COMPUTING GENERATORS OF FREE MODULES OVER ORDERS IN GROUP ALGEBRAS

WERNER BLEY AND HENRI JOHNSTON

ABSTRACT. Let E be a number field and G be a finite group. Let $\mathcal{A}$ be any $\mathcal{O}_E$-order of full rank in the group algebra $E[G]$ and X be a (left) $\mathcal{A}$-lattice. We give a necessary and sufficient condition for X to be free of given rank d over $\mathcal{A}$. In the case that the Wedderburn decomposition $E[G] \cong \oplus_\chi M_\chi$ is explicitly computable and each M_χ is in fact a matrix ring over a field, this leads to an algorithm that either gives elements $\alpha_1, \ldots, \alpha_d \in X$ such that $X = \mathcal{A}\alpha_1 \oplus \ldots \oplus \mathcal{A}\alpha_d$ or determines that no such elements exist.

Let L/K be a finite Galois extension of number fields with Galois group G such that E is a subfield of K and put $d = [K : E]$. The algorithm can be applied to certain Galois modules that arise naturally in this situation. For example, one can take X to be $\mathcal{O}_L$, the ring of algebraic integers of L, and $\mathcal{A}$ to be the associated order $\mathcal{A}(E[G]; \mathcal{O}_L) \subseteq E[G]$. The application of the algorithm to this special situation is implemented in Magma under certain extra hypotheses when $K = E = \mathbb{Q}$.

1. INTRODUCTION

Let E be a number field and G be a finite group. Let $\mathcal{A}$ be any $\mathcal{O}_E$-order of full rank in the group algebra $E[G]$ and X be a (left) $\mathcal{A}$-lattice, i.e., a (left) $\mathcal{A}$-module that is finitely generated and torsion-free over $\mathcal{O}_E$. The first result of this paper is a necessary and sufficient condition for X to be free of given rank d over $\mathcal{A}$. In order to use this criterion for computational purposes, we have to impose two hypotheses:

(H1) The Wedderburn decomposition $E[G] \cong \oplus_\chi M_\chi$, where each M_χ is a matrix ring over a division ring, is explicitly computable.
(H2) The Schur indices of all E-rational irreducible characters of G are equal to 1, i.e., each M_χ above is in fact a matrix ring over a number field.

Under these hypotheses, we give an algorithm that either computes elements $\alpha_1, \ldots, \alpha_d \in X$ such that $X = \mathcal{A}\alpha_1 \oplus \ldots \oplus \mathcal{A}\alpha_d$ or determines that no such elements exist. More generally, the group algebra $E[G]$ can be replaced by any finite product of matrix rings over number fields containing E, in which case G, and thus (H1) and (H2), play no role.

The main motivation for this work has its origins in the following special case. Let L/K be a finite Galois extension of number fields with Galois group G such that E is a subfield

Date: 30th October 2007.
2000 *Mathematics Subject Classification.* 11R33, 11Y40.
Johnston was supported by a grant from the Deutscher Akademischer Austausch Dienst.

of K and put $d = [K : E]$. One can take X to be $\mathcal{O}_L$, the ring of algebraic integers of L, and $\mathcal{A}$ to be the associated order

$$\mathcal{A}(E[G]; \mathcal{O}_L) := \{x \in E[G] \mid x(\mathcal{O}_L) \subseteq \mathcal{O}_L\}.$$

The application of the algorithm to this special situation is implemented in Magma ([BCP97]) under certain extra hypotheses when $K = E = \mathbb{Q}$. The source code and tables of numerical results are available from

`http://www.mathematik.uni-kassel.de/~bley/pub.html`.

Other Galois modules to which the algorithm can be applied include the G-stable ideals of $\mathcal{O}_L$ and, in certain cases, the torsion-free part of $\mathcal{O}_L^\times$.

The algorithm can be thought of as a non-abelian, higher rank generalization of the one given in [Ble97]; though stated for the Galois module structure of units, this can be adapted to general modules for G abelian and $d = 1$ with relatively few changes. It is also worth noting that under the same restrictions on G and d, the algorithm in [BE05] computes the Picard group $\mathrm{Pic}(\mathcal{A})$ and solves the corresponding refined discrete logarithm problem, thus computing a generator if it exists.

There is a considerable body of work related to the motivating special case of the Galois module structure of rings of integers. We briefly mention just a few of these results, using the notation above. The most progress has been made in the case that L/K is at most tamely ramified. In this setting, it is well-known that $\mathcal{A} = \mathcal{O}_E[G]$ and $\mathcal{O}_L$ is locally free over $\mathcal{O}_E[G]$ (see [Noe32]). The algorithm in [BW] determines the class of $\mathcal{O}_L$ in the locally free class group $\mathrm{Cl}(\mathcal{O}_E[G])$, and thus whether or not it is stably free (note that under hypothesis (H2) all stably free $\mathcal{A}$-modules are in fact free). Important work of Fröhlich and Taylor determines the class of $\mathcal{O}_L$ in the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ in terms of Artin root numbers of irreducible complex symplectic characters of G (see [Frö83]). Unfortunately, neither of these approaches lead to any description of generators. However, explicit generators or algorithms to find them when $K = E = \mathbb{Q}$ and $G = A_4$, D_{2p} (p odd prime), H_8, H_{12}, or $H_8 \times C_2$ are given in [Cou06], [Cou00], [Mar69], [CQ02] and [Cou98].

When no assumption regarding the ramification of L/K is made, the situation is somewhat more difficult, not least because $\mathcal{O}_L$ is not necessarily locally free over $\mathcal{A}$. Perhaps the most important result in this context is Leopoldt's Theorem, which in the case that $K = E = \mathbb{Q}$ and G is abelian shows that $\mathcal{O}_L$ is always free over $\mathcal{A}$ and, in addition, explicitly constructs an element $\alpha \in \mathcal{O}_L$ in terms of Gauss sums such that $\mathcal{O}_L = \mathcal{A}\alpha$ (see [Leo59]; Lettl gives a simplified proof in [Let90]). In the setting $K = E$ and $L/\mathbb{Q}$ abelian, progressively sharper generalizations of Leopoldt's Theorem (with explicit generators) are given in [CL93], [Ble95], [BL96] and [Joh].

In future work, we hope to eliminate hypothesis (H2). Finding an algorithm to explicitly compute Wedderburn decompositions and thereby eliminate hypothesis (H1) is an independent problem in its own right, on which some progress has been made by others. A more detailed discussion of both hypotheses is given in Section 3.

2. A Necessary and Sufficient Condition for Freeness

Let E be a number field and G be a finite group. Let $\mathcal{A}$ be any $\mathcal{O}_E$-order of full rank in the group algebra $A := E[G]$, and let $\mathcal{M}$ be some maximal $\mathcal{O}_E$-order in A containing $\mathcal{A}$. (In fact, the results of this section still hold when the group algebra $E[G]$ is replaced by any finite-dimensional semisimple E-algebra.) For any non-commutative ring R, we shall henceforth take "R-module" to mean "left R-module", unless otherwise stated.

If $\mathfrak{p}$ is a prime of $\mathcal{O}_E$ and M is an $\mathcal{O}_E$-module, we write $M_\mathfrak{p} := \mathcal{O}_{E,\mathfrak{p}} \otimes_{\mathcal{O}_E} M$ for the localization of M at $\mathfrak{p}$. We say that M is locally free of rank d if for every $\mathfrak{p}$, we have $M_\mathfrak{p}$ free over $\mathcal{A}_\mathfrak{p}$ of rank d. For an $\mathcal{A}$-lattice X, i.e., an $\mathcal{A}$-module that is finitely generated and torsion-free over $\mathcal{O}_E$, we set $\mathcal{M}X := \mathcal{M} \otimes_\mathcal{A} X$ and usually identify $\mathcal{M}X$ with the sublattice $\{\lambda x \mid \lambda \in \mathcal{M}, x \in X\}$ of the E-vector space $E \otimes_{\mathcal{O}_E} X$. We define $\mathcal{M}_\mathfrak{p}X_\mathfrak{p}$ in the same way.

The main results of this paper are consequences of the following proposition.

Proposition 2.1. *Let X be an $\mathcal{A}$-lattice. Then X is free of rank d if and only if*

(a) *X is a locally free $\mathcal{A}$-lattice of rank d, and*
(b) *there exist $\alpha_1, \ldots, \alpha_d \in X$ such that $\mathcal{M}X = \mathcal{M}\alpha_1 \oplus \ldots \oplus \mathcal{M}\alpha_d$.*

Further, when this is the case, $X = \mathcal{A}\alpha_1 \oplus \ldots \oplus \mathcal{A}\alpha_d$.

