] on arithmetically realizable classes in tame locally abelian Galois extensions of number fields.

As suggested by various experts, it seems reasonable to expect that our methods also work in the context of sums of \(k\)-th roots of inverse differents developed by Burns and Chinburg [5].

Another possible generalization concerns weakly ramified extensions (i.e. the second ramification group of every prime is trivial), as we shall now explain. For the rest of this introduction \(N/E\) is not assumed to be tame (but still Galois) unless...
otherwise stated. Recall that Chinburg defined an invariant \( \Omega(N/E, 2) \in \text{Cl}(\mathbb{Z}[G]) \), generalizing \((\mathcal{O}_N)\) in the sense that
\[
(\mathcal{O}_N) = \Omega(N/E, 2)
\]
when \( N/E \) is tamely ramified (see [8, Theorem 3.2]). When \( N/E \) is tamely ramified and locally abelian, Theorem 2 yields the equality:
\[
(\mathcal{A}_{N/E}) = \Omega(N/E, 2) .
\]
Observe that the class \( (\mathcal{A}_{N/E}) \in \text{Cl}(\mathbb{Z}[G]) \) may be defined even if \( N/E \) is not tame. In fact, Erez has shown\(^1\) that \( \mathcal{A}_{N/E} \) is \( \mathbb{Z}[G] \)-locally free if and only if \( N/E \) is a weakly ramified \( G \)-Galois extension. Therefore it is natural to wonder:\(^2\)

**Question 2.** Does \( (\mathcal{A}_{N/E}) = \Omega(N/E, 2) \) hold for every weakly ramified Galois extension \( N/E \) (whose inverse different is a square)?

Let us briefly recall what is known on \( (\mathcal{A}_{N/E}) \) in the case where \( N/E \) is a wildly and weakly ramified \( G \)-Galois extension of odd degree:

(a) \( M \otimes_{\mathbb{Z}[G]} \mathcal{A}_{N/E} \) is free over \( M \), where \( M \) is a maximal order of \( \mathbb{Q}[G] \) containing \( \mathbb{Z}[G] \) ([16, Theorem 2]);

(b) \( (\mathcal{A}_{N/E})^3 = 1 \) if \( E = \mathbb{Q}, \ [N : \mathbb{Q}] \) is a power of a prime \( p \) and \( e \) is the ramification index of \( p \) in \( N/\mathbb{Q} \) ([36, Théorème 1]); when \( p = 3 \) one even has \( (\mathcal{A}_{N/E})^3 = 1 \) by [37, Theorem 1];

(c) \( (\mathcal{A}_{N/E}) = 1 \) if, for any wildly ramified prime \( P \) of \( \mathcal{O}_N \), the decomposition group is abelian, the inertia group is cyclic and the localized extension \( E_P/\mathbb{Q}_p \) is unramified, where \( P = \mathcal{P} \cap E \) and \( p\mathbb{Z} = \mathcal{P} \cap \mathbb{Q} \) ([22, Theorem 1]).

As already mentioned Erez has also shown that \( (\mathcal{A}_{N/E}) \) is trivial when \( N/E \) is a tame extension of odd degree. It thus seems reasonable to conjecture that \( (\mathcal{A}_{N/E}) \) is trivial when \( N/E \) is a weakly ramified extension of odd degree (this was conjectured in the absolute case in [36]).

On the other hand, Chinburg’s \( \Omega(2) \) conjecture states that, for any \( G \)-Galois extension \( N/E, \Omega(N/E, 2) \) equals the Fröhlich – Cassou-Noguès class which generalizes the root number class in \( \text{Cl}(\mathbb{Z}[G]) \) to wildly ramified extensions (see [8]). If the degree of \( N/E \) is odd, the Fröhlich – Cassou-Noguès class is trivial. Therefore, assuming Chinburg’s conjecture, Question 2 reduces, when \( N/E \) is weakly ramified of odd degree, to asking whether \( (\mathcal{A}_{N/E}) \) is trivial. By this argument we know for instance that Question 2 has a positive answer for the (infinite family of) odd degree extensions in (c) satisfying the additional hypothesis that \( |E_P : \mathbb{Q}_p| \) is coprime with the inertia degree of \( \mathcal{P}/P \). In fact, Chinburg’s conjecture is true for these extensions, as shown by Bley and Cobbe (see [2]).

However, a complete answer to Question 2 seems very hard to obtain at the moment. A step towards this goal could be to compute the classes involved in specific cases where they happen to be non trivial. In the tame and locally abelian

---

\(^1\)Erez’s theorem is stated for odd degree extensions, which is the general assumption in [16]. However the proof of [16, Theorem 1] also holds for even degree extensions. At some point in the proof one needs to observe that, if \( K/F \) is a weakly ramified Galois extension (of any degree) whose inverse different is a square, then the inverse different of \( K/L \) is also a square, where \( L = K^V \) and \( V \) is a subgroup of \( \text{Gal}(K/F) \). This follows easily from Hilbert’s formula ([25, IV, Proposition 4]). The rest of Erez’s proof goes through unchanged.

\(^2\)This question, which came out in a conversation with Erez in Luminy in 2011, is in fact the original motivation for our work.
case, Theorem 3 gives an example where the equality holds and is nontrivial. It might be interesting to investigate tame and non locally abelian examples (maybe to be seeked in examples studied by Cougnard, see for instance [11]?). Building even degree wildly and weakly ramified extensions of the rationals such that the inverse different is a square would certainly be interesting in itself; computing the class defined by its square root might be possible by algorithmic means (see [36, §3], but the method used there only enables to show that the class is trivial by finding a normal basis generator), it could then maybe be compared with the Fröhlich – Cassou-Noguès class or to Chinburg’s $\Omega(2)$ invariant if they are computable.

Acknowledgement. The authors thank the referee for prompting them to think more thoroughly about the possible generalizations and connections of their work, particularly in the non-tame case.

2. Reduction to inertia subgroups

We use the notation of the Introduction, in particular $N/E$ is a tame $G$-Galois extension in which the square root of the inverse different exists. For a prime $\mathcal{P}$ of $N$, we denote by $D_{\mathcal{P}}$ (resp. $I_{\mathcal{P}}$) the decomposition subgroup (resp. inertia subgroup) of $\mathcal{P}$ in $N/E$. If $P$ is the prime ideal of $E$ below $\mathcal{P}$, we will often identify the Galois group of $N_{\mathcal{P}}/E_{P}$ with $D_{\mathcal{P}}$, where $N_{\mathcal{P}}$ (resp. $E_{P}$) is the completion of $N$ at $\mathcal{P}$ (resp. of $E$ at $P$). We let $e_{\mathcal{P}}$ denote the order of $I_{\mathcal{P}}$, recall that $e_{\mathcal{P}}$ is odd (and only depends on $P$). Let also $\mu_{e_{\mathcal{P}}}$ denote the group of $e_{\mathcal{P}}$th roots of unity in $\mathbb{Q}$ and $\mathfrak{o}_{e_{\mathcal{P}}}$ the ring of integers of $\mathbb{Q}(\mu_{e_{\mathcal{P}}})$.

In this section we show that, when $N/E$ is locally abelian, the $G$-module structure of $\mathcal{S}_{N/E}$ can be recovered by the knowledge, for finitely many primes $\mathcal{P}$ of $N$, of the $I_{\mathcal{P}}$-module structure of a certain torsion $I_{\mathcal{P}}$-module. More precisely, if Ram$(N/E)$ denotes the set of primes of $\mathcal{O}_{E}$ which ramify in $N/E$, then $\mathcal{S}_{N/E}$ can be written as a direct sum over Ram$(N/E)$ of torsion $G$-modules induced from some $I_{\mathcal{P}}$-modules $\mathcal{S}_{\chi_{\mathcal{P}}}(p, \mathfrak{o}_{e_{\mathcal{P}}}[I_{\mathcal{P}}])$ (which we shall define later, see (10)) where, for each $P \in$ Ram$(N/E)$, $\mathcal{P}$ is any fixed prime above $P$, $\chi_{\mathcal{P}}$ is an injective character of $I_{\mathcal{P}}$, $p$ is the prime number below $P$ and $\mathfrak{p}$ is a prime above $p$ in $\mathfrak{o}_{e_{\mathcal{P}}}$.

We now state the main result of this section whose proof will be given in §2.2.2.

**Theorem 2.1.** For every $P \in$ Ram$(N/E)$, choose a prime $\mathcal{P}$ of $N$ above $P$. Assume moreover that $N/E$ is locally abelian. Then, with the notation introduced above, the injections $\mathfrak{o}_{e_{\mathcal{P}}}/P \rightarrow \mathcal{O}_{N}/\mathcal{P}$ factor through $\mathcal{O}_{E}/P \rightarrow \mathcal{O}_{N}/\mathcal{P}$ and there is an isomorphism of $\mathbb{Z}[G]$-modules

$$\mathcal{S}_{N/E} \cong \bigoplus_{P \in \text{Ram}(N/E)} \left( \mathbb{Z}[G] \otimes \mathbb{Z}[I_{\mathcal{P}}] \right) \mathcal{S}_{\chi_{\mathcal{P}}}(p, \mathfrak{o}_{e_{\mathcal{P}}}[I_{\mathcal{P}}]) \otimes \mathcal{O}_{E/P} \mathfrak{o}_{e_{\mathcal{P}}}/P.$$

In Section 2.3 we will see how the above theorem, together with Theorem 1, can be used to prove Theorem 2. More precisely, we show that $\mathcal{S}_{\chi_{\mathcal{P}}}(p, \mathfrak{o}_{e_{\mathcal{P}}}[I_{\mathcal{P}}])$ (resp. $\mathcal{S}_{N/E}$) is a cohomologically trivial (torsion) $I_{\mathcal{P}}$-module (resp. $G$-module). In particular $\mathcal{S}_{\chi_{\mathcal{P}}}(p, \mathfrak{o}_{e_{\mathcal{P}}}[I_{\mathcal{P}}])$ and $\mathcal{S}_{N/E}$ define classes in $\text{Cl}(\mathbb{Z}[I_{\mathcal{P}}])$ and $\text{Cl}(\mathbb{Z}[G])$, respectively. Thus the isomorphism of Theorem 2.1 can be translated into an equality of classes in $\text{Cl}(\mathbb{Z}[G])$, which in turn will give directly Theorem 2, assuming Theorem 1.

2.1. Reductions.
2.1.1. We first reduce from global to local extensions, keeping the notation of the beginning of this section.

**Proposition 2.2.** There is an isomorphism of $\mathcal{O}_E[G]$-modules

$$S_{N/E} \cong \bigoplus_{P \in \text{Ram}(N/E)} \mathbb{Z}[G] \otimes \mathbb{Z}[D_P] S_{N_P/E_P}.$$  

*Proof.* Since $A_{N/E}$ is $G$-invariant, we can write

$$A_{N/E} = \prod_{P \in \text{Ram}(N/E)} \prod_{P|P} P^{-\epsilon_P-1}.$$  

Then, as a consequence of the next lemma, we have an isomorphism of $\mathcal{O}_E[G]$-modules

$$S_{N/E} \cong \bigoplus_{P \in \text{Ram}(N/E)} (\prod_{P|P} P^{-\epsilon_P-1})/\mathcal{O}_N.$$  

**Lemma 2.3.** Let $\mathcal{J}_1, \mathcal{J}_2 \subset \mathcal{O}_N$ be ideals with $\mathcal{J}_1 + \mathcal{J}_2 = \mathcal{O}_N$. Then there is an isomorphism of $\mathcal{O}_N$-modules

$$(\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{O}_N \xrightarrow{\sim} (\mathcal{J}_1)^{-1}/\mathcal{O}_N \times (\mathcal{J}_2)^{-1}/\mathcal{O}_N.$$  

*Proof.* We claim that the inclusions $\mathcal{J}_1^{-1} \to (\mathcal{J}_1 \mathcal{J}_2)^{-1}$ and $\mathcal{J}_2^{-1} \to (\mathcal{J}_1 \mathcal{J}_2)^{-1}$ induce $\mathcal{O}_N$-isomorphisms

(3) $\tau_1 : \mathcal{J}_1^{-1}/\mathcal{O}_N \to (\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{J}_2^{-1}$ and $\tau_2 : \mathcal{J}_2^{-1}/\mathcal{O}_N \to (\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{J}_1^{-1}$

and the natural projections $(\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{O}_N \to (\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{J}_1^{-1}$ and $(\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{O}_N \to (\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{J}_2^{-1}$ induce an $\mathcal{O}_N$-isomorphism

(4) $\tau : (\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{O}_N \to (\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{J}_1^{-1} \times (\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{J}_2^{-1}.$

Write $1 = j_1 + j_2$ with $j_1 \in \mathcal{J}_1$ and $j_2 \in \mathcal{J}_2$. To show that $\tau_1, \tau_2$ and $\tau$ are injective, we only need to show that $\mathcal{J}_1^{-1} \cap \mathcal{J}_2^{-1} \subseteq \mathcal{O}_N$ (the reverse inclusion being obvious). If $j \in \mathcal{J}_1^{-1} \cap \mathcal{J}_2^{-1}$, then $j = 1 \cdot j = j_1 j + j_2 j$ and both $j_1 j$ and $j_2 j$ belong to $\mathcal{O}_N$. This shows that $\tau_1, \tau_2$ and $\tau$ are injective.

To prove the surjectivity of $\tau_1$, let $j \in (\mathcal{J}_1 \mathcal{J}_2)^{-1}$. Then $j_1, j \in \mathcal{J}_2^{-1}$ and hence $j = j_1 j$ belongs to the class of $j$ in $(\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{J}_1^{-1}$. On the other hand $j = j_2 j \in \mathcal{J}_1^{-1}$, which shows that $\tau_1$ is surjective and the surjectivity of $\tau_2$ follows by a similar argument.

As for the surjectivity of $\tau$, take $y, z \in (\mathcal{J}_1 \mathcal{J}_2)^{-1}$. One easily sees that $x = yj_1 + zj_2$ belongs to $(\mathcal{J}_1 \mathcal{J}_2)^{-1}$ and

$$x \equiv yj_1 \equiv y - yj_2 \equiv y \mod \mathcal{J}_1^{-1} \quad \text{and} \quad x \equiv zj_2 \equiv z - zj_1 \equiv z \mod \mathcal{J}_2^{-1}.$$  

This shows that $\tau$ is surjective and complete the proof of our claim.

The lemma then follows since

$$\tau : (\mathcal{J}_1 \mathcal{J}_2)^{-1}/\mathcal{O}_N \to (\mathcal{J}_1)^{-1}/\mathcal{O}_N \times (\mathcal{J}_2)^{-1}/\mathcal{O}_N$$

is an $\mathcal{O}_N$-isomorphism. 

In a similar way we also get an isomorphism of $\mathcal{O}_E$-modules

$$(\prod_{P|P} P^{-\epsilon_P-1})/\mathcal{O}_N \cong \prod_{P|P} (P^{-\epsilon_P-1}/\mathcal{O}_N).$$
for every $P \in \text{Ram}(N/E)$. The above isomorphism is easily seen to be $G$-invariant, once the right-hand side is given a $G$-module structure by
\[
(g \cdot (x_P))_{P_0} = g(x_{g^{-1}(P_0)})
\]
for every $g \in G$, $(x_P) \in \prod_{P | P} (P^{\mathfrak{p}^{-1}_{P_0}}/\mathcal{O}_N)$ and $P_0 \mid P$. A standard argument shows that, for any prime $P_0$ above $P$, we have
\[
(6) \prod_{P | P} (P^{\mathfrak{p}^{-1}_{P_0}}/\mathcal{O}_N) \cong \text{Map}_{\mathcal{O}_{P_0}}(G, P^{\mathfrak{p}^{-1}_{P_0}}/\mathcal{O}_N) \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}[\mathcal{O}_{P_0}]} (P^{\mathfrak{p}^{-1}_{P_0}}/\mathcal{O}_N)
\]
as $\mathcal{O}_N$-modules and $\mathcal{O}_F[G]$-modules. Note also that, for every $n \in \mathbb{N}$ and every $P \mid P$, the inclusion $N \rightarrow N_P$ induces an isomorphism
\[
P^{\mathfrak{p}^{-1}_{P_0}}/\mathcal{O}_N \cong P^{\mathfrak{p}^{-1}_{P_0}}/\mathcal{O}_{N_P}/\mathcal{O}_{N_P} = S_{N_P/E_P}
\]
of $\mathcal{O}_E[D_P]$-modules.

2.1.2. Proposition 2.2 allows us to focus on local extensions. Therefore in this subsection we shall put ourselves in the following situation. We fix a rational prime $p$ and a tamely ramified Galois extension $K/k$ of $p$-adic fields inside a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. We denote by $\Gamma$ the Galois group of $K/k$. Let $\Delta \subseteq \Gamma$ be the inertia subgroup of $K/k$, which is cyclic of odd order denoted by $e$, and set $F = K^\Delta$. As usual, $\mathcal{O}_K$, $\mathcal{O}_F$ and $\mathcal{O}_k$ denote the rings of integers of $K$, $F$ and $k$, respectively, and we shall denote by $\mathfrak{p}_K$, $\mathfrak{p}_F$ and $\mathfrak{p}_k$ the corresponding maximal ideals.

If $X$ and $Y$ are sets, we denote by $\text{Map}(X,Y)$ the set of mappings from $X$ to $Y$. Consider the bijection
\[
(7) \psi_{K/k} : K \otimes_k K \rightarrow \text{Map}(\Gamma, K)
\]
defined by $\psi_{K/k}(x \otimes y)(\gamma) = x\gamma(y)$ for $x, y \in K$ and $\gamma \in \Gamma$. We give $K \otimes_k K$ its natural $\Gamma \times \Gamma$-module structure: $(\gamma, \gamma')(x \otimes y) = \gamma(x) \otimes \gamma'(y)$. Then $\psi_{K/k}$ is an isomorphism of $\Gamma \times \Gamma$-modules if we let $\Gamma \times \Gamma$ act on $\text{Map}(\Gamma, K)$ by
\[
((\gamma, \gamma')u)(\eta) = \gamma(u(\gamma^{-1}\eta\gamma'))
\]
for all $u \in \text{Map}(\Gamma, K)$, $\gamma, \gamma', \eta \in \Gamma$.

