London Mathematical Society ISSN 1461–1570

NUMERICAL EVIDENCE FOR A CONJECTURAL GENERALIZATION OF HILBERT'S THEOREM 132

W. BLEY

with an appendix by D. Kusnezow

Abstract

This paper presents an algorithm for computing numerical evidence for a conjecture whose validity is predicted by the requirement that the equivariant Tamagawa number conjectures for Tate motives as formulated by Burns and Flach are compatible with the functional equation of the Artin L-series. The algorithm includes methods for the computation of Fitting ideals and projective lattices over the integral group ring.

1. *Introduction*

For any number field L, we write $\mathcal{O}_L$ for its ring of algebraic integers. For each natural number n, we let ζ_n denote a primitive nth root of unity, and we write $\mathbb{Q}(\zeta_n)$ for the nth cyclotomic field. If n is squarefree, then Hilbert proved (see [**16**, Theorem 132]) that

$$\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})] \cdot \zeta_n = \mathcal{O}_{\mathbb{Q}(\zeta_n)}. \tag{1}$$

Let L/K denote a Galois extension of number fields with group G. In [**3**] and [**4**] we formulated a conjecture that is a wide-ranging generalization of equality (1). In this paper, we will deal exclusively with the abelian case (as presented in [**3**]), where this conjecture takes the form of an equality between two rank-one $\mathbb{Z}[G]$-sublattices of $\mathbb{C}[G]$, namely a lattice constructed from Galois Gauss sums and a lattice that is related to the choice of a finitely generated projective G-sublattice $\mathcal{L}$ of L. If L/K is at most tamely ramified, then Noether proved that $\mathcal{O}_L$ is a projective $\mathbb{Z}[G]$-module. In this case, we always take $\mathcal{L} = \mathcal{O}_L$. In general, however, if we allow wild ramification, we are not aware of any canonical candidate for $\mathcal{L}$, and we use invariants that arise from the étale cohomology of $\mathbf{G}_m$ to compensate for our choice of $\mathcal{L}$.

In [**3**] and [**4**] it is shown that our conjecture is a strong refinement of Chinburg's Ω_2-conjecture (see [**9**]). In another (probably more important) direction, it can be interpreted in terms of functional equation compatability of the 'equivariant Tamagawa number conjectures' of [**6**] and [**7**] for the pairs $(h^0(\mathrm{Spec}(L)), \mathbb{Z}[G])$ and $(h^0(\mathrm{Spec}(L))(1), \mathbb{Z}[G])$.

There is some evidence in favour of the conjecture. It has already been proved in the case where L/K is at most tamely ramified (see [**4**, Corollary 7.7]), or if $K = \mathbb{Q}$ and $L/\mathbb{Q}$ is an abelian extension of odd conductor (see [**3**, Theorem 4.1] and [**4**, Theorem 6.1]). Concerning wildly ramified (abelian) extensions L/K, $K \neq \mathbb{Q}$, there is only a very little evidence. In this paper we will deal with this situation, and we will present an algorithm that verifies the above-mentioned conjecture (up to the precision of the computation) for

Received 12 July 2002, revised 23 January 2003; *published* 24 March 2003.
2000 Mathematics Subject Classification 11R33, 11R42

certain abelian extensions L/K. The algorithm has been implemented under PARI-GP [1] for extensions L/K of odd prime degree of a real-quadratic field K, and has been applied to many examples, so that we can provide new numerical evidence for the validity of the conjecture in the wildly ramified relative case. Very recently, M. Breuning [5] has used an adapted version of this implementation, together with interesting new theoretical results, to prove (!) the conjecture for all dihedral extensions of $\mathbb{Q}$ of order 6.

The structure of the paper is as follows. In Section 2 we recall the formulation of the conjecture. In Section 3 we describe our algorithm, and in Section 4 we work out an explicit example.

2. *The conjecture*

First we briefly recall the notion of the Grothendieck–Knudsen–Mumford determinant functor. For more details, the reader is referred to [17], or for a short summary of the relevant facts, to [3, Section 2].

If R is a noetherian commutative ring, we write $\mathcal{P}(R)$ for the category of graded invertible R-modules. For each $(L, \alpha) \in \mathrm{Ob}(\mathcal{P}(R))$, one sets $L^{-1} := \mathrm{Hom}_R(L, R)$ and $(L, \alpha)^{-1} := (L^{-1}, -\alpha)$. For a finitely generated projective R-module P, we write $\det_R(P)$ for the highest exterior power of P and we use $\mathrm{rk}_R(P)$ to denote the locally constant function given by the R-rank of P. One sets

$$\mathrm{Det}_R(P) := (\det_R(P), \mathrm{rk}_R(P)) \in \mathcal{P}(R),$$

and for a bounded complex $P^\bullet$ of finitely generated projective R-modules, one defines

$$\mathrm{Det}_R(P^\bullet) := \bigotimes_{i \in \mathbb{Z}} \mathrm{Det}_R(P^i)^{(-1)^{i+1}} \in \mathcal{P}(R).$$

A *perfect complex of R-modules* is a complex of R-modules that is quasi-isomorphic to a bounded complex of finitely generated projective R-modules. We write $\mathcal{D}(R)$ for the derived category of the abelian category of R-modules, and $\mathcal{D}^{\mathrm{perf}}(R)$ for the subcategory consisting of perfect complexes. Then Det_R extends to give a well-defined functor from $\mathcal{D}^{\mathrm{perf}}(R)$ (with morphisms restricted to isomorphisms) to the category of graded invertible R-modules.

We say that a R-module N is *perfect* if it is finitely generated and of finite projective dimension. Such a module, viewed as a complex centered in degree 0, is a perfect complex, and we set $\mathrm{Det}_R(N) := \mathrm{Det}_R(N[-1])$. We write $\mathrm{Fitt}_R(N)$ for the (first) Fitting ideal of N. (We refer the reader to [19, Appendix] or [21, Section 1.4] for the basic properties of Fitting ideals.) Then

$$\mathrm{Det}_R(N) = \big(\mathrm{Fitt}_R(N)^{-1}, -\mathrm{rk}_R(N)\big).$$

Now, let L/K be an abelian extension of number fields with Galois group G. We write $\hat{G}$ for the group of linear characters of G, and for each $\chi \in \hat{G}$ we set

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g) g^{-1} \in \mathbb{C}[G].$$

If H is a subgroup of G, we write $e_H = (1/|H|) \sum_{h \in H} h$ for the associated idempotent. For any element $x \in \mathbb{C}[G]$, we define an invertible element ${}^*x$ of $\mathbb{C}[G]$ by specifying the components by

$$e_\chi({}^*x) = \begin{cases} e_\chi x, & \text{if } e_\chi x \neq 0, \\ e_\chi, & \text{if } e_\chi x = 0. \end{cases}$$

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

We let G_v and I_v denote, respectively, the decomposition and the inertia subgroup of a finite place v of K, and we choose an element $\sigma_v \in G_v$ that projects to the Frobenius element in G_v/I_v. We then define $f_v := \sigma_v e_{I_v}$, and we note that f_v does not depend on the choice of σ_v.

We define the equivariant Galois Gauss sum by

$$\tau_{L/K} := \sum_{\chi \in \hat{G}} \tau\Big(\mathbb{Q}, \mathrm{ind}_K^{\mathbb{Q}}(\chi)\Big) e_\chi \in \mathbb{C}[G]^\times,$$

where for any number field F we write $\tau(F, -)$ for the Galois Gauss sum described in [**14**, Chapter I, Section 5].

We write d_L for the absolute discriminant of L, and finally we define

$$\xi_{L/K} := \tau_{L/K} \prod_{v \mid d_L} {}^*(-f_v^{-1}) \in \mathbb{C}[G]^\times.$$

Recall that the Galois Gauss sum is the essential part of the epsilon factor, which arises in the functional equation of Artin L-functions (see [**14**, (5.22)]). Roughly speaking, the conjecture of [**3**] asserts that the lattice $\mathbb{Z}[G] \cdot \xi_{L/K}$ is equal to a $\mathbb{Z}[G]$-sublattice of $\mathbb{C}[G]$ constructed from certain algebraic data associated to L/K.

To recall the definition of this lattice, we have to introduce some more notation. For any number field F, we write $\Sigma(F)$ for the set of embeddings of F into $\mathbb{C}$, and we write $S(F)$ and $S_f(F)$ for the set of places and the set of non-archimedean places, respectively, of F. We define $H_F := \prod_{\Sigma(F)} \mathbb{Q}$ and $H_{F,\mathbb{Z}} := \prod_{\Sigma(F)} \mathbb{Z}$.

Then the natural action of G on $\Sigma(L)$ induces the structure of a $\mathbb{Z}[G]$-module on $H_{L,\mathbb{Z}}$. We write

$$\pi_L : L \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} H_L \otimes_{\mathbb{Q}} \mathbb{C},$$

for the canonical $\mathbb{C}[G]$-isomorphism defined by $\alpha \otimes x \mapsto (\sigma(\alpha)x)_{\sigma \in \Sigma(L)}$. After choosing for each $\tau \in \Sigma(K)$ an extension $\hat{\tau} \in \Sigma(L)$, we can identify $H_{L,\mathbb{Z}}$ with $H_{L/K,\mathbb{Z}} := \prod_{\Sigma(K)} \mathbb{Z}[G]$, and so we obtain a $\mathbb{C}[G]$-equivariant isomorphism

$$\begin{aligned} \pi_{L/K} : L \otimes_{\mathbb{Q}} \mathbb{C} &\xrightarrow{\sim} \prod_{\Sigma(K)} \mathbb{C}[G], \\ \alpha \otimes x &\longmapsto \left(\sum_{g \in G} \hat{\tau} g(\alpha) x g^{-1} \right)_{\tau \in \Sigma(K)}. \end{aligned}$$

We now write $\mathcal{W}(L/K)$ for the set of non-archimedean places of K that ramify wildly in L/K. For a place $w \in S_f(L)$ above v, we let K_v and L_w denote the completions of K and L with respect to v and w respectively, and we identify the decomposition group G_v with the local Galois group $\mathrm{Gal}(L_w/K_v)$. We choose a finitely generated projective $\mathcal{O}_K[G]$-sublattice $\mathcal{L}$ of L such that, for each place v of $S_f(K)$, the v-adic completion $\mathcal{L}_v$ satisfies

$$\mathcal{L}_v = \begin{cases} \mathcal{O}_{L,v}, & \text{if } v \notin \mathcal{W}(L/K), \\ \mathcal{O}_{K_v}[G] \otimes_{\mathcal{O}_{K_v}[G_v]} \mathcal{L}_w, & \text{if } v \in \mathcal{W}(L/K). \end{cases} \tag{2}$$

Here, $w \in S_f(L)$ is a chosen place above v and $\mathcal{L}_w$ is any projective $\mathcal{O}_{K_v}[G_v]$-sublattice of the maximal ideal of $\mathcal{O}_{L_w}$ such that the v-adic exponential map is both well defined and injective. These conditions are satisfied for any projective lattice that is contained in a sufficiently large power of the maximal ideal of $\mathcal{O}_{L_w}$.

