London Mathematical Society ISSN 1461–1570

PICARD GROUPS AND REFINED DISCRETE LOGARITHMS

W. BLEY AND M. ENDRES

Abstract

Let K denote a number field, and G a finite abelian group. The ring of algebraic integers in K is denoted in this paper by $\mathcal{O}_K$, and $\mathcal{A}$ denotes any $\mathcal{O}_K$-order in $K[G]$. The paper describes an algorithm that explicitly computes the Picard group $\mathrm{Pic}(\mathcal{A})$, and solves the corresponding (refined) discrete logarithm problem. A tamely ramified extension L/K of prime degree l of an imaginary quadratic number field K is used as an example; the class of $\mathcal{O}_L$ in $\mathrm{Pic}(\mathcal{O}_K[G])$ can be numerically determined.

1. *Introduction*

We fix a number field K and a finite abelian group G. For any number field L, we let $\mathcal{O}_L$ denote its ring of algebraic integers. If R is any commutative ring (always with identity 1), we write $R[G]$ for the group ring with coefficients in R.

Let $\mathcal{A} \subseteq K[G]$ denote an $\mathcal{O}_K$-order. In this paper, we describe a complete algorithm that explicitly computes the Picard group $\mathrm{Pic}(\mathcal{A})$. More precisely, we show how to construct explicit invertible $\mathcal{A}$-sublattices $\mathfrak{g}_1, \ldots, \mathfrak{g}_g$ of $K[G]$ such that

$$\mathrm{Pic}(\mathcal{A}) \simeq \bigoplus_{i=1}^{g} (\mathbb{Z}/f_i\mathbb{Z})\,[\mathfrak{g}_i]$$

with integers $f_i > 1$, $f_{i+1} \mid f_i$. Here, $[\mathfrak{g}_i]$ denotes the isomorphism class of $\mathfrak{g}_i$. In addition, we provide an algorithm that solves the corresponding *refined* discrete logarithm problem. By this, we mean the following problem: Given any invertible $\mathcal{A}$-submodule $\mathfrak{a}$ of $K[G]$, find integers x_i, $0 \leqslant x_i < f_i$, and an element $\lambda \in K[G]$ such that $\mathfrak{a} = \lambda \mathfrak{g}_1^{x_1} \ldots \mathfrak{g}_g^{x_g}$. Note that this is much finer than just solving the discrete logarithm problem in $\mathrm{Pic}(\mathcal{A})$.

Our main motivation originated in the study of the Galois module structure of integer rings $\mathcal{O}_L$ in finite abelian extensions L/K with group G. When L/K is at most tamely ramified, then it is well known, by a theorem of Noether, that $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-projective. So the natural question arises, as to whether $\mathcal{O}_L$ is actually a free $\mathcal{O}_K[G]$-module or, in other words: "Does there exist a normal integral basis?" More generally, we could ask for an explicit description (theoretical or algorithmic) of the class $[\mathcal{O}_L]$ of $\mathcal{O}_L$ in $\mathrm{Pic}(\mathcal{O}_K[G])$.

If we restrict scalars and consider $\mathcal{O}_L$ as a $\mathbb{Z}[G]$-module, then there is a well-established and beautiful theory due to Fröhlich and Taylor, which shows that $[\mathcal{O}_L]$ is always trivial in $\mathrm{Pic}(\mathbb{Z}[G])$. However, if we study $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module, the situation is poorly understood, and there are only partial theoretical results, mainly for abelian extensions of imaginary quadratic fields K (see [**1**, **13**]).

If we leave the tamely ramified case, the situation is even worse. The prototypical result in this context is due to Leopoldt, who proved that for any abelian extension $L/\mathbb{Q}$, the ring

Received 18 December 2003, revised 2 November 2004; *published* 31 January 2005.
2000 Mathematics Subject Classification 11R27, 11R33, 11G15

of integers $\mathcal{O}_L$ is free over its associated order

$$\mathcal{A}_{L/\mathbb{Q}}(\mathcal{O}_L) := \{\lambda \in \mathbb{Q}[G] \mid \lambda\mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

In general, however, $\mathcal{O}_L$ is not even locally free over $\mathcal{A}_{L/K}(\mathcal{O}_L)$ (see, for example, [7]), so that it is not clear that the concept of associated orders provides the proper framework. On the other hand, there are deep and interesting results for wildly ramified abelian extensions L/K of full ray class fields over an imaginary quadratic base field (notably by Schertz [19] and Cassou-Nogués and Taylor [8]), where in many cases $\mathcal{O}_L$ can be shown to be free over $\mathcal{A}_{L/K}(\mathcal{O}_L)$. All of these cases are geometrically motivated, as is the absolutely abelian case, which is closely connected to the geometry of the multiplicative group $\mathbf{G}_m$.

In [6], Bley has already presented algorithms for computing associated orders. Moreover, there is a computational criterion due to Fröhlich (see also [3, Lemma 2.7]), which allows one to decide whether $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}(\mathcal{O}_L)$. If this is the case, one can use the algorithms of this paper to compute the class of $\mathcal{O}_L$ in $\mathrm{Pic}(\mathcal{A}_{L/K}(\mathcal{O}_L))$.

We briefly describe the structure of this paper. In Section 2, we review the basic theoretical results used in our constructions. Our main reference here is [14]. Section 3 forms the heart of the paper, and contains a detailed description of the algorithms for computing the Picard group $\mathrm{Pic}(\mathcal{A})$ and the solution of the corresponding refined discrete logarithm problem. We have actually implemented these algorithms under PARI-GP [2]. In Section 4,tamely ramified extensions L/K of imaginary quadratic number fields K are used as examples; the class of $\mathcal{O}_L$ in $\mathrm{Pic}(\mathcal{O}_K[G])$ is numerically determined.

2. *Class groups and Picard groups*

In this section, we recall and slightly adapt the main results of [14]. Although our primary interest is the computation of Picard groups of $\mathcal{O}_K$-orders $\mathcal{A} \subseteq K[G]$, where K is a number field and G a finite abelian group, we will work here in greater generality.

Let $\mathcal{A}$ denote a commutative ring (as always, with 1). We write $\mathcal{A}^\bullet$ for the monoid of nonzerodivisors, $\mathcal{A}^\times$ for the group of invertible elements, and $T(\mathcal{A})$ for the total quotient ring. By definition, an $\mathcal{A}$-submodule $\mathfrak{a} \subseteq T(\mathcal{A})$ is regular if $\mathfrak{a} \cap T(\mathcal{A})^\times \neq \emptyset$. We call $\mathcal{A}$ a *Marot ring* if each regular ideal of $\mathcal{A}$ is generated by its set of regular elements.

We write $\mathcal{J}(\mathcal{A})$ for the group of invertible $\mathcal{A}$-submodules $\mathfrak{a} \subseteq T(\mathcal{A})$, and $\mathcal{H}(\mathcal{A}) := \{\lambda\mathcal{A} \mid \lambda \in T(\mathcal{A})^\times\}$ for the subgroup of invertible principal ideals. The quotient group $\mathcal{C}(\mathcal{A}) := \mathcal{J}(\mathcal{A})/\mathcal{H}(\mathcal{A})$ is called the *ideal class group of* $\mathcal{A}$ (or, in the terminology of [12], the *Cartier divisor group of* $\mathcal{A}$). If $\mathcal{A}$ is noetherian, then $\mathcal{C}(\mathcal{A})$ is canonically isomorphic to $\mathrm{Pic}(\mathcal{A})$ by [12, Corollary 11.7]. For $\mathfrak{a} \in \mathcal{J}(\mathcal{A})$, we write $[\mathfrak{a}] \in \mathcal{C}(\mathcal{A})$ for the class of $\mathfrak{a}$.

We let $\tilde{\mathcal{A}}$ denote the integral closure of $\mathcal{A}$ in $T(\mathcal{A})$. Following [14], we say that a Marot ring $\mathcal{A}$ is an *order*, if the following conditions are satisfied.

1. Each regular prime ideal of $\mathcal{A}$ is finitely generated.
2. Each regular prime ideal of $\mathcal{A}$ is maximal.
3. $\tilde{\mathcal{A}}$ is a finitely generated $\mathcal{A}$-module.

Let $\mathfrak{m} \subseteq \mathcal{A}$ denote a regular ideal. An invertible $\mathcal{A}$-ideal $\mathfrak{c} \in \mathcal{J}(\mathcal{A})$ is said to be *prime to* $\mathfrak{m}$, if $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$ with regular ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{A}$ such that $\mathfrak{a} + \mathfrak{m} = \mathfrak{b} + \mathfrak{m} = \mathcal{A}$. We let $\mathcal{J}_\mathfrak{m}(\mathcal{A}) \subseteq \mathcal{J}(\mathcal{A})$ denote the subgroup of invertible $\mathcal{A}$-ideals that are prime to $\mathfrak{m}$.