We define $\text{Map}(\Gamma, K)^\Delta = \text{Map}(\Gamma, K)^{\Delta \times 1}$ to be the set of invariant maps under the action of the subgroup $\Delta \times 1$ of $\Gamma \times \Gamma$. More explicitly, $\text{Map}(\Gamma, K)^\Delta$ is the set of maps $u : \Gamma \rightarrow K$ such that
\[
\delta(u(\eta)) = u(\delta \eta)
\]
for all $\delta \in \Delta$, $\eta \in \Gamma$. We may view $\text{Map}(\Gamma, K)^\Delta$ as an $F$-algebra with the pointwise operations and as a $\Gamma$-module where $\Gamma$ acts as $1 \times \Gamma$. Then there is an isomorphism of both $F$-algebras and $F[\Gamma]$-modules:
\[
(8) \text{Map}(\Gamma, K)^\Delta \rightarrow \mathbb{Q}[\Gamma] \otimes_{\mathbb{Q}[\Delta]} K, \quad u \mapsto \sum_{\gamma \in \Gamma} \gamma^{-1} \otimes u(\gamma)
\]
where $\mathbb{Q}[\Gamma] \otimes_{\mathbb{Q}[\Delta]} K$ is the tensor product over $\mathbb{Q}[\Delta]$ of the right $\mathbb{Q}[\Delta]$-module $\mathbb{Q}[\Gamma]$ with the left $\mathbb{Q}[\Delta]$-module $K$. This tensor product is given the structure of a $\Gamma$-module via its left-hand factor and the structure of an $F$-algebra via its right-hand factor.
The isomorphism $\psi_{K/k}$ introduced above yields an isomorphism of both $F$-algebras and $F[\Gamma]$-modules:

$$\psi_{K/k} : F \otimes_k K \to \text{Map}(\Gamma, K)^\Delta$$

(here $F \otimes_k K$ is considered as an $F$-algebra via its left factor and as a $\Gamma$-module via its right factor). Composing with the isomorphism in (8), we get an isomorphism

$$\tilde{\psi}_{K/k} : F \otimes_k K \to \mathbb{Q}[\Gamma] \otimes_{\mathbb{Q}[\Delta]} K.$$

Note that $\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K$ is the maximal order of $\mathbb{Q}[\Gamma] \otimes_{\mathbb{Q}[\Delta]} K$ and, using that $F/k$ is unramified, it is not difficult to show that $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K$ is the maximal $\mathcal{O}_F$-order of $F \otimes_k K$ (see [7, p. 214]). Therefore $\tilde{\psi}_{K/k}$ induces the following isomorphism of rings and $\mathcal{O}_F[\Gamma]$-modules:

$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K \cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K.$$

**Lemma 2.4.** The homomorphism $\tilde{\psi}_{K/k}$ induces an isomorphism of $\mathcal{O}_F[\Gamma]$-modules

$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{S}_{K/k} \cong \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{S}_{K/k}.$$

**Proof.** Let $n = \frac{q - 1}{2}$ where $e = \# \Delta$, so that $\mathcal{S}_{K/k} = \mathcal{P}_K^{-n}/\mathcal{O}_K$. Consider the following commutative diagram of $\mathcal{O}_F[\Gamma]$-modules with exact rows

$$
\begin{array}{cccccc}
0 & \to & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K & \to & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n} & \to & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n}/\mathcal{O}_K & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{O}_K & \to & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^{-n} & \to & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^{-n}/\mathcal{O}_K & \to & 0
\end{array}
$$

The left-hand vertical arrow is an isomorphism. Therefore it suffices to prove that the central arrow is injective (one then concludes using a cardinality argument as above). For that purpose, it is enough to show that the map $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n} \to F \otimes_k K$ is injective, thanks to the following commutative diagram of $\mathcal{O}_F[\Gamma]$-modules

$$
\begin{array}{cccccc}
\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n} & \to & F \otimes_k K & \leftarrow & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n}/\mathcal{O}_K \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} \mathcal{P}_K^{-n} & \to & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Delta]} K
\end{array}
$$

whose right-hand arrow is an isomorphism. Note that $F \otimes_k K$ is the localization of the $\mathcal{O}_k$-module $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n}$ at the multiplicative set $k^n$. The map $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n} \to F \otimes_k K$ is then injective because $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{P}_K^{-n}$ is a torsion free $\mathcal{O}_k$-module. \hfill $\square$

The above lemma is somehow unsatisfactory, as it says that the $\Gamma$-module $\mathcal{S}_{K/k}$ is induced from itself viewed as a $\Delta$-module only after tensoring with $\mathcal{O}_F$. In the next subsection, introducing torsion $\Delta$-modules coming from global cyclotomic fields, we will get rid of this scalar extension, at least when $K/k$ is abelian.

The following proposition (which may be considered as a generalization of [7, Lemma 1.4]), shows that the $\Delta$-module $\mathcal{S}_{K/k}$ breaks up in smaller pieces.

**Proposition 2.5.** The action of $\mathcal{O}_F$ on $\mathcal{S}_{K/k}$ factors through an action of $\mathcal{O}_F/\mathcal{P}_F$ and we have

$$\mathcal{S}_{K/k} \cong \bigoplus_{i=1}^{e-1} \mathcal{P}_K^{e-i}/\mathcal{P}_K^{e-i+1}$$

as $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules.
Proof. Since $\mathcal{P}_F\mathcal{O}_K = \mathcal{P}_K$, the action of $\mathcal{O}_F$ on $\mathcal{P}_K^{-i}/\mathcal{O}_K$ factors through $\mathcal{O}_F/\mathcal{P}_F$, for every $0 \leq i \leq e$. This means that the $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-module $\mathcal{S}_K/k$ has the filtration $\{\mathcal{P}_K^{-i}/\mathcal{O}_K\}_{i=0}^{n}$, where $n = \frac{e-1}{2}$. Since $\mathcal{O}_F/\mathcal{P}_F[\Delta]$ is semisimple, we have

$$\mathcal{P}_K^{-n}/\mathcal{O}_K \cong \bigoplus_{i=1}^{n} \mathcal{P}_K^{-i}/\mathcal{P}_K^{-i+1}$$

as $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-modules. Furthermore multiplication by the $e$th power of any uniformizer of $K$ induces a $\mathcal{O}_F/\mathcal{P}_F[\Delta]$-isomorphism

$$\mathcal{P}_K^{-i}/\mathcal{P}_K^{-i+1} \cong \mathcal{P}_K^{-e-i}/\mathcal{P}_K^{-i+1}. \quad \square$$

2.2. Switch to a global cyclotomic field. In this subsection we will perform a further reduction, relating the module $\mathcal{S}_{K/F}$ to a new torsion Galois module, associated to the ring of integers of a certain cyclotomic field.

Recall that $\Delta$ is cyclic of odd order $e$. As in the Introduction $\mu_e$ denotes the group of $e$th roots of unity in $\mathbb{Q}$ and $\mathfrak{o}$ is the ring of integers of $\mathbb{Q}(\mu_e)$. Let $\chi : \Delta \to \mu_e$ be a character of $\Delta$. For any $\mathfrak{o}$-module $M$, we shall consider the $\mathfrak{o}[\Delta]$-module $M(\chi)$ whose underlying $\mathfrak{o}$-module is $M$ and $\Delta$ acts as $\delta \cdot m = \chi(\delta)m$. We shall be mainly concerned with the case where $M$ is the residue field $\kappa_p = \mathfrak{o}/\mathfrak{p}$ of a prime $\mathfrak{p} \subseteq \mathfrak{o}$ not dividing $e$.

2.2.1. We start with the setting of §2.1.2: in particular $K/F$ is a $\Delta$-Galois extension of $p$-adic fields which is totally and tamely ramified of degree $e$. By standard theory $F$ contains the group of $e$th roots of unity $\mu_{e,p} \subseteq \mathbb{Q}_p$, and we can choose a uniformizer $\pi\kappa$ of $K$ such that $\pi\kappa^e \in F$ (thus $\pi\kappa^e$ is a uniformizer of $F$). Consider the map $\chi_{K/F} : \Delta \to \mu_{e,p}$ defined by

$$\chi_{K/F}(\delta) = \frac{\delta(\pi\kappa)}{\pi\kappa}.$$

Since $K/F$ is totally ramified, any unit $u \in \mathcal{O}_K^\times$ such that $u^e \in F$ lies in $F$, hence $\chi_{K/F}$ does not depend on the choice of a uniformizer $\pi\kappa$, as above. It easily follows that $\chi_{K/F}$ is a group homomorphism, hence an isomorphism comparing cardinals: $\#\Delta = e = \#\mu_{e,p}$ (see also [25, Chapitre IV, Propositions 6(a) and 7]).

Remark 2.6. Note that $\Delta$ (resp. $\mu_{e,p}$) is a $\Gamma/\Delta$-module with the conjugation (resp. Galois) action. Then $\chi_{K/F}$ is in fact an isomorphism of $\Gamma/\Delta$-modules. To prove this, it is enough to verify that, for every $\gamma \in \Gamma$ and $\delta \in \Delta$, we have $\chi_{K/F}(\gamma\delta\gamma^{-1}) = \gamma(\chi_{K/F}(\delta))$. But indeed, if $\pi\kappa$ is as above, we have

$$\chi_{K/F}(\gamma\delta\gamma^{-1}) = \frac{\gamma\delta\gamma^{-1}(\pi\kappa)}{\pi\kappa} = \gamma\left(\frac{\delta\gamma^{-1}(\pi\kappa)}{\gamma^{-1}(\pi\kappa)}\right) = \gamma(\chi_{K/F}(\delta))$$

since $\gamma^{-1}(\pi\kappa)$ is a uniformizer of $K$ whose $e$th power belongs to $F$. Hence $\chi_{K/F}$ is a $\Gamma$-isomorphism and we deduce in particular that, if $\Gamma$ is abelian, then $\mu_{e,p} \subseteq k$. The reverse implication is also true: if $\mu_{e,p} \subseteq k$, then $\Gamma$ acts trivially on $\Delta$. This implies that $\Gamma$ is abelian, since $\Gamma = \langle \gamma, \Delta \rangle$ for any $\gamma \in \Gamma$ whose image in $\Gamma/\Delta$ generates $\Gamma/\Delta$ (which is a cyclic group).

Lemma 2.7. If $\chi : \Delta \to \mu_e$ is injective, then there exists an embedding $\iota : \mathbb{Q} \to \mathbb{Q}_p$ such that $\iota \circ \chi = \chi_{K/F}$. 

Our proof is inspired by that of [7, Theorem 1.7]. Let $\varphi$ and $\phi$ be such that $\varphi(\phi) = \chi_{K/F}$ for every $\phi \in \Delta$. Note that this indeed defines an injective field homomorphism, since $\chi$ and $\chi_{K/F}$ are actually isomorphisms. Then we can extend $\varphi$ to an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ in infinitely many ways and any of these extensions satisfies the requirements of the lemma.

We now fix an injective character $\chi : \Delta \to \mu_\kappa$ and an embedding $\varphi : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ such that $\varphi \circ \chi = \chi_{K/F}$. Note that $\varphi(p) \subseteq \mathcal{O}_F$ (since $\mu_\kappa \subseteq F$) and therefore we can view any $\mathcal{O}_F$-module as a $\varphi$-module via $\varphi$.

**Proposition 2.8.** Let $p \subseteq \varphi$ be the prime ideal above $p$ such that $\varphi(p) \subset \mathcal{P}_F$. For every positive integer $i$, we have an isomorphism of $\mathcal{O}_F[\Delta]$-modules:

$$\mathcal{P}_K[\Delta]^{\mathcal{P}_K} \cong \kappa_p(\chi^i) \otimes \kappa_p \mathcal{O}_F/\mathcal{P}_F,$$

where the right-hand side of the above isomorphism is an $\mathcal{O}_F/\mathcal{P}_F$-module via its right factor and a $\Delta$-module via its left factor.

**Proof.** Let $\pi_p$ denote any uniformizer of $K$. We identify $\mathcal{O}_F/\mathcal{P}_F$ with $\mathcal{O}_K/\mathcal{P}_K$ via the inclusion $\mathcal{O}_F \subset \mathcal{O}_K$. Then sending $[\pi_p^i x] \in \mathcal{P}_K[\Delta]^{\mathcal{P}_K}$ to $[1] \otimes [x] \in \kappa_p(\chi^i) \otimes \kappa_p \mathcal{O}_F/\mathcal{P}_F$ clearly gives a $\mathcal{O}_F$-isomorphism between $\mathcal{P}_K[\Delta]^{\mathcal{P}_K}$ and $\kappa_p(\chi^i) \otimes \kappa_p \mathcal{O}_F/\mathcal{P}_F$. Observe that $\Delta$ acts as multiplication by $\chi_{K/F}^i$ on $\mathcal{P}_K^{\mathcal{P}_K}$, since

$$\delta[\pi_p^i x] = [\delta(\pi_p^i x)] = [\chi_{K/F}(\delta)^i \pi_p^i \delta(x)] = [\chi_{K/F}(\delta)^i \pi_p^i \chi_{K/F}^i x]$$

(the last equality follows from the fact that $\Delta$ acts trivially on $\mathcal{O}_K/\mathcal{P}_K = \mathcal{O}_F/\mathcal{P}_F$). Therefore $\delta \cdot [\pi_p^i x]$ maps to

$$[1] \otimes (\chi_{K/F}^i(\delta)[x]) = [1] \otimes \chi^i(\delta)[x] = \chi^i(\delta)[1] \otimes [x] = (\delta \cdot [1]) \otimes [x] = \delta \cdot ([1] \otimes [x]).$$

We are ready for the main application of the torsion $\varphi[\Delta]$-modules we have introduced. They allow us to write the $\Gamma$-module $S_{K/k}$ as induced from some $\Delta$-module, at least if $K/k$ is abelian.

**Proposition 2.9.** Let $p \subseteq \varphi$ be the prime ideal above $p$ such that $\varphi(p) \subset \mathcal{P}_F$. Assume that $K/k$ is abelian. Then $\varphi$ induces an inclusion $\kappa_p \to \mathcal{O}_k/\mathcal{P}_k$ (hence $\mathcal{O}_k/\mathcal{P}_k$ is a $\kappa_p$-module via $\varphi$) and there is an isomorphism of $\mathcal{O}_k/\mathcal{P}_k[\Gamma]$-modules

$$S_{K/k} \cong \mathcal{O}_k/\mathcal{P}_k \otimes \kappa_p \left( \mathbb{Z}[\Gamma] \otimes \mathbb{Z}[[\Delta]] \left( \bigoplus_{i=1}^{\varphi-1} \kappa_p(\chi^i) \right) \right),$$

where the right-hand side of the above isomorphism is an $\mathcal{O}_k/\mathcal{P}_k$-module via its left factor and a $\Gamma$-module via its right factor.

**Proof.** Our proof is inspired by that of [7, Theorem 1.7]. Let $n = \varphi - 1$. Using Lemma 2.4, Propositions 2.5 and 2.8, we get

$$\mathcal{O}_F/\mathcal{P}_F \otimes \mathcal{O}_k/\mathcal{P}_k \mathcal{P}_K^{-n}/\mathcal{O}_K \cong \mathbb{Z}[\Gamma] \otimes \mathbb{Z}[[\Delta]] \mathcal{P}_K^{-n}/\mathcal{O}_K \cong \mathbb{Z}[\Gamma] \otimes \mathbb{Z}[[\Delta]] \left( \bigoplus_{i=1}^{n} \kappa_p(\chi^{e_i}) \right) \otimes \kappa_p \mathcal{O}_F/\mathcal{P}_F.$$
Observe now that, since $K/k$ is abelian, we have $\mu_{e_p} \subset k$ by Remark 2.6 and hence $\iota(p) \subset O_k$. In particular we can write the above isomorphism as

$$O_F/\mathcal{P}_F \otimes_{O_k/\mathcal{P}_k} \mathcal{P}_F^n/O_K \cong \left( \bigotimes_{\mathbb{Z}[\Delta]} \left( \bigoplus_{i=1}^n \kappa_p(\chi^{e-i}) \right) \right) \otimes_{O_k/\mathcal{P}_k} O_F/\mathcal{P}_F.$$ 

Since the above is an isomorphism of $O_F/\mathcal{P}_F[\Gamma]$-modules of finite length, we can apply the Krull-Schmidt theorem to conclude (see [12, §6, Exercise 2]). □

In view of Proposition 2.9 we introduce the following notation for any prime $p \subset o$ not dividing $e$:

$$S(\chi, o[\Delta]) = \bigoplus_{i=1}^{e-1} \kappa_p(\chi^i).$$ (10)

2.2.2. We now collect the results obtained so far to complete our reduction step. We recall the setting described at the beginning of this section. Let $N/E$ be a tame $G$-Galois extension of number fields. For any prime $P$ of $O_E$ we fix a prime $P \subseteq O_N$ dividing $P$. Let $D_P$ (resp. $I_P$) denote the decomposition group (resp. the inertia subgroup) of $P$ in $G$. Then the cardinality of $I_P$ only depends on $P$ and we denote it by $e_P$. Using Lemma 2.7, we fix an injective character $\chi_P : I_P \to \mathbb{Q}_p^\times$ and an embedding $\iota_P : \mathbb{Q} \to \mathbb{Q}_p$ (where $p$ is the rational prime below $P$ and $\mathbb{Q}_p$ is an algebraic closure of $\mathbb{Q}_p$ containing the completion $N_P$ of $N$ at $P$), such that $\iota_P \circ \chi_P = \chi_N/P_P$. These choices determine a prime ideal $p$ in the ring of integers $o_{e_P}$ of $\mathbb{Q}(\mu_{e_P}) \subset \mathbb{Q}$ satisfying $\iota_P(p) \subseteq P \cap O_{e_P}$. Moreover $O_{F_P}$ is an $o_{e_P}$-module via $\iota_P$. Recall that $\text{Ram}(N/E)$ is the set of primes of $E$ that ramify in $N/E$.

Proof of Theorem 2.1. Since $N/E$ is locally abelian, $E_P$ contains the $e_P$th roots of unity in $\mathbb{Q}_p$ (as explained in Remark 2.6) and therefore $\iota_P$ induces an inclusion $o_{e_P}/p \to O_{E_P}/P_O E_P \cong O_E/P$. Moreover using Propositions 2.2 and 2.9 we have isomorphisms of $\mathbb{Z}[G]$-modules:

$$S_{N/E} \cong \bigoplus_{P \in \text{Ram}(N/E)} \mathbb{Z}[G] \otimes_{\mathbb{Z}[D_P]} S_{N_P/E_P} \cong \bigoplus_{P \in \text{Ram}(N/E)} \mathbb{Z}[G] \bigotimes_{\mathbb{Z}[D_P]} \left( \mathbb{Z}[D_P] \bigotimes_{\mathbb{Z}[I_P]} S_{\chi_P}(p, o_{e_P}[I_P]) \right) \bigotimes_{O_E/P_e_P} [p].$$ □

To translate the isomorphism of Theorem 2.1 into an equality in $\text{Cl}(\mathbb{Z}[G])$ we need the results of the next subsection.

2.3. Classes of cohomologically trivial modules. To interpret the results we have obtained so far in terms of classes in the locally free class group we recall some facts about cohomologically trivial modules.
2.3.1. In this subsection $G$ is an arbitrary finite group (we do not need it to be the Galois group of a particular extension of number fields). Recall that a $G$-module $M$ is $G$-cohomologically trivial if, for every $i \in \mathbb{Z}$ and every subgroup $G' < G$, the Tate cohomology group $\hat{H}^i(G', M)$ is trivial. If $A$ is the ring of integers of a number field, let $\text{Cl}(A[G])$ be the locally free class group of $A[G]$ (see [18, I, §2] for locally free modules and the locally free class group).

**Lemma 2.10.** Let $A$ be the ring of integers of a number field. Let $M$ be a finitely generated $A[G]$-module.


(ii) $M$ is $G$-cohomologically trivial if and only if there exists an $A[G]$-resolution $0 \to P_1 \to P_0 \to M \to 0$ of $M$ with $P_0$ and $P_1$ locally free. In this case the class $(P_0)^{-1}(P_1)$ in $\text{Cl}(A[G])$ is independent of the chosen locally free resolution of $M$ and will be denoted by $(M)_{A[G]}$.

(iii) If $G$ is a subgroup of a finite group $\hat{G}$ and $M$ is $G$-cohomologically trivial, then $M \otimes_{A[G]} A[\hat{G}]$ is $G$-cohomologically trivial and

$$ (M \otimes_{A[G]} A[\hat{G}])_{A[\hat{G}]} = \text{Ind}^\hat{G}_G ((M)_{A[G]}) $$

where $\text{Ind}^\hat{G}_G : \text{Cl}(A[G]) \to \text{Cl}(A[\hat{G}])$ is the map which sends the class $(P)_{A[G]} \in \text{Cl}(A[G])$ of a locally free $A[G]$-module $P$ to the class $(P \otimes_{A[G]} A[\hat{G}]) \in \text{Cl}(A[\hat{G}])$.