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

Essentially, we will compare $\mathbb{Z}[G]\cdot\xi_{L/K}$ to

$$\det_{\mathbb{C}[G]}(\pi_{L/K})\left(\det_{\mathbb{Z}[G]}(\mathcal{L})\right)\subseteq\det_{\mathbb{C}[G]}(H_{L/K}\otimes_{\mathbb{Z}}\mathbb{C})\simeq\mathbb{C}[G].$$

In [3], in order to compensate for our choice of lattice $\mathcal{L}$, we used the cohomology of the sheaf $\mathbf{G}_m$ on the étale site $\mathrm{Spec}(K_v)$, $v\in\mathcal{W}(L/K)$, to define a natural complex $K_w^\bullet(\mathcal{L})$ in $\mathcal{D}^{\mathrm{perf}}(\mathbb{Z}[G_v])$. This complex is then the starting point for the construction of local correction terms $I(v,\mathcal{L})$ for each $v\in\mathcal{W}(L/K)$. The following description of $K_w^\bullet(\mathcal{L})$ is very convenient for computational purposes. Let

$$0\longrightarrow L_w^\times\longrightarrow A'\longrightarrow B\longrightarrow\mathbb{Z}\longrightarrow 0 \tag{3}$$

be a 2-extension of $\mathbb{Z}$ by $L_w^\times$ with $\mathbb{Z}[G_v]$-modules A' and B of finite projective dimension. Assume further that (3) represents the local fundamental class in $H^2(G_v,L_w^\times)\simeq\mathrm{Ext}^2_{G_v}(\mathbb{Z},L_w^\times)$. Then [8, Proposition 3.5(a)] implies that there exists a $\mathcal{D}^{\mathrm{perf}}(\mathbb{Z}[G_v])$-isomorphism between $\Psi_w^\bullet(\mathcal{L}):=[A'/(1+\mathcal{L}_w)\to B]$ (centered in degrees 0 and 1) and $K_w^\bullet(\mathcal{L})$ inducing the identity maps on cohomology. Hence we can use $\Psi_w^\bullet(\mathcal{L})$ to define the correction terms $I(v,\mathcal{L})$.

We let $\lambda_{L/K,w}$ denote the composite isomorphism

$$\begin{aligned}
&\left(\mathrm{Det}_{\mathbb{Z}[G_v]}\,\Psi_w^\bullet(\mathcal{L})[1]\right)\otimes\mathbb{Q}\\
&\quad\xrightarrow{\sim}\quad \mathrm{Det}_{\mathbb{Q}[G_v]}\left(\Psi_w^\bullet(\mathcal{L})[1]\otimes\mathbb{Q}\right)\\
&\quad\longrightarrow\quad \mathrm{Det}_{\mathbb{Q}[G_v]}\left(L_w^\times/(1+\mathcal{L}_w)\otimes\mathbb{Q}\right)\otimes_{\mathbb{Q}[G_v]}\mathrm{Det}_{\mathbb{Q}[G_v]}(\mathbb{Q})^{-1}\\
&\quad\xrightarrow{\mathrm{Det}(\vartheta_w)\otimes\mathrm{id}}\quad \mathrm{Det}_{\mathbb{Q}[G_v]}(\mathbb{Q})\otimes_{\mathbb{Q}[G_v]}\mathrm{Det}_{\mathbb{Q}[G_v]}(\mathbb{Q})^{-1}\\
&\quad\longrightarrow\quad (\mathbb{Q}[G_v],0),
\end{aligned}$$

where ϑ_w denotes the isomorphism $L_w^\times/(1+\mathcal{L}_w)\otimes\mathbb{Q}\xrightarrow{\sim}\mathbb{Q}$, which is induced by the w-adic valuation map.

For each place $v\in S_f(K)$, we set

$$\mathcal{E}_{L/K,v}:={}^*\left(e_{G_v}\left(\frac{-|G_v|}{|I_v|}\right)\right)\frac{{}^*\left(e_{I_v}(1-f_vNv^{-1})\right)}{{}^*\left(e_{I_v}(1-f_v)\right)},$$

and we define a (graded) invertible $\mathbb{Z}[G]$-sublattice of $\mathbb{Q}[G]$ by setting

$$I(v,\mathcal{L}):=\mathcal{E}_{L/K,v}\cdot\lambda_{L/K,w}\left(\mathrm{Det}_{\mathbb{Z}[G_v]}\left(\Psi_w^\bullet(\mathcal{L})[1]\right)\right).$$

We are now in position to state the central conjecture of [3]. Let $\rho_{L,K}$ denote the map $\mathrm{Det}_{\mathbb{C}[G]}(\pi_{L/K})$.

Conjecture 2.1. For any lattice $\mathcal{L}$ that satisfies (2), the following statement holds:

$$\left(\mathbb{Z}[G]\cdot\xi_{L/K},[K:\mathbb{Q}]\right)=\rho_{L,K}\left(\mathrm{Det}_{\mathbb{Z}[G]}(\mathcal{L})\right)\otimes\bigotimes_{v\in\mathcal{W}(L/K)}I(v,\mathcal{L}). \tag{4}$$

Remarks 2.2. (a) In [3], Conjecture 2.1 is formulated as an equality between graded invertible $\mathbb{Z}[G]$-sublattices of $\mathrm{Det}_{\mathbb{C}[G]}(L\otimes_{\mathbb{Q}}\mathbb{C})$. The translation is achieved by applying $\rho_{L/K}^{-1}$.

(b) The central Conjecture (4.1) of [4] generalizes Conjecture 2.1 for arbitrary Galois extensions L/K of number fields (see [4, Section 5]).

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

3. *An algorithm*

Let K denote a number field of degree k over $\mathbb{Q}$. We let L/K denote an abelian extension of number fields of degree n. Our aim is to develop an algorithm to check the validity of Conjecture 2.1 up to the precision of the computation.

We assume that L/K is given by class field-theoretic data as described in [**11**, Chapters 3 and 4]. In particular, we let $\mathfrak{f} = \mathfrak{f}_{L/K}$ denote the conductor of L/K, and we write $\mathrm{cl}_{\mathfrak{f}}(K)$ for the ray class group modulo $\mathfrak{f}$. Let $\mathcal{H} \leqslant \mathrm{cl}_{\mathfrak{f}}(K)$ denote the subgroup of index n corresponding to the given extension L. If F is any intermediate field of L/K, we further assume that we are able to compute a defining polynomial for F, and also its ring of algebraic integers. In this context, recently developed algorithms due to Cohen and Roblot (see [**11**, Chapter 6] or [**22**]) are very useful.

For some (essential) parts of the algorithm we will have to make the following assumption.

HYPOTHESIS (H). If $v \in S_f(K)$ is wildly ramified in L/K, then the decomposition group G_v is cyclic.

3.1. *Computation of* $\mathcal{L}$

Let L/K denote an abelian extension of number fields, and set $G := \mathrm{Gal}(L/K)$. In this subsection we do not assume Hypothesis (H). As before, we write $\mathcal{W}(L/K)$ for the set of finite places of K that ramify wildly in L/K. For each place $v \in \mathcal{W}(L/K)$, we fix an extension $w \in S_f(L)$ above v. Henceforth we identify the place v with a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and we write $w_{\mathfrak{p}}$ for the associated normalized valuations. Likewise, w is identified with a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$, and we write $w_{\mathfrak{P}}$ for the associated normalized valuations. For $v \in S_f(K)$ and a finitely generated $\mathcal{O}_K$-module Y, we write $Y_{(v)}$ for the localization and Y_v for the completion of Y with respect to v.

We first give a brief outline of the algorithm for the computation of $\mathcal{L}$, and then we work out the single steps in greater detail.

Step 1. For each place $v \in \mathcal{W}(L/K)$, set $F = L^{G_v}$ and construct a normal basis element $\theta_v \in \mathcal{O}_L$ for L/F (that is, $L = F[G_v]\theta_v$) such that

$$w_{\mathfrak{P}}(\theta_v) > \frac{e_w}{p-1}.$$

Here, e_w denotes the ramification index of w in $L/\mathbb{Q}$ and $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$. We set

$$\mathcal{X}_{(v)} := \mathcal{O}_{F,(s)}[G_v]\theta_v,$$

where $s \in S_f(F)$ is the place uniquely determined by $w \mid s \mid v$.

Step 2. For each place $v \in \mathcal{W}(L/K)$, compute $\mathcal{X}'_{(v)} := \mathcal{X}_{(v)} \cap \mathcal{O}_L$.

Step 3. Compute $\mathcal{L} := \bigcap_{v \in \mathcal{W}(L/K)} \mathcal{X}'_{(v)}$.

PROPOSITION 3.1. *$\mathcal{L}$ is a finitely generated projective $\mathbb{Z}[G]$-sublattice of L and satisfies* (2) *with $\mathcal{L}_w = \mathcal{O}_{K_v}[G_v]\theta_v$. Moreover, the v-adic exponential map is well-defined and injective on $\mathcal{L}_w$.*

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

Proof. We consider the $\mathbb{Z}[G]$-projective sublattice $\mathcal{X} \subseteq L$ specified by its v-adic localisations (see [12, Proposition (4.21)])

$$\mathcal{X}_{(v)} = \begin{cases} \mathcal{O}_{L,(v)}, & \text{if } v \notin \mathcal{W}(L/K), \\ \mathcal{O}_{L^{G_v},(s)}[G_v]\theta_v, & \text{if } v \in \mathcal{W}(L/K), \quad w \mid s \mid v. \end{cases} \tag{5}$$

Passing from localisations to completions shows that it is enough to prove that $\mathcal{X} = \mathcal{L}$. By construction, we have $\mathcal{X} \subseteq \mathcal{O}_L$, so we can conclude that

$$\mathcal{X} = \bigcap_{v \in S_f(K)} \mathcal{X}_{(v)} = \bigcap_{v \in S_f(K)} (\mathcal{X}_{(v)} \cap \mathcal{O}_L) = \bigcap_{v \in \mathcal{W}(L/K)} \mathcal{X}'_{(v)} = \mathcal{L}.$$

By [20, Kapitel II, Satz (5.5)] and the choice of θ_v the v-adic exponential map is well-defined and injective, as claimed. □

Proposition 3.1 guarantees that $\mathcal{L}$ is a lattice, as required in the formulation of Conjecture 2.1.