Proof. If X is a free $\mathcal{A}$-lattice of rank d then (a) and (b) follow trivially.

Suppose conversely that (a) and (b) hold and let $Y = \mathcal{A}\alpha_1 \oplus \ldots \oplus \mathcal{A}\alpha_d \subseteq X$. Both X and Y are locally free $\mathcal{A}$-lattices of rank d and so for each non-zero prime $\mathfrak{p}$ of $\mathcal{O}_E$ there exists an isomorphism $f_\mathfrak{p} : Y_\mathfrak{p} \longrightarrow X_\mathfrak{p}$ of $\mathcal{A}_\mathfrak{p}$-lattices which extends naturally to an isomorphism $f_\mathfrak{p} : \mathcal{M}_\mathfrak{p}Y_\mathfrak{p} \longrightarrow \mathcal{M}_\mathfrak{p}X_\mathfrak{p}$ of $\mathcal{M}_\mathfrak{p}$-lattices. For each $\mathfrak{p}$ we have

$$[X_\mathfrak{p} : Y_\mathfrak{p}]_{\mathcal{O}_{E,\mathfrak{p}}} = [f_\mathfrak{p}(Y_\mathfrak{p}) : Y_\mathfrak{p}]_{\mathcal{O}_{E,\mathfrak{p}}} = \det_E(f_\mathfrak{p})\mathcal{O}_{E,\mathfrak{p}},$$

where the two left-most terms are generalized module indices (see [FT91, II.4]). However, $\mathcal{M}Y = \mathcal{M}X$ and so each $f_\mathfrak{p} : \mathcal{M}_\mathfrak{p}Y_\mathfrak{p} \longrightarrow \mathcal{M}_\mathfrak{p}X_\mathfrak{p} = \mathcal{M}_\mathfrak{p}Y_\mathfrak{p}$ is in fact an $\mathcal{M}_\mathfrak{p}$-automorphism and therefore also a $\mathcal{O}_{E,\mathfrak{p}}$-automorphism. Hence $\det_E(f_\mathfrak{p}) \in \mathcal{O}_{E,\mathfrak{p}}^\times$ and so $[X_\mathfrak{p} : Y_\mathfrak{p}]_{\mathcal{O}_{E,\mathfrak{p}}} = \mathcal{O}_{E,\mathfrak{p}}$ for each $\mathfrak{p}$. Together with the fact that $Y \subseteq X$, this shows that $X = Y$. □

Let R be a ring with identity and denote by R^{op} the opposite ring. If M is a free R-module of rank d, then a choice of basis for M induces an isomorphism $\mathrm{End}_R(M) \cong \mathrm{Mat}_d(R)^{\mathrm{op}}$. Note that for any subring of a left Noetherian ring, there is no distinction between left and right multiplicative inverses or units (see [Rei75, Theorem 6.4]). Hence we have $\mathrm{Aut}_R(M) := \mathrm{End}_R(M)^\times \cong \mathrm{GL}_d(R)^{\mathrm{op}} := (\mathrm{Mat}_d(R)^{\mathrm{op}})^\times$ as groups. Since $\mathrm{GL}_d(R)^{\mathrm{op}} = \mathrm{GL}_d(R)$ as sets, we shall henceforth drop the $^{\mathrm{op}}$ notation.

Corollary 2.2. *Let X be an $\mathcal{A}$-lattice. Then X is free of rank d if and only if*

(a) *X is a locally free $\mathcal{A}$-lattice of rank d,*
(b) *there exist $\beta_1, \ldots, \beta_d \in \mathcal{M}X$ such that $\mathcal{M}X = \mathcal{M}\beta_1 \oplus \ldots \oplus \mathcal{M}\beta_d$, and*
(c) *there exists $\lambda \in \mathrm{GL}_d(\mathcal{M})$ such that each $\alpha_i \in X$ where $(\alpha_1, \ldots, \alpha_d)^{\mathrm{T}} := \lambda(\beta_1, \ldots, \beta_d)^{\mathrm{T}}$.*

Further, when this is the case, $X = \mathcal{A}\alpha_1 \oplus \ldots \oplus \mathcal{A}\alpha_d$.

Most of the following notation is adopted from [BB06]. Denote the center of a ring R by $Z(R)$. Set $C := Z(A)$ and let $\mathcal{O}_C$ be the integral closure of $\mathcal{O}_E$ in C. Let $e_1, \ldots, e_r$ be the primitive idempotents of C and set $A_i := Ae_i$. Then

$$A = A_1 \oplus \cdots \oplus A_r \tag{1}$$

is a decomposition of A into indecomposable ideals. Each A_i is an E-algebra with identity element e_i. By Wedderburn's Theorem, the centers $E_i := Z(A_i)$ are finite field extensions of E via $E \to E_i$, $\alpha \mapsto \alpha e_i$, and we have E-algebra isomorphisms $A_i \cong \mathrm{Mat}_{n_i}(D_i)$ where D_i is a division ring with $Z(D_i) \cong E_i$. The decomposition (1) gives

$$C = E_1 \oplus \cdots \oplus E_r, \quad \mathcal{O}_C = \mathcal{O}_{E_1} \oplus \cdots \oplus \mathcal{O}_{E_r}, \quad \text{and} \quad \mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r, \tag{2}$$

where we have set $\mathcal{M}_i := \mathcal{M}e_i$. This in turn induces decompositions

$$\mathrm{Mat}_d(\mathcal{M}) = \mathrm{Mat}_d(\mathcal{M}_1) \oplus \ldots \oplus \mathrm{Mat}_d(\mathcal{M}_r) \text{ and} \tag{3}$$

$$\mathrm{GL}_d(\mathcal{M}) = \mathrm{GL}_d(\mathcal{M}_1) \times \ldots \times \mathrm{GL}_d(\mathcal{M}_r). \tag{4}$$

For the rest of this section we suppose $1 \leq i \leq r$ and $1 \leq j \leq d$.

Corollary 2.3. *Let X be an $\mathcal{A}$-lattice. Then X is free of rank d if and only if*

(a) *X is a locally free $\mathcal{A}$-lattice of rank d,*
(b) *for each i, there exist $\beta_{i,1}, \ldots, \beta_{i,d}$ such that $\mathcal{M}_i X = \mathcal{M}_i\beta_{i,1} \oplus \ldots \oplus \mathcal{M}_i\beta_{i,d}$, and*
(c) *there exist $\lambda_i \in \mathrm{GL}_d(\mathcal{M}_i)$ such that each $\alpha_j \in X$, where $\alpha_j := \sum_{i=1}^r \alpha_{i,j}$ and $(\alpha_{i,1}, \ldots, \alpha_{i,d})^{\mathrm{T}} := \lambda_i(\beta_{i,1}, \ldots, \beta_{i,d})^{\mathrm{T}}$.*

Further, when this is the case, $X = \mathcal{A}\alpha_1 \oplus \ldots \oplus \mathcal{A}\alpha_d$.

Let $\mathfrak{f}$ be any full two-sided ideal of $\mathcal{M}$ contained in $\mathcal{A}$. Then we have $\mathfrak{f} \subseteq \mathcal{A} \subseteq \mathcal{M} \subseteq A$. Set $\overline{\mathcal{M}} := \mathcal{M}/\mathfrak{f}$ and $\overline{\mathcal{A}} := \mathcal{A}/\mathfrak{f}$ so that $\overline{\mathcal{A}} \subseteq \overline{\mathcal{M}}$ are finite rings, and denote the canonical map $\mathcal{M} \to \overline{\mathcal{M}}$ by $m \mapsto \overline{m}$. Note that we have decompositions

$$\mathfrak{f} = \mathfrak{f}_1 \oplus \cdots \oplus \mathfrak{f}_r \quad \text{and} \quad \overline{\mathcal{M}} = \overline{\mathcal{M}_1} \oplus \cdots \oplus \overline{\mathcal{M}_r}, \tag{5}$$

where each $\mathfrak{f}_i$ is a non-zero ideal of $\mathcal{M}_i$ and $\overline{\mathcal{M}_i} := \mathcal{M}_i/\mathfrak{f}_i$.

For each i, let $U_i \subset \mathrm{GL}_d(\mathcal{M}_i)$ denote a set of representatives of the image of the natural projection $\mathrm{GL}_d(\mathcal{M}_i) \longrightarrow \mathrm{GL}_d(\overline{\mathcal{M}_i})$.