**Proof.** For (i) and the first assertion of (ii) see for example [9, Proposition 4.1] (i) is a classical result of Swan). The last assertion of (ii) follows immediately from Schanuel’s lemma.

To prove (iii), suppose that $M$ is $G$-cohomologically trivial. Then, by (i) and (ii), there exists an exact sequence of $A[G]$-modules

$$ 0 \to P_1 \to P_0 \to M \to 0 $$

with $P_0, P_1$ projective. Observe that $A[\hat{G}]$ is a free $A[G]$-module. In particular the functor $- \otimes_{A[G]} A[\hat{G}]$ from the category of $A[G]$-modules to that of $A[\hat{G}]$-modules is exact and we get an exact sequence of $A[\hat{G}]$-modules

$$ 0 \to P_1 \otimes_{A[G]} A[\hat{G}] \to P_0 \otimes_{A[G]} A[\hat{G}] \to M \otimes_{A[G]} A[\hat{G}] \to 0. $$

Note that, for $i = 0, 1$, $P_i \otimes_{A[G]} A[\hat{G}]$ is $A[\hat{G}]$-projective since $P_i$ is $A[G]$-projective (this can be easily seen using the characterization of projective modules as direct summand of free modules). In particular, the exact sequence (11) implies that $M \otimes_{A[G]} A[\hat{G}]$ is $G$-cohomologically trivial by (i) and (ii). Moreover we have

$$ (M \otimes_{A[G]} A[\hat{G}])_{A[\hat{G}]} = (P_0 \otimes_{A[G]} A[\hat{G}])^{-1}((P_1 \otimes_{A[G]} A[\hat{G}]) $$

$$ = \text{Ind}^{\hat{G}}_G ((P_0)_{A[G]})^{-1}\text{Ind}^{\hat{G}}_G ((P_1)_{A[G]}) $$

$$ = \text{Ind}^{\hat{G}}_G ((P_0)_{A[G]}(P_1)_{A[G]}) $$

$$ = \text{Ind}^{\hat{G}}_G ((M)_{A[G]}) $$

in $\text{Cl}(A[\hat{G}])$. \qed

In this section we will use the above lemma when $A = \mathbb{Z}$ but later we will also need the case where $A$ is the ring of integers of a cyclotomic field. If $M$ is
a finitely generated $\mathbb{Z}[G]$-module which is cohomologically trivial, we will denote $(M)_{\mathbb{Z}[G]} \in \text{Cl}(\mathbb{Z}[G])$ simply by $(M)$.

2.3.2. We now come back to the global setting of §2.2.2. Thus $N/E$ is a tame $G$-Galois extension of number fields. Note that every $G$-stable fractional ideal of $N$ is $\mathbb{Z}[G]$-projective (see [34, Proposition 1.3]) hence locally free by Lemma 2.10 (i). In particular, $S_{N/E}$ defines a class in $\text{Cl}(\mathbb{Z}[G])$ and in fact

$$(S_{N/E}) = (A_{N/E})(O_N)^{-1}.$$  

Note also that, for every prime $P$ of $O_E$ and any integer $i$, the $I_P$-module $(\mathfrak{o}_{eP}/p)(\chi_P^i)$ is cohomologically trivial. In fact, for every $i \in \mathbb{Z}$ and every subgroup $I < I_P$, $H^i(I, (\mathfrak{o}_{eP}/p)(\chi_P^i))$ is annihilated by $e_P$ (see [25, Chapitre VIII, Corollaire 1 to Proposition 3]) and $p$ (since $p$ annihilates $(\mathfrak{o}_{eP}/p)(\chi_P^i)$). Since $N/E$ is tame, $p$ and $e_P$ are coprime, hence $H^i(I, (\mathfrak{o}_{eP}/p)(\chi_P^i)) = 0$. Thanks to Lemma 2.10 (ii) this allows us to consider the class $((\mathfrak{o}_{eP}/p)(\chi_P^i)) \in \text{Cl}(\mathbb{Z}[I_P])$.

We end this section by showing how Theorem 2.1 can be used to reduce the proof of Theorem 2 to that of Theorem 1

**Proof of Theorem 2 assuming Theorem 1.** By Theorem 2.1 and using Lemma 2.10 (iii), we have the following equality in $\text{Cl}(\mathbb{Z}[G])$:

$$(S_{N/E}) = \prod_{P \in \text{Ram}(N/E)} \text{Ind}_{I_P}^{O_E} (S_{\chi_P} (p, \mathfrak{o}_{eP}, [I_P]))^{[O_E/P : \mathfrak{o}_{eP}/p]}.$$  

By Theorem 1, for every prime $P \in \text{Ram}(N/E)$ and every prime $\mathfrak{P} | P$ in $O_N$, we have

$$(S_{\chi_P} (p, \mathfrak{o}_{eP}, [I_P])) = 1$$

in $\text{Cl}(\mathbb{Z}[I_P])$. Thus $(S_{N/E}) = 1$ which implies $(O_N) = (A_{N/E})$. The proof of Theorem 2 is then achieved. \qed

3. Hom-representatives

We now come to the proof of Theorem 1, which will be achieved in two steps. In this section, we apply Fröhlich’s machinery to get a first description of an Hom-representative of the class involved in its statement. Then in the next section we use Stickelberger’s theorem to refine this description and complete the proof.

We are thus in the cyclotomic setting introduced in the previous section, namely we fix an odd integer $e$, a cyclic group $\Delta$ of order $e$ and an injective character $\chi : \Delta \rightarrow \mu_e$, where $\mu_e$ is the group of $e$th roots of unity in $\mathbb{Q}$. We let $\mathfrak{o}$ denote the ring of integers of the cyclotomic field $\mathbb{Q}(\mu_e)$. Let $p$ denote a rational prime such that $p \nmid e$ and let $\mathfrak{p} \subset \mathfrak{o}$ denote a prime ideal above $p$. We set $\kappa = \mathfrak{o}/\mathfrak{p}$ and for brevity we let

$$S = S_{\chi}(p, \mathfrak{o}[[\Delta]])$$

We fix a primitive $e$th root of unity $\zeta \in \mu_e$ and we let $\delta \in \Delta$ be defined by $\chi(\delta) = \zeta$.

3.1. Hom description of the class group. In this section and the following one, we are interested in determining a class in the class group $\text{Cl}(\mathbb{Z}[[\Delta]])$. In order to do so, at some point we shall have to consider class groups of a group algebra with a larger coefficient ring. Further in Section 5 we shall also need a description of the class group of the group algebra $\mathbb{Z}[G]$ where $G$ is any finite group. So we will recall Fröhlich’s Hom-description in a quite general form. If $L$ is any number field with
$L \subset \overline{\mathbb{Q}}$, we set $\Omega_L = \text{Gal}(\overline{\mathbb{Q}}/L)$ and we let $\mathfrak{o}_L$ and $J(L)$ denote the ring of integers and the idele group of $L$, respectively.

3.1.1. Fröhlich’s Hom-description of $\text{Cl}(\mathfrak{o}_L[G])$, where $L$ is a number field and $G$ is a finite group, is the group isomorphism

\[
\text{Cl}(\mathfrak{o}_L[G]) \cong \frac{\text{Hom}_{\Omega_L}(RG, J(L'))}{\text{Hom}_{\Omega_L}(RG, (L')^\times) \text{Det}(\mathcal{U}(\mathfrak{o}_L[G]))}
\]

given by the explicit construction of a representative homomorphism of the class of any locally free rank one module, see [18, Theorem 1]. This construction will be shown and used in the next subsections. We now briefly explain the objects involved in (12), referring to [18] for a more complete account.

We begin with the upper part, where $RG$ is the additive group of virtual characters of $G$ with values in $\overline{\mathbb{Q}}$. The number field $L'$ is “big enough”, in particular it is Galois over $\mathbb{Q}$, contains $L$ and the values of the characters of $G$. In our cyclotomic setting described above, we shall only be concerned with the cases where $L = \mathbb{Q}$ or $\mathbb{Q}(\mu_\ell)$ and $G = \Delta$; since $\Delta$ is cyclic of order $\ell$, in these cases one can take $L' = \mathbb{Q}(\mu_{\ell^k}) \subset \overline{\mathbb{Q}}$. The homomorphisms in $\text{Hom}_{\Omega_L}(RG, J(L'))$ are those which commute with the natural actions of $\Omega_L$ on $RG$ and $J(L')$.

In the lower part, $\text{Hom}_{\Omega_L}(RG, (L')^\times)$ is the subgroup of $\text{Hom}_{\Omega_L}(RG, J(L'))$ yielded by the diagonal embedding of $(L')^\times$ into $J(L')$. The second factor needs some more explanations. First

\[\mathcal{U}(\mathfrak{o}_L[G]) = \prod_{l} \mathfrak{o}_{L_1}(G)^\times \subseteq \prod_{l} L_1[G]^\times,\]

where $l$ runs over all places of $L$ and $\mathfrak{o}_{L_1}$ denotes the ring of integers of a completion $L_1$ of $L$ at $l$ (with $\mathfrak{o}_{L_1} = L_1$ if $l$ is archimedean). Let $x = (x_1)_1 \in \prod_{l} L_1[G]^\times$, the character function $\text{Det}(x) = (\text{Det}(x_1))_1$ is defined componentwise. For each place $l$ of $L$ the ‘semi-local’ component $\text{Det}(x_1)$ takes values in $(L'_l \otimes_{L_1} L_1)^\times$, embedded in $J_l(L') = \prod_{\mathfrak{p} \mid l}(L'_\mathfrak{p})^\times$, where $\mathfrak{p}$ runs over the prime ideals of $\mathfrak{o}_{L_1}$ above $l$, through the isomorphism of $L'$-algebras

\[
L'_l \otimes_{L_1} L_1 \cong \prod_{\mathfrak{p} \mid l} L'_\mathfrak{p}
\]

built on the various embeddings of $L'$ in $\overline{L}_1$, a given algebraic closure of $L_1$, that fix $l$. By linearity we only need to define the character function $\text{Det}(x_1)$ on the irreducible characters $\theta$ of $G$. Write $x_1 = \sum_{g \in G} x_{1,g} g$, then $\text{Det}_g(x_1)$ is the image in $J_l(L')$, under isomorphism (13), of the determinant of the matrix

\[
\sum_{g \in G} x_{1,g} \Theta(g)
\]

where $\Theta$ is any matrix representation of the character $\theta$ and the $(i, j)$-entry of the above matrix $\sum_{g \in G} \Theta_{i,j}(g) \otimes x_{1,g}$ indeed belongs to $L'_l \otimes_{L_1} L_i$.

Note that, by $\Omega_L$-equivariance, the values of $\text{Det}(x_1) = (\text{Det}(x_1)_{\mathfrak{p}})_{\mathfrak{p} \mid l}$ in $J_l(L')$ are determined by those of any component $\text{Det}(x_1)_{\mathfrak{p}}$, see [18, II, Lemma 2.1]. In the following we may thus implicitly assume that a place $\mathfrak{p}$ of $L'$ is fixed above each place $l$ of $L$ and focus on the $\mathfrak{p}$-component $\text{Det}(x_1)_{\mathfrak{p}}$, that we shall indeed plainly denote by $\text{Det}(x_1)$, omitting the unnecessary subscript. Let $l$ denote the rational place below $l$ and $\overline{\mathbb{Q}}_l$ an algebraic closure of $\mathbb{Q}_l$ containing $L'_\mathfrak{p}$. The resulting local
function \( \text{Det}(x_i) \) belongs to \( \text{Hom}_{\Omega_{L_i}}(R_{G,L}, (L'_\mathcal{L})^\times) \), where \( R_{G,L} \) is the group of virtual characters of \( G \) with values in \( \mathbb{T}_L \) and \( \Omega_{L_i} = \text{Gal}(\mathbb{T}_L, L_i) \).

3.1.2. We now assume that \( G \) is abelian. With the above notation and assuming that

\[ \text{Proposition 3.1.} \]

of a place \( \mathcal{L} \) above \( L \). We shall use the following result in Section 4.

\[ \text{Proposition 3.1.} \quad \text{With the above notation and assuming that } G \text{ is abelian, the group homomorphism } \text{Det} : L_1[G]^\times \to \text{Hom}_{\Omega_{L_1}}(R_{G,L}, (L'_\mathcal{L})^\times) \text{ is injective.} \]

\[ \text{Proof.} \quad \text{See [18, (II.5.2)].} \]

3.2. Hom-representative of \( (S) \). In this subsection we use Fröhlich’s construction to get a representative homomorphism of the class of \( \kappa(\chi^i) \), where \( i \) is any integer such that \( 0 \leq i \leq e - 1 \). These representative homomorphisms yield a representative for the class of the torsion module \( S \).

Recall that \( \Delta = (\delta) \) and that the \( o[\Delta]\)-module \( \kappa(\chi^i) \) is defined to be \( \kappa = o/p \) as \( o \)-module, with action of \( \Delta \) given by \( \delta \cdot x = \chi^i(\delta)x = \zeta^i x \) for any \( x \in \kappa \).

3.2.1. Let us fix an integer \( 0 \leq i \leq e - 1 \), and let \( \phi_i : o[\Delta] \to \kappa(\chi^i) \) be the only \( o[\Delta]\)-module homomorphism which sends 1 to 1, hence \( \delta \) to \([\zeta^i]\), the class of \( \zeta^i \) in \( \kappa \). Note that \( \phi_i \) is surjective and set

\[ M_i = po[\Delta] + (\delta - \zeta^i)o[\Delta] \subset o[\Delta] \, . \]

Then the sequence of \( o[\Delta]\)-modules

\[ 0 \to M_i \to o[\Delta] \xrightarrow{\phi_i} \kappa(\chi^i) \to 0 \]

is exact (since clearly \( M_i \subseteq \ker(\phi_i) \) and \( \#(o[\Delta]/M_i) = \#(o/p[\Delta]/(\delta - [\zeta^i])) = \#o/p \)).

In the next proposition, we will show, by finding explicit local generators, that \( M_i \) is a locally free \( o[\Delta]\)-module. Anyway, this fact can be also shown as follows (see also the proof of [9, Proposition 4.1]): \( o[\Delta] \) is \( \Delta \)-cohomologically trivial (it is a free \( \mathbb{Z}[\Delta]\)-module) and the same holds \( \kappa(\chi^i) \) as observed in §2.3.2. Therefore from the above exact sequence, we see that \( M_i \) is \( \Delta \)-cohomologically trivial. Since it is also \( o \)-torsion free (being a submodule of \( o[\Delta] \)), we deduce that it is \( o[\Delta]\)-projective (this can be seen following the proof of [25, Chapitre IX, Théorème 7], with \( \mathbb{Z} \) replaced by \( o \), and using [26, Section 14.4, Exercice 1]). In particular, by Lemma 2.10 (i), the \( o[\Delta]\)-module \( M_i \) is locally free and we have, by Lemma 2.10 (ii),

\[ (\kappa(\chi^i))_{o[\Delta]} = (o[\Delta])_{o[\Delta]}^{-1}(M_i)_{o[\Delta]} = (M_i)_{o[\Delta]} \in \text{Cl}(o[\Delta]) \, . \]

For any place \( q \) of \( o \) we denote by \( o_q \) the completion of \( o \) at \( q \) (note that \( o_q = \mathbb{C} \) when \( q \) is infinite). With a harmless abuse of notation, we will denote by \( \zeta \) the image of \( \zeta \) under the embedding \( o \to o_p \). For every \( 0 \leq k \leq e - 1 \), we consider the idempotent

\[ \varepsilon_k = \frac{1}{e} \sum_{j=0}^{e-1} \zeta^{kj} \delta^{-j} \in o_p[\Delta] \, . \]
Proposition 3.2. For every place $q$ of $\mathfrak{o}$, $\mathfrak{o}_q \otimes \mathfrak{o} M_i = x_{i,q} \mathfrak{o}_q[D]$ with
\[
x_{i,q} = \begin{cases} 
1 & \text{if } q \neq p, \\
1 + (p-1)\varepsilon_i & \text{if } q = p.
\end{cases}
\]

Proof. If $q \neq p$, since $\mathfrak{po}_q = \mathfrak{o}_q$, we have $\mathfrak{o}_q[D] = \mathfrak{o}_q \otimes \mathfrak{o} M_i$, so we can take $x_{i,q} = 1$.

Assume $q = p$. Since $1 = \sum_{k=0}^{e-1} \varepsilon_k$ and $\varepsilon_k \varepsilon_k = \delta_{h,k} \varepsilon_k$, one has
\[
\mathfrak{o}_p[D] = \bigoplus_{k=0}^{e-1} \varepsilon_k \mathfrak{o}_p[D].
\]

Now set $\tilde{\phi}_i = \phi_i \otimes \text{id} : \mathfrak{o}[\Delta] \otimes \mathfrak{o} \mathfrak{o}_p = \mathfrak{o}_p[D] \to \kappa^{(\chi^i)} \otimes \mathfrak{o}_p = \kappa^{(\chi^i)}$, then $\tilde{\phi}_i(\varepsilon_i) = 1$ and
\[
\mathfrak{po}_p[D] + (1 - \varepsilon_i) \mathfrak{o}_p[D] \subseteq \ker(\tilde{\phi}_i) = \mathfrak{o}_p \otimes \mathfrak{o} M_i.
\]
By the above properties of the idempotents we have
\[
\mathfrak{o}_p[D]/(\mathfrak{po}_p[D] + (1 - \varepsilon_i) \mathfrak{o}_p[D]) \cong \varepsilon_i \mathfrak{o}_p[D]/\varepsilon_i \mathfrak{po}_p[D] \cong \kappa^{(\chi^i)},
\]
so that
\[
\mathfrak{po}_p[D] + (1 - \varepsilon_i) \mathfrak{o}_p[D] = \mathfrak{o}_p \otimes \mathfrak{o} M_i.
\]
We have indeed $\mathfrak{po}_p[D] + (1 - \varepsilon_i) \mathfrak{o}_p[D] = (1 + (p-1)\varepsilon_i) \mathfrak{o}_p[D]$: using the equalities
\[
p = (1 + (p-1)\varepsilon_i)(p - (p-1)\varepsilon_i),
\]
\[
1 - \varepsilon_i = (1 + (p-1)\varepsilon_i)(1 - \varepsilon_i),
\]
we get $\mathfrak{po}_p[D] + (1 - \varepsilon_i) \mathfrak{o}_p[D] \subseteq (1 + (p-1)\varepsilon_i) \mathfrak{o}_p[D]$, since $(p) = \mathfrak{po}_p$; the reverse inclusion follows from
\[
1 + (p-1)\varepsilon_i = p\varepsilon_i + 1 - \varepsilon_i.
\]
Therefore we can take $x_{i,p} = 1 + (p-1)\varepsilon_i$. \hfill \Box

In view of (15), we get the following representative homomorphism of the class of $\kappa^{(\chi^i)}$ in $\text{Cl}(\mathfrak{o}[\Delta])$.

Corollary 3.3. The homomorphism $v_i$ with values in the idèles group $J(\mathbb{Q}(\zeta))$, defined at any place $q$ of $\mathfrak{o}$ by
\[
v_i(\chi^h)_q = \text{Det}_{\chi^h}(x_{i,q}) = \begin{cases} 
p & \text{if } q = p, \ i \equiv h \pmod{e}, \\
1 & \text{otherwise.}
\end{cases}
\]
represents the class $(\kappa^{(\chi^i)})_{\mathfrak{o}[\Delta]}$ in $\text{Hom}_{\mathbb{Q}(\zeta)}(R_{\Delta}, J(\mathbb{Q}(\zeta)))$.