Henceforth we assume that $\mathcal{A}$ is an order, and we write $\mathfrak{f} := \{\lambda \in \tilde{\mathcal{A}} \mid \lambda\tilde{\mathcal{A}} \subseteq \mathcal{A}\}$ for the conductor of $\mathcal{A}$. Note that $\tilde{\mathcal{A}}$ is a Dedekind ring in the sense of [14, Section 2]. An element $\lambda \in T(\tilde{\mathcal{A}})^\times$ is called *multiplicatively congruent to* 1 *modulo* $\mathfrak{f}$, if $\lambda = \lambda_1/\lambda_2$ with

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

$\lambda_1, \lambda_2 \in \tilde{\mathcal{A}}^\bullet$, such that $\lambda_1\tilde{\mathcal{A}} + \mathfrak{f} = \lambda_2\tilde{\mathcal{A}} + \mathfrak{f} = \tilde{\mathcal{A}}$ and $\lambda_1 \equiv \lambda_2 \pmod{\mathfrak{f}}$. In this case, we write $\lambda \equiv 1 \pmod[\times]{\mathfrak{f}}$. We set

$$\mathcal{S}_\mathfrak{f}(\tilde{\mathcal{A}}) := \{\lambda\tilde{\mathcal{A}} \mid \lambda \in T(\tilde{\mathcal{A}})^\times,\ \lambda \equiv 1 \pmod[\times]{\mathfrak{f}}\},$$

and we define the (generalized) ray class group modulo $\mathfrak{f}$ by

$$\mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}}) := \mathcal{J}_\mathfrak{f}(\tilde{\mathcal{A}})/\mathcal{S}_\mathfrak{f}(\tilde{\mathcal{A}}).$$

For $\tilde{\mathfrak{a}} \in \mathcal{J}_\mathfrak{f}(\tilde{\mathcal{A}})$, we write $[\tilde{\mathfrak{a}}]_\mathfrak{f} \in \mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}})$ for the corresponding class.

We consider the following diagram.

$$\begin{array}{ccccccccc}
\mathcal{A}^\times & \longrightarrow & (\mathcal{A}/\mathfrak{f})^\times & \xrightarrow{\sigma} & \mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}}) & \xrightarrow{\psi} & \mathcal{C}(\mathcal{A}) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \| & & \varepsilon\downarrow & & \\
\tilde{\mathcal{A}}^\times & \longrightarrow & (\tilde{\mathcal{A}}/\mathfrak{f})^\times & \xrightarrow{\tilde{\sigma}} & \mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}}) & \xrightarrow{\tilde{\psi}} & \mathcal{C}(\tilde{\mathcal{A}}) & \longrightarrow & 0
\end{array} \tag{1}$$

All unlabelled arrows are defined in the natural way. For an element $\lambda + \mathfrak{f} \in (\mathcal{A}/\mathfrak{f})^\times$, we set $\sigma(\lambda + \mathfrak{f}) := [\lambda\tilde{\mathcal{A}}]_\mathfrak{f}$. For the definition of ψ, we recall from [14, Satz 11(i)] that in each class $c \in \mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}})$, we may choose an invertible ideal $\tilde{\mathfrak{a}} \subseteq \tilde{\mathcal{A}}$ with $\tilde{\mathfrak{a}} + \mathfrak{f} = \tilde{\mathcal{A}}$. Then one defines $\psi(c) := [\tilde{\mathfrak{a}} \cap \mathcal{A}] \in \mathcal{C}(\mathcal{A})$. The definitions of $\tilde{\sigma}$ and $\tilde{\psi}$ are completely analogous. For a class $c \in \mathcal{C}(\mathcal{A})$, we choose a regular ideal $\mathfrak{a} \in c$, and we put $\varepsilon(c) := [\mathfrak{a}\tilde{\mathcal{A}}] \in \mathcal{C}(\tilde{\mathcal{A}})$.

PROPOSITION 2.1. *Diagram* (1) *commutes, and the rows are exact.*

Proof. Commutativity follows from [14, Satz 7(i)]. The bottom sequence is essentially the sequence of [14, Satz 11], and the exactness of the top sequence follows easily from [14, Satz 12] and its proof. □

REMARK 2.2. These sequences are reminiscent of well-known exact sequences in global class field theory. Indeed, if $\mathcal{A}$ is an order in a number field K, then the bottom row is the basic sequence of [17, Satz 7.5.2], and the top row is its analog for ring class field extensions.

For later reference, we introduce the canonical group homomorphism

$$\mu_\mathcal{A} : \mathcal{J}(\mathcal{A}) \longrightarrow \mathcal{J}(\tilde{\mathcal{A}}), \qquad \mathfrak{a} \mapsto \mathfrak{a}\tilde{\mathcal{A}}$$

and we note that the following statement holds.

PROPOSITION 2.3. *The sequence*

$$0 \longrightarrow \frac{(\tilde{\mathcal{A}}/\mathfrak{f})^\times}{(\mathcal{A}/\mathfrak{f})^\times} \xrightarrow{\iota} \mathcal{J}(\mathcal{A}) \xrightarrow{\mu_\mathcal{A}} \mathcal{J}(\tilde{\mathcal{A}})$$

is exact. Here, ι *is induced by* $a + \mathfrak{f} \mapsto a\mathcal{A} + \mathfrak{f}$.

Proof. By [14, Satz 8(i)], it suffices to prove the injectivity of ι. This is obvious, from the fact that $a\mathcal{A} + \mathfrak{f} = \mathcal{A} \iff a \in \mathcal{A}$. □

There is a standard exact sequence

$$0 \longrightarrow D(\mathcal{A}) \longrightarrow \mathcal{C}(\mathcal{A}) \longrightarrow \mathcal{C}(\tilde{\mathcal{A}}) \longrightarrow 0, \tag{2}$$

induced by the functor $\_\otimes_\mathcal{A}\tilde{\mathcal{A}}$, where $D(\mathcal{A})$ is usually called the *kernel group*.

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

To determine $D(\mathcal{A})$, we consider the sequence

$$0 \longrightarrow \mathcal{A}^\times \longrightarrow \tilde{\mathcal{A}}^\times \longrightarrow \frac{(\tilde{\mathcal{A}}/\mathfrak{f})^\times}{(\mathcal{A}/\mathfrak{f})^\times} \xrightarrow{\vartheta} \mathcal{C}(\mathcal{A}) \xrightarrow{\varepsilon} \mathcal{C}(\tilde{\mathcal{A}}) \longrightarrow 0, \tag{3}$$

where all the unlabelled maps are defined naturally. The map ϑ is induced by $\bar{\alpha} \mapsto [\alpha\tilde{\mathcal{A}} \cap \mathcal{A}]$, $\alpha \in (\tilde{\mathcal{A}}/\mathfrak{f})^\times$, and ε is defined as in diagram (1).

Proposition 2.4. *The sequence* (3) *is exact, and therefore*

$$D(\mathcal{A}) \simeq \frac{(\tilde{\mathcal{A}}/\mathfrak{f})^\times}{(\mathcal{A}/\mathfrak{f})^\times \operatorname{im}(\tilde{\mathcal{A}}^\times)}.$$

Proof. This is essentially a reformulation of [**14**, Satz 10]; see also [**18**, Satz (12.9) and (12.11)], which covers the case when $\mathcal{A}$ is an order in a number field. □

We now focus on the following special situation, which occurs frequently in arithmetic and is the basic setup for the algorithms that we will develop in Section 3. Let R denote a Dedekind domain and K its field of fractions, and let A be a finite-dimensional, commutative, reduced K-algebra. We let $\mathcal{A} \subseteq A$ be an R-order (in the sense of [**11**, Definition (23.2)]), and we write $\tilde{\mathcal{A}}$ for the integral closure of R in A. We shall always assume that K is perfect. Then there is an isomorphism of K-algebras

$$A \simeq K_1 \times \ldots \times K_s,$$

where K_i/K, $i = 1, \ldots, s$, is a finite field extension. In view of this identification, one has

$$\tilde{\mathcal{A}} \simeq R_1 \times \ldots \times R_s,$$

where R_i denotes the integral closure of R in K_i. Since $\mathcal{A}$ is noetherian, it is in particular a Marot ring, by [**15**, Theorem 7.2]. Since $\mathcal{A}$ has Krull dimension one, it follows easily that each regular prime ideal of $\mathcal{A}$ is maximal. Indeed, if $\mathfrak{p}_j := \{\alpha = (a_1, \ldots, a_s) \in \mathcal{A} \mid a_j = 0\}$, then $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ is exactly the set of minimal prime ideals. Hence $\mathcal{A}$ is also an order in the sense of [**14**, Section 3]. Finally, note that $A = T(\mathcal{A}) = T(\tilde{\mathcal{A}})$.

Examples 2.5. Let K be a number field and put $R = \mathcal{O}_K$. We fix an algebraic closure K^c of K.

(a) Let L/K denote a finite field extension, and let $A = L$. Then $\mathcal{A}$ is any $\mathcal{O}_K$-order of L. For example, if $\alpha \in K^c$ is integral, then $\mathcal{A} = \mathcal{O}_K[\alpha]$ is an order in $A = K(\alpha)$.

(b) Let G be a finite abelian group, and set $A = K[G]$. Then $\mathcal{A}$ is any $\mathcal{O}_K$-order in $K[G]$; in particular, this example includes all orders arising as associated orders, as described in the introduction.

(c) The last example is motivated by the study of integral module structures in arithmetic geometry (see, for example, [**20**]). Let G denote a finite abelian group on which $\mathrm{Gal}(K^c/K)$ acts from the left. Then one is naturally led to consider (Hopf) orders in the K-algebra $A = (K^c[G])^{\mathrm{Gal}(K^c/K)}$, where $\mathrm{Gal}(K^c/K)$ acts by

$$\omega\left(\sum_{g\in G} \lambda_g g\right) = \sum_{g\in G} \omega(\lambda_g)\omega(g)$$

for $\omega \in \mathrm{Gal}(K^c/K)$, $\lambda_g \in K^c$. For more specific examples and questions arising in this context, the reader is referred to [**5**].

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

3. *Algorithms*

3.1. *Setup and notation*

In this section, K always denotes a fixed number field. Let $K_1, \ldots, K_s$ be finite field extensions of K, and set $A = K_1 \times \ldots \times K_s$. Moreover, we fix an $\mathcal{O}_K$-order $\mathcal{A} \subseteq A$. We present algorithms for the computation of $\mathrm{Pic}(\mathcal{A})$, and an algorithmic solution to the corresponding refined discrete logarithm problem. The idea of our approach to computing $\mathrm{Pic}(\mathcal{A})$ has already been very roughly sketched out in [4]; our solution to the discrete logarithm problem considerably improves on [3, Section 2.2, Steps 3–5].