Corollary 2.4. *Let X be an $\mathcal{A}$-lattice. Suppose that*

(a) *X is a locally free $\mathcal{A}$-lattice of rank d, and*
(b) *for each i, there exist $\beta_{i,1}, \ldots, \beta_{i,d}$ such that $\mathcal{M}_i X = \mathcal{M}_i\beta_{i,1} \oplus \ldots \oplus \mathcal{M}_i\beta_{i,d}$.*

Then X is free of rank d over $\mathcal{A}$ if and only if

(c) *there exist $\lambda_i \in U_i$ such that each $\alpha_j \in X$, where $\alpha_j := \sum_{i=1}^r \alpha_{i,j}$ and $(\alpha_{i,1}, \ldots, \alpha_{i,d})^{\mathrm{T}} := \lambda_i(\beta_{i,1}, \ldots, \beta_{i,d})^{\mathrm{T}}$.*

Further, when this is the case, $X = \mathcal{A}\alpha_1 \oplus \ldots \oplus \mathcal{A}\alpha_d$.

Proof. If condition (c) holds, then the result follows immediately from Corollary 2.3.

Suppose conversely that X is free of rank d over $\mathcal{A}$. Then by Corollary 2.3 there exist $\lambda_i \in \mathrm{GL}_d(\mathcal{M}_i)$ such that each $\alpha_j \in X$ where the α_j's are defined as above. However, as $\mathfrak{f}$ is a two-sided ideal of $\mathcal{A}$, we have

$$\begin{aligned} & \bigoplus_{i=1}^{r} (\lambda_i + \mathrm{Mat}_d(\mathfrak{f}_i))(\beta_{i,1}, \ldots, \beta_{i,d})^{\mathrm{T}} \\ \subseteq & \bigoplus_{i=1}^{r} \lambda_i (\beta_{i,1}, \ldots, \beta_{i,d})^{\mathrm{T}} + \bigoplus_{i=1}^{r} \mathrm{Mat}_d(\mathfrak{f}_i)(\mathcal{M}_i X)^d \\ = & (\alpha_1, \ldots, \alpha_d)^{\mathrm{T}} + \bigoplus_{i=1}^{r} \mathrm{Mat}_d(\mathfrak{f}_i)(\mathcal{M}_i X)^d \subseteq X^d. \end{aligned}$$

Thus we can suppose without loss of generality that $\lambda_i \in U_i$ for each i. □

Let L/K be a Galois extension of number fields with Galois group G such that E is a subfield of K. Let $d = [K : E]$ and write $\mathcal{O}_L$ for the ring of integers of L. One of the main applications of Corollary 2.4 is to determine whether the ring of integers $\mathcal{O}_L$ is free of rank d over the associated order $\mathcal{A} = \mathcal{A}(E[G]; \mathcal{O}_L) := \{x \in E[G] \mid x(\mathcal{O}_L) \subseteq \mathcal{O}_L\}$.

In the case that G is abelian and $E = K$, the maximal order $\mathcal{M}$ is unique and everything can be made completely explicit in terms of the absolutely irreducible characters of G. We refer the reader to [Ble97, Section 2.2]. The combination of Theorem 2.8 and Lemma 2.9 of loc. cit. is essentially equivalent to Corollary 2.4 given here specialized to the abelian case.

We also remark that in the case that $E = K$ and L/K is an at most tamely ramified Kummer extension with G cyclic, results of Ichimura (see [Ich04, Theorem 2.2]) are, though not exactly the same, very similar to Corollary 2.4 when applied to this special situation.

3. The Algorithm

Let E be a number field and G be a finite group. Let $\mathcal{A}$ be any $\mathcal{O}_E$-order of full rank in the group algebra $E[G]$ and let X be an $\mathcal{A}$-lattice. In this section, we give an algorithm based on Corollary 2.4 that either computes elements $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_L$ such that $X = \mathcal{A}\alpha_1 \oplus \ldots \oplus \mathcal{A}\alpha_d$, or determines that no such elements exist. In other words, the algorithm determines whether X is free over $\mathcal{A}$, and if so, computes explicit generators.

We require the hypotheses (H1) and (H2) formulated in the introduction, which we now recall and briefly remark upon. Note that the algorithm still works if the group algebra $E[G]$ is replaced by any finite product of matrix rings over number fields containing E, in which case G, and thus (H1) and (H2), play no role.

(H1) The Wedderburn decomposition $E[G] \cong \oplus_\chi M_\chi$, where each M_χ is a matrix ring over a division ring, is explicitly computable.

If G is abelian the Wedderburn decomposition can be explicitly computed from the

character table. For G non-abelian, many decompositions can be found in the literature or computed "by hand". Note that this problem is equivalent to explicitly finding all irreducible $E[G]$-modules up to isomorphism. An effective method that dates back to Schur to solve this important computational task in the case where G is soluble is likely to be implemented in Magma v2.14.

(H2) The Schur indices of all E-rational irreducible characters of G are equal to 1, i.e., each M_χ above is in fact a matrix ring over a number field.

This holds, for example, whenever
(a) G is abelian, dihedral or symmetric;
(b) G is a p-group where p is an odd prime; or
(c) E contains a primitive m-th root of unity, where m is the exponent of G.
A full discussion of Schur indices is given in [Isa94, Chapter 10]. An algorithm of Nebe and Unger to compute the Schur index will be implemented in Magma v2.14 (a paper on this work is in preparation).

Before we sketch the individual steps of the algorithm we briefly digress to describe the presentation of our data. We always assume that $\mathcal{O}_E[G]$-modules X are given by an $\mathcal{O}_E$-pseudo-basis as described, for example, in [Coh00, Definition 1.4.1]. To be more precise, we assume that $V := E \otimes_{\mathcal{O}_E} X$ is given by an E-basis $v_1, \dots, v_m$ together with matrices $A(\sigma) \in \mathrm{GL}_m(E)$ for each $\sigma \in G$ describing the action of G,

$$\begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}^\sigma = A(\sigma) \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}.$$

Then $X = \mathfrak{a}_1 w_1 \oplus \dots \mathfrak{a}_m w_m$, where each $\mathfrak{a}_i$ is a fractional ideal of $\mathcal{O}_E$ and each $w_i \in V$. Similarly, $\mathcal{A} = \mathfrak{b}_1 \lambda_1 \oplus \dots \mathfrak{b}_n \lambda_n$ with fractional $\mathcal{O}_E$-ideals $\mathfrak{b}_i$ and $\lambda_i \in E[G]$.

Algorithm 3.1. *Input: $\mathcal{A}$ and X as above.*

(1) *Compute $d := \dim_E(E \otimes_{\mathcal{O}_E} X)/|G|$ and check that $d \in \mathbb{N}$.*
(2) *Compute a maximal $\mathcal{O}_E$-order $\mathcal{M}$ in $E[G]$ containing $\mathcal{A}$.*
(3) *Compute the central primitive idempotents e_i and the components $\mathcal{M}_i := \mathcal{M}e_i$.*
(4) *Compute the conductor $\mathfrak{c}$ of $\mathcal{A}$ in $\mathcal{M}$ and the components $\mathfrak{c}_i := \mathfrak{c}e_i$.*
Then compute the ideals $\mathfrak{g}_i := \mathfrak{c}_i \cap \mathcal{O}_{E_i}$ and $\mathfrak{f}_i := \mathfrak{g}_i \mathcal{M}_i$ for each i.
(5) *For each i, compute $\beta_{i,1}, \dots, \beta_{i,d}$ such that $\mathcal{M}_i X = \mathcal{M}_i\beta_{i,1} \oplus \dots \oplus \mathcal{M}_i\beta_{i,d}$.*
(6) *Check that X is locally free of rank d over $\mathcal{A}$.*
(7) *For each i, compute a set of representatives $U_i \subset \mathrm{GL}_d(\mathcal{M}_i)$ of the image of the natural projection map $\mathrm{GL}_d(\mathcal{M}_i) \longrightarrow \mathrm{GL}_d(\overline{\mathcal{M}_i})$, where $\overline{\mathcal{M}_i} := \mathcal{M}_i/\mathfrak{f}_i$.*
(8) *Find a tuple $(\lambda_i) \in \prod_{i=1}^r U_i$ such that that each $\alpha_j \in X$, where $\alpha_j := \sum_{i=1}^r \alpha_{i,j}$ and $(\alpha_{i,1}, \dots, \alpha_{i,d})^{\mathrm{T}} := \lambda_i(\beta_{i,1}, \dots, \beta_{i,d})^{\mathrm{T}}$. For such a tuple, $X = \mathcal{A}\alpha_1 \oplus \dots \oplus \mathcal{A}\alpha_d$.*

Before commenting on the individual steps, we remark that steps (1) to (4) can be done in full generality without assuming hypotheses (H1) or (H2).