Remark 3.2. Let L/K be a weakly ramified Galois extension of number fields (that is, all the second ramification groups in lower numbering are trivial) of odd degree. Let $\mathfrak{a}_{L/K}$ denote the square root of the inverse different (see [13, (1.2)]). Then $\mathfrak{a}_{L/K}$ is a finitely generated $\mathbb{Z}[G]$-projective sublattice of L (see [13, Theorem 2.2]). We set $\mathfrak{a}^{(w)}_{L/K} := \prod \mathfrak{P}^{w_{\mathfrak{P}}(\mathfrak{a}_{L/K})}$, where the product extends over all primes $\mathfrak{P}$ of $\mathcal{O}_L$ that are wildly ramified in L/K. Then $\mathfrak{a}^{(w)}_{L/K}$ is also $\mathbb{Z}[G]$-projective. If we choose an element $\beta \in \mathcal{O}_K$ such that $w_{\mathfrak{P}}(\beta\mathfrak{a}^{(w)}_{L/K}) > e_w/(p-1)$ for all $v \in \mathcal{W}(L/K)$, then we may take $\mathcal{L} = \beta\mathfrak{a}^{(w)}_{L/K}$.

We now go into greater detail concerning Steps 1–3. Let N_v denote the smallest integer such that $N_v > e_w/(p-1)$. For our purposes later, it is of advantage to construct a normal basis element θ_v such that the index $[\mathfrak{P}^{N_v} : \mathcal{O}_F[G_v]\theta_v]$ is small. To achieve this, it is possible in principle to adapt the algorithm of [2, Section 2.1]. In practice, however, the following naive approach is usually sufficient. A randomly chosen element $\theta \in \mathcal{O}_L$ will almost always generate a normal basis of L/F. Let $\mathfrak{p}'$ denote the prime ideal of $\mathcal{O}_F$ corresponding to the place s. If (p, π_v) is a two-element representation of $\mathfrak{p}'$ (such as, for example, that computed by [10, Algorithm 4.7.10]), then $w_{\mathfrak{p}'}(\pi_v) = 1$ and we may take $\theta_v := \pi_v^t\theta$ with $t \in \mathbb{N}_0$ large enough to ensure that $te_{w|s} + w_{\mathfrak{P}}(\theta) > e_w/(p-1)$. Here, $e_{w|s}$ denotes the ramification index of $w \mid s$ in L/F.

Henceforth, we assume that each $\mathcal{X}_{(v)}$ is given by an explicit basis over $\mathbb{Z}$. For the computation of $\mathcal{X}'_{(v)}$ in Step 2, we first use Hermite normal form (HNF) techniques over $\mathbb{Z}$ to compute a finite set $Z_1 \subseteq \mathfrak{P}^{n_v}$ of representatives of $\mathfrak{P}^{n_v}/\mathcal{O}_{L^{G_v}}[G_v]\theta_v$, where $n_v := w_{\mathfrak{P}}(\theta_v)$. Let $Z := Z_1 \cap \mathcal{X}_{(v)}$.

Lemma 3.3. *Let $v \in \mathcal{W}(L/K)$, and set $F = L^{G_v}$. Let Z' denote a finite set of $\mathbb{Z}$-generators of $\mathcal{O}_F[G_v]\theta_v$. Then $Z \cup Z'$ is a finite set of $\mathbb{Z}$-generators of $\mathcal{X}'_{(v)}$.*

Proof. It is enough to show that Z constitutes a set of representatives of $\mathcal{X}'_{(v)}/\mathcal{O}_F[G_v]\theta_v$. Hence it suffices to prove that $\mathcal{X}'_{(v)} = \mathcal{X}_{(v)} \cap \mathfrak{P}^{n_v}$, which is clear from the definitions. □

In order to compute the set Z, we represent each $z \in Z_1$ in the form

$$z = \sum_{g \in G_v} x_g g(\theta_v), \qquad x_g \in L^{G_v},$$

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

and we check that the condition $w_{\mathfrak{P}'}(x_g) \geqslant 0$, $\mathfrak{P} \mid \mathfrak{p}' \mid \mathfrak{p}$ in $L/L^{G_v}/K$, holds for all $g \in G_v$ (see [**10**, Algorithm 4.8.17]). Again using HNF techniques (over $\mathbb{Z}$), we may assume that each of the $\mathcal{O}_K$-lattices $\mathcal{X}'_{(v)}$ is given by a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_m$, $m = [L : \mathbb{Q}]$, $\omega_i \in \mathcal{O}_L$. This completes the description of Step 2.

To carry out Step 3, it suffices to explain how to compute the intersection $X \cap Y$ of two full $\mathbb{Z}$-sublattices $X, Y \subseteq L$ given in the form

$$X = \mathbb{Z}\mu_1 \oplus \ldots \oplus \mathbb{Z}\mu_m, \qquad \mu_i \in L,$$
$$Y = \mathbb{Z}\nu_1 \oplus \ldots \oplus \mathbb{Z}\nu_m, \qquad \nu_i \in L.$$

Let $b : L \times L \to \mathbb{Q}$, $b(\alpha, \beta) = \mathrm{tr}_{L/\mathbb{Q}}(\alpha\beta)$ denote the usual trace form. For any full $\mathbb{Z}$-lattice $V \subseteq L$, we set $V^* := \{\alpha \in L \mid b(\alpha, V) \subseteq \mathbb{Z}\}$. Then one has the formula $X \cap Y = (X^* + Y^*)^*$. So we compute the dual basis (with respect to b) $\mu_1^*, \ldots \mu_m^*$ and $\nu_1^*, \ldots \nu_m^*$ of X^* and Y^*. Applying HNF techniques to $X^* + Y^*$, we obtain a $\mathbb{Z}$-basis of $X^* + Y^*$. Dualizing again yields the intersection $X \cap Y$.

3.2. *The local fundamental class*

In this subsection (and also in the next one) we have to assume Hypothesis (H). We fix $v \in \mathcal{W}(L/K)$ and an extension $w \mid v$, and we write $D = G_v$ for the decomposition group. Let g_0 denote a generator of D. Our aim is to describe an algorithm that computes a 2-extension (3) that represents the fundamental class of local class field theory.

We consider the canonical exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{N_D} \mathbb{Z}[D] \xrightarrow{g_0 - 1} \mathbb{Z}[D] \xrightarrow{\mathrm{aug}} \mathbb{Z} \longrightarrow 0,$$

where aug is induced by $g \mapsto 1$, $g \in D$, and $N_D = \sum_{g \in D} g$. We will compute $H^2(D, L_w^\times) \simeq \mathrm{Ext}_D^2(\mathbb{Z}, L_w^*)$ with respect to this resolution. Let $(\_\,, L_w/K_v)$ denote the local Artin symbol, and let $\varepsilon_v \in K_v^\times$ be such that $(\varepsilon_v, L_w/K_v) = g_0$. Then the G-embedding $\varphi : \mathbb{Z} \to L_w^\times$ defined by $\varphi(1) = \varepsilon_v$ represents the local fundamental class. We shall now explain how to find ε_v.

Let $\mathfrak{p}$ again denote the prime ideal of $\mathcal{O}_K$ corresponding to v. We write $\mathfrak{f} = \mathfrak{p}^s\mathfrak{f}'$ with $\mathfrak{p} \nmid \mathfrak{f}'$. Let $U_v \subseteq K_v^\times$ denote the local units, and write $U_v^{(i)}$, $i > 0$, for the higher principal units. Then $U_v^{(s)} \subseteq N_{L_w/K_v}(L_w^\times)$, and the composite map

$$K_v^\times / U_v^{(s)} \longrightarrow K_v^\times / N_{L_w/K_v}(L_w^\times) \xrightarrow{(\_\,, L_w/K_v)} D$$

is surjective. If $\pi_v \in K^\times$ is a uniformizing element for v, then $K_v^\times = \pi_v^{\mathbb{Z}} \times U_v$ and we obtain the isomorphisms

$$K_v^\times / U_v^{(s)} \simeq \pi_v^{\mathbb{Z}} \times U_v / U_v^{(s)} \simeq \pi_v^{\mathbb{Z}} \times \left(\mathcal{O}_K/\mathfrak{p}^s\right)^\times.$$

Since $\pi_v^{|D|} \in \ker(\_\,, L_w/K_v)$, we finally obtain an epimorphism

$$\pi_v^{\mathbb{Z}}/\pi_v^{|D|\mathbb{Z}} \times \left(\mathcal{O}_K/\mathfrak{p}^s\right)^\times \longrightarrow D,$$

induced by the local Artin map. Provided that we know how to compute local Artin symbols, it is now a finite problem to compute ε_v.

REMARK 3.4. In this way we have actually constructed ε_v in $K^\times$. By multiplying with $\pi_v^{|D|}$ (if necessary), we may also assume that $w_{\mathfrak{p}}(\varepsilon_v) > 0$. For computational purposes it is an advantage to choose ε_v with small v-adic valuation. Since $U_v/U_v^{(s)} \simeq (\mathcal{O}_K/\mathfrak{p}^s)^\times$ is mapped

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

surjectively onto the inertia subgroup I_v, we can always achieve $w_{\mathfrak{p}}(\varepsilon_v) = 1$ in the totally ramified case.

It finally remains to describe how to compute local Artin symbols for elements $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$. Let $\mathfrak{f} = \prod_{k=0}^{r} \mathfrak{p}_k^{s_k}$ be the prime ideal factorization of the conductor $\mathfrak{f}$, and assume that $\mathfrak{p} = \mathfrak{p}_0$. We set $e = w_{\mathfrak{p}}(\alpha)$, and we choose an element $\pi \in \mathcal{O}_K$ such that

$$w_{\mathfrak{p}_j}(\pi) = \begin{cases} 0, & \text{if } j > 0, \\ 1, & \text{if } j = 0. \end{cases}$$

If we let $\xi \in \mathcal{O}_K$ denote a solution of the simultanous congruences

$$\xi \equiv \pi^e \pmod{\mathfrak{p}_k^{s_k}}, \qquad k = 1, \dots, r,$$
$$\xi \equiv \frac{\pi^e}{\alpha} \pmod{\mathfrak{p}_0^{s_0}},$$

then class field theory shows that $(\alpha, L_w/K_v) = (\mathfrak{c}, L/K)$, where

$$\mathfrak{c} = \xi \prod_{\mathfrak{q}|\pi, \mathfrak{q}\neq\mathfrak{p}} \mathfrak{q}^{-e v_{\mathfrak{q}}(\pi)}.$$

Recall that L/K is given by $\mathrm{cl}_{\mathfrak{f}}(K)$ and a subgroup $\mathcal{H}$ of index $|G|$. Assume that the integral ideal $\mathfrak{c}_0$ corresponds to g_0 via the global reciprocity isomorphism. Using [**11**, Algorithm 4.3.2] it is then easy to compute $d \in \mathbb{Z}/|D|\mathbb{Z}$ such that $\mathfrak{c} = \mathfrak{c}_0^d$ in $\mathrm{cl}_{\mathfrak{f}}(K)/\mathcal{H}$. So in order to solve our problem we have to find an element $\alpha = \varepsilon_v$ such that $d \equiv 1 \pmod{|D|}$.