Proof. By Fröhlich’s theory, Equality (15) and Proposition 3.2, we know that $(v_i)_q = \text{Det}(x_{i,q})$ represents the class $(\kappa^{(\chi^i)})_{\mathfrak{o}[\Delta]}$. Let $h \in \{0, \ldots, e-1\}$, then
\[
\text{Det}_{\chi^h}(\varepsilon_i) = \frac{1}{\varepsilon} \sum_{j=0}^{e-1} \zeta^{(i-h)j} = \begin{cases} 
0 & \text{if } i \not\equiv h \pmod{e} \\
1 & \text{if } i \equiv h \pmod{e},
\end{cases}
\]
because $\zeta^{i-h}$ is a root of the polynomial $\sum_{j=0}^{e-1} X^j$ precisely when $(i - h) \not\equiv 0 \pmod{e}$. The result follows. \hfill \Box

In order to get a representative homomorphism for the class $(\kappa^{(\chi^i)}) \in \text{Cl}(\mathbb{Z}[\Delta])$, we just need to take the norm of $v_i$, namely
\[
\mathcal{N}(v_i) = \mathcal{M}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(v_i)
\]
represents $(\kappa^{(\chi^i)})$ in $\text{Hom}_{\mathbb{Q}(\zeta)}(R_{\Delta}, J(\mathbb{Q}(\zeta)))$, see [18, Theorem 2]. Before recalling the definition of $\mathcal{M}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$, we introduce some notation and make a remark.
For any $\alpha \in (\mathbb{Z}/e\mathbb{Z})^\times$, let $\sigma_\alpha \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ be the automorphism defined by $\sigma_\alpha(\zeta) = \zeta^\alpha$. For any integer $n$, we let $\bar{n}$ denote its class modulo $e$, and we may write $\sigma_n$ instead of $\sigma_{\bar{n}}$ if $n$ is coprime with $e$.

**Remark 3.4.** The map $\alpha \mapsto \sigma_\alpha$ is a group isomorphism

$$\sigma : (\mathbb{Z}/e\mathbb{Z})^\times \to \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

which sends the subgroup $\langle \bar{p} \rangle$ to the decomposition subgroup of $p | p$ (see [19, §13.2, Corollary to Theorem 2]), specifically $p^{\sigma_\alpha} = p$. Hence, if $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$, we may denote by $p^{\sigma_\Lambda}$ the ideal associated with $\Lambda$. The prime ideals above $p$ in $\mathfrak{p}$ are exactly the conjugates $p^{\sigma_\Lambda}$ with $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$ and, for $\alpha \in (\mathbb{Z}/e\mathbb{Z})^\times$,

$$p^{\sigma_\alpha} = p^{\sigma_\Lambda} \iff \alpha \in \Lambda.$$  

By definition, one has

$$N(v_i)(\chi^h)_q = \left( \prod_k v_i((\chi^h)_e^{\sigma_k})^{-1} \right) = \prod_k (v_i(\chi^{hk})_{q^{\sigma_k}})^{\sigma_k^{-1}},$$

where the product runs over the integers $k$ such that $0 \leq k \leq e - 1$ and $k$ is coprime to $e$.

**Proposition 3.5.** For any place $q$ of $\mathfrak{o}$ and for any $0 \leq h \leq e - 1$, we have

$$N(v_i)(\chi^h)_q = \begin{cases} 1 & \text{if } q \nmid p, \\ p^{n(\Lambda, i, h)} & \text{if } q = p^{\sigma_\Lambda} \text{ for some } \Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle, \end{cases}$$

where we have set $n(\Lambda, i, h) = \#\{ \alpha \in \Lambda : \alpha \bar{i} = \bar{h} \}$. 

**Proof.** The case $q \nmid p$ follows immediately from the above, so we assume that $q = p^{\sigma_\Lambda}$ for some $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$. Then $q^{\sigma_k} = p$ if and only if $\bar{k}^{-1} \in \Lambda$, by (16). We conclude since, using Corollary 3.3,

$$v_i(\chi^{hk})_{q^{\sigma_k}} = \begin{cases} p & \text{if } \bar{k}^{-1} \in \Lambda, i \equiv hk \pmod{e}; \\ 1 & \text{otherwise}. \end{cases}$$

Since the Hom-description is an isomorphism, the class $(S) = \prod_{i=1}^{\frac{e-1}{2}} (\kappa(\chi^i))$ is represented in $\text{Hom}_{\Omega^0}(\mathcal{R}_\Delta, J(\mathbb{Q}(\zeta)))$ by the homomorphism $s = \prod_{i=1}^{\frac{e-1}{2}} N(v_i)$. We immediately get the following result.

**Corollary 3.6.** The representative morphism $s \in \text{Hom}_{\Omega^0}(\mathcal{R}_\Delta, J(\mathbb{Q}(\zeta)))$ of the class $(S)$ satisfies, for $0 \leq h \leq e - 1$:

$$s(\chi^h)_q = \begin{cases} 1 & \text{if } q \nmid p, \\ p^{\sum_{i=0}^{\frac{e-1}{2}} n(\Lambda, i, h)} & \text{if } q = p^{\sigma_\Lambda} \text{ for some } \Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle. \end{cases}$$

3.2.2. We compute the numbers $n(\Lambda, i, h)$ introduced above for $\Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$, $i, h \in \{0, \ldots, e - 1\}$. We extend the definition to $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle (p \text{ mod } e') \rangle$ for any divisor $e'$ of $e$, $i', h' \in \mathbb{Z}$, by setting:

$$n(\Lambda', i', h') = \#\{ \alpha' \in \Lambda' : \alpha'(i' \text{ mod } e') = (h' \text{ mod } e') \}.$$  

Of course $n(\Lambda', i', h')$ only depends on $\Lambda'$ and the residue classes $(i' \text{ mod } e')$ and $(h' \text{ mod } e')$ of $i'$ and $h'$ modulo $e'$. For any divisor $d$ of $e$, let $f_d$ denote the (multiplicative) order of $p$ modulo $d$ (thus $f_e = f$). The greatest common divisor of integers $a, b$ is denoted by $\gcd(a, b)$. 
Lemma 3.7. Let \( \Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times / \langle \bar{p} \rangle \), \( i, h \in \{0, \ldots, e-1\} \), then:

(i) \( n(\Lambda, i, h) \neq 0 \Rightarrow \gcd(i, e) = \gcd(h, e) \);
(ii) suppose \( \gcd(i, e) = \gcd(h, e) = d \) and set \( i = di', h = dh', e = de' \), one has

\[
n(\Lambda, i, h) = \begin{cases} f/f' & \text{if } (h' \mod e') \in (i' \mod e')\Lambda', \\ 0 & \text{otherwise}, \end{cases}
\]

where \( \Lambda' = (\Lambda \mod e') \in (\mathbb{Z}/e'\mathbb{Z})^\times / (\langle \bar{p} \mod e' \rangle) \).

Proof. Suppose \( n(\Lambda, i, h) \neq 0 \). Let \( \alpha \in \Lambda \) be such that \( \alpha \bar{a} = \bar{h} \) and let \( a \in \alpha \) (so \( a \in \mathbb{Z} \)), then \( ai \equiv h \pmod{e} \) and the equality \( \gcd(i, e) = \gcd(h, e) \) follows since \( \gcd(a, e) = 1 \).

We now assume the condition of assertion (ii) is satisfied and use the same notations. If \( d = e \), \( n(\Lambda, i, h) = n(\Lambda, 0, 0) = \#\Lambda = f = f/f_1 \) and \( 0 \notin 0'\Lambda' \) is always satisfied. Otherwise, \( \gcd(i', e') = 1 \) and one has, for any \( \alpha' \in (\mathbb{Z}/e'\mathbb{Z})^\times \):

\[
\alpha'(i' \mod e') = (h' \mod e') \iff \alpha' = (h' \mod e')(i' \mod e')^{-1} ,
\]
hence \( n(\Lambda', i', h') = 1 \) or 0 depending on whether \((h' \mod e')(i' \mod e')^{-1} \) belongs to \( \Lambda' \) or not. We thus only have to show that

\[
(17) \quad n(\Lambda, i, h) = \frac{f}{f'} n(\Lambda', i', h').
\]

As above, let \( \alpha \in \Lambda \) and \( a \in \alpha \). We may rewrite \( n(\Lambda, i, h) \) as

\[
n(\Lambda, i, h) = \#\{0 \leq k \leq f - 1 : a\bar{p}^k \bar{i} = \bar{h}\} \\
= \#\{0 \leq k \leq f - 1 : ap^k i \equiv h \pmod{e}\} \\
= \#\{0 \leq k \leq f - 1 : ap^k i' \equiv h' \pmod{e'}\} .
\]

Note that, if we set \( \alpha' = (\alpha \mod e') \), then \( a \in \alpha' \) and \( \alpha' \in \Lambda' \), hence, similarly:

\[
n(\Lambda', i', h') = \#\{0 \leq k \leq f'/e' - 1 : ap^k i' \equiv h' \pmod{e'}\} .
\]

The result follows since \( f/e' \) is the order of \( p \) in \((\mathbb{Z}/e'\mathbb{Z})^\times \).

3.3. The content of \( s \). In this subsection we compute the contents of the idèles \( \mathcal{N}(v_i)(\chi^h) \) and \( s(\chi^h) \) for \( 0 \leq i, h \leq e - 1 \). Recall that the content of an idèle \( x = (x_q)_q \in J(\mathbb{Q}(\zeta)) \) is the fractional ideal \( \text{cont}(x) = \prod_q q^{\text{val}_q(x_q)} \) of \( \mathbb{Q}(\zeta) \), where \( \text{val}_q \) is the \( q \)-valuation and the product runs over finite prime ideals \( q \) of \( \mathcal{O} \).

Since the valuation of \( p \) at a prime ideal \( q = p^{n_\Lambda} \) with \( \Lambda \in (\mathbb{Z}/e\mathbb{Z})^\times / \langle \bar{p} \rangle \) equals 1, it follows from Proposition 3.5 and Corollary 3.6 that

\[
(18) \quad \text{cont}(\mathcal{N}(v_i)(\chi^h)) = p^{\sum n(\Lambda, i, h)\sigma_\Lambda} \\
(19) \quad \text{cont}(s(\chi^h)) = p^{\sum_{i=0}^{e-1} n(\Lambda, i, h)\sigma_\Lambda}
\]

where in each sum \( \Lambda \) runs over \((\mathbb{Z}/e\mathbb{Z})^\times / \langle \bar{p} \rangle \).

3.3.1. Since \( \mathcal{N}(v_i) \) and \( s \) are \( \Omega_\mathbb{Q} \)-equivariant, their values on \( R_\Lambda \) are determined by the values at \( \chi^d \), with \( d \mid e \). Namely, if \( h \) is an integer and \( d \) is the greatest common divisor of \( h \) and \( e \), we write \( h = dh' \) and get

\[
(20) \quad \mathcal{N}(v_i)(\chi^h) = \mathcal{N}(v_i)(\chi^{dh'\sigma'}) = \mathcal{N}(v_i)(\chi^{dh})^{\sigma'}
\]

and analogously for \( s \).
For any $d \mid e$, write $e = de'$ and set $ζ_e' = ζ^d$ (thus $ζ_e = ζ$); for $α' \in (ℤ/e'ℤ)^×$, let $σ_{e',α'} \in \text{Gal}(Q(ζ_e')/Q)$ be the automorphism sending $ζ_e'$ to $ζ_e'$ (thus $σ_{e,α'} = σ_{α'}$). Since $e' \mid e$, $Q(ζ_e') \subseteq Q(ζ)$, hence $σ_{e',α'}$ can be lifted in $\text{Gal}(Q(ζ)/Q)$ (in $φ(ε)/φ(ε')$ different ways). To ease notation, if $j$ is an integer with $\text{gcd}(j,e') = 1$, we may write $σ_{e',j}$ instead of $σ_{e',(j \mod e')}$.

We also set $o_{e'} = ℤ[ζ_e']$ and $p_{e'} = p \cap o_{e'}$ (thus $o_e = o$ and $p_e = p$). If $α' \in (ℤ/e'ℤ)^×$, the ideal $p_{e'}^{σ_{e',α'}}$ only depends on the class of $α'$ modulo $(p \mod e')$. So if $Λ' \in (ℤ/e'ℤ)^×/((p \mod e'))$, we denote by $p_{e'}^Λ'$ the ideal $p_{e'}^{σ_{e',α'}}$ where $α'$ is any lift of $Λ'$ in $(ℤ/e'ℤ)^×$.

**Lemma 3.8.** Let $d \mid e$ and set $e = de'$. Let $Λ' \in (ℤ/e'ℤ)^×/((p \mod e'))$, then

$$\sum_{σ_Λ} p_{e'}^σ = p_{e'}^{σ_{Λ'}(ζ_e)}.$$ 

where the sum is on the elements $Λ$ of the coset $Λ'$ in $(ℤ/eℤ)^×/((p \mod e))$.

**Proof.** Let $Λ \in (ℤ/eℤ)^×/((p \mod e))$ and $Λ' \in (ℤ/e'ℤ)^×/((p \mod e'))$, then since $p \mid p_{e'}o$, 

$$Λ \ni Λ' \Rightarrow σ_{Λ_0(ζ_e')} = σ_{Λ'} \Rightarrow p^σ | p_{e'}^{Λ'}.$$

It follows that $p\sum_{σ_Λ} σ_Λ | p_{e'}^{Λ'}$. Since $Q(ζ)/Q(ζ_e')$ is unramified at $p_{e'}$, the number of primes above $p_{e'}$ in $o$ equals

$$\frac{ϕ(ε') \text{ ideals of } ℤ[ζ_e']}{f_{e'}} = \frac{#(ℤ/eℤ)^×/((p \mod e'))}{#(ℤ/e'ℤ)^×/((p \mod e'))} = Λ' \text{ (as a coset in } (ℤ/e'ℤ)^×/((p \mod e'))) \text{. The result follows.} \quad \square$$

**Proposition 3.9.** Let $d \mid e$ and set $e = de'$, then

$$\text{cont}(N(v_i)(χ^d)) = \begin{cases} o & \text{if } \text{gcd}(i,e) \neq d \\ p_{e'}^{σ_{e'}o_{e'}}^f & \text{if } \text{gcd}(i,e) = d \end{cases}$$

where $i = di'$ and $Λ' \in (ℤ/e'ℤ)^×/((p \mod e'))$ is such that $(i' \mod e')^{-1} \in Λ'_i$.

**Proof.** Since $\text{gcd}(d,e) = d$, the result is clear from (18) and Lemma 3.7 in the case $\text{gcd}(i,e) \neq d$, hence we now assume $\text{gcd}(i,e) = d$ and write $i = di'$. Then $i'$ and $e'$ are coprime so let $Λ' \in (ℤ/e'ℤ)^×/((p \mod e'))$ be such that $(i' \mod e')^{-1} \in Λ'$. From Lemma 3.7 we know that $n(Λ, i, d) = f_{e'}$ if $Λ \in Λ'_i$; otherwise, hence from (18) we get

$$\text{cont}(N(v_i)(χ^d)) = \frac{1}{f_{e'}} \sum_{σ_Λ} σ_Λ$$

and the result follows using Lemma 3.8. \quad \square

**Remark 3.10.** Using (20), it follows that, for every $i, h \in \{0, \ldots, e-1\}$, the ideal $\text{cont}(N(v_i)(χ^h))$ is either trivial or, if $\text{gcd}(i,e) = \text{gcd}(h,e) = d$, the extension to $o$ of an ideal of $o_{e'}(e' = e/d)$ whose absolute norm is congruent to 1 modulo $e$. (Indeed, by definition of $f_{e'}$, the absolute norm of $p_{e'}^{f_{e'}}$ and of its conjugates is $(p^f_{e'})^j = p^f$ which is congruent to 1 modulo $e$.)

3.3.2. Here we compute the content of $s$. For any divisor $e'$ of $e$, we denote by $Z_{e'}$ the subgroup of $(ℤ/e'ℤ)^×$ of elements congruent to 1 modulo $e'$, namely

$$Z_{e'} = \sigma^{-1}(\text{Gal}(Q(ζ)/Q(ζ_e'))).$$
where $\sigma : \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta')) \to (\mathbb{Z}/e\mathbb{Z})^\times$ is the isomorphism of Remark 3.4. Recall the definitions of the relative norm and Stickelberger's element:

$N_{e,e'} = \sum_{\alpha \in \mathbb{Z}_{e'}} \sigma_{\alpha} \in \mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta'))]$ ;

$\Theta_{e'} = \frac{1}{e'} \sum_{1 \leq j \leq e'-1 \atop (j,e') = 1} j\sigma_{e',j}^{-1} \in \mathbb{Q}[\text{Gal}(\mathbb{Q}(\zeta_e)/\mathbb{Q})]$ .

We need to introduce further elements in various group algebras. For any divisors $d$ and $e'$ of $e$, let

$H_{e'} = \{ \beta' \in (\mathbb{Z}/e'\mathbb{Z})^\times : \exists b \in \beta', \frac{e' + 1}{2} \leq b \leq e' - 1 \}$

and set

$H_{e,d} = \sum_{\alpha \in (\mathbb{Z}/e\mathbb{Z})^\times} \sum_{\alpha \in H_{e'}} \sigma_\alpha^{-1} \sum_{\beta \in \Lambda} \beta^{-1} \in \mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})]$ .

Note that $H_e = H_{e,1}$.

**Lemma 3.11.** Let $d \mid e$, then $\text{cont}(s(\chi^d)) = p^{H_{e,d}}$.

*Proof.* Rewrite $H_{e,d}$ as

$H_{e,d} = \sum_{\beta \in \Lambda} \sum_{\beta^{-1} \in \mathbb{H}_e} \sigma_\beta$ ,

where $\Lambda$ runs over $(\mathbb{Z}/e\mathbb{Z})^\times/\langle \bar{p} \rangle$. It follows that

$p^{H_{e,d}} = p^{\sum_{\beta \in \Lambda} \sum_{\beta^{-1} \in \mathbb{H}_e} \sigma_\beta} = \sum_{\beta \in \Lambda} \sum_{\beta^{-1} \in \mathbb{H}_e} \sigma_\beta$ .

But $\# \{ \beta \in \Lambda : \beta^{-1} \bar{d} \in \mathbb{H}_e \} = \sum_{i=1}^{\frac{e}{d}+1} n(\Lambda, i, d)$, which yields the result by (19). □

**Lemma 3.12.** Let $d \mid e$ and set $e = de'$, then

$H_{e,d} = H_{e'}N_{e,e'} \quad \text{and} \quad H_{e'} = (2 - \sigma_{e',2})\Theta_{e'}$ .