Before introducing any further notation, we relate this setup to our motivating example, as mentioned in the introduction. If G is a finite abelian group, then we write $\hat{G}$ for its group of abelian characters. Let $\chi_1, \ldots, \chi_s$ denote a set of representatives of $\hat{G}$ modulo the action of $\mathrm{Gal}(K^c/K)$. For $i \in \{1, \ldots, s\}$, let K_i denote the field extension of K generated by $\{\chi_i(g) \mid g \in G\}$. Then we have an isomorphism of K-algebras

$$\Phi : K[G] \longrightarrow K_1 \times \ldots \times K_s,$$

induced by $\Phi(g) = (\chi_1(g), \ldots, \chi_s(g))$ for $g \in G$. Whereas Φ depends on the choice of the χ_i, the components K_i depend only on the $\mathrm{Gal}(K^c/K)$-orbits of $\hat{G}$. It is straightforward to implement algorithms that, for a given group G, compute $K_1, \ldots, K_s$ and isomorphisms Φ and Φ^{-1}. For more details on this issue, the interested reader is referred to the PARI-implementation of our algorithm. Therefore the problem of computing $\mathrm{Pic}(\mathcal{A})$ for $\mathcal{O}_K$-orders $\mathcal{A} \subseteq K[G]$ is reduced to the more general setup of this section. In the same way, one can also deal with Examples 2.5 (a) and (c) (for (c), use the explicit Wedderburn decomposition of [5, Lemma 2.2]).

We return to the setup described at the beginning of this section, and we fix some further notation. For $i = 1, \ldots, s$, we set $n_i := [K_i : K]$. We suppose that each $\mathcal{O}_K$-module $\mathcal{O}_{K_i}$ is given by an integral pseudo-basis $(\omega_{ij}, \mathfrak{a}_{ij})_{1 \leqslant j \leqslant n_i}$ (for a definition, see [10, Definition 1.4.1]); that is

$$\mathcal{O}_{K_i} = \mathfrak{a}_{i1}\omega_{i1} \oplus \ldots \oplus \mathfrak{a}_{in_i}\omega_{in_i}, \tag{4}$$

with fractional $\mathcal{O}_K$-ideals $\mathfrak{a}_{ij}$ and elements $\omega_{ij} \in K_i$. Then the set $\{\omega_{ij} \mid 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant n_i\}$ forms a K-basis of A, and $(\omega_{ij}, \mathfrak{a}_{ij})_{1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant n_i}$ is an integral pseudo-basis for the maximal order $\tilde{\mathcal{A}}$. To simplify our notation, we set $n := [A : K]$ and write $(\omega_k, \mathfrak{a}_k)_{1 \leqslant k \leqslant n}$ for this pseudo-basis, but we always bear in mind that it actually comes in component-wise pieces. Furthermore, we assume that the $\mathcal{O}_K$-order $\mathcal{A}$ is given by a pseudo-basis $(v_k, \mathfrak{b}_k)_{1 \leqslant k \leqslant n}$.

For the computation of $\mathcal{C}(\mathcal{A})$, we use the top sequence of diagram (1). Therefore we have to develop algorithms for the computation of $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$ and $(\mathcal{A}/\mathfrak{f})^\times$.

3.2. *Computation of* $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$

The $\tilde{\mathcal{A}}$-ideal $\mathfrak{f}$ naturally decomposes as a direct sum $\mathfrak{f} = \mathfrak{f}_1 \oplus \ldots \oplus \mathfrak{f}_s$, where each $\mathfrak{f}_i$, $i = 1, \ldots, s$, is an integral ideal of $\mathcal{O}_{K_i}$. In the same way, the ray class group $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$ decomposes as a direct product of ray class groups in number fields,

$$\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}}) = \mathrm{cl}_{\mathfrak{f}_1}(K_1) \oplus \ldots \oplus \mathrm{cl}_{\mathfrak{f}_s}(K_s).$$

We first describe how to compute $\mathfrak{f}_1, \ldots, \mathfrak{f}_s$. To that end, we let $\mathrm{Tr} = \mathrm{Tr}_{A/K} : A \longrightarrow K$ denote the usual trace map, and we observe that $\mathrm{Tr} = \sum_{i=1}^{s} \mathrm{Tr}_{K_i/K}$. Since A/K is separable,

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

the trace form

$$b : A \times A \longrightarrow K, \qquad b(\lambda_1, \lambda_2) := \mathrm{Tr}(\lambda_1\lambda_2),$$

is non-degenerate, and for any full $\mathcal{O}_K$-submodule $M \subseteq A$, we identify the $\mathcal{O}_K$-linear dual of M with $M^* := \{\lambda \in A \mid \mathrm{Tr}(\lambda M) \subseteq \mathcal{O}_K\}$. If M is given by a pseudo-basis $(\mu_k, \mathfrak{c}_k)_{1\leqslant k\leqslant n}$, then M^* is easy to compute. Indeed, if $\mu_1^*, \ldots, \mu_s^* \in A$ is the dual basis of $\mu_1, \ldots, \mu_s$ with respect to the trace form, then $(\mu_k^*, \mathfrak{c}_k^{-1})_{1\leqslant k\leqslant n}$ is a pseudo-basis of M^*. Obviously, the dual basis $\mu_1^*, \ldots, \mu_s^*$ can be computed by means of simple linear algebra.

LEMMA 3.1. *Let $M, N \subseteq A$ denote full $\mathcal{O}_K$-submodules. Put*

$$\mathfrak{f}(M, N) := \{\lambda \in A \mid \lambda M \subseteq N\}.$$

Then $\mathfrak{f}(M, N)^* = MN^*$.

Proof. This is an easy adaption of the proof of [6, Lemma 4.2]. □

The product MN^* can be computed by applying the Hermite normal form (for short, the HNF) algorithm in Dedekind domains; see for example [10, Algorithm 1.4.7 and Section 1.5.2]. We will use Lemma 3.1 for two different applications, as follows.

(1) If $M = \tilde{\mathcal{A}}$ and $N = \mathcal{A}$, then $\mathfrak{f}(M, N)$ is the conductor of $\mathcal{A}$.

(2) If $M = \mathfrak{a}$ and $N = \mathfrak{b}$, with invertible $\mathcal{A}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{f}(M, N) = \mathfrak{a}^{-1}\mathfrak{b}$.

Using (1), we are able to compute a pseudo-basis $(\mu_k, \mathfrak{d}_k)_{1\leqslant k\leqslant n}$ of the conductor $\mathfrak{f}$. We let $\pi_i : A \longrightarrow K_i$ denote the projection on the ith component. Explicitly, if $\lambda = \sum_{i=1}^{s}\sum_{j=1}^{n_i} x_{ij}\omega_{ij}$ with $x_{ij} \in K$ and ω_{ij} as in (4), then $\pi_i(\lambda) = \sum_{j=1}^{n_i} x_{ij}\omega_{ij}$. Then $(\pi_i(\mu_k), \mathfrak{d}_k)_{1\leqslant k\leqslant n}$ is a pseudo-generating set of $\mathfrak{f}_i$, and we can use the HNF algorithm in Dedekind domains to compute a pseudo-basis of $\mathfrak{f}_i$.

In each of the components, we now use [10, Algorithm 4.3.1] to compute integral ideals $\mathfrak{c}'_{ij}$ of $\mathcal{O}_{K_i}$ coprime to $\mathfrak{f}_i$ and integers $d_{ij} > 1$ such that

$$\mathrm{cl}_{\mathfrak{f}_i}(K_i) = \bigoplus_{j=1}^{t_i} \left(\mathbb{Z}/d_{ij}\mathbb{Z}\right)[\mathfrak{c}'_{ij}]_{\mathfrak{f}_i}.$$

For $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant t_i$, we define

$$\mathfrak{c}_{ij} := \mathcal{O}_{K_1} \oplus \ldots \oplus \mathcal{O}_{K_{i-1}} \oplus \mathfrak{c}'_{ij} \oplus \mathcal{O}_{K_{i+1}} \oplus \ldots \oplus \mathcal{O}_{K_s}.$$

Then $\mathfrak{c}_{ij} + \mathfrak{f} = \tilde{\mathcal{A}}$, and

$$\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}}) = \bigoplus_{i=1}^{s}\bigoplus_{j=1}^{t_i} \left(\mathbb{Z}/d_{ij}\mathbb{Z}\right)[\mathfrak{c}_{ij}]_{\mathfrak{f}}.$$

Applying [10, Algorithm 4.3.2] in each of the components, it is now obvious how to give a refined discrete logarithm algorithm in $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$.

In order to simplify our notation, we assume that the ray class group is given in the form

$$\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}}) = \bigoplus_{k=1}^{t} \left(\mathbb{Z}/d_k\mathbb{Z}\right)[\mathfrak{c}_k]_{\mathfrak{f}} \tag{5}$$

with $t = \sum_{i=1}^{s} t_i$, integers $d_k > 1$ and integral $\tilde{\mathcal{A}}$-ideals $\mathfrak{c}_k$ such that $\mathfrak{c}_k + \mathfrak{f} = \tilde{\mathcal{A}}$.

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

3.3. *Computation of* $(\mathcal{A}/\mathfrak{f})^\times$

For the computation of $(\mathcal{A}/\mathfrak{f})^\times$, we follow very closely the strategy applied by Cohen in [10, Section 4.2]. Since we have to deal with abelian groups (that is, $\mathbb{Z}$-modules) in this subsection, it is useful and natural to work with $\mathbb{Z}$-basis of the $\mathcal{O}_K$-modules that occur during the computation of the finite abelian group $(\mathcal{A}/\mathfrak{f})^\times$.