3.3. *Computation of* $I(v, \mathcal{L})$

We continue to use the notation introduced in the previous subsection. In particular, we assume Hypothesis (H). For any subgroup U of $L_w^\times$ that contains $1 + \mathcal{L}_w$, we set $U(\mathcal{L}_w) := U/(1 + \mathcal{L}_w)$.

So far we have constructed a map φ such that the following diagram has exact rows and columns.

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & & & & & \\
 & & \downarrow & & \downarrow & & & & & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{N_D} & \mathbb{Z}[D] & \xrightarrow{g_0-1} & \mathbb{Z}[D] & \xrightarrow{\mathrm{aug}} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \bar{\varphi}\downarrow & & \downarrow & & \| & & \| & & \\
0 & \longrightarrow & L_w^\times(\mathcal{L}_w) & \longrightarrow & A & \longrightarrow & \mathbb{Z}[D] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & & & \\
 & & \mathrm{cok}(\bar{\varphi}) & = & \mathrm{cok}(\bar{\varphi}) & & & & & & \\
 & & \downarrow & & \downarrow & & & & & & \\
 & & 0 & & 0 & & & & & &
\end{array} \tag{6}$$

Here, $\bar{\varphi}$ is the composite of φ and the canonical map $L_w^\times \to L_w^\times(\mathcal{L}_w)$, and A denotes the push-out of $\bar{\varphi}$ and N_D. Since we assume that the v-adic valuation of $\varphi(1) = \varepsilon_v$ is positive, $\bar{\varphi}$ is indeed injective. In addition, this assumption ensures that $\mathrm{cok}(\bar{\varphi})$ is a finite $\mathbb{Z}[D]$-module. Since φ represents the local fundamental class, it is also of finite projective dimension.

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

We define objects of $\mathcal{D}^{\mathrm{perf}}(\mathbb{Z}[D])$:

$$\Psi^\bullet := [\mathbb{Z}[D] \xrightarrow{g_0-1} \mathbb{Z}[D]],$$
$$\Psi_w^\bullet(\mathcal{L}) := [A \longrightarrow \mathbb{Z}[D]],$$

where the first terms are placed in degree 0. Then diagram (6) leads to a distinguished triangle in $\mathcal{D}^{\mathrm{perf}}(\mathbb{Z}[D])$:

$$\Psi^\bullet \longrightarrow \Psi_w^\bullet(\mathcal{L}) \longrightarrow \mathrm{cok}(\bar{\varphi})[0]. \tag{7}$$

Applying $\mathrm{Det}_{\mathbb{Z}[D]}(\_)$ to (7) gives an equality

$$\lambda_{L/K,w}\big(\mathrm{Det}_{\mathbb{Z}[D]}(\Psi_w^\bullet(\mathcal{L})[1])\big) = \lambda_{w,\bar{\varphi}}\big(\mathrm{Det}_{\mathbb{Z}[D]}(\Psi^\bullet[1])\big) \otimes_{\mathbb{Z}[D]} \mathrm{Det}_{\mathbb{Z}[D]}(\mathrm{cok}(\bar{\varphi})[1]),$$

where $\lambda_{w,\bar{\varphi}}$ denotes the composite isomorphism

$$\begin{aligned}
\big(\mathrm{Det}_{\mathbb{Z}[D]}(\Psi^\bullet[1])\big) \otimes \mathbb{Q} &\xrightarrow{\sim} \mathrm{Det}_{\mathbb{Q}[D]}\big(\Psi^\bullet[1] \otimes \mathbb{Q}\big) \\
&\longrightarrow \mathrm{Det}_{\mathbb{Q}[D]}(\mathbb{Q}) \otimes_{\mathbb{Q}[D]} \mathrm{Det}_{\mathbb{Q}[D]}(\mathbb{Q})^{-1} \\
&\xrightarrow{\mathrm{Det}(\bar{\varphi})\otimes\mathrm{id}} \mathrm{Det}_{\mathbb{Q}[D]}(L_w^\times(\mathcal{L}_w) \otimes \mathbb{Q}) \otimes_{\mathbb{Q}[D]} \mathrm{Det}_{\mathbb{Q}[D]}(\mathbb{Q})^{-1} \\
&\xrightarrow{\mathrm{Det}(\vartheta_w)\otimes\mathrm{id}} \mathrm{Det}_{\mathbb{Q}[D]}(\mathbb{Q}) \otimes_{\mathbb{Q}[D]} \mathrm{Det}_{\mathbb{Q}[D]}(\mathbb{Q})^{-1} \\
&\longrightarrow (\mathbb{Q}[D], 0).
\end{aligned}$$

A standard computation yields

$$\lambda_{w,\bar{\varphi}}\big(\mathrm{Det}_{\mathbb{Z}[D]}(\Psi^\bullet[1])\big) = \left(\left(\frac{1}{|D|} w_{\mathfrak{P}}(\varphi(1)) e_D + (g_0 - 1)(1 - e_D)\right)\mathbb{Z}[D], 0\right) \tag{8}$$

(see [**4**, Section 4.2] for a computation in a similar, but more complicated situation).

Therefore the main task in the computation of $I(v, \mathcal{L})$ is the computation of $\mathrm{det}_{\mathbb{Z}[D]}(\mathrm{cok}(\bar{\varphi})[1]) = \mathrm{Fitt}_{\mathbb{Z}[D]}(\mathrm{cok}(\bar{\varphi}))^{-1}$.

To that end, we first describe a procedure to compute a representation of the finite $\mathbb{Z}[D]$-module $\mathrm{cok}(\bar{\varphi})$ of the form

$$\mathrm{cok}(\bar{\varphi}) = \langle a_1 \rangle \times \ldots \times \langle a_s \rangle, \qquad \mathrm{ord}(a_i) = m_i, \tag{9}$$

together with its D-action, determined by a matrix $S_0 = S(g_0) \in \mathrm{Mat}_{s,s}(\mathbb{Z})$ such that

$$g_0(a_1, \ldots, a_s)^{\tilde{}} = S_0(a_1, \ldots, a_s)^{\tilde{}}. \tag{10}$$

Here and in what follows, $x^{\tilde{}}$ means the transpose of a matrix or vector x. Note that the ith column of S_0 is only defined modulo m_i.

In the next subsection we will then develop an algorithm which uses data of this kind to compute the Fitting ideal of a finite $\mathbb{Z}[D]$-module.

We set $F = L^D$, and we recall that $\mathcal{X}'_{(v)} = \mathcal{O}_{F,(s)}[D]\theta_v \cap \mathcal{O}_L$ with $w \mid s \mid v$ (see Section 3.1). As in Proposition 3.1, we set $\mathcal{L}_w = \mathcal{O}_{K_v}[D]\theta_v$. Let $\mathfrak{p}_v$ and $\mathfrak{P}_w$ denote, respectively, the valuation ideals in K_v and in L_w.

LEMMA 3.5. *There exists a positive integer m such that $\mathfrak{P}^m \subseteq \mathcal{X}'_{(v)}$. For each such m, one has $\mathfrak{P}_w^m \subseteq \mathcal{L}_w$, and the natural map*

$$\alpha : \mathcal{X}'_{(v)}/\mathfrak{P}^m \longrightarrow \mathcal{L}_w/\mathfrak{P}_w^m$$

is an isomorphism.

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

Proof. Let $\mathfrak{q}$ be the prime of $\mathcal{O}_F$ corresponding to the place s. Let h be a positive integer such that $\mathfrak{q}^h = b\mathcal{O}_F$, $b \in \mathcal{O}_F$. Since $\mathcal{O}_F[D]\theta_v$ is of finite index in $\mathcal{O}_L$, there is a positive integer t such that $b^t\mathcal{O}_L \subseteq \mathcal{O}_{F,(s)}[D]\theta_v$. Hence $\mathfrak{P}^{hte_{w/s}} \subseteq \mathcal{X}'_{(v)}$. Because $K_v = F_s$, one obviously has $\mathfrak{P}_w^m \subseteq \mathcal{L}_w$. The natural map $\mathcal{O}_L/\mathfrak{P}^m \longrightarrow \mathcal{O}_{L_w}/\mathfrak{P}_w^m$ is an isomorphism. Hence it suffices to show that α is surjective. Let $\lambda\theta_v \in \mathcal{L}_w$ with $\lambda \in \mathcal{O}_{K_v}[D]$. If we choose $\mu \in \mathcal{O}_K[D]$ such that $\lambda - \mu \in \mathfrak{p}_v^m$, then

$$\lambda\theta_v = \mu\theta_v + (\lambda - \mu)\theta_v \equiv \mu\theta_v \,(\mathrm{mod}\,\mathfrak{P}_w^m). \qquad \square$$

We choose m minimal, subject to the condition of Lemma 3.5. Then $U_w/U_w^{(m)} \simeq (\mathcal{O}_L/\mathfrak{P}^m)^\times$, and in addition

$$\mathrm{cok}(\bar{\varphi}) \simeq \frac{\pi_w^{\mathbb{Z}} \times U_w/U_w^{(m)}}{\varphi(1)^{\mathbb{Z}} \times (1 + \mathcal{L}_w)/U_w^{(m)}}. \tag{11}$$

We write $\mathrm{ex} : \mathcal{X}'_{(v)}/\mathfrak{P}^m \longrightarrow (\mathcal{O}_L/\mathfrak{P}^m)^\times$ for the truncated exponential map. Then (11) together with Lemma (3.5) implies that

$$\mathrm{cok}(\bar{\varphi}) = \frac{\pi_w^{\mathbb{Z}} \times (\mathcal{O}_L/\mathfrak{P}^m)^\times}{\varphi(1)^{\mathbb{Z}} \times \mathrm{ex}(\mathcal{X}'_{(v)}/\mathfrak{P}^m)}. \tag{12}$$