**Remark 3.13.** Note that the first equality is not ambiguous, even though it contains a slight abuse of notation: $H_{e'}$ belongs to $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta_e)/\mathbb{Q})]$ whereas $N_{e,e'}$ and $H_{e,d}$ belong to $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})]$. Nevertheless, if $\alpha' \in (\mathbb{Z}/e'\mathbb{Z})^\times$, then $\sigma_\alpha N_{e,e'}$ does not depend on the choice of a lift $\alpha$ of $\alpha'$ in $(\mathbb{Z}/e\mathbb{Z})^\times$. Indeed

$\sigma_\alpha N_{e,e'} = \sum_{\beta \in \mathbb{Z}_e} \sigma_{\alpha\beta}$

is the sum of all the lifts of $\sigma_{e',\alpha'}$ in $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Thus in order to get an equality in $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})]$, one just has to replace each term $\sigma_{e',\alpha'-1}N_{e,e'}$ of the sum $H_{e'}N_{e,e'}$ by $\sigma_{\alpha'-1}N_{e,e'}$, where $\alpha$ is any lift of $\alpha'$ in $(\mathbb{Z}/e\mathbb{Z})^\times$. 
Proof. We begin with the first equality. We suppose we have fixed a lift \( \alpha \in (\mathbb{Z}/e\mathbb{Z})^\times \) of each \( \alpha' \in (\mathbb{Z}/e'\mathbb{Z})^\times \). In view of the previous remark,

\[
H_{e'}N_{e,e'} = \sum_{\alpha' \in \mathcal{H}_{e'}} \sigma_{\alpha' \beta} = \sum_{\alpha' \in \mathcal{H}_{e'}} \sigma_{\alpha' \beta}^{-1},
\]

since \( \mathbb{Z}_{e'} \) is a subgroup of \( \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \). We are thus left to show that the map

\[
(\alpha', \beta) \in \mathcal{H}_{e'} \times \mathbb{Z}_{e'} \mapsto \alpha \beta \in \{ \gamma \in (\mathbb{Z}/e\mathbb{Z})^\times : \gamma \bar{d} \in \mathcal{H}_e \}
\]

is a well-defined one-to-one correspondence.

We first show that the if \( (\alpha', \beta) \in \mathcal{H}_{e'} \times \mathbb{Z}_{e'} \), then indeed \( \alpha \beta \in \{ \gamma \in (\mathbb{Z}/e\mathbb{Z})^\times : \gamma \bar{d} \in \mathcal{H}_e \} \). Of course \( \alpha \beta \in (\mathbb{Z}/e\mathbb{Z})^\times \), so we have to show that \( \alpha \beta \bar{d} \in \mathcal{H}_e \). Let \( a \in \alpha' \) be such that \( \frac{a + 1}{e} \leq a \leq \frac{e - 1}{e} \). Observe that \( ad \in \alpha \beta \bar{d} \). In fact since \( \beta \in \mathbb{Z}_{e'} \), there exists \( t \in \mathbb{Z} \) such that \( 1 + te' \in \beta \) and clearly

\[
ad \equiv \text{ad}(1 + te') \quad (\text{mod } e).
\]

Since clearly \( \text{ad}(1 + te') \in \alpha \beta \bar{d} \), we deduce \( \text{ad} \in \alpha \beta \bar{d} \). Now \( \frac{a + 1}{e} \leq \frac{e - 1}{e} \leq ad \leq e - d \leq e - 1 \), hence \( \alpha \beta \bar{d} \in \mathcal{H}_e \). Thus the map in (21) is well-defined.

To show that it is one-to-one, we define its inverse. Suppose \( \gamma \in (\mathbb{Z}/e\mathbb{Z})^\times \) is such that \( \gamma \bar{d} \in \mathcal{H}_e \). Since \( d \mid e \), there exists \( c \in \gamma \) such that \( \frac{a + 1}{e} \leq cd \leq e - 1 \), hence \( \frac{e - 1}{e} \leq c \leq 1 \). This shows that \( \alpha' = (c \mod e') \in (\mathbb{Z}/e'\mathbb{Z})^\times \) belongs to \( \mathcal{H}_{e'} \).

In particular \( \alpha' \) is the image of \( \gamma \) in \( (\mathbb{Z}/e'\mathbb{Z})^\times \). Since \( \alpha' \) is also the image of \( \alpha \) in \( (\mathbb{Z}/e'\mathbb{Z})^\times \), there exists a unique \( \beta \in \mathbb{Z}_{e'} \) such that \( \gamma = \alpha \beta \). It is clear that the map sending \( \gamma \) to \( (\alpha', \beta) \) is the inverse of (21).

We now show the second equality of the lemma. To simplify notations in this proof, we write \( \sigma_{\epsilon} \) instead of \( \sigma_{\epsilon,k} \). We note that \( \sigma_{\epsilon} = \sigma_{\epsilon + 1}^{-1} \) and compute

\[
e'(2 - \sigma_{\epsilon})\Theta_{e'} = \sum_{\frac{a + 1}{e} \leq \frac{e - 1}{e}} 2j\sigma_{j}^{-1} = \sum_{\frac{a + 1}{e} \leq \frac{e - 1}{e}} j\sigma_{j}^{-1}.
\]

Let \( j, j' \in \{ k \in \mathbb{Z} : 1 \leq k \leq e' - 1, (k, e') = 1 \} \), then \( j' \equiv \frac{a + 1}{e}j \mod e' \) if and only if \( j \equiv 2j' \mod e' \), hence the coefficient of \( \sigma_j^{-1} \) in the second sum above is \( 2j' \) if \( 1 \leq j' \leq \frac{e - 1}{2} \), \( 2j' - e' \) otherwise. Therefore

\[
e'(2 - \sigma_{\epsilon})\Theta_{e'} = e' \sum_{\frac{a + 1}{e} \leq \frac{e - 1}{e}} \sigma_{j}^{-1}
\]

and the result follows.

Combining Lemmas 3.11 and 3.12 yields:

**Proposition 3.14.** Let \( d \mid e \) and set \( e = de' \), then

\[
\text{cont}(s(\chi^d)) = p^{(2 - \sigma_{e'})(\Theta_{e'}N_{e,e'})}.
\]

4. **Explicit unit element**

This section is devoted to finding an explicit unit element associated to the class of \( S \) in \( \text{Cl}(\mathbb{Z}[\Delta]) \), yielding the proof of its triviality. We keep the notation introduced in the previous section.
4.1. A Jacobi sum to describe \((S)\).

4.1.1. We start introducing Jacobi sums associated to the residue fields of the intermediate extensions of \(\mathbb{Q}(\zeta)/\mathbb{Q}\). We denote by \(\mu_{\infty}\) the subgroup of roots of unity in \(\mathbb{Q}^{\times}\) and we let \(\zeta\) denote an element of order \(p\) of \(\mu_{\infty}\).

Let \(e'\) be any divisor of \(e\) and recall that \(\mathfrak{o}_{e'} = \mathbb{Z}[\zeta_{e'}]\) and \(\mathfrak{p}_{e'} = \mathfrak{p} \cap \mathfrak{o}_{e'}\) respectively denote the ring of integers and the prime ideal below \(\mathfrak{p}\) in the subfield \(\mathbb{Q}(\zeta_{e'})\) of \(\mathbb{Q}(\zeta)\). Let \(\theta, \theta'\) denote multiplicative characters of \(\mathfrak{o}_{e'}/\mathfrak{p}_{e'}\), namely homomorphisms \((\mathfrak{o}_{e'}/\mathfrak{p}_{e'})^\times \to \mu_{\infty}\), extended to \(\mathfrak{o}_{e'}/\mathfrak{p}_{e'}\) by the convention \(\theta(0) = \theta'(0) = 0\).

The Jacobi sum relative to \(\theta\) and \(\theta'\) is:

\[
J(\theta, \theta') = \sum_{x \in \mathfrak{o}_{e'}/\mathfrak{p}_{e'}} \theta(x) \theta'(1-x).
\]

We will mostly be concerned with the case where \(\theta = \theta' = \left(\frac{p}{\mathfrak{p}_{e'}}\right)^{-1}\) is the inverse of the \(e'\)th power residue symbol, and we set \(J_{e'} = J\left(\left(\frac{p}{\mathfrak{p}_{e'}}\right)^{-1}, \left(\frac{p}{\mathfrak{p}_{e'}}\right)^{-1}\right)\). Specifically, for any \(x \in (\mathfrak{o}_{e'}/\mathfrak{p}_{e'})^\times\), \(\left(\frac{x}{\mathfrak{p}_{e'}}\right)\) is the \(e'\)th root of unity defined by the congruence

\[
\left(\frac{x}{\mathfrak{p}_{e'}}\right) \equiv x^{e'\varphi(e')^{-1}} \pmod{\mathfrak{p}_{e'}}.
\]

One shows that \(J_{e'} \in \mathfrak{o}_{e'}\).

As it is well-known, the factorization of the Jacobi sum can be written in a nice way using the Stickelberger element. More precisely, we have the following classical result about the ideal of \(\mathfrak{o}_{e'}\) generated by \(J_{e'}\). For details and for a proof see for instance [19, Proposition 15.3.2 and its proof in Chapter 15].

**Theorem 4.1** (Stickelberger). One has \((2 - \sigma_{e', 2})\Theta_{e'} \in \mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})]\) and

\[
(J_{e'}) = \mathfrak{p}_{e'}^{(2 - \sigma_{e', 2})\Theta_{e'}}.
\]

4.1.2. In view of Proposition 3.14 we deduce, since \(\mathfrak{p}^{N_{e', e}} = \mathfrak{p}_{e'}^{f/f_{e'}}\), that the content of the representative homomorphism \(s\), evaluated at \(\chi^d\) with \(d \mid e\) and \(e = de'\), is the principal ideal given by:

\[
\text{cont}(s(\chi^d)) = \left(J_{e'}^{f/f_{e'}}\right).
\]

We now use the above generator of the content ideal to define an element \(c_s\) in \(\text{Hom}_{\mathbb{Q}}(\mathcal{R}_{\Delta}, \mathbb{Q}(\zeta)^\times)\). We shall multiply \(J_{e'}^{f/f_{e'}}\) by a suitable unit in order to ensure that \(sc_{e'}^{-1}\) lies in \(\text{Det}(\mathcal{U}(\mathbb{Z}[\Delta]))\). Let \(c_s\) denote the only homomorphism in \(\text{Hom}_{\mathbb{Q}}(\mathcal{R}_{\Delta}, \mathbb{Q}(\zeta)^\times)\) such that, for any \(d \mid e\),

\[
c_s(\chi^d) = -(-J_{e'})^{f/f_{e'}}
\]

where \(e = de'\).

The first step to our goal is easy. Let \(\mathcal{M}\) denote the maximal order in \(\mathbb{Q}[\Delta]\).

**Corollary 4.2.** The homomorphism \(sc_{e'}^{-1}\) represents the class \((S)\) and belongs to \(\text{Det}(\mathcal{U}(\mathcal{M}))\).
Proof. The first part of the assertion is immediate since $c_s^{-1}$ lies in the denominator of the Hom-description. Further it is clear from above that, for any divisor $d$ of $e$, one has the following equality of ideals:

$$(c_s(x^d)) = \text{cont}(s(x^d)) .$$

It follows that $(sc_s^{-1})_q$ takes unit values for every place $q$, namely $sc_s^{-1}$ belongs to $\text{Hom}_{\mathbb{Q}_q}(R_\Delta, U(\mathbb{Q}(\zeta)))$, which equals $\text{Det}(U(M))$ in view of [18, (1.2.19)], in which the $+$ sign disappears since the abelian group $\Delta$ has no symplectic character. □

The choice of signs in the above definition of $c_s$ enables us to show the following much stronger result which, together with Lemma 4.4 below, is a reformulation of Theorem 1.

**Theorem 4.3.** The homomorphism $sc_s^{-1}$ belongs to $\text{Det}(U(\mathbb{Z}[\Delta]))$. In particular $(S)$ is trivial in $\text{Cl}(\mathbb{Z}[\Delta])$.

**Proof.** First assume that $q \nmid e$ and let $q\cap\mathbb{Z} = q\mathbb{Z}$. One has $M_q(= M\otimes_{\mathbb{Z}}\mathbb{Z}_q) = \mathbb{Z}_q[\Delta]$ by [12, Proposition 27.1] and $M_{\mathbb{Q}} = \mathbb{R}[\Delta]$, so we get that $(sc_s^{-1})_q \in \text{Det}(\mathbb{Z}_q[\Delta]^\times)$ (recall that $Z_{\mathbb{Q}} = \mathbb{R}$) and we focus on the case $q \mid e$.

Recall from Corollary 3.6 that, when $q \mid e$,

$$(23) \quad (sc_s^{-1})_q = c_s^{-1} ,$$

where $c_s^{-1}$ is seen as a morphism with values in $\mathbb{Q}(\zeta)$, diagonally embedded in $J_q(\mathbb{Q}(\zeta)) = \prod_{q\mid q} \mathbb{Q}(\zeta)_q$.

For any $i = 0, \ldots, e-1$, set

$$A_i = \left\{ x \in \mathfrak{a}/p : \left( \frac{x}{p} \right)^{-1} \left( \frac{1-x}{p} \right)^{-1} = \zeta^i \right\}$$

and $n_i = \#A_i$, then

$$J_e = \sum_{i=0}^{e-1} n_i \zeta^i .$$

The main result is the following.

**Lemma 4.4.** Let $u_s = \sum_{i=0}^{e-1} n_i \delta^i \in \mathbb{Z}[\Delta]$. For any prime ideal $q$ of $\mathfrak{a}$ above a rational prime $q$ such that $q \mid e$, $u_s \in \mathbb{Z}_q[\Delta]^\times$, and

$$(sc_s^{-1})_q = \text{Det}(u_s^{-1}) \in \text{Det}(\mathbb{Z}_q[\Delta]^\times) .$$

**Proof.** We first show that, for any $d \mid e$

$$(24) \quad \text{Det}_{\mathfrak{a}^{(e)}(u_s)} = -(-J_{e'}J_{e_e})_{\mathfrak{f}^{(d)}e_{e_e}} ,$$

where $e = de'$ as usual. Thanks to the Davenport-Hasse theorem [19, Theorem 1 and Exercise 18 in Chapter 11]

$$(25) \quad (-1)^{f_{e_e}J_{e}J_{e_e}} = \sum_{x \in \mathfrak{a}/\mathfrak{p}}\left( \frac{N_{e,e'}(x)}{\mathfrak{p}_{e'}} \right)^{-d} \left( \frac{N_{e,e'}(1-x)}{\mathfrak{p}_{e'}} \right)^{-d} ,$$

where $N_{e,e'} : \mathfrak{a}/\mathfrak{p} \to \mathfrak{a}_{e'}/\mathfrak{p}_{e'}$ is the residual relative norm map. For any $x \in \mathfrak{a}/\mathfrak{p},$

$$\left( \frac{x}{p} \right)^d \equiv \left( \frac{x^{\nu'_{e_e}}}{x} \right)^d \equiv \left( \sum_{i=0}^{f_{e_e}J_{e}} \mathfrak{p}_{e'}^{ij_{e}} \right)^{\nu'_{e_e}-1} \equiv N_{e,e'}(x) \frac{1}{\mathfrak{p}_{e'}}^{i_{e_e}-1} \pmod{\mathfrak{p}} .$$
Thus
\[
\left( \frac{x}{p} \right)^d = \left( \frac{N_{e,e'}(x)}{p'} \right)
\]
and therefore
\[
-(J_{e'})^{-f/f} = \sum_{x \in \mathcal{O}/p} \left( \frac{x}{p} \right)^{-d} \left( \frac{1-x}{p} \right)^{-d} = \sum_{i=0}^{e-1} \sum_{x \in A_i} \zeta^i = \sum_{i=0}^{e-1} n_i \zeta^i = \text{Det}_{\chi}(u_s) .
\]
Assume that \( q \mid e \). For any divisor \( d \) of \( e \) (once again \( e = de' \)), we deduce from (23) and (24) that
\[
(s_{c_s}^{-1})_q = -(J_{e'})^{-f/f} = \text{Det}_{\chi}(u_s^{-1}) .
\]
The assertion of Corollary 4.2 implies that there exists \( w_q \in \mathcal{M}_q \times q \) such that
\[
(s_{c_s}^{-1})_q = \text{Det}(w_q) .
\]
It follows that \( \text{Det}(w_q) = \text{Det}(u_s) \), so by Proposition 3.1 we must have \( w_q = u_s \in \mathcal{M}_q \cap \mathbb{Z}_q[\Delta] = \mathbb{Z}_q[\Delta]^\times \) (see [23, Exercise 4, Section 25]).

We have shown that \( s_{c_s}^{-1} \in \text{Det}(U(\mathbb{Z}[\Delta])) \), namely \( s_{c_s}^{-1} \) lies in the denominator of the Hom-description of \( \text{Cl}(\mathbb{Z}[\Delta]) \) and thus \( (S) = 1 \). Further we can change \( s_{c_s}^{-1} \) by multiplying its \( q \)-component, whenever \( q \nmid e \), by its inverse (which also belongs to \( \text{Det}(\mathbb{Z}_q[\Delta]^\times) \)) if \( q \cap \mathbb{Z} = q \mathbb{Z} \), to get the representative of \( (S) \) announced in Theorem 1, whose proof is now complete.

5. THE CLASS OF THE SQUARE ROOT OF THE INVERSE DIFFERENT IN LOCALLY ABELIAN EXTENSIONS

In this section we put ourselves in the global setting described in the Introduction. In particular \( N/E \) is a tame \( G \)-Galois extension of number fields. When \( N/E \) is locally abelian and \( C_{N/E} \) is a square, Theorem 2, together with Taylor’s theorem, implies that \( (A_{N/E}) \in \text{Cl}(\mathbb{Z}[G]) \) is determined by the Artin root numbers of symplectic representations of \( G \) (see Corollary 5.2). Using this, one immediately deduces that \( (A_{N/E}) = 1 \) if \( N/E \) has odd degree (in fact this is true even without assuming that \( N/E \) is locally abelian by a result of Erez, [16, Theorem 3]) or is abelian. We will also prove that \( (A_{N/E}) = 1 \) if no real place of \( E \) becomes complex in \( N/E \). We will then show that this hypothesis is necessary. More precisely, in the case where \( G \) is the binary tetrahedral group, we will exhibit a totally complex tame \( G \)-Galois extension \( N/\mathbb{Q} \) such that \( C_{N/\mathbb{Q}} \) is a square and \( (A_{N/\mathbb{Q}}) \neq 1 \), thus proving Theorem 3. To explain how we found this example, we shall first verify that \( (A_{N/\mathbb{Q}}) = 1 \) if \( N/\mathbb{Q} \) is a tame locally abelian \( G \)-Galois extension such that \( C_{N/\mathbb{Q}} \) is a square and \( G \) is a group of order at most 24 which is not isomorphic to the binary tetrahedral group.

5.1. Root numbers of extensions unramified at infinity. In order to describe explicitly the relation between \( (A_{N/E}) \) and the Artin root numbers, we briefly recall some properties of these numbers and the definition of the Fröhlich–Cassou-Noguès class \( t_G W_{N/E} \in \text{Cl}(\mathbb{Z}[G]) \).
5.1.1. We will omit the definition of the root numbers and just recall some of their standard properties (see [21]). Let $\Gamma$ be a finite group and let $K/k$ be a $\Gamma$-extension of local or global fields of characteristic 0. Let $\chi : \Gamma \to \mathbb{C}$ be a complex virtual character and let $W(K/k,\chi) \in \mathbb{C}$ denote the root number of $\chi$. Then:

- if $\chi_1, \chi_2 : \Gamma \to \mathbb{C}$ are virtual characters, then
  
  $$W(K/k,\chi_1 + \chi_2) = W(K/k,\chi_1)W(K/k,\chi_2);$$

- if $\Gamma'$ is a subgroup of $\Gamma$, corresponding to the subextension $K/k'$, and $\phi : \Gamma' \to \mathbb{C}$ is a virtual character, then
  
  $$W(K/k,\text{Ind}^{\Gamma}_{\Gamma'}\phi) = W(K/k',\phi);$$

- if $\Gamma$ is a quotient of $\Gamma$, corresponding to the subextension $K/k'$, and $\phi : \Gamma \to \mathbb{C}$ is a virtual character, then
  
  $$W(K/k,\text{Inf}^{\Gamma}_{\Gamma'}\phi) = W(K'/k,\phi).$$

If $K/k$ is an extension of local fields, we have

$$W(K/k,\chi)W(K/k,\overline{\chi}) = \det_\chi(-1).$$

Here $\overline{\chi}$ denotes the conjugate character of $\chi$ and $\det_\chi : k^\times \to \mathbb{C}^\times$ is the map obtained by composing the determinant of $\chi$ with the local reciprocity map $k^\times \to \Gamma$.