To begin with, we recall that the conductor $\mathfrak{f}$ decomposes as a direct sum $\mathfrak{f} = \mathfrak{f}_1 \oplus \ldots \oplus \mathfrak{f}_s$, where each $\mathfrak{f}_i$ is an integral ideal of $\mathcal{O}_{K_i}$. In each component, we compute the prime ideal factorization of $\mathfrak{f}_i$ (for example, with the PARI routine `idealfactor`); we may therefore assume that we have a prime ideal factorization

$$\mathfrak{f} = \prod_{i \in I} \mathfrak{P}_i^{e_i} = \bigcap_{i \in I} \mathfrak{P}_i^{e_i},$$

where I denotes a finite index set, each $\mathfrak{P}_i$ is a regular prime ideal of $\tilde{\mathcal{A}}$, and $e_i \geqslant 1$. For $i \in I$, we set $\mathfrak{p}_i := \mathfrak{P}_i \cap \mathcal{A}$, and we let $J \subseteq I$ denote a maximal subset such that $\mathfrak{p}_{j_1} \neq \mathfrak{p}_{j_2}$ for $j_1, j_2 \in J$, $j_1 \neq j_2$. For $j \in J$, we define

$$\mathfrak{q}_j := \bigcap_{i \in I,\ \mathfrak{p}_i = \mathfrak{p}_j} (\mathfrak{P}_i^{e_i} \cap \mathcal{A}) = \left(\bigcap_{i \in I,\ \mathfrak{p}_i = \mathfrak{p}_j} \mathfrak{P}_i^{e_i} \right) \cap \mathcal{A}.$$

PROPOSITION 3.2. *Assume the above notation; then the following statements hold.*

(a) $\mathfrak{q}_j$ *is* $\mathfrak{p}_j$*-primary for* $j \in J$.

(b) $\mathfrak{q}_s + \mathfrak{q}_t = \mathcal{A}$ *for* $s, t \in J$, $s \neq t$.

(c) $\mathfrak{f} = \prod_{j \in J} \mathfrak{q}_j = \bigcap_{j \in J} \mathfrak{q}_j$ *is the unique primary decomposition of* $\mathfrak{f}$*, when* $\mathfrak{f}$ *is considered as an* $\mathcal{A}$*-ideal.*

Proof. (a) Since $\tilde{\mathcal{A}}$ is Dedekind, its primary ideals are exactly the powers of its prime ideals. Hence each of the ideals $\mathfrak{P}_i^{e_i} \cap \mathcal{A}$ is primary, and obviously it must be $\mathfrak{p}_j$-primary, if $\mathfrak{P}_i \cap \mathcal{A} = \mathfrak{p}_j$. By [12, Corollary 3.8], $\mathfrak{q}_j$ is $\mathfrak{p}_j$-primary.

(b) Since each of the ideals $\mathfrak{p}_j$, $j \in J$, is maximal, one has $\mathfrak{p}_s + \mathfrak{p}_t = \mathcal{A}$ for $s, t \in J$, $s \neq t$. Since $\mathcal{A}$ is noetherian, there exists a positive integer k_j such that $\mathfrak{p}_j^{k_j} \subseteq \mathfrak{q}_j$ for each $j \in J$. This implies that the assertion holds.

(c) The equality of ideals is obvious. Since each of the primes $\mathfrak{p}_j$, $j \in J$, is minimal over $\mathfrak{f}$, there are no embedded primes, and uniqueness follows from [12, Theorem 3.10 (c)]. □

Using the HNF algorithm in Dedekind domains (or even in $\mathbb{Z}$), it is easy to compute the ideals $\mathfrak{p}_j$ and $\mathfrak{q}_j$. See [10, Section 1.5.2], and in particular [10, Algorithm 1.5.1], for more details.

The Chinese remainder theorem implies that the canonical map

$$\varphi : (\mathcal{A}/\mathfrak{f})^\times \xrightarrow{\simeq} \prod_{j \in J} (\mathcal{A}/\mathfrak{q}_j)^\times$$

is an isomorphism. If we succeed in making φ (or rather its inverse) explicit, the computation of $(\mathcal{A}/\mathfrak{f})^\times$ is reduced to the computation of $(\mathcal{A}/\mathfrak{q})^\times$ for a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ of $\mathcal{A}$. We first address the problem of computing $(\mathcal{A}/\mathfrak{q})^\times$.

We consider the natural exact sequence

$$1 \longrightarrow \frac{1+\mathfrak{p}}{1+\mathfrak{q}} \xrightarrow{\iota} (\mathcal{A}/\mathfrak{q})^\times \xrightarrow{\pi} (\mathcal{A}/\mathfrak{p})^\times \longrightarrow 1.$$

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

The homomorphisms ι and π are obviously effective in the sense of [**10**, Definition 4.1.5]. By [**10**, Algorithm 4.1.8] it therefore suffices to compute $(1+\mathfrak{p})/(1+\mathfrak{q})$ and $(\mathcal{A}/\mathfrak{p})^\times$. Note that for the application of [**10**, Algorithm 4.1.8], it is essential to have a discrete logarithm algorithm in $(1+\mathfrak{p})/(1+\mathfrak{q})$.

We turn to the computation of $(\mathcal{A}/\mathfrak{p})^\times$. Let $\mathfrak{P}$ denote a prime of $\tilde{\mathcal{A}}$ lying over $\mathfrak{p}$; that is, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{A}$ (note that $\mathfrak{P}$ is already known from the computation of $\mathfrak{p}$). Since $\tilde{\mathcal{A}}$ decomposes as a direct product of Dedekind domains, we easily obtain a discrete logarithm algorithm in $(\tilde{\mathcal{A}}/\mathfrak{m})^\times$ for any integral regular $\tilde{\mathcal{A}}$-ideal $\mathfrak{m}$ by componentwise application of [**10**, Algorithm 4.2.18]. Let $q := |\mathcal{A}/\mathfrak{p}|$ and $\tilde{q} := |\tilde{\mathcal{A}}/\mathfrak{P}|$. Then $(\tilde{\mathcal{A}}/\mathfrak{P})^\times$ is cyclic of order $\tilde{q}-1$, and we let $\tilde{a}$ denote a generator. We randomly choose $a \in \mathcal{A} \setminus \mathfrak{p}$, and we compute the discrete logarithm of a in $(\tilde{\mathcal{A}}/\mathfrak{P})^\times$, namely $a \equiv \tilde{a}^n \pmod{\mathfrak{P}}$. If $(n, \tilde{q}-1) = (\tilde{q}-1)/(q-1)$, then the class of a generates $(\mathcal{A}/\mathfrak{p})^\times$. Unfortunately, the discrete logarithm algorithm in $(\tilde{\mathcal{A}}/\mathfrak{P})^\times$ is very time-consuming (see the comment in [**10**, Algorithm 4.2.18, Step 1]), so that the naive algorithm of simply randomly choosing $a \in \mathcal{A} \setminus \mathfrak{p}$ until one finds an element of exact order $q-1$ in $(\mathcal{A}/\mathfrak{p})^\times$ is probably similarly (in)efficient.

Let us turn to the computation of $(1+\mathfrak{p})/(1+\mathfrak{q})$. We define $k := \min\{s \in \mathbb{N}_0 \mid \mathfrak{p}^{2^s} \subseteq \mathfrak{q}\}$. If $k = 0$, we have $\mathfrak{p} = \mathfrak{q}$, so that we are done. We henceforth assume that $k > 0$, and we consider the filtration

$$\mathfrak{p} = \mathfrak{p} + \mathfrak{q} \supseteq \mathfrak{p}^2 + \mathfrak{q} \supseteq \ldots \supseteq \mathfrak{p}^{2^{k-1}} + \mathfrak{q} \supseteq \mathfrak{p}^{2^k} + \mathfrak{q} = \mathfrak{q}.$$

We observe that the map

$$\frac{\mathfrak{p}^{2^a} + \mathfrak{q}}{\mathfrak{p}^{2^{a+1}} + \mathfrak{q}} \longrightarrow \frac{1 + \mathfrak{p}^{2^a} + \mathfrak{q}}{1 + \mathfrak{p}^{2^{a+1}} + \mathfrak{q}}$$

induced by $x \mapsto 1+x$ is an isomorphism of abelian groups. Applying HNF techniques over $\mathbb{Z}$, it is easy to compute the left-hand side. As in [**10**, Section 4.2], we inductively compute $(1+\mathfrak{p})/(1+\mathfrak{q})$ using the short exact sequences

$$1 \longrightarrow \frac{1 + \mathfrak{p}^{2^a} + \mathfrak{q}}{1 + \mathfrak{p}^{2^{a+1}} + \mathfrak{q}} \longrightarrow \frac{1 + \mathfrak{p}}{1 + \mathfrak{p}^{2^{a+1}} + \mathfrak{q}} \longrightarrow \frac{1 + \mathfrak{p}}{1 + \mathfrak{p}^{2^a} + \mathfrak{q}} \longrightarrow 1$$

for $a = 1, 2, \ldots, k-1$. It is straightforward but quite lengthy to adapt [**10**, Algorithms 4.2.15, 4.2.16 and 4.2.18] for our purposes, and this is therefore left to the reader. For a detailed description, the reader is also referred to the paper [**16**] of Klüners and Pauli, which deals with the case of orders in number fields (our example (a)).