Remark 3.6. Let $n_v = w_{\mathfrak{P}}(\theta_v)$. The v-adic exponential map is defined for $\alpha \in \mathcal{O}_L$ with $w_{\mathfrak{P}}(\alpha) > e_w/(p-1)$ by

$$\exp(\alpha) = \sum_{n=0}^{\infty} \frac{\alpha^n}{n!}.$$

Our objective is to determine $N \in \mathbb{N}$ such that $w_{\mathfrak{P}}(\alpha^n/n!) \geqslant m$ for all $n \geqslant N$. One easily shows that $w_p(n!) < n/(p-1)$ (see [**23**, p. 49]), and it therefore suffices to take $N \geqslant m/(n_v - e_w/(p-1))$. Then we have

$$\mathrm{ex}(\alpha) = \sum_{n=0}^{N} \frac{\alpha^n}{n!} \in \left(\mathcal{O}_L/\mathfrak{P}^m\right)^\times. \tag{13}$$

We shall now describe how to apply Smith normal form (SNF) techniques to determine generators $a_1, \ldots, a_s$ as in (9) together with a matrix S_0 that explicitly gives the D-action on $\mathrm{cok}(\bar{\varphi})$. Using [**11**, Algorithm 4.2.21], we first compute a representation of $(\mathcal{O}_L/\mathfrak{P}^m)^\times$ of the form

$$\left(\mathcal{O}_L/\mathfrak{P}^m\right)^\times = \langle b_1\rangle \times \ldots \times \langle b_t\rangle, \qquad \mathrm{ord}(b_i) = k_i. \tag{14}$$

We set $b_0 := \pi_w$, and we compute $A \in \mathrm{Mat}_{t+1,t+1}(\mathbb{Z})$ such that

$$g_0(b_0, \ldots, b_t)^\sim = A(b_0, \ldots, b_t)^\sim.$$

To achieve this, we apply Algorithm 4.2.24 of [**11**] to $b_1, \ldots, b_t$, and we immediately obtain rows 1 to t. For the computation of the first row, we apply [**11**, Algorithm 4.2.24] to $g_0(\pi_w)/\pi_w$. This leads to a matrix A of the form

$$A = \begin{pmatrix} 1 & a_{01} & \cdots & a_{0t} \\ 0 & a_{11} & \cdots & a_{1t} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{t1} & \cdots & a_{tt} \end{pmatrix}. \tag{15}$$

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

Without loss of generality, we may assume that the subgroup $\mathrm{ex}(\mathcal{X}'_{(v)}/\mathfrak{P}^m)$ is also generated by t elements. Denote by $c_1, \ldots, c_t \in (\mathcal{O}_L/\mathfrak{P}^m)^\times$ a set of such generators, and set $c_0 := \varphi(1)$. Using the same techniques as for the computation of A, we obtain a matrix B such that

$$(c_0, \ldots, c_t)^\sim = B(b_0, \ldots, b_t)^\sim. \tag{16}$$

Let $S = UBV$ with $U, V \in \mathrm{Gl}_{t+1}(\mathbb{Z})$ denote the SNF of B. Let c and b denote the transposes of $(c_0, \ldots, c_t)$ and $(b_0, \ldots, b_t)$, respectively. Then $Uc = SV^{-1}b$ and the components of $a := V^{-1}b$ form a set of generators of $\mathrm{cok}(\bar{\varphi})$. The corresponding orders $m_i = \mathrm{ord}(a_i)$ are given by the diagonal elements of S. Moreover, the action of g_0 on $\mathrm{cok}(\bar{\varphi})$ on a is explicitly described by $g_0 \cdot a = (V^{-1}AV) \cdot a$. Hence we have $S_0 = V^{-1}AV$. Of course, we may delete the ith row and column in S_0 if the diagonal element s_{ii} of S equals 1.

3.4. *Computation of Fitting ideals*

In this subsection we let G denote any finite abelian group. Let C be a finite $\mathbb{Z}[G]$-module given as a direct product

$$C = \langle c_1 \rangle \times \ldots \times \langle c_s \rangle, \qquad \mathrm{ord}(c_i) = m_i,$$

together with matrices $A(g)$, $g \in G$, such that

$$g(c_1, \ldots, c_s)^\sim = A(g)(c_1, \ldots, c_s)^\sim.$$

Note that the ith column of $A(g)$ is only determined modulo m_i.

Our objective is to compute the Fitting ideal $\mathrm{Fitt}_{\mathbb{Z}[G]}(C)$. Let $G = \{g_1, \ldots, g_n\}$.

Step 1. Compute the integer kernel N of the matrix

$$M = \begin{pmatrix} & & m_1 & \\ A(g_1)^\sim, \ldots, A(g_n)^\sim, & & \ddots & \\ & & & m_s \end{pmatrix}.$$

Put $m = ns$, and let $z_1, \ldots, z_m$ denote a $\mathbb{Z}$-basis of N.

Step 2. For $z = (x_{1g_1}, \ldots, x_{sg_1}, x_{1g_2}, \ldots, x_{sg_2}, \ldots, x_{1g_n}, \ldots, x_{sg_n}, y_1, \ldots, y_s) \in \{z_1, \ldots, z_m\}$, define an element $\lambda_z \in \mathbb{Z}[G]^s$ by

$$\lambda_z = \left(\sum_{k=1}^{n} x_{ig_k} g_k \right)_{i=1,\ldots,s}.$$

Step 3. Let Ω denote the set of all subsets $I \subseteq \{1, \ldots, m\}$ of cardinality s. For each subset $I \in \Omega$, compute $\delta_I := \det(\lambda_{z_i})_{i \in I} \in \mathbb{Z}[G]$.

Step 4. Let A denote the matrix defined by

$$(\delta_I)_{I \in \Omega} = (g_1, \ldots, g_n)A.$$

Compute the HNF H of A.

Step 5. Output H (the columns of H correspond to a $\mathbb{Z}$-basis of $\mathrm{Fitt}_{\mathbb{Z}[G]}(C)$).

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

Proof of the correctness of the algorithm. Consider the epimorphism

$$\pi : \mathbb{Z}[G]^s \longrightarrow C,$$
$$(\lambda_1, \ldots, \lambda_s)^{\sim} \mapsto \sum_{i=1}^{s} \lambda_i c_i.$$

Let Q denote the kernel of π. By definition, the Fitting ideal of C is generated by all determinants of $s \times s$ matrices with columns in Q. If we set $\lambda_i = \sum_{k=1}^{n} x_{ik} g_k$, $x_{ik} \in \mathbb{Z}$, then one easily deduces that

$$\lambda = (\lambda_1, \ldots, \lambda_s)^{\sim} \in Q \iff \sum_{k=1}^{n} \sum_{i=1}^{s} A(g_k)_{ij} x_{ik} \equiv 0 \,(\mathrm{mod}\, m_j), \qquad j = 1, \ldots s.$$

Hence $\lambda \in Q$ if and only if the x_{ik} are the first m components of an integer solution of the system of linear equations in Step 1. Therefore the elements $\lambda_{z_1}, \ldots, \lambda_{z_m}$ of Step 2 constitute a $\mathbb{Z}$-basis of Q, so that the correctness of the algorithm is now immediate from the definition of the Fitting ideal. □

Remarks 3.7. (a) This naive approach is in fact very inefficient. As a consequence of working entirely over $\mathbb{Z}$, we must compute $\binom{ns}{s}$ determinants of $s \times s$ matrices over $\mathbb{Z}[G]$. Possibly a more efficient approach is to use a set $\{b_1, \ldots, b_t\}$, $t \leqslant s$, $b_i = \sum_{j=1}^{s} r_{ij} c_j$, of $\mathbb{Z}[G]$-generators of C in order to define π, as follows:

$$\pi : \mathbb{Z}[G]^t \longrightarrow C;$$
$$(\lambda_1, \ldots, \lambda_t)^{\sim} \mapsto \sum_{i=1}^{t} \lambda_i b_i.$$

This leads to a smaller system of linear equations in Step 1, and in Step 3 one has only to evaluate $\binom{tn}{t}$ determinants of $t \times t$ matrices.

In applications, one often knows that $Q = \ker(\pi)$ is $\mathbb{Z}[G]$-projective. Moreover, for small groups G, the Picard group $\mathrm{Pic}(\mathbb{Z}[G])$ is often trivial, so that Q is actually a free $\mathbb{Z}[G]$-module. It would be very desirable to have an algorithm (analogous to the HNF algorithm over $\mathbb{Z}$) that computes a $\mathbb{Z}[G]$-basis in this case. A method that computes a small set of $\mathbb{Z}[G]$-generators (without assuming the triviality of $\mathrm{Pic}(\mathbb{Z}[G])$) is described below in Appendix A.

(b) For the computation of the determinants $\det(\lambda_{ij})$, $\lambda_{ij} \in \mathbb{Q}[G]$, we suggest computing the Wedderburn decomposition of $\mathbb{Q}[G]$ explicitly, as follows:

$$\omega : \mathbb{Q}[G] \xrightarrow{\simeq} K_1 \times \ldots \times K_l, \tag{17}$$

and then evaluating the determinants in the single components. This is easy, because we can work over fields. Then one goes back to $\mathbb{Q}[G]$ via ω^{-1}.

(c) If $\mathcal{M}$ denotes the maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$, then

$$\mathcal{M} \simeq \mathcal{O}_{K_1} \times \ldots \times \mathcal{O}_{K_l}.$$

Thus we can use the isomorphism ω to compute the Fitting ideal

$$\begin{aligned} \mathrm{Fitt}_{\mathcal{M}}(C \otimes_{\mathbb{Z}[G]} \mathcal{M}) &= \mathrm{Fitt}_{\mathbb{Z}[G]}(C) \otimes_{\mathbb{Z}[G]} \mathcal{M} \\ &= \mathrm{Fitt}_{\mathbb{Z}[G]}(C)\mathcal{M}. \end{aligned}$$

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

Let $e_1, \dots, e_l$ denote the idempotents corresponding to the decomposition (17). Then

$$\mathrm{Fitt}_{\mathcal{M}}(C \otimes_{\mathbb{Z}[G]} \mathcal{M}) = \bigoplus_{i=1}^{l} \mathrm{Fitt}_{e_i \mathcal{M}}(C \otimes_{\mathbb{Z}[G]} e_i \mathcal{M}) \quad \text{and} \quad e_i \mathcal{M} \simeq \mathcal{O}_{K_i}.$$

Thus we can use HNF techniques over Dedekind domains to compute the Fitting ideal over the maximal order. Unfortunately, we could not find an algorithm that computes $\mathrm{Fitt}_{\mathbb{Z}[G]}(C)$ from knowledge of $\mathrm{Fitt}_{\mathbb{Z}[G]}(C)\mathcal{M}$.