If $K/k$ is an extension of number fields, there is a decomposition

$$W(K/k,\chi) = \prod_P W(K_P/k_P,\chi_{D_P}).$$

Here the product is taken over all places $P$ of $k$; for a such $P$, $\mathcal{P}$ is any fixed place of $K$ above $P$ and $\chi_{D_P}$ denotes the restriction of $\chi$ to the decomposition group $D_P$ of $\mathcal{P}$ (which we view as a character of $\text{Gal}(K_P/k_P)$).

5.1.2. We come back to the global setting where $N/E$ is a tame $G$-Galois extension of number fields. Let $S_G$ denote the group of symplectic characters, namely the free abelian group generated by the characters of the irreducible symplectic representations of $G$. Recall (see [26, Section 13.2], [21, III]) that an irreducible representation $\rho : G \to GL(V)$ on a complex vector space $V$ is called symplectic if $V$ admits a nontrivial $G$-invariant alternating bilinear form. Symplectic characters are real-valued and their degree is even. Moreover an irreducible character $\chi : G \to \mathbb{C}$ is symplectic if and only if its Frobenius-Schur indicator is $-1$:

$$\frac{1}{\#G} \sum_{g \in G} \chi(g^2) = -1.$$

Let $W_{N/E} \in \text{Hom}(S_G,\mathbb{C}^\times)$ be defined by $W_{N/E}(\theta) = W(N/E,\theta)$ for $\theta \in S_G$. As shown by Fröhlich, we actually have $W_{N/E} \in \text{Hom}_{\mathcal{O}_\mathbb{Q}}(S_G,\{\pm 1\})$ ([18, I, Proposition 6.2]).

Let $L'/\mathbb{Q}$ be a Galois extension containing all the values of the characters of $G$. We now recall the definition of the map

$$t_G : \text{Hom}_{\mathcal{O}_\mathbb{Q}}(S_G,\{\pm 1\}) \to \text{Cl}(\mathbb{Z}[G]),$$

which is due to Ph. Cassou-Noguès. One first defines a map

$$t'_G : \text{Hom}_{\mathcal{O}_\mathbb{Q}}(S_G,\{\pm 1\}) \to \text{Hom}_{\mathcal{O}_\mathbb{Q}}(R_G,J(L')).$$
as follows. Let $f \in \text{Hom}_{\mathbb{Q}_S}(S_G, \{\pm 1\})$ and let $\theta$ be an irreducible character of $G$. If $l$ is a place of $L'$, the idèle $t'_G(f)(\theta) \in J(L')$ has $l$-component

$$\tilde{f}(\theta)_l = \begin{cases} f(\theta) & \text{if } l \text{ is finite and } \theta \text{ is symplectic} \\ 1 & \text{otherwise.} \end{cases}$$

The map $t_G$ is then obtained by composing $t'_G$ with the projection

$$\text{Hom}_{\mathbb{Q}_S}(R_G, J(L')) \rightarrow \text{Cl}(\mathbb{Z}[G])$$

induced by the Hom-description (see Section 3.1).

The class $t_GW_{N/E}$ appears in the following celebrated result of M. Taylor ([31, Theorem 1]).

**Theorem 5.1** (M. Taylor). Let $N/E$ be a tame $G$-Galois extension of number fields. Then

$$(\mathcal{O}_N) = t_GW_{N/E} \quad \text{in } \text{Cl}(\mathbb{Z}[G]).$$

Combining the above theorem with Theorem 2 we get the following result.

**Corollary 5.2.** Let $N/E$ be a tame locally abelian $G$-Galois extension of number fields such that $C_{N/E}$ is a square. Then

$$(A_{N/E}) = t_GW_{N/E} \quad \text{in } \text{Cl}(\mathbb{Z}[G]).$$

In particular, if $G$ has no symplectic representations (for instance if $G$ is abelian or has odd order), then $(A_{N/E})$ is trivial.

5.1.3. We now want to prove that $(A_{N/E})$ is also trivial if $N/E$ is a tame locally abelian $G$-Galois extension which is unramified at infinite places, namely if real places of $E$ do not become complex in $N$. Under this assumption we will show that $W_{N/E}$ is in fact trivial and for this we need some results on symplectic characters, which we now recall.

We dispose of a useful induction theorem for symplectic characters which is due to Martinet (see [21, III, Theorem 5.1]). Before giving its statement, recall that an irreducible complex character of $G$ is said to be quaternionic if it has degree 2 and is lifted from a symplectic character of a quotient of $G$ isomorphic to the generalized quaternion group $H_{4n}$ for some $n \geq 2$. For every natural number $n \geq 2$, the quaternion group $H_{4n}$ of order $4n$ can be described by the following presentation

$$H_{4n} = \langle \sigma, \tau \mid \sigma^n = \tau^4, \tau^4 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle.$$  

**Theorem 5.3** (Martinet). A symplectic character of $G$ can be written as a $\mathbb{Z}$-linear combination of characters of the form $\text{Ind}_{H}^{G} \theta$ for some subgroups $H$ of $G$ where either

- $\theta = \psi + \overline{\psi}$ with $\psi : H \rightarrow \mathbb{C}$ an irreducible character of degree 1 or
- $\theta$ is a quaternionic character of $H$.

In order to use the above theorem, we will need some facts about generalized quaternions $H_{4n}$ and their complex characters. Note first that $\langle \sigma \rangle$ is normal in $H_{4n}$ since it has index 2. One easily sees that the maximal abelian quotient of $H_{4n}$ is $H_{4n}/\langle \sigma^2 \rangle$, which has order 4. Thus $H_{4n}$ has precisely four irreducible characters of degree 1. As for the remaining irreducible characters of $H_{4n}$, let $\varphi : \langle \sigma \rangle \rightarrow \mathbb{C}^\times$ be an injective homomorphism. Thus $\varphi$ can be also thought as an irreducible character of $\langle \sigma \rangle$ of degree 1. Using Mackey’s criterion ([26, Proposition 23]), it is easy to show that, if $1 \leq k \leq 2n - 1$ and $k \neq n$, then $\text{Ind}_{\langle \sigma \rangle}^{H_{4n}} \varphi^k$ is an irreducible character of
$G$ of degree 2. Computing explicitly the values $\text{Ind}_{(\sigma)}^{H_{4n}} \varphi^k$ (via [26, Théorème 12]), one finds that $\text{Ind}_{(\sigma)}^{H_{4n}} \varphi^k$ is always real-valued and

$$\text{Ind}_{(\sigma)}^{H_{4n}} \varphi^k = \text{Ind}_{(\sigma)}^{H_{4n}} \varphi^h$$

if and only if $\varphi^h = \overline{\varphi}^k$, i.e. $h = 2n - k$. Hence we have $n - 1$ distinct irreducible characters of degree 2 and a standard counting argument (see [26, Corollary 2 to Proposition 5]) shows that these, together with the four degree-one characters mentioned above, give the set of all irreducible complex characters of $H_{4n}$.

**Remark 5.4.** When $n = 2$, we recover the classical quaternion group $H_8$. For future use, we denote by $\psi_i$, $i = 1, 2, 3, 4$ the four one-dimensional characters (with $\psi_1$ denoting the trivial character) and by $\phi$ the two-dimensional irreducible character of $H_8$. It is well-known that $\phi$ is symplectic (this can be shown by computing its Frobenius-Schur indicator, using the explicit values of $\phi$ given for instance in [26, Exercice 3, Section 12.2]).

In the following lemma, which will be useful in the proof of the next proposition, we describe the abelian subgroups of $H_{4n}$ and the restriction to such subgroups of an irreducible character of $H_{4n}$ of degree 2.

**Lemma 5.5.** Let $\theta : H_{4n} \to \mathbb{C}$ be an irreducible character of degree 2. Let $H'$ be an abelian subgroup of $H_{4n}$. Then either

- $H' \subseteq \langle \sigma \rangle$ and there exists a character $\rho : H' \to \mathbb{C}$ of degree 1, such that $\text{Res}_{H'}^{H_{4n}} \theta = \rho + \overline{\rho}$ or
- $H'$ is cyclic of order 4, contains $\langle \tau^2 \rangle$ and $\text{Res}_{H'}^{H_{4n}} \theta = \text{Ind}_{\langle \tau^2 \rangle}^{H_{4n}} \rho$, where $\rho : \langle \tau^2 \rangle \to \mathbb{C}$ is a character of degree 1.

**Proof.** By the above discussion, we know that there exists a character $\chi : \langle \sigma \rangle \rightarrow \mathbb{C}$ of degree 1 such that $\theta = \text{Ind}_{\langle \sigma \rangle}^{H_{4n}} \chi$. Then we have (see [26, Proposition 22])

$$\text{Res}_{H'}^{H_{4n}} \theta = \text{Res}_{H'}^{H_{4n}} \text{Ind}_{\langle \sigma \rangle}^{H_{4n}} \chi = \sum_{s \in \mathcal{S}} \text{Ind}_{\langle \sigma \rangle}^{H_{4n}} \chi_s$$

where $\mathcal{S}$ is a set of representatives of $H' \setminus H_{4n} / \langle \sigma \rangle$ and, for $s \in \mathcal{S}$, $\chi_s : H' \cap \langle \sigma \rangle \rightarrow \mathbb{C}$ is the character defined by $\chi_s(x) = \chi(s^{-1}xs)$ for every $x \in H' \cap \langle \sigma \rangle$.

We now distinguish two cases. First suppose that $H' \subseteq \langle \sigma \rangle$, i.e. $H' \cap \langle \sigma \rangle = H'$. Then we can take $\mathcal{S} = \{\text{id}, \tau\}$ and $\chi_{\text{id}} = \text{Res}_{H'}^{H_{4n}} \chi$, $\chi_{\tau} = \text{Res}_{H'}^{H_{4n}} \chi$ (since $\chi(\tau^{-1}x\tau) = \chi(x^{-1}) = \chi(x)$ for $x \in H'$). Thus we can take $\rho = \text{Res}_{H'}^{H_{4n}} \chi$ to get the result.

Now suppose that $H' \not\subseteq \langle \sigma \rangle$. We first show that $H'$ contains $\langle \tau^2 \rangle$ and is cyclic of order 4. Let $x \in H'$ and $x \not\in \langle \sigma \rangle$. One easily sees that $x\sigma x^{-1} = \sigma^{-1}$, in particular $x$ acts as $-1$ on the cyclic group $H' \cap \langle \sigma \rangle$. Since $H'$ is abelian we also have $xyx^{-1} = y$ for every $y \in H' \cap \langle \sigma \rangle$. This shows that $H' \cap \langle \sigma \rangle$ is a subgroup of exponent 2 of $\langle \sigma \rangle$. Therefore we have $H' \cap \langle \sigma \rangle = \langle \tau^2 \rangle$. Note that $H' \cap \langle \sigma \rangle$ has index 2 in $H'$ because

$$4n = \#(H' \cdot \langle \sigma \rangle) = \#(\langle \sigma \rangle) \#(H') / \#(H' \cap \langle \sigma \rangle) = 2n \#(H') / \#(H' \cap \langle \sigma \rangle).$$

Hence $H'$ has order 4 and is cyclic since $\tau^2$ is the only element of order 2 in $H_{4n}$ (as it follows by an easy calculation using the presentation of $H_{4n}$ given in (28)). We now come to the character $\text{Res}_{H'}^{H_{4n}} \theta$. Since $H' \not\subseteq \langle \sigma \rangle$, we can choose the set of
We have to prove that

\[ \text{Proposition 5.6.} \]

is a square if and only if the inertia subgroups all have odd order.

Recall from the Introduction that in a tame Galois extension the inverse different is a square if and only if the inertia subgroups all have odd order.

**Proposition 5.6.** Let \( N/E \) be a tame locally abelian Galois extension of number fields whose inverse different is a square. Suppose moreover that no archimedean place of \( E \) ramifies in \( N \) (i.e. real places stay real). Then \( W_{N/E} = 1 \).

**Proof.** We have to prove that \( W(N/E, \chi) = 1 \) for every symplectic character \( \chi \) of \( G \). Thanks to Theorem 5.3, \( \chi \) can be written as

\[ \chi = \sum_{H \leq G} n_H \text{Ind}_{H}^{G} \theta_H \]

where \( n_H \in \mathbb{Z} \) and \( \theta_H : H \rightarrow \mathbb{C} \) is either a quaternionic character of \( H \) or can be written as \( \theta_H = \psi + \overline{\psi} \) for some irreducible character \( \psi : H \rightarrow \mathbb{C} \) of degree 1. Thanks to the properties of the Artin root number recalled in §5.1.1, we have

\[ W(N/E, \chi) = \prod_{H \leq G} W(N/N^H, \theta_H)^{n_H}. \]

Of course, to prove that \( W(N/E, \chi) = 1 \) it is sufficient to prove that \( W(N/N^H, \theta_H) = 1 \) for every subgroup \( H \leq G \). Observe that, for every subgroup \( H \leq G \), \( N/N^H \) is a tame locally abelian extension whose inverse different is a square (since its inertia subgroups have odd order) and no archimedean place of \( N^H \) ramifies in \( N \) (in other words \( N/N^H \) satisfy the hypotheses of the proposition). Therefore, replacing if necessary \( G \) by one of its subgroup \( H \) and \( N/E \) by \( N^H/E \), it suffices to show that \( W(N/E, \theta) = 1 \) where \( \theta : G \rightarrow \mathbb{C} \) is either a quaternionic character of \( G \) or \( \theta = \psi + \overline{\psi} \) for some irreducible character \( \psi : G \rightarrow \mathbb{C} \) of degree 1.

Suppose first that \( \theta \) is quaternionic. In particular, for some \( n \geq 2 \), there exists a surjection \( G \rightarrow H_n \) and a symmetric character \( \theta' : H_n \rightarrow \mathbb{C} \) such that \( \theta = \text{Ind}_{H_n}^{G} \theta' \) (in particular \( \theta' \) is irreducible). Then, if \( N/N' \) is the subextension corresponding to the kernel of \( G \rightarrow H_n \) (thus \( H_n \cong \text{Gal}(N'/E) \)), we have \( W(N/E, \theta) = W(N'/E, \theta') \). So we are reduced to show that \( W(N'/E, \theta') = 1 \). Note that \( \theta' \) has degree 2 (see the list of irreducible characters of \( H_n \) given in §5.1.3). By (27), it is sufficient to show that, for every place \( P \) of \( E \), we have \( W(N'/E_P, \theta'_{D_P}) = 1 \), where \( \theta'_{D_P} \) denotes the restriction of \( \theta' \) to the decomposition group \( D_P \) of a fixed place \( P \) of \( N' \) above \( P \). Note that \( N'/E \) is locally abelian since \( N/E \) is. In particular \( D_P \) is abelian and by Lemma 5.5 we have either

(a) \( \theta'_{D_P} = \rho + \overline{\rho} \) for some character \( \rho : D_P \rightarrow \mathbb{C} \) of degree 1 or
(b) \( D_P \) is cyclic of order 4, contains \( \langle \tau^2 \rangle \) and \( \theta'_{D_P} = \text{Ind}_{\langle \tau^2 \rangle}^{D_P} \rho \) for some character \( \rho : \langle \tau^2 \rangle \rightarrow \mathbb{C} \) of degree 1.

In case (a), by (26) we have

\[ W(N'_P/E_P, \theta'_{D_P}) = W(N'_P/E_P, \rho)W(N'_P/E_P, \overline{\rho}) = \det_{\exists}(-1). \]

Let \( r_P : E_P^\times \rightarrow D_P \) denote the local reciprocity map so that \( \rho \circ r_P = \det_{\rho} \) (since \( \rho \) has degree 1). If \( P \) is archimedean, then \( N'_P/E_P \) is trivial by hypothesis and in particular \( r_P(-1) = 1 \) and \( \det_{\rho}(-1) = 1 \). If instead \( P \) is a finite place, then, by
class field theory, \( r_p(-1) \) belongs to the inertia subgroup \( I_P \) of \( \mathcal{P} \) in \( N'/E \), since \(-1\) is a unit of \( E_P \). In particular, \( r_p(-1)^{e_P} = 1 \) and \( e_P = \# I_P \) is odd (\( N'/E \) has inertia subgroups of odd order since the same holds for \( N/E \)). But we also have \( r_p(-1)^2 = 1 \) and therefore \( r_p(-1) = 1 \), which implies that \( \det r_p(-1) = 1 \) also in this case.

In case (b), if \( \rho \) is trivial, then \( W(N'_P/E_P, \theta'_\sigma) = W(N'_P/E'_P, \rho) = 1 \) (here \( N'_P/E'_P \) is the subextension corresponding to \( \langle \tau^2 \rangle \subset D_P \)). If instead \( \rho \) is nontrivial (i.e. \( \rho \) is the sign character of \( \langle \tau^2 \rangle \)), then one easily sees that \( \theta'_\sigma = \text{Ind}_{Z}^{D_P}(\nu) = \nu + P \), where \( \nu : D_P \to \mathbb{C}^\times \) is a character of order 4. Thus we conclude as in case (a).

The case where \( \theta = \psi + \overline{\psi} \) for some irreducible character \( \psi : H \to \mathbb{C}^\times \) is also similar to the above case (a).

Remark 5.7. Let \( \mathcal{P} \) be a non-real archimedean place of \( N \) and suppose that \( \mathcal{P} \) lies above a real place \( P \) of \( E \). Then \( E_P = \mathbb{R} \) and \( N_P = \mathbb{C} \) and the reciprocity map \( r_P : \mathbb{R}^\times \to \text{Gal}(\mathbb{C}/\mathbb{R}) \) is nontrivial on \(-1\) (in fact \( \text{Ker}(r_P) = \{ x \in \mathbb{R}^\times, x > 0 \} \)). For this reason the arguments of the proof of the above proposition do not apply in the case where real places of \( E \) are allowed to become complex in \( N \). In fact, as we shall see, the hypothesis on real places of Proposition 5.6 is necessary.

Combining Proposition 5.6 with Corollary 5.2 and Theorem 2, we get the following result.

**Theorem 5.8.** Let \( N/E \) be a tame locally abelian \( G \)-Galois extension of number fields whose inverse different is a square. Suppose moreover that no archimedean place of \( E \) ramifies in \( N \). Then

\[
(\mathcal{A}_{N/E}) = (\mathcal{O}_N) = 1
\]

in \( \text{Cl}(\mathbb{Z}[G]) \).

### 5.2. An inverse different whose square root has nontrivial class.

In this section we will exhibit a group \( G \) and a tame locally abelian \( G \)-Galois extension \( N/Q \) whose inverse different is a square and \((\mathcal{A}_{N/Q}) \neq 1 \) in \( \text{Cl}(\mathbb{Z}[G]) \). The first step is to find a good candidate for the group \( G \), which we would also like to be of smallest possible order. For this reason, we deduce some conditions \( G \) has to satisfy in order for an extension with the above properties to exist.

**Lemma 5.9.** Suppose that \( N/Q \) is a tame locally abelian \( G \)-Galois extension whose inverse different is a square and \((\mathcal{A}_{N/Q}) \neq 1 \) in \( \text{Cl}(\mathbb{Z}[G]) \). Then

(i) \( G \) is generated by elements of odd order;

(ii) \( G \) has an irreducible symplectic representation.