We finally outline a procedure for making φ^{-1} explicit. We suppose that we have already computed

$$\left(\mathcal{A}/\mathfrak{q}_j\right)^\times = \bigoplus_{k=1}^{r_j} \left(\mathbb{Z}/d_{jk}\mathbb{Z}\right) \overline{\alpha_{jk}}, \qquad \alpha_{jk} \in \mathcal{A},$$

for each $j \in J$. We set $\mathfrak{a}_j = \mathfrak{q}_j$ and $\mathfrak{b}_j = \bigcap_{k \neq j} \mathfrak{q}_k$. Then $\mathfrak{a}_j + \mathfrak{b}_j = \mathcal{A}$. We will briefly indicate below how to compute $a_j \in \mathfrak{a}_j$ and $b_j \in \mathfrak{b}_j$ such that $a_j + b_j = 1$. If we set $\delta_{jk} = b_j \alpha_{jk} + a_j$, $j \in J$, $k = 1, \ldots, r_j$, then the classes $[\delta_{jk}]$ generate $(\mathcal{A}/\mathfrak{f})^\times$; moreover, $\varphi^{-1}(\overline{\alpha_{jk}}) = \overline{\delta_{jk}}$.

Let $\mathfrak{a}$ and $\mathfrak{b}$ denote $\mathcal{A}$-ideals such that $\mathfrak{a}+\mathfrak{b} = \mathcal{A}$. As from the beginning of this subsection, we assume that $\mathcal{A}$, $\mathfrak{a}$ and $\mathfrak{b}$ are given by $\mathbb{Z}$-bases. Let $\omega = (\omega_1, \ldots, \omega_m)$ denote a $\mathbb{Z}$-basis of $\mathcal{A}$, and let $z \in \mathbb{Z}^m$ be the column vector such that $1 = \omega z$. Furthermore, let $A, B \in \mathbb{Z}^{m \times m}$ denote the matrix such that ωA and ωB are $\mathbb{Z}$-bases of $\mathfrak{a}$ and $\mathfrak{b}$, respectively. Note that all of

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

this data can be computed efficiently by means of linear algebra. It is then straightforward to adapt [**10**, Algorithm 1.3.2]. In other words, if $(A|B)U = (0|H)$ with $U \in \mathrm{Gl}_{2m}(\mathbb{Z})$ computes the HNF of $(A|B)$, then H is the $m \times m$ identity matrix, and we derive

$$1 = \omega(0|H)\begin{pmatrix}0\\ z\end{pmatrix} = \omega(A|B)U\begin{pmatrix}0\\ z\end{pmatrix} = \omega Ax + \omega By$$

with

$$U\begin{pmatrix}0\\ z\end{pmatrix} = \begin{pmatrix} x\\ y\end{pmatrix}.$$

Hence we obtain $a + b = 1$ with $a = \omega Ax \in \mathfrak{a}$ and $b = \omega By \in \mathfrak{b}$.

If, in a more general situation, $\mathcal{A}$, $\mathfrak{a}$ and $\mathfrak{b}$ are given by $\mathcal{O}_K$-pseudo-bases, then one can avoid the conversion to $\mathbb{Z}$-bases and apply [**10**, Theorem 1.4.6 and Algorithm 1.4.7] to compute the composition $1 = a+b$. Since it is straightforward to adapt the above algorithm, we leave the details to the reader.

In the following subsections, we assume that $(\mathcal{A}/\mathfrak{f})^\times$ is given in the following form

$$(\mathcal{A}/\mathfrak{f})^\times = \bigoplus_{k=1}^{r} (\mathbb{Z}/e_k\mathbb{Z})\,\overline{\epsilon_k}, \qquad \epsilon_k \in \mathcal{A},\ \epsilon_k\mathcal{A} + \mathfrak{f} = \mathcal{A}. \tag{6}$$

3.4. *Computation of* $\mathcal{C}(\mathcal{A})$

For the computation of $\mathcal{C}(\mathcal{A})$, we consider the exact sequence

$$(\mathcal{A}/\mathfrak{f})^\times \xrightarrow{\sigma} \mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}}) \xrightarrow{\psi} \mathcal{C}(\mathcal{A}) \longrightarrow 0.$$

If we are merely interested in the structure of $\mathcal{C}(\mathcal{A})$ as an abstract abelian group, we need only to apply [**10**, Algorithm 4.1.7]. Our ultimate goal, however, is to solve the (refined) discrete logarithm problem in $\mathcal{C}(\mathcal{A})$, and some extra care has therefore to be taken, mainly in order to make the map ψ effective in the sense of [**10**, Definition 4.1.5].

Although most of our abelian groups are usually written multiplicatively, we will use the more convenient additive notation in the following algorithm.

ALGORITHM 3.3. This algorithm computes integral $\mathcal{A}$-ideals $\mathfrak{g}_i$ such that $\mathfrak{g}_i + \mathfrak{f} = \mathcal{A}$ and integers $f_i \geqslant 1$ such that

$$\mathcal{C}(\mathcal{A}) = \bigoplus_{i=1}^{g} (\mathbb{Z}/f_i\mathbb{Z})\,[\mathfrak{g}_i].$$

It also computes the additional information needed for the computation of refined discrete logarithms. We assume that $\mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}})$ and $(\mathcal{A}/\mathfrak{f})^\times$ are given as in (5) and (6).

1. [Express the relations given by $\sigma((\mathcal{A}/\mathfrak{f})^\times)$ in terms of the generators of $\mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}})$.]

Using the refined discrete logarithm algorithm in $\mathcal{C}_\mathfrak{f}(\tilde{\mathcal{A}})$ compute, for $k = 1, \ldots, r$, elements $\xi_k \in A^\times$ and integers $x_{1k}, \ldots, x_{tk}$ such that

$$\epsilon_k\tilde{\mathcal{A}} = \xi_k\mathfrak{c}_1^{x_{1k}} \ldots \mathfrak{c}_t^{x_{tk}}, \qquad \xi_k \equiv 1 \ (\mathrm{mod}^\times\ \mathfrak{f}).$$

Set $\epsilon'_k = \epsilon_k/\xi_k$, and let $(x_{1k}, \ldots, x_{tk})$ be the kth column of a $(t \times r)$-matrix P. Then

$$(\epsilon'_1\tilde{\mathcal{A}}, \ldots, \epsilon'_r\tilde{\mathcal{A}}) = (\mathfrak{c}_1, \ldots, \mathfrak{c}_t)P.$$

The $\mathbb{Z}$-span of the columns of P represents all the relations with respect to the generators represented by $\mathfrak{c}_1, \ldots, \mathfrak{c}_t$.

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

2. [Compute the Smith Normal Form (for short, the SNF) of P.]

Let D be the diagonal matrix with entries $d_1, \dots, d_t$. Compute the HNF H of $(P|D)$, so that $(0|H) = (P|D)W$, and then the SNF $S = UHV$ of H. The matrices W, U and V will be needed below.

Now the $\mathbb{Z}$-span of the columns of S represents all the relations with respect to the new generators defined by $(\mathfrak{c}_1, \dots, \mathfrak{c}_t)U^{-1}$. Note that these representatives of the generators of $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$ are in general not integral.

3. [Compute integral representatives of the generators of $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$.]

Compute a matrix Q such that all entries of $C = U^{-1} + Q$ are non-negative integers and each entry of the kth row of Q is divisible by d_k. Then compute the integral $\tilde{\mathcal{A}}$-ideals $\tilde{\mathfrak{g}}_1, \dots, \tilde{\mathfrak{g}}_t$, defined by

$$(\tilde{\mathfrak{g}}_1, \dots, \tilde{\mathfrak{g}}_t) = (\mathfrak{c}_1, \dots, \mathfrak{c}_t)C.$$

4. [Compute the additional data needed for the computation of refined discrete logarithms. This step can be skipped if it is not intended to compute refined discrete logarithms.]

(a) Using the refined discrete logarithm in $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$, compute the elements $\alpha_1, \dots, \alpha_t \in \mathcal{A}$ such that

$$\alpha_k \tilde{\mathcal{A}} = \mathfrak{c}_k^{d_k}, \qquad k = 1, \dots, t.$$

(b) Compute, for $i = 1, \dots, t$, the elements $\gamma_i \in \mathcal{A}$ defined by

$$\gamma_i = \prod_{k=1}^{t} \alpha_k^{Q_{ki}/d_k}.$$

Then $(\gamma_1 \tilde{\mathcal{A}}, \dots, \gamma_t \tilde{\mathcal{A}}) = (\mathfrak{c}_1, \dots, \mathfrak{c}_t)Q$.

(c) From

$$\begin{aligned}&\big(0, \dots, 0, (\tilde{\mathfrak{g}}_1, \dots, \tilde{\mathfrak{g}}_t)S\big)\\ &\quad = \big(\epsilon_1' \tilde{\mathcal{A}}, \dots, \epsilon_r' \tilde{\mathcal{A}}, \alpha_1 \tilde{\mathcal{A}}, \dots, \alpha_t \tilde{\mathcal{A}}\big) W \begin{pmatrix} 0 & 0 \\ 0 & V \end{pmatrix} + \big(0, \dots, 0, \gamma_1^{S_{11}} \tilde{\mathcal{A}}, \dots, \gamma_t^{S_{tt}} \tilde{\mathcal{A}}\big)\end{aligned}$$

compute elements $\beta_k \in \tilde{\mathcal{A}}$ such that $\tilde{\mathfrak{g}}_k^{S_{kk}} = \beta_k \tilde{\mathcal{A}}$, $k = 1, \dots, t$.

5. [Compute representatives for the generators of $\mathcal{C}(\mathcal{A})$.]