3.5. *Computation of* $\rho_{L/K}(\det_{\mathbb{Z}[G]}(\mathcal{L}))$

The algorithm of Subsection 3.1 produces a finitely generated projective $\mathbb{Z}[G]$-sublattice $\mathcal{L}$ of L given by a $\mathbb{Z}$-basis $\omega_1, \dots, \omega_m$, $m = [L : \mathbb{Q}]$, $\omega_i \in \mathcal{O}_L$. We choose a normal basis element θ of L/K and a $\mathbb{Z}$-basis $\nu_1, \dots, \nu_k$, $k = [K : \mathbb{Q}]$, of $\mathcal{O}_K$. Then $\nu_1\theta, \dots, \nu_k\theta$ is a $\mathbb{Q}[G]$-basis of L.

In the first step of our procedure to compute $\rho_{L/K}(\det_{\mathbb{Z}[G]}(\mathcal{L}))$, we determine the matrix $A \in \mathrm{Mat}_{k,m}(\mathbb{Q}[G])$ such that

$$(\omega_1, \dots, \omega_m) = (\nu_1\theta, \dots, \nu_k\theta)A.$$

Let Ω denote the set of all subsets $I \subseteq \{1, \dots, m\}$ of cardinality k, and write a_i for the ith column of A. For each $I \in \Omega$, we set

$$\delta_I := \det (a_i)_{i \in I},$$

and we compute the invertible $\mathbb{Z}[G]$-module

$$\mathfrak{a} = \mathfrak{a}_{\theta, \nu_1, \dots, \nu_k} := \langle \delta_I : I \in \Omega \rangle_{\mathbb{Z}}.$$

Then we have

$$\rho_{L/K}\big(\det_{\mathbb{Z}[G]}(\mathcal{L})\big) = \mathfrak{a} \cdot \rho_{L/K}(\nu_1\theta \wedge \ldots \wedge \nu_k\theta),$$

so that it remains to give an explicit expression for $\rho_{L/K}(\nu_1\theta \wedge \ldots \wedge \nu_k\theta)$. By the definition of $\rho_{L/K}$, we obtain

$$\begin{aligned}
&\rho_{L/K}(\nu_1\theta \wedge \ldots \wedge \nu_k\theta) \\
&\quad = \left(\sum_{g \in G} \hat{\tau} g (\nu_1\theta) g^{-1}\right)_{\tau \in \Sigma(K)} \wedge \ldots \wedge \left(\sum_{g \in G} \hat{\tau} g (\nu_k\theta) g^{-1}\right)_{\tau \in \Sigma(K)} \\
&\quad = \det \left(\sum_{g \in G} \hat{\tau} g (\nu_i\theta) g^{-1}\right)_{\substack{\tau \in \Sigma(K) \\ i = 1, \dots, k}} (w_1 \wedge \ldots \wedge w_k),
\end{aligned}$$

where $w_1, \dots, w_k$ denotes the canonical $\mathbb{C}[G]$-basis of $\mathbb{C}[G]^k$. Finally, we obtain

$$\det \left(\sum_{g \in G} \hat{\tau} g (\nu_i\theta) g^{-1}\right)_{\tau, i} = \det (\tau(\nu_i))_{\tau, i} \, \mathcal{N}_{K/\mathbb{Q}}(\theta)$$

with the norm-resolvent

$$\mathcal{N}_{K/\mathbb{Q}}(\theta) := \prod_{\tau \in \Sigma(K)} \sum_{g \in G} \hat{\tau} g(\theta) g^{-1} \in \mathbb{C}[G].$$

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

Summing up, we have derived the following expression, which is very convenient for our computational purposes:

$$\rho_{L/K}(\det_{\mathbb{Z}[G]}(\mathcal{L})) = \mathfrak{a} \cdot \det\left(\tau(v_i)\right)_{\substack{\tau \in \Sigma(K) \\ i=1,\dots,k}} \cdot \mathcal{N}_{K/\mathbb{Q}}(\theta).$$

Remarks 3.8. (a) For the computation of $\mathfrak{a}$, the same remarks apply as for the computation of Fitting ideals (see Remark 3.7).

(b) We represent each element λ of $\mathfrak{a}$ as a column vector $v \in \mathbb{Q}^n$ with respect to the $\mathbb{Q}$-basis of $\mathbb{Q}[G]$ consisting of the group elements $g_1, \dots, g_n$. By clearing denominators and applying the HNF algorithm, we may assume that the invertible $\mathbb{Z}[G]$-submodule $\mathfrak{a} \subseteq \mathbb{Q}[G]$ is given in HNF.

3.6. *Computation of* $\xi_{L/K}$

Recall that $\xi_{L/K} = \tau_{L/K} \prod_{v|d_L} {}^*(-f_v^{-1})$. If we write χ_0 for the trivial character of G, then by [**14**, Chapter III, (2.1)], one has

$$\tau\left(\mathbb{Q}, \mathrm{ind}_K^{\mathbb{Q}}(\chi)\right) = \tau\left(\mathbb{Q}, \mathrm{ind}_K^{\mathbb{Q}}(\chi_0)\right)\tau(K, \chi).$$

Furthermore, by [**18**, Chapter II, Theorem 8.1(iii)], we have

$$\tau\left(\mathbb{Q}, \mathrm{ind}_K^{\mathbb{Q}}(\chi_0)\right) = \pm \det\left(\tau(v_i)\right)_{\tau \in \Sigma(K), i=1,\dots,k},$$

where we continue to use the notation of Subsection 3.5. Hence we have

$$\xi_{L/K} = \pm \left(\prod_{v|d_L} {}^*(-f_v^{-1}) \right) \cdot \det\left(\tau(v_i)\right)_{\tau,i} \cdot \sum_{\chi \in \hat{G}} \tau(K, \chi) e_\chi.$$

Finally, we apply [**11**, Algorithm 6.2.4 (4)] for the computation of $\tau(K, \chi)$.

3.7. *Numerical verification of the conjecture*

It is easily checked that the grading in the formulation of Conjecture (2.1) is correct, so that the real task is to check the equality of the underlying invertible $\mathbb{Z}[G]$-modules. Hence we have to verify that

$${\xi_{L/K}}^{-1} \cdot \rho_{L/K}(\det_{\mathbb{Z}[G]}(\mathcal{L})) \prod_{v \in \mathcal{W}(L/K)} I(v, \mathcal{L}) = \mathbb{Z}[G].$$

Summarizing the computations and results of the previous subsections, we see that this is equivalent to proving that the invertible $\mathbb{Z}[G]$-submodule $\lambda \cdot I \subset \mathbb{C}[G]$, with

$$\lambda = \left(\prod_{v|d_L} {}^*(-f_v^{-1}) \right)^{-1} \left(\sum_{\chi \in \hat{G}} \tau(K, \chi) e_\chi \right)^{-1} \mathcal{N}_{K/\mathbb{Q}}(\theta), \tag{18}$$

and

$$I = \mathfrak{a} \prod_{v \in \mathcal{W}(L/K)} \mathcal{E}_{L/K,v} \cdot \Lambda_{w,\varphi_v} \cdot \mathrm{Fitt}_{\mathbb{Z}[G_v]}(\mathrm{cok}(\bar{\varphi}_v))^{-1}, \tag{19}$$

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

is actually equal to $\mathbb{Z}[G]$. Here, we write φ_v for the map φ constructed in Subsection 3.2 for a fixed place $v \in \mathcal{W}(L/K)$, and Λ_{w,φ_v} is defined by

$$\Lambda_{w,\varphi_v} = \frac{1}{|G_v|} w\mathfrak{P}(\varphi_v(1))e_{G_v} + (g_{v,0} - 1)(1 - e_{G_v})$$

with $\langle g_{v,0}\rangle = G_v$ (compare this to (8)). By definition, I is an invertible $\mathbb{Z}[G]$-submodule of $\mathbb{Q}[G]$ for which we compute its HNF (see Remark 3.9 (b)). The element λ lives a priori in $\mathbb{C}[G]$, but from [**15**, Section 9, (i) and (ii)] one may actually deduce that it is an element in $\mathbb{Q}[G]$. Multiplying I by the scalar λ gives a $\mathbb{Z}[G]$-submodule of $\mathbb{C}[G]$, given by a $\mathbb{Z}$-basis $\lambda_1, \ldots, \lambda_n \in \mathbb{C}[G]$. These elements are expected to be in $\mathbb{Z}[G]$. If this is confirmed by the results of our computation, we round off the coefficients of each λ_i (see Remark 3.9 (a)) and obtain elements $\tilde{\lambda}_1, \ldots, \tilde{\lambda}_n \in \mathbb{Z}[G]$. Then we compute the HNF of $\langle \tilde{\lambda}_1, \ldots, \tilde{\lambda}_n\rangle_{\mathbb{Z}}$, and check whether $\langle \tilde{\lambda}_1, \ldots, \tilde{\lambda}_n\rangle_{\mathbb{Z}} = \mathbb{Z}[G]$. If this holds true, Conjecture 2.1 is verified up to the precision of the computation.

Remarks 3.9. (a) In principle, it is possible to do all the computations exactly, so that our algorithm would really prove the validity of Conjecture 2.1 for a given extension L/K. Indeed, the Galois Gauss sums $\tau(K, \chi)$ and also the coefficients of $\mathcal{N}_{K/\mathbb{Q}}(\theta)$ are algebraic numbers, so that we could perform all the computations in a large enough number field.

(b) For the computation of the ideal I, we need to know how to invert invertible ideals $M = \langle \lambda_1, \ldots, \lambda_n\rangle_{\mathbb{Z}} \subseteq \mathbb{Q}[G]$. Let $b : \mathbb{Q}[G] \times \mathbb{Q}[G] \longrightarrow \mathbb{Q}$ denote the non-degenerate bilinear form induced by

$$b(g, h) = \begin{cases} 1, & \text{if } gh = 1, \\ 0, & \text{otherwise,} \end{cases}$$

for $g, h \in G$. Then it is easily shown that

$$M^{-1} = \{\lambda \in \mathbb{Q}[G] \mid b(\lambda, M) \subseteq \mathbb{Z}\}.$$

Therefore $M^{-1} = \langle \lambda_1^*, \ldots, \lambda_n^*\rangle_{\mathbb{Z}}$, where $\lambda_1^*, \ldots, \lambda_n^*$ denotes the dual basis of $\lambda_1, \ldots, \lambda_n$ with respect to b.