(1) If we replace $E[G]$ by some finite product of matrix rings over number fields A, then we define $d := \dim_E(E \otimes_{\mathcal{O}_E} X)/\dim_E(A)$.
(2) An algorithm for computing $\mathcal{M}$ is described in [Fri00, Kapitel 3 and 4].
(3) Each central primitive idempotent corresponds to an irreducible E-character χ_i and we have $e_i = \frac{n_i}{|G|}\sum_{g\in G}\chi(g^{-1})g$ with $n_i = \chi_i(1)$.
(4) In practice, we compute some multiple of the conductor. For example, one can use the method outlined in [BB06, 3.2 (f) and (g)]. Also see [BB06, Remark 3.3].
(5) This step is described in Section 5.
(6) Successful completion of step (5) shows that $\mathcal{M}X$ is a free $\mathcal{M}$-module of rank d. Therefore X is locally free of rank d over $\mathcal{A}$ except possibly at the (finite number of) primes of $\mathcal{O}_E$ dividing the generalized module index $[\mathcal{M} : \mathcal{A}]_{\mathcal{O}_E}$. An algorithm to compute local basis elements (and thus to check local freeness) at these primes is given in [BW, Section 4.2]. Note that in the motivating case $X = \mathcal{O}_L$ for some number field L (see introduction), $\mathcal{M}X$ is always locally free over $\mathcal{M}$ and so checking local freeness can be performed independently of step (5) and therefore without hypotheses (H1) or (H2). (To see this, note that $\mathcal{M}X$ is projective over $\mathcal{M}$ by [Rei75, Theorem 21.4], and L is free over $K[G]$ and thus $E[G]$ by the normal basis theorem.)
(7) This step is described in Section 6.
(8) The number of tests for this step can be greatly reduced by using a method analogous to the one outlined [Ble97, Section 2]. We briefly describe this approach in Section 7. However, even with this improvement, the enumeration is the most time-consuming part of the whole algorithm.

4. Computing Associated Orders

Let X be a finitely generated $\mathcal{O}_E[G]$-module in the free $E[G]$-space $V := E \otimes_{\mathcal{O}_E} X$. In this section, we shall assume that an $E[G]$-basis $v_1, \ldots, v_d$ of V is known. The aim is to compute the order

$$\mathcal{A}(X) = \mathcal{A}(E[G]; X) := \{\lambda \in E[G] \mid \lambda X \subseteq X\}.$$

We describe an algorithm which combines and contains all of the methods of [Ble97], [Bur00, Appendix] and [BE05, Lemma 3.1].

For further applications, such as the computation of conductors, we consider a more general problem and describe an algorithm to compute

$$\mathcal{A}(X, Y) = \mathcal{A}(E[G]; X, Y) := \{\lambda \in E[G] \mid \lambda X \subseteq Y\},$$

where $Y \subseteq V$ is another full $\mathcal{O}_E[G]$-submodule. Without loss of generality we may assume that $X, Y \subseteq E[G]^d$.

We denote by $t : E[G] \times E[G] \longrightarrow E$ any symmetric, non-degenerate E-bilinear pairing. For computational purposes we usually use the trace pairing which is characterized by

$$t(g, h) = \begin{cases} 1 & \text{if } gh = 1, \\ 0 & \text{otherwise,} \end{cases} \qquad \text{for } g, h \in G.$$

We let $s : E[G]^d \times E[G]^d \longrightarrow E$ be the d-fold orthogonal sum of t. For any $\mathcal{O}_E[G]$-module M in $E[G]^d$, respectively $E[G]$, we identify the linear dual $M^* := \mathrm{Hom}_{\mathcal{O}_E}(M, \mathcal{O}_E)$ with $\{\lambda \in E[G]^d \mid s(\lambda, M) \subseteq \mathcal{O}_E\}$, respectively $\{\lambda \in E[G] \mid t(\lambda, M) \subseteq \mathcal{O}_E\}$. If M is given by a pseudo-basis $(\mu_k, \mathfrak{c}_k)_k$, then M^* is easy to compute. Indeed, if $\{\mu_k^*\}$ is the dual basis of $\{\mu_k\}$ with respect to s, respectively t, then $(\mu_k^*, \mathfrak{c}_k^{-1})_k$ is a pseudo-basis of M^*. It is clear that the dual basis $\{\mu_k^*\}$ can be computed by means of straightforward linear algebra.

We now define an $E[G]$-module homomorphism

$$\begin{aligned}(\cdot,\cdot) : E[G]^d \times EG^d &\longrightarrow E[G],\\ (\mu,\nu) &\mapsto \sum_{g\in G} s(g\mu,\nu)g^{-1}.\end{aligned}$$

This homomorphism satisfies

$$t((\mu,\nu),\delta) = s(\nu,\delta\mu) = s(\nu\delta,\mu) \tag{6}$$

for $\mu, \nu \in E[G]^d$ and $\delta \in E[G]$.

Lemma 4.1. *Let V be a free $E[G]$-space of rank d and let X, Y be two full $\mathcal{O}_E[G]$-submodules of V. Then $(X, Y^*) = \mathcal{A}(X, Y)^*$.*

Proof. Using (6), this is essentially the same as the proof of [BB96, Lemma 4.2]. □

Remark 4.2. The main application is the following. Let L/K be a finite Galois extension of number fields with Galois group G such that E is a subfield of K and put $d = [K : E]$. Let I be an ambiguous (i.e. G-stable) ideal of the ring of integers $\mathcal{O}_L$ and define the associated order to be $\mathcal{A}(E[G]; I) := \{x \in E[G] \mid x(I) \subseteq I\}$. In [Gir99], an algorithm to compute a normal basis element for L over K (i.e. a generator for L as a $K[G]$-module) is given, and from this it is easy to determine an $E[G]$-basis of L. (It is also often easy to do this by trial and error.) Hence we can apply the above method to compute the associated order and then, assuming hypotheses (H1) and (H2), find generators using Algorithm 3.1.

Remark 4.3. The method of this section together with Algorithm 3.1 can also be used to investigate the Galois module structure of units as in [Ble97]. For a number field L, write U_L for the algebraic units of L and $\mu(L)$ for the subgroup of roots of unity. Set $X := U_L/\mu(L)$ and write A for the semisimple algebra which acts naturally on $\mathbb{Q} \otimes_{\mathbb{Z}} X$. The following cases can be considered:

(a) $L/\mathbb{Q}$ a totally real Galois extension, $A = \mathbb{Q}[G]/\left(\sum_{g\in G} g\right)$;

(b) $L/\mathbb{Q}$ a CM Galois extension with complex conjugation τ, $A = \mathbb{Q}[G]/\left(\tau - 1, \sum_{g\in G} g\right)$;

(c) L/K a Galois extension of a quadratic imaginary field K, $A = \mathbb{Q}[G]/\left(\sum_{g\in G} g\right)$.

Note that by [**?**, Lemma 5.27] the module $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is free over A, so that $\mathcal{M}X$ is always locally free over $\mathcal{M}$. Hence checking local freeness can be performed without the assumption of hypotheses (H1) and (H2).

Remark 4.4. It is always possible to compute an $E[G]$-basis $V = E \otimes_{\mathcal{O}_E} X$ under hypotheses (H1) and (H2) by using a weaker version of Proposition 5.3 in which the ring of integers and its ideals are replaced by the appropriate number field.

5. Modules over Maximal Orders in Matrix Rings over Number Fields

Let $n \in \mathbb{N}$, let F be a number field and let $\mathcal{O} = \mathcal{O}_F$ denote the ring of integers of F.