If S is the identity matrix, then set $g = 1$, $\mathfrak{g}_1 = \mathcal{A}$ and $f_1 = 1$. Otherwise, let g be the largest index such that $S_{gg} \neq 1$. For $k = 1, \dots, g$, compute $\mathfrak{g}_k = \tilde{\mathfrak{g}}_k \cap \mathcal{A}$ and set $f_k = S_{kk}$. Output $(\mathfrak{g}_1, \dots, \mathfrak{g}_g)$, $(f_1, \dots, f_g)$ and U; also, if Step 4 has been done, $(\gamma_1, \dots \gamma_t)$ and $(\beta_1, \dots, \beta_t)$.

REMARKS 3.4. (a) If we do not intend to compute refined discrete logarithms, then the algorithm becomes much simpler and faster. In Step 1, it suffices to compute a matrix P such that

$$(\sigma(\overline{\epsilon}_1), \dots, \sigma(\overline{\epsilon}_r)) = \big([\mathfrak{c}_1]_{\mathfrak{f}}, \dots, [\mathfrak{c}_t]_{\mathfrak{f}}\big)\, P.$$

This can be achieved by applying the discrete logarithm algorithm in $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$, which is much faster than its refined version. Step 4 can be skipped completely. The output $(\mathfrak{g}_1, \dots, \mathfrak{g}_g)$, $(f_1, \dots, f_g)$ and U suffices for the computation of discrete logarithms.

(b) Note that for $k = 1, \dots, r$ the principal $\mathcal{A}$-ideals $\epsilon_k' \mathcal{A}$ are contained in $\mathcal{J}_{\mathfrak{f}}(\mathcal{A})$. Indeed, if $\xi_k = \lambda_1/\lambda_2$ with $\lambda_1, \lambda_2 \in \tilde{\mathcal{A}}^{\bullet}$ such that $\lambda_1 \tilde{\mathcal{A}} + \mathfrak{f} = \lambda_2 \tilde{\mathcal{A}} + \mathfrak{f} = \tilde{\mathcal{A}}$ and $\lambda_1 \equiv \lambda_2 \pmod{\mathfrak{f}}$,

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

then there exists an element $\mu \in \tilde{\mathcal{A}}$ such that $\lambda_1\mu \equiv \lambda_2\mu \equiv 1 \pmod{\mathfrak{f}}$, and hence we have $\epsilon_k'\mathcal{A} = (\epsilon_k\lambda_2\mu\mathcal{A})/(\lambda_1\mu\mathcal{A}) \in \mathcal{J}_{\mathfrak{f}}(\mathcal{A})$.

(c) By the choice of the matrix Q in Step 3, we have

$$([\mathfrak{c}_1]_{\mathfrak{f}}, \dots, [\mathfrak{c}_t]_{\mathfrak{f}})U^{-1} = ([\mathfrak{c}_1]_{\mathfrak{f}}, \dots, [\mathfrak{c}_t]_{\mathfrak{f}})C$$

in $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$. Using C instead of U^{-1} has the advantage that the representatives $\tilde{\mathfrak{g}}_1, \dots, \tilde{\mathfrak{g}}_t$ are integral and satisfy $\tilde{\mathfrak{g}}_k + \mathfrak{f} = \tilde{\mathcal{A}}$. Therefore, $\psi([\tilde{\mathfrak{g}}_k]_{\mathfrak{f}}) = [\mathfrak{g}_k]$ in $\mathcal{C}(\mathcal{A})$, by [**14**, Satz 7].

(d) In Step 4(a), the refined discrete logarithm algorithm produces elements $\alpha_k \in \tilde{\mathcal{A}}$ such that $\alpha_k \equiv 1 \pmod[\times]{\mathfrak{f}}$. So, indeed, $\alpha_k \in \mathcal{A}$; moreover, $\alpha_k\mathcal{A} \in \mathcal{J}_{\mathfrak{f}}(\mathcal{A})$. The method used to compute the element β_k in Step 4(c) ensures that $\beta_k\mathcal{A} \in \mathcal{J}_{\mathfrak{f}}(\mathcal{A})$. This will be vital for the refined discrete logarithm algorithm described in the next subsection.

3.5. *The refined discrete logarithm problem*

Let $\mathfrak{a} \subseteq A$ be an invertible $\mathcal{A}$-module. Our intention is to compute an element $\xi \in A^\times$ and integers $x_1, \dots, x_g$ such that $0 \leqslant x_j < f_j$ and $\mathfrak{a} = \xi\mathfrak{g}_1^{x_1} \dots \mathfrak{g}_g^{x_g}$.

Let $\tilde{\mathfrak{c}} \subseteq \tilde{\mathcal{A}}$ denote an invertible $\tilde{\mathcal{A}}$-ideal in the class $[\mathfrak{a}\tilde{\mathcal{A}}] \in \mathcal{C}(\tilde{\mathcal{A}})$, such that $\tilde{\mathfrak{c}} + \mathfrak{f} = \tilde{\mathcal{A}}$. Then there exists $y \in A^\times$ such that $\tilde{\mathfrak{c}} = y\mathfrak{a}\tilde{\mathcal{A}}$. By construction, the invertible $\mathcal{A}$-ideal $\mathfrak{a}' := y\mathfrak{a}(\tilde{\mathfrak{c}} \cap \mathcal{A})^{-1}$ is in the kernel of $\mu_{\mathcal{A}} : \mathcal{J}(\mathcal{A}) \longrightarrow \mathcal{J}(\tilde{\mathcal{A}})$. By Proposition 2.3, there exists a unique element $\eta = ((z+\mathfrak{f}) \bmod (\mathcal{A}/\mathfrak{f})^\times)$ in $(\tilde{\mathcal{A}}/\mathfrak{f})^\times/(\mathcal{A}/\mathfrak{f})^\times$ such that $\mathfrak{a}' = z\mathcal{A}+\mathfrak{f}$. More precisely, the proof of [**14**, Satz 8 ii)] implies that η is determined by the requirement that $z \in \mathfrak{a}'$. If $z' \in \tilde{\mathcal{A}}$ satisfies $zz' \equiv 1 \pmod{\mathfrak{f}}$, then the proof of [**14**, Satz 10 i)] shows that $\mathfrak{c} = z'y\mathfrak{a}$ is an integral ideal such that $\mathfrak{c} + \mathfrak{f} = \mathcal{A}$. By the definition of ψ, it follows that $\psi([\mathfrak{c}\tilde{\mathcal{A}}]_{\mathfrak{f}}) = [\mathfrak{a}] \in \mathcal{C}(\mathcal{A})$, so that the discrete logarithm problem can be solved by the method of [**10**, Section 4.1.3].

If we apply [**10**, Algorithm 4.2.21] component-wise, it is straightforward to compute $(\tilde{\mathcal{A}}/\mathfrak{f})^\times$; in addition, we can use [**10**, Algorithm 4.2.24] to solve the discrete logarithm problem in $(\tilde{\mathcal{A}}/\mathfrak{f})^\times$. Since $(\mathcal{A}/\mathfrak{f})^\times$ is also explicitly known, it is easy (use [**10**, Algorithm 4.1.7]) to compute $\mathcal{L} = \{z_1, \dots, z_m\} \subseteq \tilde{\mathcal{A}}$ and integers $h_1, \dots, h_m > 1$ such that

$$\frac{(\tilde{\mathcal{A}}/\mathfrak{f})^\times}{(\mathcal{A}/\mathfrak{f})^\times} = \bigoplus_{j=1}^{m} \big(\mathbb{Z}/h_j\mathbb{Z}\big)\,[z_j], \qquad z_j \in \tilde{\mathcal{A}} \text{ with } z_j\tilde{\mathcal{A}} + \mathfrak{f} = \tilde{\mathcal{A}},$$

where $[z_j]$ denotes the class of z_j.

Here is a detailed description of the refined discrete logarithm algorithm in $\mathcal{C}(\mathcal{A})$. If x denotes a vector or matrix, we write x^{tr} for its transpose.

ALGORITHM 3.5. Let $\mathfrak{a} \subseteq A$ be an invertible $\mathcal{A}$-ideal. Further input comprises the output of Algorithm 3.3, and the data $\mathcal{L}, h_1, \dots, h_m$ as described above. This algorithm computes $\xi \in A^\times$ and integers $x_1, \dots, x_g$ such that $0 \leqslant x_j < f_j$ and $\mathfrak{a} = \xi\mathfrak{g}_1^{x_1} \dots \mathfrak{g}_g^{x_g}$.

1. Compute an integral $\tilde{\mathcal{A}}$-ideal $\tilde{\mathfrak{c}}$ such that $\tilde{\mathfrak{c}} + \mathfrak{f} = \tilde{\mathcal{A}}$ and $[\tilde{\mathfrak{c}}] = [\mathfrak{a}\tilde{\mathcal{A}}]$ in $\mathcal{C}(\mathcal{A})$.

2. Applying the refined discrete logarithm algorithm in $\mathcal{C}(\tilde{\mathcal{A}})$, we compute $y \in A$ such that $\tilde{\mathfrak{c}} = y\mathfrak{a}\tilde{\mathcal{A}}$.

3. Compute $\mathfrak{a}' = y\mathfrak{a}(\tilde{\mathfrak{c}} \cap \mathcal{A})^{-1}$, and find the unique element

$$z = z_1^{r_1} \dots z_m^{r_m}, \qquad 0 \leqslant r_j < h_j,$$

such that $z \in \mathfrak{a}'$.

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

4. Compute z' such that $zz' \equiv 1 \pmod{\mathfrak{f}}$, and set $\mathfrak{c} = z'y\mathfrak{a}$.

5. Applying the refined discrete logarithm algorithm in $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$, we compute $\xi' \in A$, and integers $y'_1, \ldots, y'_t$, $0 \leqslant y'_k < d_k$, such that

$$\mathfrak{c}\tilde{\mathcal{A}} = \xi' \mathfrak{c}_1^{y'_1} \ldots \mathfrak{c}_t^{y'_t}.$$

Note that $\xi'\mathcal{A} \in \mathcal{J}_{\mathfrak{f}}(\mathcal{A})$.