4. *An example*

The algorithm described in Section 3 was implemented under PARI-GP [**1**], Version 2.0.20, for cyclic extensions L/K of odd prime degree l of a real quadratic number field K. For simplicity we also assumed that the class number of K is trivial. We describe an explicit example. All the computations were done with a real precision of 28 significant digits. Let $K = \mathbb{Q}(\sqrt{3})$, and set $\omega = \sqrt{3}$. We let $\mathfrak{f} = \mathfrak{p}_0^3\mathfrak{p}_1$ with

$$\mathfrak{p}_0 = (\omega), \qquad \mathfrak{p}_1 = (5).$$

The PARI function `bnrinit` computes the ray class group $\mathrm{cl}_{\mathfrak{f}}(K)$, which is of order 36, generated by two elements $[\mathfrak{g}_1]$ and $[\mathfrak{g}_2]$, where $\mathfrak{g}_1 = (1 + 6\omega)$, $\mathfrak{g}_2 = (11)$, $\mathrm{ord}([\mathfrak{g}_1]) = 12$ and $\mathrm{ord}([\mathfrak{g}_2]) = 3$. We let L denote the class field corresponding to the subgroup $\mathcal{H} = \langle 3[\mathfrak{g}_1], [\mathfrak{g}_1] + [\mathfrak{g}_2]\rangle$. Then L has conductor $\mathfrak{f}$. We use the PARI-routine `bnrstark` to compute the defining polynomial

$$h(x) = x^6 - 30x^4 - 10x^3 + 225x^2 + 150x - 275.$$

Let α denote a root of h, so that $L = \mathbb{Q}(\alpha)$.

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

By applying `bnfinit`, we obtain the ring of integers, the ideal class group and a system of fundamental units for L. The class number of L is 1.

We let $\mathfrak{c}_0 = \mathfrak{g}_1$ be a fixed representative of $\mathrm{cl}_{\mathfrak{f}}(K)/\mathcal{H}$, and we use `nfgaloisconj` to compute $G = \mathrm{Gal}(L/K)$. It is absolutely essential for the subsequent computations that we choose $g_0 \in G$ such that $(\mathfrak{c}_0, L/K) = g_0$. In this specific example, g_0 is given by the substitution

$$\alpha \leftarrow \frac{1}{5}\alpha^5 - \frac{2}{5}\alpha^4 - 5\alpha^3 + 8\alpha^2 + 24\alpha - 20.$$

If we carry out the algorithm of Subsection 3.1, we obtain a $\mathbb{Z}[G]$-projective sublattice $\mathcal{L} \subseteq L$, which is given by $\mathcal{L} = \mathcal{O}_K[G]\theta_v$, where $\theta_v = 3\alpha + 3$ is a normal basis element satisfying the valuation condition of Step 1 at the only wildly ramified place $v = \mathfrak{p}_0 \in \mathcal{W}(L/K)$.

As described in Subsection 3.2, we fix a map $\varphi_v : \mathbb{Z} \longrightarrow L_w^\times$ by setting $\varphi_v(1) = -2\omega + 3$. The main effort of the whole computation is now the determination of $\mathrm{Fitt}_{\mathbb{Z}[G]}(\mathrm{cok}(\bar{\varphi}_v))$. We easily check that $\mathfrak{P}^{12} \subseteq \mathcal{O}_K[G]\theta_v$, so that we may take $m = 12$. By applying `idealstar`, we obtain a representation of $(\mathcal{O}_L/\mathfrak{P}^m)^\times$ as in (14), with

$$\begin{aligned}
b_1 &= \frac{-2}{5}\alpha^5 - \frac{1}{10}\alpha^4 + \frac{1}{5}\alpha^3 - \frac{1}{9}2\alpha^2 - \frac{3}{2}\alpha + 1;\\
b_2 &= \alpha^2 + 2\alpha + 2;\\
b_3 &= \frac{1}{10}\alpha^5 + \frac{1}{5}\alpha^3 + \frac{5}{2}\alpha^2 + \frac{3}{2}\alpha + \frac{9}{2};\\
b_4 &= \frac{-2}{5}\alpha^5 + \frac{1}{5}\alpha^4 - \frac{1}{10}\alpha^3 + 3\alpha^2 - \frac{7}{2}\alpha - \frac{7}{2};\\
b_5 &= \frac{-3}{10}\alpha^5 - \frac{3}{10}\alpha^4 - \frac{3}{10}\alpha^3 - \frac{3}{2}\alpha - 2;\\
b_6 &= \frac{-3}{10}\alpha^5 - \frac{3}{10}\alpha^4 - \frac{3}{10}\alpha^3 - \frac{9}{2}\alpha - 2.
\end{aligned}$$

The corresponding orders are $k_1 = 54$, $k_2 = 9$, $k_3 = 9$, $k_4 = 9$, $k_5 = 3$ and $k_6 = 3$. As a uniformizing element for $\mathfrak{P}$, we use

$$\pi_w = \frac{1}{10}\alpha^4 + \frac{1}{5}\alpha^3 - \frac{3}{2}\alpha^2 - \frac{3}{2}\alpha + 4,$$

and we set $b_0 := \pi_w$. Using the PARI-function `ideallog`, we compute the matrix A of (15), which is given by

$$A = \begin{pmatrix}
1 & 48 & 7 & 6 & 0 & 1 & 2\\
0 & 7 & 2 & 3 & 4 & 1 & 2\\
0 & 36 & 4 & 8 & 3 & 0 & 2\\
0 & 18 & 6 & 1 & 6 & 0 & 0\\
0 & 18 & 6 & 8 & 7 & 1 & 1\\
0 & 0 & 0 & 6 & 0 & 1 & 0\\
0 & 18 & 6 & 0 & 3 & 0 & 1
\end{pmatrix}.$$

The finite group $\mathcal{O}_K[G]\theta_v/\mathfrak{P}^m$ is of order 27, and we use $N = 4$ for the computation of the truncated exponential map. Computing the SNF of the matrix B of (16), we get

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

$S = \mathrm{diag}(54, 9, 9, 3, 3, 1, 1)$ and

$$S_0 = \begin{pmatrix} 13 & 4 & 0 & 0 & 1 \\ 30 & 7 & 3 & 0 & 1 \\ 0 & 2 & 4 & 1 & 0 \\ 18 & 6 & 6 & 1 & 1 \\ 36 & 6 & 0 & 0 & 1 \end{pmatrix},$$

as described at the end of Subsection 3.3.

The Fitting ideal algorithm of Subsection 3.4 produces

$$H = \begin{pmatrix} 54 & 27 & 27 \\ 0 & 27 & 0 \\ 0 & 0 & 27 \end{pmatrix},$$

where the columns of H correspond to group ring elements of $\mathbb{Z}[G]$ with respect to the basis $1, g_0, g_0^2$.

For the computation of $\rho_{L/K}(\det_{\mathbb{Z}[G]}(\mathcal{L}))$, we use $\nu_1 = 1$, $\nu_2 = \omega$ and $\theta = \theta_v$. This choice leads to the invertible $\mathbb{Z}[G]$-submodule $\mathfrak{a} = \mathbb{Z}[G]$. For the extensions $\hat{\tau}_1$ and $\hat{\tau}_2$ of $\tau_1 = \mathrm{id}$ and $\tau_2 : \sqrt{d} \mapsto -\sqrt{d}$, we choose the embeddings of L into $\mathbb{C}$ uniquely determined by

$$\hat{\tau}_1 : \alpha \mapsto -4.232158344254195574103447999,$$
$$\hat{\tau}_2 : \alpha \mapsto -2.313012978428015564785340824.$$

Then we obtain

$$\begin{aligned} \mathcal{N}_{K/\mathbb{Q}}(\theta) = {} & 810.017807631172841752337 1276 \\ & + 255.945175443589494220895 7510 \cdot g_0 \\ & + (-785.370752248604214421786 5714) \cdot g_0^2. \end{aligned}$$

The evaluation of the Gauss sums leads to

$$\begin{aligned} \tau_{L/K} = {} & (39.721957119571611108376902 14 - 0.000000000000000000000000006i) \\ & + (-57.933764642353232032986283 89 + 0.000000000000000000000000014i) \cdot g_0 \\ & + (21.675909137919375511664274 43 - 0.000000000000000000000000007i) \cdot g_0^2. \end{aligned}$$

The quotient $\lambda := \mathcal{N}_{K/\mathbb{Q}}(\theta)/\xi_{L/K}$, which is known to be rational, is then given by

$$\begin{aligned} \lambda = {} & (26.999999999999999999999999 + 0.000000000000000000000000000i) \\ & + (35.999999999999999999999998 + 0.000000000000000000000000001i) \cdot g_0 \\ & + (17.999999999999999999999999 - 0.000000000000000000000000002i) \cdot g_0^2, \end{aligned}$$

and for the $\mathbb{Z}[G]$-submodule I of (19) we obtain

$$I = \left\langle \frac{1}{9}, \frac{1}{9} g_0, \frac{1}{243}(19 + 10g_0 + g_0^2) \right\rangle_{\mathbb{Z}}.$$

Finally, we compute λI, which is given by the $\mathbb{Z}$-generators

$$2.99999\ldots + 3.99999\ldots g_0 + 1.99999\ldots g_0^2;$$
$$1.99999\ldots + 2.99999\ldots g_0 + 3.99999\ldots g_0^2;$$
$$2.99999\ldots + 3.99999\ldots g_0 + 2.99999\ldots g_0^2.$$

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

As predicted by Conjecture 2.1, all the coefficients are approximately rational integers. To simplify the presentation of these numerical results, we have given only 6 decimal digits. In fact, the computation produced group ring elements whose coefficients agree with rational integers in the first 27 decimal digits. If we round off and compute the HNF, we finally see that $\lambda I = \mathbb{Z}[G]$, and we have thus numerically verified Conjecture 2.1.

The algorithm has been applied to many more examples, each time establishing the validity of Conjecture 2.1; see Appendix B for the numerical results.

Acknowledgements. I am very grateful to D. Kusnezow, who implemented the algorithm under PARI-GP, and to M. Breuning, for his careful reading of this manuscript. This work was supported by a DFG grant.

Appendix A. *Small generating sets for $\mathbb{Z}[G]$-lattices*

by D. Kusnezow

Let G denote an abelian group of order n. In this appendix, we address the problem of computing a small set of $\mathbb{Z}[G]$-generators of a $\mathbb{Z}[G]$-sublattice $M \subseteq \mathbb{Z}[G]^s$, $s \in \mathbb{N}$.

Let $\hat{G}$ denote the group of abelian characters of G. The absolute Galois group $\Omega = \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ acts on $\hat{G}$, and the $\mathbb{Q}[G]$-irreducible characters are parametrized by the Ω-orbits of $\hat{G}$. If we set $\mathbb{Q}(\chi) := \mathbb{Q}(\chi(G))$, then the orbit of an abelian character χ is given by $[\chi] := \{\chi^\omega \mid \omega \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})\}$. We choose a set $\{\chi_1, \ldots, \chi_r\}$ of representatives of $\hat{G}$ modulo the action of Ω. For each $\chi \in \hat{G}$, we extend χ by linearity to $\mathbb{Q}[G]$, and we fix an isomorphism

$$\omega : \mathbb{Q}[G] \longrightarrow \bigoplus_{i=1}^{r} \mathbb{Q}(\chi_i), \qquad \lambda \mapsto (\chi_i(\lambda))_i.$$

Note that ω depends on the choice of $\chi_1, \ldots, \chi_r$.