**Proof.** Since \( Q \) has no nontrivial extension unramified at every finite prime, \( G \) is generated by the inertia subgroups of finite primes. As recalled before Proposition 5.6, these subgroups have odd order in our situation. Furthermore, if \( G \) has no symplectic representation, then \((\mathcal{A}_{N/Q}) = 1 \) by Corollary 5.2.

5.2.1. We now show that there is no group of order smaller than 24 satisfying properties (i) and (ii) of Lemma 5.9.

**Lemma 5.10.** Let \( H \) be a group. Then the following are equivalent:

- \( H \) has no proper normal subgroup of index a power of 2;
- \( H \) is generated by elements of odd order.
Proof. Let $H'$ be the subgroup generated by the elements of odd order of $H$. Then $H'$ is normal and it is easy to see that $H/H'$ has order a power of 2. Moreover it is clear that $H'$ is contained in every normal subgroup of $H$ of index a power of 2. This shows the equivalence in the statement. $\square$

Lemma 5.11. Let $H$ be a group of order 20. Then $H$ is not generated by elements of odd order.

Proof. Let $a$ be the number of Sylow 5-subgroups of $H$. Then using Sylow’s theorems we know that $a$ divides 4 (the index of a Sylow 5-subgroup in $H$) and $a \equiv 1 \pmod{5}$. So there is only one Sylow 5-subgroup which is normal and has index 4. We conclude using Lemma 5.10. $\square$

We shall use the following fact in the proof of the next result.

Remark 5.12. Let $\rho : G \to GL(V)$ be an irreducible symplectic representation on a complex vector space $V$ of dimension $2m$. By scalar restriction, $\rho$ defines a real representation $V_R$ of $G$, of dimension $4m$. The commuting algebra

$$D = \{ f \in \text{End}(V_R) : f \text{ is } G\text{-invariant} \}$$

clearly contains $\mathbb{C}$ (i.e. scalar multiplications by elements of $\mathbb{C}$) and is in fact isomorphic to the division algebra of quaternions $\mathbb{H}$ (see [26, Remarque 2, §13.2]). Thus $V$ becomes a $\mathbb{H}$-vector space of dimension $m$, which we denote by $V_\mathbb{H}$, and we get a homomorphism $\rho_\mathbb{H} : G \to GL(V_\mathbb{H})$ which fits in a commutative diagram

$$\begin{array}{ccc}
G & \xrightarrow{\rho} & GL(V) \\
\downarrow \rho_\mathbb{H} & & \uparrow \\
GL(V_\mathbb{H}) & & &
\end{array}$$

Proposition 5.13. Let $H$ be a group of order less than 24 which is generated by elements of odd order. Then $H$ has no irreducible symplectic representations.

Proof. We shall use that for any irreducible representation $\rho$ of $H$, we have $\deg \rho | \#H$ and $\deg \rho \leq 4$ since $(\deg \rho)^2 \leq \#H < 24$.

We prove the proposition arguing by contradiction. Suppose $H$ has an irreducible symplectic representation $\rho_\mathbb{H} : H \to GL_2(\mathbb{C})$. Then $d = \deg \rho_\mathbb{H}$ is even, so that $\#H$ must be even and $d$ is either 2 or 4.

Suppose that $d = 4$, then $\#H \geq d^2 = 16$ and $d = 4 | \#H$. This implies that $\#H = 16$ or 20. The first possibility is trivially excluded, while the second is ruled out by Lemma 5.11.

Then we must have $d = 2$. By Remark 5.12, this implies that $\rho_\mathbb{H}$ factors through an homomorphism $\rho_\mathbb{H} : H \to \mathbb{H}_\times \subseteq GL_2(\mathbb{C})$. In particular $H$ has a quotient $\tilde{H}$ isomorphic to a finite subgroup of $\mathbb{H}_\times$. The finite subgroups of $\mathbb{H}_\times$ are well-known (see for instance [13, p. 305]): since $\#\tilde{H} < 24$, $\tilde{H}$ is either cyclic or generalized quaternion. On the one hand, $\tilde{H}$ cannot be cyclic, since otherwise $\rho_\mathbb{H}$ would be the inflation of a representation of a cyclic group and would not be irreducible since $d = 2$. On the other hand, $\tilde{H}$ cannot be isomorphic to $H_{2n}$ for any $n \geq 2$, since otherwise $\tilde{H}$ (and hence $H$) would have a subgroup of index 2 ($\langle \sigma \rangle$ has index 2 in $H_{4n}$, with notation as in §5.1.3), which is forbidden by Lemma 5.10. $\square$
5.2.2. We now recall the definition and some properties of the binary tetrahedral group \( \hat{A}_4 \). We will then show that \( \hat{A}_4 \) is the only group of order 24 satisfying property (i) of Lemma 5.9 (we will see in §5.2.3 that it also satisfies property (ii)). We refer the reader to [24, Section 8.2] for any unproven assertion concerning \( \hat{A}_4 \). This group is isomorphic to \( S\mathbb{L}_2(F_3) \) and can be presented as

\[
A_4 = \langle \alpha, \beta \mid \alpha^3 = \beta^3 = (\alpha\beta)^2 \rangle.
\]

The center \( Z(\hat{A}_4) = \langle \alpha^3 \rangle \) is the only subgroup of order 2 of \( \hat{A}_4 \) and \( \hat{A}_4/Z(\hat{A}_4) \) is isomorphic to \( A_4 \), the alternating group on four letters. We thus have an exact sequence

\[
1 \to Z(\hat{A}_4) \to \hat{A}_4 \to A_4 \to 1.
\]

Moreover, \( \hat{A}_4 \) has no subgroup of index 2: in particular, thanks to Lemma 5.10, it satisfies property (i) of Lemma 5.9 (and the above exact sequence is non-split).

The group \( A_4 \) has other properties which will be useful later: every subgroup of \( A_4 \) is cyclic, except for its Sylow 2-subgroup, which is normal and isomorphic to the quaternion group \( H_8 \). For simplicity we will denote the Sylow 2-subgroup of \( A_4 \) by \( H_4 \). In fact, \( A_4 \) is also isomorphic to \( H_8 \times \mathbb{Z}/3\mathbb{Z} \) where \( \eta : \mathbb{Z}/3\mathbb{Z} \to \text{Aut}(H_8) \cong S_4 \) is any nontrivial homomorphism and \( S_4 \) is the permutation group on four elements.

**Remark 5.14.** The extension (29) is a representation group for \( A_4 \), in the sense of Schur, as we now recall. Let \( \hat{H} \) be a finite group and let \( M(H) \) denote its Schur multiplier (thus \( M(H) = H^2(H, \mathbb{C}^\times) \cong H_2(H, \mathbb{Z}) \), see [27, Definition 9.6, Chapter 2]). A representation group for \( H \) (see [27, Definition 9.10, Chapter 2]) is a central extension of \( H \) by a group \( Z \)

\[
1 \to Z \to \hat{H} \to H \to 1
\]

such that

- (RG1) \( \hat{H} \) has no proper subgroup \( H' \) such that \( \hat{H} = H'Z \);
- (RG2) \( \#M(H) = \#(Z \cap [\hat{H}, \hat{H}]) \), where \([\hat{H}, \hat{H}]\) denotes the commutator subgroup of \( \hat{H} \);
- (RG3) \( \#\hat{H} = \#H \cdot \#M(H) \).

One can show that if the above properties are satisfied, then \( Z \cong M(H) \) (see [27, (9.15), Chapter 2]). Schur showed that \( M(A_4) \) has order 2 (see [27, (2.22), Chapter 3]) and it is easy to check that the extension (29) is indeed a representation group for \( A_4 \). In fact, Schur also showed that the extension (29) is the only representation group for \( A_4 \) up to isomorphism (see [27, Exercise 5, Chapter 2, §9]). One often says briefly that \( \hat{A}_4 \) is the representation group of \( A_4 \).

**Proposition 5.15.** A group of order 24 which is generated by elements of odd order is isomorphic to \( \hat{A}_4 \).

**Proof.** Let \( \hat{H} \) be a group of order 24 which is generated by elements of odd order. We will first prove that the center \( Z(\hat{H}) \) of \( \hat{H} \) has order 2 and \( \hat{H} \) fits into an exact sequence

\[
1 \to Z(\hat{H}) \to \hat{H} \to A_4 \to 1.
\]

The second step will consist in showing that the above sequence is a representation group for \( A_4 \), which implies in particular that \( \hat{H} \) is isomorphic to \( \hat{A}_4 \) by Remark 5.14.
In order to prove the first step, we argue as in the proof of Lemma 5.11. Let \( a \) be the cardinality of the set of Sylow 3-subgroups of \( \tilde{H} \). Then, by Sylow’s theorems, \( a \) divides 8 (the index of any Sylow 3-subgroup of \( \tilde{H} \)) and \( a \equiv 1 \mod 3 \). Moreover the case \( a = 1 \) is excluded by Lemma 5.10, hence \( a = 4 \).

Since conjugation permutes the Sylow 3-subgroups of \( \tilde{H} \), we get a homomorphism \( \varphi : \tilde{H} \to S_4 \) and we want to determine \( \# \ker(\varphi) \). Observe that \( \ker(\varphi) \) is contained in the normalizer of any Sylow 3-subgroup of \( \tilde{H} \), which has index \( a = 4 \). Thus \( \# \ker(\varphi) \) divides 6. Since \( \ker(\varphi) \) is normal, \( \# \ker(\varphi) \) is not divisible by 3, otherwise \( \tilde{H} \) would have a normal subgroup of index a power of 2, which is impossible by Lemma 5.10. The case \( \# \ker(\varphi) = 1 \) is also excluded because otherwise \( \tilde{H} \cong S_4 \) and \( S_4 \) has a subgroup of index 2 (namely \( A_4 \)), again contradicting Lemma 5.10.

Thus \( \ker(\varphi) \) is a normal subgroup of order 2 of \( \tilde{H} \) and \( \tilde{H}/\ker(\varphi) \cong A_4 \), in other words \( \tilde{H} \) fits into an exact sequence

\[ 1 \to \ker(\varphi) \to \tilde{H} \to A_4 \to 1. \]

Of course \( \ker(\varphi) \) is contained in \( Z(\tilde{H}) \), being a normal subgroup of order 2. Furthermore the image of \( Z(\tilde{H}) \) in \( A_4 \) is trivial since \( Z(A_4) \) is trivial. Hence \( \ker(\varphi) = Z(\tilde{H}) \) and we get (30), completing the first step of the proof.

To prove the second step, we have to show that (30) satisfies the properties of a representation group for \( A_4 \) (see Remark 5.14). Let \( \tilde{H}' \) be a subgroup of \( \tilde{H} \) such that \( \tilde{H}'Z(\tilde{H}) = \tilde{H} \). Then, since \( Z(\tilde{H}) \) is normal in \( \tilde{H} \), we have

\[ \# \tilde{H}' = \frac{\# \tilde{H} \cdot (\# \tilde{H}' \cap Z(\tilde{H}))}{\# Z(\tilde{H})} = 12 \cdot (\# \tilde{H}' \cap Z(\tilde{H})) . \]

Thus \( \# \tilde{H}' \) is either 12 or 24. The case \( \# \tilde{H}' = 12 \) being excluded by Lemma 5.10, we deduce \( \tilde{H} = \tilde{H}' \), i.e. \( \tilde{H} \) satisfies property (RG1).

Observe now that the surjection \( \tilde{H} \to A_4 \) induces a surjection \( [\tilde{H}, \tilde{H}] \to [A_4, A_4] \) on commutator subgroups, whose kernel is \( Z(\tilde{H}) \cap [\tilde{H}, \tilde{H}] \). In particular

\[ 4 = \# [A_4, A_4] = \frac{\# [\tilde{H}, \tilde{H}]}{\# (Z(\tilde{H}) \cap [\tilde{H}, \tilde{H}])} . \]

This shows that \( \# [\tilde{H}, \tilde{H}] \) is either 8 or 4, according to whether \( Z(\tilde{H}) \cap [\tilde{H}, \tilde{H}] = Z(\tilde{H}) \) or not. We claim that \( \# [\tilde{H}, \tilde{H}] \) cannot be 4. For, if \( \# [\tilde{H}, \tilde{H}] = 4 \), then \( \tilde{H} \) has a quotient of order 6 and hence also a subgroup of index 2, which is a contradiction by Lemma 5.10. Thus \( \# [\tilde{H}, \tilde{H}] = 8 \) and \( Z(\tilde{H}) \cap [\tilde{H}, \tilde{H}] = Z(\tilde{H}) \), so that \( \tilde{H} \) satisfies (RG2).

Finally since \( \# Z(\tilde{H}) = 2 = \# M(A_4) \), \( \tilde{H} \) also satisfies (RG3) and hence (30) is a representation group for \( A_4 \). In particular by Schur’s uniqueness result recalled in Remark 5.14, \( \tilde{H} \cong A_4 \). \( \Box \)

5.2.3. We now want to verify that \( \tilde{A}_4 \) also satisfies property (ii) of Lemma 5.9. We first recall the list and some properties of the irreducible complex characters of \( \tilde{A}_4 \).

We start with the group \( A_4 \), which has four irreducible complex characters. Three have degree 1 and are inflated from characters of the maximal abelian quotient of \( A_4 \) (which is cyclic of order 3), while the remaining one has degree 3 and is real. Inflating these characters to \( \tilde{A}_4 \), we get three characters \( \chi_1, \chi_2 \) and \( \chi_3 \) of degree 1 (one of these, say \( \chi_1 \), is the trivial character, the other two are non-real) and a real character \( \chi_4 \) of degree 3. Now \( \tilde{A}_4 \) has seven conjugacy classes (see [24,
Lemma 5.16. We have complex characters (see [26]). We are going to use some standard notation and results on $\chi$. We first describe the induction of an irreducible character of $A_4$ where

\[
\text{Ind}_{H_8}^A \psi_1 = \chi_1 + \chi_2 + \chi_3 ,
\]

\[
\text{Ind}_{H_8}^A \psi_i = \chi_4 \quad \text{for } i = 2, 3, 4 ,
\]

\[
\text{Ind}_{H_8}^A \phi = \chi_5 + \chi_6 + \overline{\chi_6} .
\]

Proof. We can write

\[
\text{Ind}_{H_8}^A \psi_1 = \sum_{j=1}^{7} (\text{Ind}_{H_8}^A \psi_1, \chi_j)_{A_4} \chi_j ,
\]

where $(\text{Ind}_{H_8}^A \psi_1, \chi_j)_{A_4} \geq 0$ for any $1 \leq j \leq 7$, since $\text{Ind}_{H_8}^A \psi_1$ is the character of a representation of $A_4$. Taking degrees, we get

\[3 = [A_4 : H] \deg \psi_1 = \deg \text{Ind}_{H_8}^A \psi_1 = \sum_{j=1}^{7} (\text{Ind}_{H_8}^A \psi_1, \chi_j)_{A_4} \deg \chi_j .\]

Moreover, by definition, $\chi_1$, $\chi_2$ and $\chi_3$ are trivial on $H_8$. Therefore, if $j \in \{1, 2, 3\}$, then $\text{Res}_{H_8}^{A_4} \chi_j = \psi_1$ and, by Frobenius reciprocity,

\[
(\text{Ind}_{H_8}^A \psi_1, \chi_j)_{A_4} = (\psi_1, \text{Res}_{H_8}^{A_4} \chi_j)_{H_8} = 1 \quad \text{for } j = 1, 2, 3.
\]

Then $(\text{Ind}_{H_8}^A \psi_1, \chi_j)_{A_4} = 0$ if $4 \leq j \leq 7$ and we get the first equality of the lemma.

Next we show the second equality. We fix $i \in \{2, 3, 4\}$. It is sufficient to show that $\text{Ind}_{H_8}^A \psi_i$ is irreducible, since it has degree 3 and $\chi_4$ is the only irreducible character of $A_4$ of degree 3. To prove that $\text{Ind}_{H_8}^A \psi_i$ is irreducible, we shall use Mackey’s irreducibility criterion (see [26, Proposition 23]). Since $H_8$ is normal in $\tilde{A}_4$, we have to check that, for every $g \in \tilde{A}_4 \setminus H_8$, $\psi_i$ is different from the representation $\psi_{1}^{g} : H_8 \to \mathbb{C}^\times$ defined by $\psi_{1}^{g}(x) = \psi_{1}(g^{-1} x g)$ for every $x \in H_8$. Observe that the kernel of $\psi_i$ has order 4 and therefore is not normal in $\tilde{A}_4$ (see §5.2.2). We deduce that the normalizer of $\ker \psi_i$ in $\tilde{A}_4$ is $H_8$. Hence, for every $g \in \tilde{A}_4 \setminus H_8$, there exists $y \in \ker \psi_i$ such that $g^{-1} y y \not\in \ker \psi_i$ and in particular $\psi_{1}^{g}(y) = \psi_{1}(g^{-1} y y) \neq 1$. Thus
\psi_i \text{ is trivial on } y, \text{ while } \psi_i'' \text{ is not. Thus, for every } g \in \tilde{A}_4 \setminus H_8, \psi_i'' \neq \psi_i \text{ and hence } \text{Ind}_{H_8}^\tilde{A}_4 \psi_i \text{ is irreducible and equals } \chi_4.