6. Set $(y_1, \ldots, y_t)^{\mathrm{tr}} = U(y'_1, \ldots, y'_t)^{\mathrm{tr}}$, and compute the integers $v_1, \ldots, v_t, x_1, \ldots, x_t$ such that $y_k = v_k f_k + x_k$, $0 \leqslant x_k < f_k$. (Note that for $k > g$, one automatically has $y_k = v_k$ and $x_k = 0$.)

7. Set $\xi = (\xi' \beta_1^{v_1} \ldots \beta_t^{v_t})/(\gamma_1^{y_1} \ldots \gamma_t^{y_t} z'y)$, and output $\xi, x_1, \ldots, x_g$.

REMARKS 3.6. (a) For the solution of the discrete logarithm problem, it suffices in Step 5 to apply the discrete logarithm algorithm in $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$ to compute $y'_1, \ldots, y'_t$ such that

$$[\mathfrak{c}\tilde{\mathcal{A}}]_{\mathfrak{f}} = [\mathfrak{c}_1]_{\mathfrak{f}}^{y'_1} \ldots [\mathfrak{c}_t]_{\mathfrak{f}}^{y'_t}.$$

In Step 7, we skip the computation of ξ.

(b) Steps 1 and 2 can be done component-wise using [**9**, Algorithm 6.5.10]. In fact, this algorithm can be easily adapted to solve the refined discrete logarithm problem in each component (see also Cohen's comment in [**10**, p. 209]).

(c) Step 3 seems to be the most time-consuming part of the algorithm. Nevertheless it is a big improvement, compared to [**3**, p. 250, Steps 4 and 5]. In practice, it turns out that it is much faster to avoid the computation of $(\tilde{\mathfrak{c}} \cap \mathcal{A})^{-1}$. The test for $z \in \mathfrak{a}'$ is then replaced by one for $z(\tilde{\mathfrak{c}} \cap \mathcal{A}) \subseteq y\mathfrak{a}$, which can be performed by the method of [**10**, 1.5.2(3)].

(d) By construction, $(y_1, \ldots, y_t)^{\mathrm{tr}}$ solves the discrete logarithm problem in $\mathcal{C}_{\mathfrak{f}}(\tilde{\mathcal{A}})$ with respect to the basis $([\mathfrak{c}_1]_{\mathfrak{f}}, \ldots, [\mathfrak{c}_t]_{\mathfrak{f}})U^{-1}$. Hence $(x_1, \ldots, x_t)$ is a solution of the discrete logarithm problem with respect to the basis $[\mathfrak{g}_1], \ldots, [\mathfrak{g}_t]$. The final step, Step 7, takes account of the difference between U^{-1} and C, the relations given by S and the equality $\mathfrak{c} = z'y\mathfrak{a}$. In fact, the definitions immediately imply that $\mathfrak{c}\tilde{\mathcal{A}} = z'y\xi\tilde{\mathfrak{g}}_1^{x_1} \ldots \tilde{\mathfrak{g}}_g^{x_g}$. Both the ideals $\mathfrak{c}$ and $z'y\xi\mathfrak{g}_1^{x_1} \ldots \mathfrak{g}_g^{x_g}$ are mapped to $\mathfrak{c}\tilde{\mathcal{A}}$ by $\mu_{\mathcal{A}}$ as a consequence of [**14**, Satz 7 ii)]. Since both these ideals are contained in $\mathcal{J}_{\mathfrak{f}}(\mathcal{A})$, it follows from [**14**, Satz 9] that they are actually equal.

4. *Examples*

We implemented our algorithms using PARI-GP [**2**]. In this section, we describe our numerical examples, and make some observations derived from the computed data. The source files of our program and the results of our computations are given in Appendix A.

Essentially, we looked at two classes of examples. The first class consists of extensions L/K, where K is a quadratic number field and L is the Hilbert class field of K. We recall that a defining polynomial for L can be computed using the PARI-function `quadhilbert`. By Noether's theorem, $\mathcal{O}_L$ is a locally free $\mathcal{O}_K[G]$-module. We computed $\mathrm{Pic}(\mathcal{O}_K[G])$ and the discrete logarithm of the class of $\mathcal{O}_L$. The results of these computations can be found in the file Hilbert.log.

Let K denote a number field with class number $h_K = 1$. We fix a prime l that does not ramify in $K/\mathbb{Q}$, and we let G denote the cyclic group of order l. We then let $\mathfrak{p}$ denote a prime ideal of $\mathcal{O}_K$, and we assume that l divides the degree $[K(\mathfrak{p}) : K]$, where $K(\mathfrak{p})$ denotes the ray class group of conductor $\mathfrak{p}$. Let L/K denote the unique subextension of $K(\mathfrak{p})/K$

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

of degree l. We set $\mathcal{A} := \mathcal{O}_K[G]$, and we choose an identification of G with $\mathrm{Gal}(L/K)$. Then $\mathcal{O}_L$ is an invertible $\mathcal{A}$-module. In all of our examples, we are interested in the class of $\mathcal{O}_L$ in $\mathrm{Pic}(\mathcal{A})$, which depends on L and the chosen isomorphism $G \simeq \mathrm{Gal}(L/K)$.

We view all our number fields as subfields of the complex numbers $\mathbb{C}$, and we set $\zeta_l = \exp(2\pi i/l)$. We further assume that $K \cap \mathbb{Q}(\zeta_l) = \mathbb{Q}$. Let $E = K(\zeta_l)$. Then the Wedderburn decomposition of $K[G]$ is given by $K[G] \simeq K \oplus E$. Since l divides $[K(\mathfrak{p}) : K]$, the absolute norm of $\mathfrak{p}$ is congruent to 1 modulo l, and hence $\mathfrak{p}$ splits completely in E/K. Moreover, we have $(\mathcal{O}_K/l)^\times \simeq (\mathcal{O}_E/(1-\zeta_l))^\times$.

As described in [6], we choose a normal basis element $\theta \in L$, and we compute the $\mathcal{A}$-module

$$\mathcal{A}_\theta := \{\lambda \in K[G] \mid \lambda(\theta) \subseteq \mathcal{O}_L\}.$$

Then $\mathcal{A}_\theta \simeq \mathcal{O}_L$ as an $\mathcal{A}$-module. Hence $\mathcal{A}_\theta$ is an invertible $\mathcal{A}$-submodule of $K[G]$, and we may first compute $\mathrm{Pic}(\mathcal{A})$ and then apply the (refined) discrete logarithm algorithm to determine the class of $\mathcal{O}_L$.

Since $h_K = 1$, the standard exact sequence (2) is of the form

$$0 \longrightarrow \frac{(\tilde{\mathcal{A}}/\mathfrak{f})^\times}{(\mathcal{A}/\mathfrak{f})^\times \,\mathrm{im}(\tilde{\mathcal{A}}^\times)} \xrightarrow{\vartheta} \mathrm{Pic}(\mathcal{A}) \xrightarrow{\varepsilon} \mathrm{cl}_E \longrightarrow 0,$$

where cl_E denotes the ideal class group of E. Identifying $\tilde{\mathcal{A}}$ with $\mathcal{O}_K \oplus \mathcal{O}_E$, we obtain $\mathfrak{f} = l\mathcal{O}_K \oplus (1-\zeta_l)\mathcal{O}_E$ from [11, (27.8)]. Our assumptions also imply that $\mathcal{A} = \mathcal{O}_K[G]$ is a fibre product as in [11, Section 42], and this immediately leads to

$$\frac{(\mathcal{O}_K/l)^\times}{\mathrm{im}(\mathcal{O}_E^\times)} \simeq \frac{(\tilde{\mathcal{A}}/\mathfrak{f})^\times}{(\mathcal{A}/\mathfrak{f})^\times \,\mathrm{im}(\tilde{\mathcal{A}}^\times)},$$

induced by $a + l\mathcal{O}_K \mapsto (a,1) + \mathfrak{f} \in (\tilde{\mathcal{A}}/\mathfrak{f})^\times \simeq (\mathcal{O}_K/l)^\times \oplus (\mathcal{O}_E/(1-\zeta_l))^\times$. Here $\mathrm{im}(\mathcal{O}_E^\times)$ denotes the image of $\mathcal{O}_E^\times$ in $(\mathcal{O}_K/l)^\times \simeq (\mathcal{O}_E/(1-\zeta_l))^\times$. Hence we obtain the short exact sequence

$$0 \longrightarrow (\mathcal{O}_K/l)^\times / \,\mathrm{im}(\mathcal{O}_E^\times) \xrightarrow{\partial} \mathrm{Pic}(\mathcal{A}) \xrightarrow{\varepsilon} \mathrm{cl}_E \longrightarrow 0, \tag{7}$$

which we could also have derived from the Mayer–Vietories sequence of [11, Section 42]. The boundary map ∂ can be described explicitly. For $\bar{a}$, we let $M_{\bar{a}} := \{(x,y) \in \mathcal{O}_K \oplus \mathcal{O}_E \mid ax \equiv y \pmod{(1-\zeta_l)}\}$, and we view $M_{\bar{a}}$ as an $\mathcal{A}$-submodule of $K[G]$. Then $\partial(\bar{a})$ is equal to the class of $M_{\bar{a}}$.

We looked first at the examples treated by Ayala and Schertz in [1, Satz 1], where $l = 2$ and $K = \mathbb{Q}(\sqrt{d_K})$, with $d_K = -8, -11, -19, -43, -67, -163$. Let p denote a prime that splits in $K/\mathbb{Q}$, $p = \mathfrak{p}\bar{\mathfrak{p}}$, such that $p \equiv 1 \pmod 4$. For the computation of L, we implemented an adapted version of [10, Algorithm 6.3.27].