The primitive idempotents of $\mathbb{Q}[G]$ are then given by $e_i = \sum_{\psi \in [\chi_i]} e_\psi$, $i = 1, \ldots, r$, where e_ψ denotes the usual idempotent associated to the absolutely irreducible character ψ.

The strategy for our algorithm is to adapt the Hermite normal form (HNF) algorithm over $\mathbb{Z}$. As a first step, we develop a method that will replace the Euclidean algorithm.

ALGORITHM A.1. Given a $\mathbb{Z}[G]$-ideal $I = \langle \lambda_1, \ldots, \lambda_m \rangle_{\mathbb{Z}[G]} \subseteq \mathbb{Z}[G]$, this algorithm computes a set of generators $\mathcal{V}$ for I of cardinality $2r$.

Step 1. Perform the HNF-algorithm over $\mathbb{Z}$ to obtain at most n $\mathbb{Z}$-generators for I. Set $\mathcal{K} \leftarrow I$, $\mathcal{V} \leftarrow \emptyset$ and $i \leftarrow 1$.

Step 2. Compute a two-element representation of the $\mathcal{O}_{\mathbb{Q}(\chi_i)}$-ideal $\chi_i(\mathcal{K})$, $\chi_i(\mathcal{K}) = (a, b)$, and let $\alpha, \beta \in \mathcal{K}$ be such that $\chi_i(\alpha) = a$ and $\chi_i(\beta) = b$. Set $\mathcal{V} \leftarrow \mathcal{V} \cup \{\alpha, \beta\}$.

Step 3. If $i = r$ terminate the algorithm. If $i < r$, compute the kernel of $\chi_i : \mathcal{K} \to \mathcal{O}_{\mathbb{Q}(\chi_i)}$ and set $\mathcal{K} \leftarrow \ker(\chi_i)$, $i \leftarrow i + 1$. Go to Step 2.

REMARKS A.1. (a) In Step 2, one could also check whether $\chi_i(\mathcal{K})$ is principal. This leads to a generating set $\mathcal{V}$ with $|\mathcal{V}| < 2r$ (note that for the trivial character χ_0 one has $\mathbb{Q}(\chi_0) = \mathbb{Q}$).

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

(b) To compute the kernel of χ_i in Step 3, one has to compute the integer kernel of a system of linear equations arising from $\lambda \in \ker(\chi_i) \iff \lambda e_i = 0$. Applying the HNF algorithm over $\mathbb{Z}$, we may assume that in each iteration $\mathcal{K}$ is given by at most n $\mathbb{Z}$-generators.

(c) Since $\chi_i : \mathbb{Z}[G] \to \mathcal{O}_{\mathbb{Q}(\chi_i)}$ is surjective, it follows that in Step 2 one has $\mathcal{K} = \langle \alpha, \beta \rangle_{\mathbb{Z}[G]} + \ker(\chi_i)$. This proves the correctness of the algorithm.

Now let $M \subseteq \mathbb{Z}[G]^s$, $s > 0$, be a $\mathbb{Z}[G]$-module. Using HNF techniques over $\mathbb{Z}$, we may always assume that M is given by $\mathbb{Z}[G]$-generators $m_1, \dots, m_k \in \mathbb{Z}[G]^s$ with $k \leqslant ns$. Let $m_j = (\lambda_{1j}, \dots, \lambda_{sj})^\sim$ with $\lambda_{ij} \in \mathbb{Z}[G]$. We will always identify M with the matrix $(m_1, \dots, m_k)$.

ALGORITHM A.2. Given M as above, this algorithm computes a set of $\mathbb{Z}[G]$-generators $\bar{m}_1, \dots, \bar{m}_N$ of M with $N \leqslant 2rs$.

Step 1. Set $i \leftarrow s$, $\bar{M} \leftarrow \emptyset$ and $A \leftarrow M$. (We always identify $A = (a_{ij})$ with the $\mathbb{Z}[G]$-module generated by the columns of A.)

Step 2. Set $I \leftarrow \langle a_{i1}, \dots, a_{ik} \rangle_{\mathbb{Z}[G]}$ and apply Algorithm A.1 to compute a set $\mu_1, \dots, \mu_t$ of $\mathbb{Z}[G]$-generators of I with $t \leqslant 2r$.

Step 3. Compute $\bar{a}_1, \dots, \bar{a}_t \in A$ such that $\bar{a}_{ij} = \mu_j$, $j = 1, \dots, t$, and set $\bar{M} \leftarrow \{\bar{a}_1, \dots, \bar{a}_t\} \cup \bar{M}$.

Step 4. For $j = 1, \dots, k$ represent a_{ij} as a linear combination of the $\bar{a}_{iv} = \mu_v$, $v = 1, \dots, t$ as follows:

$$a_{ij} = \sum_{v=1}^{t} \xi_v \bar{a}_{iv}, \qquad \xi_v \in \mathbb{Z}[G],$$

and eliminate the ith row in A by elementary column operations.

Step 5. If $i = 1$, terminate the algorithm. Otherwise, set $i \leftarrow i - 1$ and go to Step 2.

REMARKS A.2. (a) Algorithm A.2 produces a matrix $\bar{M}$ in the following block form.

$$\begin{pmatrix}
* & * & * & & & * \\
0 & * & * & & & * \\
0 & 0 & \cdot & & & * \\
0 & 0 & 0 & \cdot & & * \\
0 & 0 & 0 & 0 & \cdot & * \\
0 & 0 & 0 & 0 & 0 & *
\end{pmatrix}$$

In addition, each of the s blocks has at most $2r$ columns.

Applying Algorithm A.2 to the module $\langle \lambda_{z_1}, \dots, \lambda_{z_m} \rangle_{\mathbb{Z}[G]}$ arising in Step 2 of the Fitting ideal algorithm of Section 3.4 enormously reduces the number of determinants that have to be computed in Step 3 of that algorithm. Even without considering the special form of the new generating system, we have only to evaluate at most $\binom{2rs}{s}$ determinants (compare Remark 3.7 (a)).

(b) For the computation of $\bar{a}_1, \dots, \bar{a}_t$ in Step 3 of Algorithm A.2, we need to find a representation of the form $\mu_j = \sum_{v=1}^{k} x_v a_{iv}$, $x_v \in \mathbb{Z}[G]$ for each $j = 1, \dots, t$. Then $\bar{a}_j = \sum_{v=1}^{k} x_v a_v$. This leads to a system of linear equations with integral coefficients, for which we compute an integral solution.

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

Appendix B. *Numerical computations*

This appendix contains the PARI sources of our implementation of the algorithm described in Section 3, and also a file of examples to which it was applied. These files may be found at

`http://www.lms.ac.uk/jcm/6/lms2002-021/appendix-b`.

References

1. C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, 'User's guide to PARI/GP', 2000; `http://www.parigp-home.de`. 69, 82

2. W. Bley, 'Computing associated orders and Galois generating elements of unit lattices', *J. Number Theory* 62 (1997) 242–256. 73

3. W. Bley and D. Burns, 'Étale cohomology and a generalisation of Hilbert's theorem 132', *Math. Z.* 239 (2002) 1–25. 68, 68, 68, 68, 69, 70, 71, 71, 71

4. W. Bley and D. Burns, 'Equivariant epsilon constants, discriminants and étale cohomology', *J. London Math. Soc.*, to appear. 68, 68, 68, 68, 71, 71, 76

5. M. Breuning, 'On equivariant global epsilon constants for certain dihedral extensions', *Math. Comp.*, to appear. 69

6. D. Burns, 'Equivariant Tamagawa numbers and Galois module theory I', *Compositio Math.* 129 (2001) 203–237. 68

7. D. Burns, 'Equivariant Tamagawa numbers and Galois module theory II', preprint, 1998. 68

8. D. Burns and M. Flach, 'On Galois structure invariants associated to Tate motives', *Amer. J. Math.* 120 (1998) 1343–1397. 71

9. T. Chinburg, 'On the Galois structure of algebraic integers and S-units', *Invent. Math.* 74 (1983) 321–349. 68

10. H. Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math. 138 (Springer, Berlin/Heidelberg/New York, 1995). 73, 74

11. H. Cohen, *Advanced topics in computational number theory*, Grad. Texts in Math. 193 (Springer, New York/Berlin/Heidelberg, 2000). 72, 72, 75, 77, 77, 77, 81

12. C. Curtis and I. Reiner, *Methods of representation theory*, vol. I, Wiley Classics Library (Wiley, New York/Chichester/Brisbane/Toronto, 1994). 73

13. B. Erez, 'A survey of recent work on the square root of the inverse different', *Journées arithmétiques*, Exp. Congr., Luminy/Fr. 1989, *Astérisque* 198–200 (1991) 133–152. 73, 73

14. A. Fröhlich, *Galois module structure of algebraic integers* (Springer, Heidelberg, 1983). 70, 70, 81

15. A. Fröhlich, 'L-values at zero and multiplicative Galois module structure (also Galois–Gauss sums and additive Galois module structure)', *J. Reine Angew. Math.* 397 (1989) 42–99. 82

16. D. Hilbert, 'Die Theorie der algebraischen Zahlkörper', *Jahresber. Deutsch. Math.-Verein.* 4 (1897). 68

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press

17. F. Knudsen and D. Mumford, 'The projectivity of the moduli space of stable curves I: Preliminaries on "det" and "Div" ', *Math. Scand.* 39 (1976) 19–55. 69

18. J. Martinet, 'Character theory and Artin L-functions', *Algebraic number fields* (ed. A. Fröhlich, Academic Press, 1977). 81

19. B. Mazur and A. Wiles, 'Class fields of abelian extensions of $\mathbb{Q}$', *Invent. Math.* 76 (1984) 179–330. 69

20. J. Neukirch, *Algebraische Zahlentheorie* (Springer, Heidelberg, 1992). 73

21. C. Popescu, 'On a refined Stark conjecture for function fields', *Compositio Math.* 116 (1999) 321–367. 69

22. X. F. Roblot, 'Algorithmes de factorisation dans les extensions relatives et application de la conjecture de Stark à la construction des corps de classes de rayon', Thesis, Université Bordeaux I, 1997. 72

23. L. Washington, *Introduction to cyclotomic fields*, Grad. Texts in Math. 83 (Springer, New York/Heidelberg/Berlin, 1982). 77

W. Bley bley@math.uni-augsburg.de
http://www.math.uni-augsburg.de/∼bley

Institut für Mathematik
Universität Augsburg
Universitätsstrasse 8
D-86135 Augsburg
Germany

https://doi.org/10.1112/S1461157000000383 Published online by Cambridge University Press