Proposition 5.1. *For each ideal $\mathfrak{a}$ of $\mathcal{O}$, let*

$$\Lambda_{\mathfrak{a},n} = \begin{pmatrix} \mathcal{O} & \cdots & \mathcal{O} & \mathfrak{a}^{-1} \\ \vdots & \ddots & \vdots & \vdots \\ \mathcal{O} & \cdots & \mathcal{O} & \mathfrak{a}^{-1} \\ \mathfrak{a} & \cdots & \mathfrak{a} & \mathcal{O} \end{pmatrix}$$

denote the ring of all $n \times n$ matrices (x_{ij}) where x_{11} ranges over all elements of $\mathcal{O}$, ..., x_{1n} ranges over all elements over $\mathfrak{a}^{-1}$, and so on. (For $n = 1$, we take $\Lambda_{\mathfrak{a},n} = \mathcal{O}$.) Then $\Lambda_{\mathfrak{a},n}$ is a maximal $\mathcal{O}$-order in $\mathrm{Mat}_n(F)$ and every maximal $\mathcal{O}$-order in $\mathrm{Mat}_n(F)$ is isomorphic to one of this form, for some ideal $\mathfrak{a}$ of $\mathcal{O}$.

Proof. This is a special case of [Rei75, Corollary 27.6]. □

Even though we can compute maximal orders (using [Fri00, Kapitel 3 and 4]), we do not automatically get them in the above "nice form". We may assume that a maximal $\mathcal{O}$-order $\Lambda \subset \mathrm{Mat}_n(F)$ is given as an $\mathcal{O}$-module by a $\mathcal{O}$-pseudo basis. We briefly describe how to find an isomorphism that transforms Λ into the "nice form" described in Proposition 5.1.

Let $Z \subseteq F^n$ denote the $\mathcal{O}$-module generated by the first column of Λ. Let

$$Z = \mathcal{O}z_1 \oplus \ldots \oplus \mathcal{O}z_{n-1} \oplus \mathfrak{a}z_n, \quad z_i \in F^n,$$

be the Steinitz form of Z for some ideal $\mathfrak{a}$ of $\mathcal{O}$. (The Steinitz form of a torsion-free, finitely generated module over a Dedekind domain is the form given in [FT91, Theorem 13(b)].)

Lemma 5.2. *Let $S = (z_1, \ldots, z_n) \in \mathrm{GL}_n(F)$ be the matrix with columns $z_1, \ldots, z_n$. Then $\Lambda = S\Lambda_{\mathfrak{a},n}S^{-1}$.*

Proof. It is easy to see that $\Lambda = \{\lambda \in \mathrm{Mat}_n(F) \mid \lambda Z \subseteq Z\}$. With a slight abuse of notation we may write $Z = (z_1, \ldots, z_n)(\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{a})^{\mathrm{T}} = S(\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{a})^{\mathrm{T}}$ and deduce

$$\begin{aligned} & \lambda Z \subseteq Z \\ \iff \quad & \lambda S(\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{a})^{\mathrm{T}} \subseteq S(\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{a})^{\mathrm{T}} \\ \iff \quad & SS^{-1}\lambda S(\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{a})^{\mathrm{T}} \subseteq S(\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{a})^{\mathrm{T}} \\ \iff \quad & S^{-1}\lambda S(\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{a})^{\mathrm{T}} \subseteq (\mathcal{O}, \ldots, \mathcal{O}, \mathfrak{a})^{\mathrm{T}} \\ \iff \quad & S^{-1}\lambda S \subseteq \Lambda_{\mathfrak{a},n} \end{aligned}$$

□

Replacing Λ by $S^{-1}\Lambda S$ and a Λ-module X by $S^{-1}X$ we may without loss of generality assume that our maximal order is in the above "nice form". We fix some maximal $\mathcal{O}$-order $\Lambda = \Lambda_{\mathfrak{a},n}$ in $\mathrm{Mat}_n(F)$ for the rest of this section and now turn to the problem of determining whether a Λ-module X is free of finite rank, and if so, whether generators can be computed. Let e_{kl} denote the matrix $(x_{ij}) \in \Lambda \subset \mathrm{Mat}_n(F)$ with $x_{ij} = 0$ for $(i,j) \neq (k,l)$ and $x_{kl} = 1$.

Proposition 5.3. *Let X be a Λ-module. Then X is free of rank d over Λ, if and only if there exist $\omega_{1,1}, \ldots, \omega_{1,n}, \ldots, \omega_{d,1}, \ldots, \omega_{d,n}$ such that*

$$e_{11}X = \mathcal{O}\omega_{1,1} \oplus \ldots \oplus \mathcal{O}\omega_{1,n-1} \oplus \mathfrak{a}^{-1}\omega_{1,n} \oplus \ldots \oplus \mathcal{O}\omega_{d,1} \oplus \ldots \oplus \mathcal{O}\omega_{d,n-1} \oplus \mathfrak{a}^{-1}\omega_{d,n}$$

Further, when this is the case, $X = \Lambda\omega_1 \oplus \ldots \oplus \Lambda\omega_d$ where $\omega_j := e_{11}\omega_{j,1} + \ldots + e_{n1}\omega_{j,n}$, $j = 1, \ldots, d$.

Proof. Suppose that X is free of rank d over Λ. Then e_{11} "cuts out the first row of each Λ" in $X \cong \oplus_{i=1}^{d}\Lambda$ and so $e_{11}X$ is of the desired form.

Now suppose conversely that there exist $\omega_{1,1}, \ldots, \omega_{1,n}, \ldots, \omega_{d,1}, \ldots, \omega_{d,n}$ such that

$$e_{11}X = \mathcal{O}\omega_{1,1} \oplus \ldots \oplus \mathcal{O}\omega_{1,n-1} \oplus \mathfrak{a}^{-1}\omega_{1,n} \oplus \ldots \oplus \mathcal{O}\omega_{d,1} \oplus \ldots \oplus \mathcal{O}\omega_{d,n-1} \oplus \mathfrak{a}^{-1}\omega_{d,n}$$

and define $\omega_j = e_{11}\omega_{j,1} + \ldots + e_{n,1}\omega_{j,n}$ for $j = 1, \ldots, d$.

For $i \neq n$ and all j, we have $\omega_{j,i} \in e_{11}X \subset X$ and so $e_{i1}\omega_{j,i} \in X$. Furthermore, $e_{n1} \in \Lambda\mathfrak{a}^{-1}$ and $\omega_{j,n} \in \mathfrak{a}e_{11}X \subseteq \mathfrak{a}X$ for all j, so $e_{n1}\omega_{j,n} \in X$. Therefore $\omega_j \in X$ for all j and so $\Lambda\omega_1 \oplus \ldots \oplus \Lambda\omega_d \subseteq X$.

Note that $X = e_{11}X \oplus \cdots \oplus e_{nn}X$ since $e_{11} + \ldots + e_{nn}$ is the $n \times n$ identity matrix. Furthermore, for all j, k we have

$$e_{1k}\omega_j = e_{1k}(e_{11}\omega_{j,1} + \ldots + e_{n1}\omega_{j,n}) = e_{1k}e_{k1}\omega_{j,k} = e_{11}\omega_{j,k} = \omega_{j,k}.$$

Therefore, since $\mathcal{O}e_{1k} \subseteq \Lambda$ for $k \neq n$ and $\mathfrak{a}^{-1}e_{1n} \subseteq \Lambda$, we have

$$\begin{aligned} e_{11}X &= \mathcal{O}\omega_{1,1} \oplus \ldots \oplus \mathcal{O}\omega_{1,n-1} \oplus \mathfrak{a}^{-1}\omega_{1,n} \oplus \ldots \oplus \mathcal{O}\omega_{d,1} \oplus \ldots \oplus \mathcal{O}\omega_{d,n-1} \oplus \mathfrak{a}^{-1}\omega_{d,n} \\ &= \mathcal{O}e_{11}\omega_1 \oplus \ldots \oplus \mathcal{O}e_{1(n-1)}\omega_1 \oplus \mathfrak{a}^{-1}e_{1n}\omega_1 \oplus \ldots \oplus \mathcal{O}e_{11}\omega_d \oplus \ldots \oplus \mathcal{O}e_{1(n-1)}\omega_d \oplus \mathfrak{a}^{-1}e_{1n}\omega_d \\ &\subseteq \Lambda\omega_1 \oplus \ldots \oplus \Lambda\omega_d. \end{aligned}$$

Finally, observe that

$$\begin{aligned} e_{ii}X &= e_{i1}e_{11}e_{1i}X \subseteq e_{i1}e_{11}X \subseteq e_{i1}(\Lambda\omega_1 \oplus \ldots \oplus \Lambda\omega_d) \\ &\subseteq \Lambda\omega_1 \oplus \ldots \oplus \Lambda\omega_d \quad \text{for } i \neq n, \text{ and} \\ e_{nn}X &= e_{n1}e_{11}e_{1n}X = (\mathfrak{a}e_{n1})e_{11}(\mathfrak{a}^{-1}e_{1n})X \subseteq (\mathfrak{a}e_{n1})e_{11}X \\ &\subseteq (\mathfrak{a}e_{n1})(\Lambda\omega_1 \oplus \ldots \oplus \Lambda\omega_d) \subseteq \Lambda\omega_1 \oplus \ldots \oplus \Lambda\omega_d, \end{aligned}$$

so therefore $X = e_{11}X \oplus \cdots \oplus e_{nn}X \subseteq \Lambda\omega_1 \oplus \ldots \oplus \Lambda\omega_d$. □