Note that in this situation, one has $E = K$ and $\partial : (\mathcal{O}_K/2)^\times \longrightarrow \mathrm{Pic}(\mathcal{A})$ is an isomorphism. Moreover, one has an isomorphism

$$(\mathcal{O}_K/2)^\times \longrightarrow \left((\mathcal{O}_K/4)^\times / \{\pm 1\}\right)^2 \simeq (\mathrm{cl}_4(K))^2$$

induced by $\bar{\gamma} \mapsto \bar{\gamma^2}$.

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

We computed a fair number of examples, and compared the class of $\mathcal{O}_L$ in $\mathrm{Pic}(\mathcal{A})$ with the class of $\mathfrak{p}$ in $\mathrm{cl}_4(K)$. An inspection of the computational results led us to formulate the following theorem.

THEOREM 4.1. *Let $K = \mathbb{Q}(\sqrt{d_K})$ with $d_K = -8, -11, -19, -43, -67, -163$. Let p denote a prime that splits in $K/\mathbb{Q}$, $p = \mathfrak{p}\bar{\mathfrak{p}}$, such that $p \equiv 1 \pmod 4$. Let L/K denote the unique quadratic subextension of $K(\mathfrak{p})/K$. Let π denote a generator of $\mathfrak{p}$. Then π^{-1} is a square in $(\mathcal{O}_K/4)^\times/\{\pm 1\}$. We denote its inverse image in $(\mathcal{O}_K/2)^\times$ by $\sqrt{\pi^{-1}}$. Then $[\mathcal{O}_L] = \partial(\sqrt{\pi^{-1}})$ in $\mathrm{Pic}(\mathcal{O}_K[G])$.*

REMARK 4.2. For the discriminants $d_K = -3, -4, -7$, $\mathrm{Pic}(\mathcal{O}_K[G])$ is trivial.

Proof of Theorem 4.1. The group $(\mathcal{O}_K/4)^\times/\{\pm 1\}$ is cyclic, and the norm map $N_{K/\mathbb{Q}}$ induces a short exact sequence

$$0 \longrightarrow \left((\mathcal{O}_K/4)^\times/\{\pm 1\}\right)^2 \longrightarrow (\mathcal{O}_K/4)^\times/\{\pm 1\} \longrightarrow (\mathbb{Z}/4)^\times \longrightarrow 0.$$

Since $N_{K/\mathbb{Q}}(\pi) \equiv 1 \pmod 4$, we see that the class of π is indeed a square in $(\mathcal{O}_K/4)^\times/\{\pm 1\}$.

Since $h_K = 1$, there is a relative integral basis for L/K of the form

$$\mathcal{O}_L = \mathcal{O}_K \oplus \mathcal{O}_K \frac{a + \sqrt{d}}{2}$$

with $a, d \in \mathcal{O}_K$ and $d\mathcal{O}_K = \mathfrak{p}$ (see also [**1**, proof of Satz 1]). Let $\theta = (a + \sqrt{d})/2$, and write $G = \langle\sigma\rangle$, $e_0 = (1 + \sigma)/2$ and $e_1 = (1 - \sigma)/2$. Then

$$\mathcal{A}_\theta = \left\langle 1, \frac{1}{a}(1 + \sigma) \right\rangle_{\mathcal{O}_K}.$$

By definition, we have

$$\begin{aligned} \partial(\bar{a}^{-1}) &= \{xe_0 + ye_1 \mid x, y \in \mathcal{O}_K,\ x \equiv ay \pmod 2\} \\ &= \langle ae_0 + e_1, 2e_0 \rangle_{\mathcal{O}_K}. \end{aligned}$$

Hence $\mathcal{A}_\theta = \xi \cdot \partial(\bar{a}^{-1})$ with $\xi = (1/a)e_0 + e_1$. From the fact that $\mathrm{Tr}_{L/K}((a + \sqrt{d})/2) = \frac{1}{4}(a^2 - d)$, we deduce that $a^2 \equiv d \pmod 4$, and this immediately implies that the theorem holds. □

From now on, we assume that $l \neq 2$. We again fix an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d_K})$ with class number $h_K = 1$, and we assume that l does not ramify in $K/\mathbb{Q}$. Let p denote a split prime such that $p \equiv 1 \pmod l$. If $\mathfrak{p}$ denotes a prime ideal lying over p, then there exists a unique subextension L/K of degree l of $K(\mathfrak{p})/K$.

Let $\mathfrak{P}$ denote a prime of E lying over $\mathfrak{p}$. For $j = 1, \ldots, l-1$, we write $\sigma_j \in \Delta := \mathrm{Gal}(E/K)$ for the automorphism that sends ζ_l to ζ_l^j. Inspired by Greither's paper [**13**], we consider the integral $\mathcal{O}_E$-ideal $\mathfrak{a} = \mathfrak{P}^{l\theta}$, where

$$\theta = \frac{1}{l} \sum_{i=1}^{l-1} i\sigma_i^{-1} \in \mathbb{Z}[\Delta]$$

is the standard lth Stickelberger element. We now assume that $[\mathcal{O}_L]$ is in the kernel of ε. Then $\mathfrak{a}$ is necessarily principal, by [**13**, Theorem 1.6], and we let $\alpha \in \mathcal{O}_E$ denote a generator of $\mathfrak{a}$. Moreover, the sequence (7) shows that in this case the class of $\mathcal{O}_L$ in $\mathrm{Pic}(\mathcal{A})$ does not depend on the choice of the isomorphism $G \simeq \mathrm{Gal}(L/K)$.

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

We set

$$e = \begin{cases} 0, & \text{if } l \text{ splits in } K/\mathbb{Q}, \\ 1, & \text{if } l \text{ is inert in } K/\mathbb{Q}, \end{cases}$$

and we consider the element $\vartheta((\pi^e, \alpha)) \in \mathrm{Pic}(\mathcal{A})$. In all of our examples (always assuming that $\varepsilon([\mathcal{O}_L])$ is trivial), we observe that $\vartheta((\pi^e, \alpha) = [\mathcal{O}_L]$. A detailed listing of our numerical data can be found in the file conjecture.log.

The smallest values for which $[\mathcal{O}_L]$ fails to be in the kernel of ε are listed in [**13**, Table 3].

Appendix A.

This appendix contains the source files of our program and the results of our computations. These, as well as a "README" file, can be found at

`http://www.lms.ac.uk/jcm/8/lms2003-035/appendix-a`.

References

1. E. J. Ayala and R. Schertz, 'Eine Bemerkung zur Galoismodulstruktur in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern', *J. Number Theory* 44 (1994) 41–46. 1, 13, 14

2. C. Batut, K. Belabas, D. Bernardi and H. Cohen, 'User's guide to PARI/GP', M. Olivier, 2000, `http://pari.math.u-bordeaux.fr`. 2, 12

3. W. Bley, 'Computing associated orders and Galois generating elements of unit lattices', *J. Number Theory* 62 (1997) 242–256. 2, 5, 12

4. W. Bley, 'An algorithmic approach to determining local and global module structures', Appendix to [**7**]. 5

5. W. Bley and R. Boltje, 'Lubin–Tate formal groups and module structure over Hopf orders', *J. Théor. Nombres Bordx.* 11 (1999) 269–305. 4, 5

6. W. Bley and D. Burns, 'Über arithmetische assoziierte Ordnungen', *J. Number Theory* 58 (1996) 361–387. 2, 6, 13

7. D. Burns, 'On the equivariant structure of ideals in abelian extensions of local fields', *Comment. Math. Helv.* 75 (2000) 1–44. 2, 15

8. P. Cassou-Nogués and M. Taylor, *Elliptic functions and rings of integers*, Progr. Math. 66 (Birkhäuser, 1986). 2

9. H. Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math. 138 (Springer, New York, 1995). 12

10. H. Cohen, *Advanced topics in computational number theory*, Grad. Texts in Math. 193 (Springer, New York, 2000). 5, 6, 7, 8, 9, 11, 12, 13

11. C. Curtis and I. Reiner, *Methods of representation theory*, vol. I, Wiley Classics Lib. (Wiley-Interscience, New York, 1994). 4, 13

12. D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Grad. Texts in Math. 150 (Springer, New York, 1995). 2, 7

13. C. Greither, 'On normal integral bases in ray class fields over imaginary quadratic fields', *Acta Arith.* 83 (1997) 315–329. 1, 14, 15

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press

14. F. Halter-Koch, 'Die Klassengruppe einer kommutativen Ordnung', *Math. Nachr.* 168 (1994) 97–108. 2, 3, 4, 11, 12

15. J. A. Huckaba, *Commutative rings with zero divisors* (Marcel Dekker, 1988). 4

16. J. Klüners and S. Pauli, 'Computing residue class rings and Picard groups of arbitrary orders', preprint, 2003, www.math.tu-berlin.de/~pauli. 8

17. H. Koch, *Algebraische Zahlentheorie* (Vieweg, 1997). 3

18. J. Neukirch, *Algebraische Zahlentheorie* (Springer, Heidelberg, 1992). 4

19. R. Schertz, 'Galoismodulstruktur und Elliptische Funktionen', *J. Number Theory* 39 (1991) 285–326. 2

20. M. J. Taylor, 'Mordell–Weil groups and the Galois module structure of rings of integers', *Ill. J. Math.* 32 (1988) 428–452. 4

W. Bley bley@math.uni-augsburg.de
M. Endres me@mendres.org

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

https://doi.org/10.1112/S1461157000000875 Published online by Cambridge University Press