To prove the last equality of the lemma, let \chi_{\mathfrak{n}_8} \text{ and } \chi_{\tilde{A}_4} \text{ be the characters of the regular representation of } H_8 \text{ and } \tilde{A}_4, \text{ respectively (in particular } \text{Ind}_{H_8}^\chi_{\mathfrak{n}_8} = \chi_{\tilde{A}_4}). \text{ Then we have}

\begin{align*}
\chi_{\mathfrak{n}_8} &= \psi_1 + \psi_2 + \psi_3 + \psi_4 + 2\phi, \\
\chi_{\tilde{A}_4} &= \chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 2\chi_5 + 2\chi_6 + 2\chi_7.
\end{align*}

Using the first two equalities of the statement of the present lemma, we deduce that

\begin{align*}
\chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 2\text{Ind}_{H_8}^\chi_{\mathfrak{n}_8} &= \text{Ind}_{H_8}^\chi_{\mathfrak{n}_8} \\
&= \chi_{\tilde{A}_4} \\
&= \chi_1 + \chi_2 + \chi_3 + 3\chi_4 + 2\chi_5 + 2\chi_6 + 2\chi_7
\end{align*}

and therefore \text{Ind}_{H_8}^\chi_{\mathfrak{n}_8} = \chi_5 + \chi_6 + \chi_7. \quad \Box

**Proposition 5.17.** The only irreducible symplectic character of \( \tilde{A}_4 \) is \( \chi_5 \).

**Proof.** Observe first that if \( i \neq 5 \), then \( \chi_i \) is not symplectic because either it has odd degree or it takes non real values. So we are left to prove that \( \chi_5 \) is symplectic. We will use that an irreducible representation is symplectic if and only if its Frobenius-Schur indicator is \(-1\) (see [26, Proposition 38]). So we have to prove that

\[ \frac{1}{24} \sum_{g \in \tilde{A}_4} \chi_5(g^2) = -1. \]

Thanks to Lemma 5.16 we have

\[ \frac{1}{24} \sum_{g \in \tilde{A}_4} \chi_5(g^2) = \frac{1}{24} \sum_{g \in \tilde{A}_4} (\text{Ind}_{H_8}^\chi_{\mathfrak{n}_8})(g^2) - \frac{1}{24} \sum_{g \in \tilde{A}_4} \chi_6(g^2) - \frac{1}{24} \sum_{g \in \tilde{A}_4} \chi_6(g^2). \]

The terms involving \( \chi_6 \) and \( \overline{\chi}_6 \) are trivial since the Frobenius-Schur indicator of an irreducible character which takes non real values is trivial (see [26, Proposition 38]). As for the term involving \( \text{Ind}_{H_8}^\chi_{\mathfrak{n}_8} \), since \( H_8 \) is normal in \( \tilde{A}_4 \), the formula for the character of an induced representation (see [26, Théorème 12]) gives \( (\text{Ind}_{H_8}^\chi_{\mathfrak{n}_8})(g^2) = 0 \) if \( g^2 \not\in H_8 \). Now observe that, an element \( g \in \tilde{A}_4 \) belongs to \( H_8 \) if and only if \( g^2 \in H_8 \). Moreover if \( h \in H_8 \), then

\[ h^2 = \begin{cases} 
\text{id} & \text{if } h = \text{id}, z \\
z & \text{otherwise},
\end{cases} \]

where \( z \) is the only nontrivial square of \( H_8 \) (thus \( z = \tau^2 \) in the presentation of \( H_8 \) given in §5.1.3). We deduce that

\[ \sum_{g \in \tilde{A}_4} (\text{Ind}_{H_8}^\chi_{\mathfrak{n}_8})(g^2) = \sum_{g \in H_8} (\text{Ind}_{H_8}^\chi_{\mathfrak{n}_8})(g^2) = 2(\text{Ind}_{H_8}^\chi_{\mathfrak{n}_8})(\text{id}) + 6(\text{Ind}_{H_8}^\chi_{\mathfrak{n}_8})(z). \]

We have

\[ (\text{Ind}_{H_8}^\chi_{\mathfrak{n}_8})(\text{id}) = \deg \text{Ind}_{H_8}^\chi_{\mathfrak{n}_8} = [\tilde{A}_4 : H_8] \deg \phi = 6. \]
The formula for the character of an induced representation, together with the fact that $H_8$ is normal in $\tilde{A}_4$ and $z \in Z(\tilde{A}_4)$, gives
\[
(\text{Ind}^{\tilde{A}_4}_{H_8}\phi)(z) = \frac{1}{\#H_8} \sum_{g \in \tilde{A}_4} \phi(g^{-1}zg) = 3\phi(z) = -6,
\]
where the last equality follows from the explicit computation of the values of $\phi$ (see for instance [26, Exercice 3, Section 12.2]). It follows, as desired, that
\[
\sum_{g \in \tilde{A}_4} (\text{Ind}^\tilde{A}_4_{H_8}\phi)(g^2) = -24.
\]
Thus $\tilde{A}_4$ satisfies the properties of Lemma 5.9 and has smallest possible order. In fact we also have that a tame $\tilde{A}_4$-Galois extension whose inverse different is a square of $\mathbb{Q}$ is automatically locally abelian, even locally cyclic.

**Theorem 5.18.** The group $\tilde{A}_4$ is the group of smallest order satisfying properties (i) and (ii) of Lemma 5.9. Moreover, if $N/\mathbb{Q}$ is a tame $\tilde{A}_4$-Galois extension whose inverse different is a square, then $N/\mathbb{Q}$ is locally cyclic.

**Proof.** The first assertion follows by Propositions 5.13, 5.15 and 5.17. As for the last assertion, $\tilde{A}_4$ and $H_8$, the only noncyclic subgroups of $\tilde{A}_4$, cannot be the decomposition subgroup of an archimedean place of $N$, since the latter is of order dividing 2. Suppose one of $\tilde{A}_4$ and $H_8$ is the decomposition subgroup of a finite place of $N$, then this place has to be ramified since decomposition subgroups of unramified places are cyclic. But finite primes have odd inertia degree in $N/\mathbb{Q}$, since $C_{N/\mathbb{Q}}$ is a square, thus $H_8$ cannot be a decomposition subgroup. The same holds for $\tilde{A}_4$ itself: its quotient by the inertia subgroup would have to be cyclic, hence the commutator $[\tilde{A}_4,\tilde{A}_4]$ would have to be contained in the inertia subgroup. But $[\tilde{A}_4,\tilde{A}_4] = H_8$ (as we showed in the proof of Proposition 5.15) and therefore $\tilde{A}_4$ cannot be the decomposition group of a place of $N$. It follows that $N/\mathbb{Q}$ is locally cyclic.

5.2.4. We now explicitly describe a tame $\tilde{A}_4$-Galois extension $N/\mathbb{Q}$ whose inverse different is a square. We use the results of Bachoc and Kwon [1], who studied the embedding problem of $A_4$-extensions in $\tilde{A}_4$-extensions. We briefly recall how the $\tilde{A}_4$-Galois extension we are interested in is constructed, although this construction is not strictly necessary for our purpose. We begin with the polynomial
\[
X^4 - 2X^3 - 7X^2 + 3X + 8
\]
which is irreducible over $\mathbb{Q}$ and let $\gamma$ be any fixed root of it (in an algebraic closure of $\mathbb{Q}$). Then, up to conjugation, $K = \mathbb{Q}(\gamma)$ is the totally real field of degree four over $\mathbb{Q}$ of smallest discriminant having trivial class number and Galois closure with Galois group isomorphic to $A_4$ (see [3, tables at pp. 395-396]). An easy computation with PARI [32] reveals that the Galois closure $M/\mathbb{Q}$ of $K$ is explicitly given by the polynomial
\[
X^{12} - 23X^{10} + 125X^8 - 231X^6 + 125X^4 - 23X^2 + 1.
\]
A further computation gives that the discriminant of $M/\mathbb{Q}$ is $163^8$ (in particular $M/\mathbb{Q}$ is tame) and the four primes above 163 in $M/\mathbb{Q}$ have ramification index 3 (in particular $C_{M/\mathbb{Q}}$ is a square). Let $k$ denote the only degree 3 subextension of
$M/Q$, it follows that $k/Q$ is totally ramified above 163 and unramified elsewhere, and $M/k$ is unramified at every finite place.

Using again PARI, we get that the narrow class number of $K$ equals 2. In other words the maximal abelian extension of $K$ which is unramified at finite places has degree 2 over $K$. Moreover $K/Q$ has the same discriminant as $k/Q$. Therefore $K$ satisfies the hypotheses of [1, Proposition 3.1(1)] and there exists a unique number field $\tilde{K}$ of degree 8 over $Q$ with the following properties:

- $K \subset \tilde{K}$ and $\tilde{K}/K$ is unramified outside the primes ramifying in $M/k$ (i.e. $\tilde{K}$ is a pure embedding of $K$);
- the Galois closure $N/Q$ of $\tilde{K}$ has Galois group $\tilde{A}_4$.

It follows from $K \subset \tilde{K}$ and the definition of $M$ and $N$ that $M \subset N$ (see Figure 1). From the above we get that $\tilde{K}/K$ is unramified at every finite place, thus the same holds for $N/M$ and for $N/k$. This shows that $N/Q$ is tame and that its inverse different is a square (since the same holds for $k/Q$).

Since the class number of $K$ is trivial, $\tilde{K}/K$ is ramified at some archimedean place (in fact $\tilde{K}$ is the narrow Hilbert class field of $K$). In particular $\tilde{K}$ is not totally real and therefore $N$ is totally complex (being a non-totally real Galois extension of $Q$). In other words the archimedean place of $Q$ is ramified in $N$, so the extension $N/Q$ does not satisfy the hypotheses of Proposition 5.6.

Bachoc and Kwon also compute a polynomial defining $\tilde{K}$ (see [1, table of p. 9, first line]):

$$X^8 + 14X^6 + 23X^4 + 9X^2 + 1.$$  

With the help of PARI, we get that $N/Q$ is explicitly given by the polynomial

$$X^{24} - 3X^{23} - 2X^{22} + 16X^{21} - 12X^{20} + 52X^{19} - 324X^{18} - 436X^{17} + 3810X^{16} - 1638X^{15} - 8012X^{14} - 12988X^{13} + 67224X^{12} - 76152X^{11} + 41175X^{10} - 39587X^9 + 70068X^8 - 66440X^7 + 38488X^6 - 23248X^5 + 16672X^4 - 6976X^3 + 2816X^2 - 1280X + 512.$$  

5.2.5. We now want to verify that $t_{\tilde{A}_4}W_{N/Q} \in \text{Cl}(\mathbb{Z}[\tilde{A}_4])$ is nontrivial. We first show that $W_{N/Q} \in \text{Hom}_{\mathfrak{g}(\tilde{A}_4)}(S_{\tilde{A}_4}, \{\pm 1\})$ is not trivial.

**Proposition 5.19.** We have $W(N/Q, \chi_5) = -1$, i.e. $W_{N/Q}$ is not trivial.
Proof. By Lemma 5.16 and the properties of root numbers recalled in §5.1.1, we have
\( W(N/k, \chi_6) = W(N/k, \phi)W(N/k, \chi_6)^{-1}W(N/k, \overline{\chi_6})^{-1} \).

We first show that \( W(N/k, \phi) = -1 \). Since \( k/Q \) is cyclic of degree 3, it is totally real with three real places and \( \text{Gal}(N/k) = H_8 \), the unique Sylow 2-subgroup of \( \tilde{A}_4 \). We will show that
\[
W(N_p/k_p, \phi_{D_p}) = \begin{cases} -1 & \text{if } P \text{ is a real place of } k \\ 1 & \text{otherwise} \end{cases}
\]
which implies, by (27), that \( W(N/k, \phi) = -1 \) (recall that \( \phi_{D_p} \) denotes the restriction of \( \phi \) at \( P \)). If \( P \) is a finite prime of \( k \), then one shows the triviality of \( W(N_p/k_p, \phi_{D_p}) \) as in the proof of Proposition 5.6 (case (a)). Suppose that \( P \) is a real place of \( k \), then the decomposition subgroup \( D_P \) of a place \( P \) of \( N \) above \( P \) is cyclic of order 2, since \( N \) is totally imaginary, and therefore \( D_P = Z(A_4) = (\alpha^3) \) since the center is the only subgroup of order 2 of \( A_4 \). In particular, by Lemma 5.5, we must have \( \phi_{D_P} = \nu + \overline{\nu} \) where \( \nu : D_P \to \{\pm 1\} \) is a character (thus in fact \( \nu = \overline{\nu} \) and \( \phi_{D_P} = 2\nu \)). Actually, since \( \phi(\alpha^3) = -2 \) (as remarked in the proof of Lemma 5.16), \( \nu \) must be the sign character, i.e. the only nontrivial character of \( D_P \). We therefore obtain
\[
W(N_p/k_p, \phi_{D_p}) = W(N_p/k_p, \nu)W(N_p/k_p, \overline{\nu}) = \det_{\nu}(-1) = \nu \circ r_P(-1) = -1,
\]
where as usual \( r_P : k_P^* = \mathbb{R}^* \to D_P \) is the local reciprocity map at \( P \) (which is nontrivial on \(-1\) precisely because \( P \) is ramified in \( N/k \)).

As for the factor \( W(N/Q, \chi_6)^{-1}W(N/Q, \overline{\chi_6})^{-1} \) in (31), using (27) as above, we are reduced to the local setting (here local means corresponding to a place of \( Q \)). Again, if \( P \) is a place of \( N \), either finite or archimedean,
\[
W(N/Q, (\chi_6)_{D_P})W(N/Q, (\overline{\chi_6})_{D_P}) = \det_{(\chi_6)_{D_P}}(-1).
\]

Observe that the determinant of \( \chi_6 \) is trivial on \( H_8 \) (which is the commutator subgroup of \( \tilde{A}_4 \)). If \( P \) is archimedean, \( D_P \) is cyclic of order 2 and therefore \( D_P \subset H_8 \), since \( H_8 \) is the Sylow 2-subgroup of \( \tilde{A}_4 \). In particular \( \det_{(\chi_6)_{D_P}} = 1 \). If instead \( P \) lies above a finite rational prime \( p \), then, as in the proof of Proposition 5.6, the reciprocity map \( r_P : Q_p^* \to D_P \) is trivial on \(-1\), since \( r_P(-1) \) is of order dividing 2 and belongs to the inertia subgroup \( I_P \) which has odd order. In particular \( \det_{(\chi_6)_{D_P}}(-1) = 1 \).

Concerning the map \( t_{\tilde{A}_4} \), we have the following result.

Lemma 5.20. The map
\[
t_{\tilde{A}_4} : \text{Hom}_{\mathbb{Q}_3}(S_{\tilde{A}_4}, \{\pm 1\}) \to \text{Cl}(\mathbb{Z}[\tilde{A}_4])
\]
is an isomorphism between groups of order 2.

Proof. Consider the following diagram
\[
\begin{array}{ccc}
\text{Hom}_{\mathbb{Q}_3}(S_{\tilde{A}_4}, \{\pm 1\}) & \xrightarrow{t_{\tilde{A}_4}} & \text{Cl}(\mathbb{Z}[\tilde{A}_4]) \\
\varphi & & \downarrow \text{res} \\
\text{Hom}_{\mathbb{Q}_3}(S_{H_8}, \{\pm 1\}) & \xrightarrow{t_{H_8}} & \text{Cl}(\mathbb{Z}[H_8])
\end{array}
\]
(32)
where \( res \) is induced by restriction of scalars from \( \mathbb{Z}[[A_4]] \) to \( \mathbb{Z}[H_8] \). To define \( \varphi \), observe that each of \( A_4 \) and \( H_8 \) has precisely one irreducible symplectic representation \((\chi_5 \blacklozenge \phi)\), respectively. This means that \( S_{A_4} \) and \( S_{H_8} \) both have \( \mathbb{Z} \)-rank 1 and \( \Omega_2 \) acts trivially on them. Of course \( \Omega_2 \) acts trivially on \( \{\pm 1\} \) too, so that \( \text{Hom}_{\Omega_2}(S_{A_4}, \{\pm 1\}) \) and \( \text{Hom}_{\Omega_2}(S_{H_8}, \{\pm 1\}) \) both have order 2. Then we let \( \varphi \) be the only isomorphism between \( \text{Hom}_{\Omega_2}(S_{A_4}, \{\pm 1\}) \) and \( \text{Hom}_{\Omega_2}(S_{H_8}, \{\pm 1\}) \). In particular

\[
\varphi(f)(\phi) = f(\chi_5)
\]

for \( f \in \text{Hom}_{\Omega_2}(S_{A_4}, \{\pm 1\}) \).

We claim that the above diagram is commutative. First observe that, thanks to [18, Theorem 12], we have a commutative diagram:

\[
\begin{array}{c}
\text{Hom}_{\Omega_2}(R_{A_4}, J(L')) \xrightarrow{\text{res}} \text{Cl}(\mathbb{Z}[[A_4]]) \\
\downarrow \varphi \\
\text{Hom}_{\Omega_2}(R_{H_8}, J(L')) \xrightarrow{\text{res}} \text{Cl}(\mathbb{Z}[H_8])
\end{array}
\]

where \( L' \) is a large enough number field, the horizontal arrows are the projections induced by the Hom-description and the map \( \text{res} \) on the left satisfies \( \text{res}(f)(\chi) = f(\text{Ind}_{H_8}^{A_4}\chi) \) for any \( f \in \text{Hom}_{\Omega_2}(R_{A_4}, J(L')) \) and any character \( \chi \) of \( H_8 \). Thus it is sufficient to prove that the diagram

\[
\begin{array}{c}
\text{Hom}_{\Omega_2}(S_{A_4}, \{\pm 1\}) \xrightarrow{t'_{A_4}} \text{Hom}_{\Omega_2}(R_{A_4}, J(L')) \\
\downarrow \varphi \\
\text{Hom}_{\Omega_2}(S_{H_8}, \{\pm 1\}) \xrightarrow{t'_{H_8}} \text{Hom}_{\Omega_2}(R_{H_8}, J(L'))
\end{array}
\]

is commutative (the definition of \( t'_{A_4} \) and \( t'_{H_8} \) is recalled in §5.1.2). Take \( f \in \text{Hom}_{\Omega_2}(S_{A_4}, \{\pm 1\}) \), then for any irreducible character \( \chi \) of \( H_8 \) we have, on the one hand,

\[
\text{res}(t'_{A_4}(f))(\chi) = t'_{A_4}(f)(\text{Ind}_{H_8}^{A_4}\chi) = \begin{cases} 
\text{res}^A\varphi(f)(f(\chi_5 + \chi_6 + \chi_7)) & \text{if } \chi = \phi \\
\text{res}^A\varphi(f)(f(\chi_1 + \chi_2 + \chi_3)) & \text{if } \chi = \psi_1 \\
\text{res}^A\varphi(f)(f(\chi_4)) & \text{otherwise},
\end{cases}
\]

by Lemma 5.16. In particular, using the definition of \( t'_{A_4} \) and Proposition 5.17, we get, for every place \( l \) of \( L' \),

\[
\text{res}(t'_{A_4}(f))(\chi)_l = \begin{cases} 
f(\chi_5) & \text{if } l \text{ is finite and } \chi = \phi \\
1 & \text{otherwise},
\end{cases}
\]

On the other hand we have

\[
t'_{H_8}(\varphi(f))(\chi)_l = \begin{cases} 
\varphi(f)(\chi) & \text{if } l \text{ is finite and } \chi = \phi \\
1 & \text{otherwise}
\end{cases}
= \begin{cases} 
f(\chi_5) & \text{if } l \text{ is finite and } \chi = \phi \\
1 & \text{otherwise},
\end{cases}
\]

and we have proved our claim.

Now the bottom horizontal arrow of (32) is an isomorphism, by a result of Fröhlich (see [18, I, Proposition 7.2]). Swan showed that the right-hand vertical
Combining the above lemma (in fact just the injectivity of $t_{\tilde{A}_4}$) with Proposition 5.19 and Corollary 5.2, we get the main result of this section and prove Theorem 3 of the Introduction.

**Theorem 5.21.** For the above $\tilde{A}_4$-extension $N/Q$ one has $t_{\tilde{A}_4}W_{N/Q} \neq 1$ in $\text{Cl}(\mathbb{Z}[\tilde{A}_4])$. In particular the classes of $\mathcal{A}_{N/Q}$ and $\mathcal{O}_N$ are both equal to the nontrivial element in $\text{Cl}(\mathbb{Z}[\tilde{A}_4])$.

**Remark 5.22.** Recall that $N/k$ is unramified at every finite place and that $\text{Gal}(N/k) = H_8$. Therefore $\mathcal{A}_{N/k} = \mathcal{O}_N$ and in particular $(\mathcal{A}_{N/k}) = (\mathcal{O}_N)$ in $\text{Cl}(\mathbb{Z}[H_8])$. Note that, in the proof of Proposition 5.17, we have shown that $W_{N/k}$ is nontrivial. Moreover, since $t_{H_8}$ is an isomorphism by [18, I, Proposition 7.2], we get that $t_{H_8}W_{N/k}$ is the nontrivial element of $\text{Cl}(\mathbb{Z}[H_8])$. Thus $N/k$ gives another example of a tame (in fact unramified at finite places) Galois extension whose inverse different is a square and the square root of the inverse different has nontrivial class in the locally free class group. Anyway, the case of $N/Q$ is perhaps more suggestive, since $\mathcal{A}_{N/Q} \neq \mathcal{O}_N$. 

**References**


(Luca Caputo)
E-mail address: luca.caputo@gmx.com

(Stéphane Vinatier, corresponding author)
XLIM-DMI UMR 7252 CNRS-Université de Limoges, 123 Avenue Albert Thomas, 87060 Limoges Cedex, France
E-mail address: stephane.vinatier@unilim.fr