Corollary 5.4. *Let X be a Λ-module. Then X is free of rank d over Λ if and only if $e_{11}X$ is of rank dn and Steinitz class $[\mathfrak{a}^{-d}]$ as an $\mathcal{O}$-module.*

We now give a description of Step (5) of Algorithm 3.1. Fix i, set $\Lambda = S^{-1}\mathcal{M}_i S$ and replace X by $S^{-1}X$, where S is as in Lemma 5.2. It is straightforward to see that it suffices to determine elements $\omega_{1,1}, \ldots, \omega_{d,n}$ satisfying the equation of Proposition 5.3. First, compute a Steinitz form for $e_{11}X$, i.e. find $b_j \in e_{11}X$ and an ideal $\mathfrak{b}$ of $\mathcal{O}$ such that

$$e_{11}X = \mathcal{O}b_1 \oplus \ldots \oplus \mathcal{O}b_{dn-1} \oplus \mathfrak{b}b_{dn}$$

(one can use the Magma function `SteinitzForm`) and check that $[\mathfrak{b}] = [\mathfrak{a}^{-d}]$ in $\mathrm{Cl}(\mathcal{O})$. Let $Y = \mathcal{O}b_{d(n-1)+1} \oplus \ldots \oplus \mathcal{O}b_{nd-1} \oplus \mathfrak{b}b_{dn}$ and compute $\mathfrak{a}Y$. This is a free $\mathcal{O}$-module of rank d and so we can compute an $\mathcal{O}$-basis, $c_1, \ldots, c_d$, which is also a "$\mathfrak{a}^{-1}$ basis" of Y. Now we can take $\omega_{j,n} = c_j$ for $j = 1, \ldots, d$ and $\{\omega_{j,k} \mid k \neq n\} = \{b_1, \ldots, b_{d(n-1)}\}$.

6. Enumerating Units

Let $d, n \in \mathbb{N}$, let F be a number field and let $\mathcal{O} = \mathcal{O}_F$ denote the ring of integers of F. Let Λ be some maximal $\mathcal{O}$-order of $\mathrm{Mat}_n(F)$. By Lemma 5.2 we may assume that Λ is of the "nice form" $\Lambda_{\mathfrak{a},n}$. Let $\mathfrak{g}$ be some non-zero ideal of $\mathcal{O}_F$ and let $\mathfrak{f} := \mathfrak{g}\Lambda$. Throughout this section, we identify $\mathrm{Mat}_d(\Lambda)$ with a subring of $\mathrm{Mat}_{dn}(F)$ in the obvious way. We wish to compute a set of representatives $U \subset \mathrm{GL}_d(\Lambda)$ of the image of the natural projection map $\pi : \mathrm{GL}_d(\Lambda) \longrightarrow \mathrm{GL}_d(\overline{\Lambda})$ where $\overline{\Lambda} = \Lambda/\mathfrak{f}$.

Definition 6.1. Let $i, j \in \{1, \ldots, nd\}$ with $i \neq j$ and let

$$x \in \begin{cases} \mathcal{O}/\mathfrak{g}, & \text{if } i, j \nmid n \text{ or } i, j \mid n, \\ \mathfrak{a}^{-1}/\mathfrak{g}\mathfrak{a}^{-1}, & \text{if } i \nmid n \text{ and } j \mid n, \\ \mathfrak{a}/\mathfrak{g}\mathfrak{a}, & \text{if } j \nmid n \text{ and } i \mid n. \end{cases}$$

Then the elementary matrix $\mathrm{E}_{ij}(x)$ is the matrix in $\mathrm{GL}_d(\overline{\Lambda})$ that has 1 in every diagonal spot, has x in the (i, j)-spot and is zero elsewhere. Let $\mathrm{E}(\overline{\Lambda})$ denote the subgroup of $\mathrm{GL}_d(\overline{\Lambda})$ generated by all elementary matrices and define $\mathrm{E}(\Lambda)$ analogously. Note $\pi(\mathrm{E}(\Lambda)) = \mathrm{E}(\overline{\Lambda})$.

Proposition 6.2. *Let $\varepsilon : \mathcal{O}_F^\times \to (\mathcal{O}_F/\mathfrak{g})^\times$ be the natural projection map and let V be the subgroup of matrices $(x_{ij}) \in \mathrm{GL}_d(\overline{\Lambda})$ with $x_{11} \in \varepsilon(\mathcal{O}_F^\times)$, $x_{ii} = 1$ for $i \neq 1$ and $x_{ij} = 0$ for $i \neq j$. Then $\pi(\mathrm{GL}_d(\Lambda))$ is generated by $\mathrm{E}(\overline{\Lambda})$ and V.*

Proof. Let $R := \mathcal{O}/\mathfrak{g}$ and consider the R-modules $X := \oplus_{i=1}^d R^n$ and $Y := \oplus_{i=1}^d (R^{n-1} \oplus \mathfrak{a}/\mathfrak{g}\mathfrak{a})$. We choose $\xi \in F^\times$ and an integral ideal $\mathfrak{b}$ such that

$$\mathfrak{a} = \xi\mathfrak{b}, \quad \mathfrak{b} + \mathfrak{g} = \mathcal{O}.$$

Let $b \in \mathfrak{b}$ and $y \in \mathfrak{g}$ such that $b + y = 1$. Then we have an isomorphism $\mathcal{O}/\mathfrak{g} \longrightarrow \mathfrak{a}/\mathfrak{a}\mathfrak{g}$ of R-modules defined by $z + \mathfrak{g} \mapsto zb\xi + \mathfrak{a}\mathfrak{g}$. The inverse is given by $z + \mathfrak{a}\mathfrak{g} \mapsto \xi^{-1}z + \mathfrak{g}$.

This induces an isomorphism $\varphi\colon X \to Y$, and as a consequence we obtain an isomorphism

$$\begin{array}{rcl} \psi\colon \mathrm{GL}_{nd}(R) & \longrightarrow & \mathrm{GL}_d(\overline{\Lambda}), \\ \overline{A} = (\overline{A}_{ij})_{1 \leq i,j \leq d} & \mapsto & (\overline{\Phi_2 A_{ij} \Phi_1})_{1 \leq i,j \leq d} \end{array}$$

where $A_{ij} \in \mathrm{Mat}_n(\mathcal{O})$,

$$\Phi_1 = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \xi^{-1} \end{pmatrix} \text{ and } \Phi_2 = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & b\xi \end{pmatrix}.$$

One easily verifies that $\psi(\mathrm{E}_{nd}(R)) = \mathrm{E}(\overline{\Lambda})$ where $\mathrm{E}_{nd}(R)$ denotes the group generated by elementary matrices of $\mathrm{Mat}_{nd}(R)$. From [Bas68, Corollary (9.3), p.267] we deduce $\mathrm{SL}_{nd}(R) = \mathrm{E}_{nd}(R)$. Hence we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{SL}_{nd}(R) & \longrightarrow & \mathrm{GL}_{nd}(R) & \xrightarrow{\det} & R^\times & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \psi}\ \simeq & & \downarrow{\scriptstyle \psi}\ \simeq & & \downarrow{\scriptstyle =} & & \\ 1 & \longrightarrow & \mathrm{E}(\overline{\Lambda}) & \longrightarrow & \mathrm{GL}_d(\overline{\Lambda}) & \xrightarrow{\det'} & R^\times & \longrightarrow & 1 \end{array}$$

where $\det' := \det \circ \psi^{-1}$. The diagram

$$\begin{array}{ccccccccc} & & & & \mathrm{GL}_d(\Lambda) & \xrightarrow{\det} & \mathcal{O}^\times & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \varepsilon} & & \\ 1 & \longrightarrow & \mathrm{E}(\overline{\Lambda}) & \longrightarrow & \mathrm{GL}_d(\overline{\Lambda}) & \xrightarrow{\det'} & R^\times & \longrightarrow & 1 \end{array}$$

also has exact rows and a straightforward computation shows that it commutes. This immediately implies the assertions of the proposition. □

We now give a description of Step (7) of Algorithm 3.1. Fix i, and set $n = n_i$, $\Lambda = S^{-1}\mathcal{M}_i S$ with S as in Lemma 5.2, $\mathfrak{g} = \mathfrak{g}_i, F = E_i$ and $U = U_i$. Using, for example, [Coh93, Algorithm 6.5.8], compute a generating set $\{a_1, \ldots, a_s\}$ for $\mathcal{O}_F^\times$. Then $\{\varepsilon(a_1), \ldots, \varepsilon(a_s)\}$ is a generating set for $\varepsilon(\mathcal{O}_F^\times)$ and using the obvious isomorphism we have a generating set for V. The group $\mathrm{E}(\Lambda)$ is generated by the elementary matrices $\mathrm{E}_{ij}(b_{ijk})$ for $i, j \in \{1, \ldots, n\}$, $i \neq j$ where for fixed i, j, $\{b_{ijk}\}$ is a $\mathbb{Z}$-spanning set for $\mathcal{O}/\mathfrak{g}$, $\mathfrak{a}/\mathfrak{g}\mathfrak{a}$ or $\mathfrak{a}^{-1}/\mathfrak{g}\mathfrak{a}^{-1}$, as appropriate. Such spanning sets can be computed using Hermite Normal Form techniques described, for example, in [Coh93, Chapter 2.4]. By Corollary 6.2, we now have an explicit generating set for $\pi(\mathrm{GL}_d(\Lambda))$, and so it is straightforward to compute the desired set of representatives $U = U_i$.

7. Reducing the Number of Final Tests

The final number of tests in step (8) of Algorithm 3.1 can be enormous. For example, if $G \simeq S_4$ (the symmetric group with 24 elements) and $\mathcal{A} = \mathbb{Z}[G]$, then a computation shows that there are approximately 4.4×10^{18} tuples $(\lambda_i) \in \prod_{i=1}^r U_i$, which need to be tested. In this section, we describe an ad hoc method analogous to the one outlined in [Ble97, Section 2] to reduce the number of tests required.

However, even with this improvement, the number of tests which need to be performed is still very large. Despite this, somewhat surprisingly, we can find generating elements in many S_4-examples. It would be interesting to have an explanation, possibly probabilistic or heuristic in nature, for this phenomena.

The improvement is based on the following simple observation. Let

$$\begin{aligned} \mathcal{M}X &= \mathfrak{a}_1 v_1 \oplus \ldots \oplus \mathfrak{a}_m v_m, \\ X &= \mathfrak{b}_1 w_1 \oplus \ldots \oplus \mathfrak{b}_m w_m, \end{aligned}$$

be $\mathcal{O}_E$-pseudo-basis representations of $\mathcal{M}X$ and X. Let $A \in \mathrm{GL}_m(E)$ be the transformation matrix such that

$$\begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} = A \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}.$$

We now apply the Hermite Normal Form algorithm in Dedekind domains (see [Coh00, Algorithm 1.4.7]) to the matrix A and the list of ideals $(\mathfrak{b}_1, \ldots, \mathfrak{b}_m)$, though we reduce rows rather than columns. We obtain a matrix $U \in \mathrm{GL}_m(E)$ and a list of ideals $(\mathfrak{c}_1, \ldots, \mathfrak{c}_m)$ such that the matrix $H = UA$ is upper triangular with 1 on each diagonal entry. Moreover,

$$\mathfrak{c}_1 h_1 \oplus \ldots \oplus \mathfrak{c}_m h_m = \mathfrak{b}_1 a_1 \oplus \ldots \oplus \mathfrak{b}_m a_m,$$

where $h_1, \ldots, h_m$ denote the rows of H and $a_1, \ldots, a_m$ denote the rows of A. This immediately implies that $U(w_1, \ldots, w_m)^{\mathrm{T}}$ together with the list of ideals $(\mathfrak{c}_1, \ldots, \mathfrak{c}_m)$ is also a pseudo-basis for X.

Now suppose that the vector $(x_1, \ldots, x_m) \in E^m$ defines an element $x = \sum_{i=1}^m x_i v_i \in \mathcal{M}X$. Then we have

$$x \in X \iff (x_1, \ldots, x_m)H^{-1} \in (\mathfrak{c}_1, \ldots, \mathfrak{c}_m). \tag{7}$$

Since H^{-1} is upper triangular, this leads to a much more efficient enumeration. In addition, in many cases the coefficients $x_1, \ldots, x_m$ can be easily computed by a clever choice of basis $v_1, \ldots, v_m$. To illustrate this, we conclude this section with a brief discussion of the case where $G \simeq S_n$, $E = \mathbb{Q}$ and $X \subseteq E[G]$ is locally free of rank 1.

Let

$$\Phi : \mathbb{Q}[G] \longrightarrow \bigoplus_{i=1}^{r} \mathrm{Mat}_{n_i}(\mathbb{Q})$$

be the explicitly computable isomorphism that gives the Wedderburn decomposition of $\mathbb{Q}[G]$. Let $\mathcal{M} \subseteq \mathbb{Q}[G]$ be the maximal order such that $\Phi(\mathcal{M}) = \oplus_{i=1}^r \mathrm{Mat}_{n_i}(\mathbb{Z})$. For reasons of efficiency, we choose to work with matrices and henceforth consider $\mathcal{M}X$ as a module over $\oplus_{i=1}^r \mathrm{Mat}_{n_i}(\mathbb{Z})$ via the isomorphism Φ^{-1}. Let $B = (B_1, \ldots, B_r)$ denote a $\oplus_{i=1}^r \mathrm{Mat}_{n_i}(\mathbb{Z})$-basis of $\mathcal{M}X$. Let $e_{i,kl} = (\ldots, e_{kl}, \ldots) \in \oplus_{j=1}^r \mathrm{Mat}_{n_j}(\mathbb{Z})$, $i = 1, \ldots, r$, $1 \leq k, l \leq n_i$, denote the tuple of matrices with the matrix e_{kl} in the i-th position and the zero matrix everywhere else. Then the set $\{e_{i,kl}B\}$ forms a $\mathbb{Z}$-basis of $\mathcal{M}X$.

Now let $(\lambda_1, \ldots, \lambda_r) \in \prod_i U_i$. Then the coefficients $(x_{i,kl})_{i,k,l}$ of $(\lambda_1 B_1, \ldots, \lambda_r B_r)$ with respect to the basis $\{e_{i,kl}B\}$ are given by the coefficients of the matrices λ_i because

$$\lambda_i B_i = \left(\sum_{1 \le k,l \le n_i} \lambda_{i,kl} e_{kl} \right) B_i = \sum_{1 \le k,l \le n_i} \lambda_{i,kl} \left(e_{kl} B_i \right).$$

8. Implementation and Computational Results

In this section, we describe the cases for which Algorithm 3.1 has been implemented in Magma ([BCP97]). The source code and tables of numerical results are available from

`http://www.mathematik.uni-kassel.de/~bley/pub.html`.

Let L/K be a finite Galois extension of number fields with Galois group G such that E is a subfield of K and put $d = [K : E]$. As discussed in Section 4, Algorithm 3.1 can be applied in this situation with $X = \mathcal{O}_L$ and $\mathcal{A} = \mathcal{A}(E[G]; \mathcal{O}_L)$. However, for the sake of simplicity, all aspects of the implementation in Magma are restricted to the case $K = E = \mathbb{Q}$.

Let $\mathcal{A}_{L/\mathbb{Q}} = \mathcal{A}(\mathbb{Q}[G]; \mathcal{O}_L)$. We have the following:

(a) For any finite Galois extension $L/\mathbb{Q}$, we can compute the associated order $\mathcal{A}_{L/\mathbb{Q}}$ and check that $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/\mathbb{Q}}$, provided that Magma can compute the ring of integers $\mathcal{O}_L$ and that the Magma function `AutomorphismGroup(L)` works. Of course, this can be improved if theoretical information for either the ring of integers or the Galois group is available.

(b) For $G = A_4, S_4, D_n$ or G abelian, we can explicitly compute the Wedderburn decomposition of $\mathbb{Q}[G]$ so that hypothesis (H1) is satisfied (here D_n is the dihedral group of order $2n$).

(c) We can compute generators α_i such that $\mathcal{M}_i \mathcal{O}_L = \mathcal{M}_i \alpha_i$ whenever $G = A_4, S_4, D_n$ or G abelian. This works very well for small n and small abelian groups. For example, we successfully ran many experiments with dihedral groups D_n and $n \le 10$. Note however, that our implementation requires that all the fields E_i have class number 1.

(d) We can compute a generator α such that $\mathcal{O}_L = \mathcal{A}_{L/\mathbb{Q}} \alpha$ whenever $G = A_4$, D_n with n small or G a small abelian group. For dihedral groups "small" means something like $n \le 10$, for abelian groups experiments show that we can easily deal with groups of order ≤ 20. For S_4-extensions the number of checks required in the final enumeration is simply too large to be done in a naive way. Indeed, there are five Wedderburn components of $\mathbb{Q}[S_4]$ and if $L/\mathbb{Q}$ is tame, then the numbers of elements in the sets U_i (notation as in Proposition 2.4) are

$$|U_1| = 2, \quad |U_2| = 2, \quad |U_3| = 2304, \quad |U_4| = 22020096, \quad |U_5| = 22020096.$$

Note that these numbers are smaller if $L/\mathbb{Q}$ is wildly ramified.

The authors implemented the reduction method outlined in Section 7 and, to their surprise, were able to compute generating elements in all of their examples. As already

mentioned, it would be very interesting to have some explanation for this unexpected phenomenon.

(e) The algorithm as implemented in Magma is not deterministic, i.e., the program will produce different generators for the same extension when run at different times. The relevant steps, where different choices may finally lead to different generators, are the choice of a normal basis element for $L/\mathbb{Q}$ and the order of the final enumeration.

The authors computed generators for more than 140 extensions $L/\mathbb{Q}$ with Galois group A_4 taken from the tables of [KM]. This might lead one to speculate, for example, that every such extension has the property that $\mathcal{O}_L$ is free over $\mathcal{A}_{L/\mathbb{Q}}$. In principle, one can prove or disprove this assertion in the following way.

It is well-known that the locally free class group $\mathrm{Cl}(\mathbb{Z}[A_4])$ is trivial (see [Cou06], for example), and from this it is straightforward to show that $\mathrm{Cl}(\mathcal{A})$ is also trivial for any order $\mathcal{A}$ with $\mathbb{Z}[A_4] \subseteq \mathcal{A} \subseteq \mathbb{Q}[A_4]$. Since $\mathbb{Q}[A_4]$ satisfies the Eichler condition relative to $\mathbb{Z}$ (see [Rei75, Definitions 34.3 and 38.1]), a result of Jacobinski shows that if an $\mathcal{A}$-module has trivial class in $\mathrm{Cl}(\mathcal{A})$, then it is in fact free over $\mathcal{A}$ (see [Rei75, Theorem 38.2], for example). Hence we are reduced to establishing whether $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/\mathbb{Q}}$ for every A_4-extension $L/\mathbb{Q}$.

In fact, for any number field K and finite group G, it is possible to check in a finite amount of time whether every extension L/K with Galois group G has the property that $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K} := \mathcal{A}(K[G]; L)$. By Noether's Theorem (see [Noe32]), we have local freeness at all primes of $\mathcal{O}_K$ that are at most tamely ramified in L/K. Therefore, it suffices to check all extensions of p-adic fields $K_\mathfrak{p}$ with Galois group H, where $\mathfrak{p}$ ranges over all primes of $\mathcal{O}_K$ dividing the order of G and H ranges over all solvable subgroups of G. Enumerating all such extensions is possible using the algorithm of [PR01] (this gives generating polynomials for all extensions of a p-adic field $K_\mathfrak{p}$ of given degree and discriminant), and local freeness can be checked using the method outlined in [BW, Section 4.2].

9. Acknowledgments

The authors are grateful to the Deutscher Akademischer Austausch Dienst (German Academic Exchange Service) for a grant allowing the second named author to visit Cornelius Greither at Universität der Bunderswehr München for the 2006-07 academic year, thus making this collaboration possible. The authors also wish to thank John Cannon for useful correspondence regarding features to appear in the next version of Magma.

References

[Bas68] H. Bass, *Algebraic K-theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[BB96] W. Bley and D. Burns, *Über arithmetische assoziierte Ordnungen*, J. Number Theory **58** (1996), no. 2, 361–387.

[BB06] W. Bley and M. Boltje, *Computation of locally free class groups*, Algorithmic Number Theory (F. Hess, S.Pauli, and M.Pohst, eds.), Lecture Notes in Computer Science, no. 4076, Springer, 2006, pp. 72–86.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), no. 3/4, 235–265.

[BE05] W. Bley and M. Endres, *Picard groups and refined discrete logarithms*, LMS J. Comput. Math. **8** (2005), 1–16.

[BL96] N. P. Byott and G. Lettl, *Relative Galois module structure of integers of abelian fields*, J. Théor. Nombres Bordeaux **8** (1996), 125–141.

[Ble95] W. Bley, *A Leopoldt-type result for rings of integers of cyclotomic extensions*, Canad. Math. Bull. **38** (1995), 141–148.

[Ble97] ———, *Computing associated orders and Galois generating elements of unit lattices*, J. Number Theory **62** (1997), no. 2, 361–387.

[Bur00] D. Burns, *On the equivariant structure of ideals in abelian extensions of local fields (with an appendix by W. Bley)*, Comment. Math. Helv. **75** (2000), no. 1, 1–44.

[BW] W. Bley and S. M. J. Wilson, *Computations in relative algebraic K-groups*, preprint.

[CL93] S.-P. Chan and C.-H. Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. reine angew. Math. **434** (1993), 205–220.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, no. 138, Springer-Verlag, 1993.

[Coh00] ———, *Advanced topics is computational number thoery*, Graduate Texts in Mathematics, no. 193, Springer-Verlag, 2000.

[Cou98] J. Cougnard, *Anneaux d'entiers stablement libres sur* $\mathbb{Z}[H_8 \times C_2]$, J. Théor. Nombres Bordeaux **10** (1998), no. 1, 163–201.

[Cou00] ———, *Construction de base normale pour les extensions de* $\mathbb{Q}$ *à groupe* D_4, J. Théor. Nombres Bordeaux **12** (2000), no. 2, 399–409.

[Cou06] ———, *Normal integral bases for* A_4 *extensions of the rationals*, Math. Comp. **75** (2006), no. 253, 485–496.

[CQ02] J. Cougnard and J. Queyrut, *Construction de bases normales pour les extensions galoisiennes absolues à groupe de Galois quaternionien d'ordre 12*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 87–102.

[Fri00] C. Friedrichs, *Berechnung von Maximalordnungen über Dedekindringen*, Ph.D. thesis, Technische Universität Berlin, 2000.

[Frö83] A. Fröhlich, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), no. 1, Springer-Verlag, Berlin, 1983.

[FT91] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, no. 27, Cambridge Univ. Press, Cambridge, 1991.

[Gir99] K. Girstmair, *An algorithm for the construction of a normal basis*, J. Number Theory **78** (1999), no. 1, 36–45.

[Ich04] H. Ichimura, *On the ring of integers of a tame Kummer extension over a number field*, J. Pure Appl. Algebra **187** (2004), no. 1-3, 169–182.

[Isa94] I. M. Isaacs, *Character theory of finite groups*, Dover, New York, 1994.

[Joh] H. Johnston, *Relative Galois module structure of rings of integers of absolutely abelian number fields*, to appear in Crelle.

[KM] J. Klüners and G. Malle, *A database for number fields*, http://www.math.uni-duesseldorf.de/∼klueners/minimum/minimum.html.

[Leo59] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine angew. Math. **201** (1959), 119–149.

[Let90] G. Lettl, *The ring of integers of an abelian number field*, J. reine angew. Math. **404** (1990), 162–170.

[Mar69] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre* $2p$, Ann. Inst. Fourier (Grenoble) **19** (1969), no. 1, 1–80.

[Noe32] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. reine angew. Math. **167** (1932), 147–152.

[PR01] S. Pauli and X.-F. Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Math. Comp. **70** (2001), no. 236, 1641–1659.

[Rei75] I. Reiner, *Maximal orders*, Academic Press, London-New York, 1975.

Werner Bley, Fachbereich für Mathematik und Informatik der Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, Germany
E-mail address: bley@mathematik.uni-kassel.de
URL: http://www.mathematik.uni-kassel.de/∼bley

Henri Johnston, St. Hugh's College, St. Margaret's Road, Oxford OX2 6LE, UK
E-mail address: henri@maths.ox.ac.uk
URL: http://www.maths.ox.ac.uk/∼henri