MATHEMATICS OF COMPUTATION
Volume 89, Number 326, November 2020, Pages 2931–2963
https://doi.org/10.1090/mcom/3543
Article electronically published on June 1, 2020

COMPUTING ISOMORPHISMS BETWEEN LATTICES

TOMMY HOFMANN AND HENRI JOHNSTON

Abstract. Let K be a number field, let A be a finite-dimensional semisimple K-algebra, and let Λ be an $\mathcal{O}_K$-order in A. It was shown in previous work that, under certain hypotheses on A, there exists an algorithm that for a given (left) Λ-lattice X either computes a free basis of X over Λ or shows that X is not free over Λ. In the present article, we generalize this by showing that, under weaker hypotheses on A, there exists an algorithm that for two given Λ-lattices X and Y either computes an isomorphism $X \to Y$ or determines that X and Y are not isomorphic. The algorithm is implemented in Magma for $A = \mathbb{Q}[G]$, $\Lambda = \mathbb{Z}[G]$, and Λ-lattices X and Y contained in $\mathbb{Q}[G]$, where G is a finite group satisfying certain hypotheses. This is used to investigate the Galois module structure of rings of integers and ambiguous ideals of tamely ramified Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to $Q_8 \times C_2$, the direct product of the quaternion group of order 8 and the cyclic group of order 2.

1. Introduction

Let K be a number field with ring of integers $\mathcal{O}_K$. Let A be a finite-dimensional semisimple K-algebra, and let Λ be an $\mathcal{O}_K$-order in A. For example, if G is a finite group, then the group ring $\mathcal{O}_K[G]$ is an order in the group algebra $K[G]$. A Λ-lattice is a (left) Λ-module that is finitely generated and torsion-free over $\mathcal{O}_K$. In previous work [BJ08, BJ11] of Bley and the second named author, it was shown that, under certain hypotheses on A, there exists an algorithm that for a given Λ-lattice X either computes a free basis of X over Λ or shows that X is not free over Λ. In the present paper, we generalize this by showing that, under the (weaker) hypotheses on A discussed below, there exists an algorithm that for two given Λ-lattices X and Y either computes an isomorphism $X \to Y$ or determines that X and Y are not isomorphic.

The key theoretical results of the present article are necessary and sufficient conditions for the existence of an isomorphism $X \to Y$ between two given Λ-lattices (see §3). One of these criteria forms the basis of the main algorithm (Algorithm 4.1).

Let $A = A_1 \oplus \cdots \oplus A_r$ be the decomposition of A into indecomposable two-sided ideals and let K_i denote the center of the simple algebra A_i. A key step of Algorithm 4.1 requires the following two hypotheses, which are discussed in detail in §5.

Received by the editor March 2, 2019, and, in revised form, January 13, 2020.
2010 *Mathematics Subject Classification.* Primary 11R33, 11Y40, 16Z05.
The first author was supported by Project II.2 of SFB-TRR 195 "Symbolic Tools in Mathematics and their Application" of the German Research Foundation (DFG).
The second author was supported by EPSRC First Grant EP/N005716/1 "Equivariant Conjectures in Arithmetic".

(H1) For each i, we can compute an explicit isomorphism $A_i \cong \mathrm{Mat}_{n_i \times n_i}(D_i)$ of K-algebras, where D_i is a skew field with center K_i.
(H2) For each i, every maximal $\mathcal{O}_K$-order Δ_i in D_i has the following properties:
  (a) we can solve the principal ideal problem for fractional left Δ_i-ideals, and
  (b) Δ_i has the locally free cancellation property.

The key step in question is the computation of isomorphisms of certain lattices over maximal orders in each simple component A_i (see §6). Two other crucial steps are the computation of endomorphism rings (a method for the more general problem of computing homomorphism groups is given in §7) and isomorphism testing for localized lattices (see §8). An ad hoc method for reducing the number of tests required in the last (and most expensive) step of Algorithm 4.1 is outlined in §9.

An important motivation for this work is the investigation of the Galois module structure of rings of integers and their ambiguous ideals. Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. The classical Normal Basis Theorem says that L is free of rank 1 as a module over the group algebra $K[G]$. A much more difficult problem is that of determining the structure of the ring of integers $\mathcal{O}_L$ over an order such as $\mathcal{O}_K[G]$. More generally, one can consider the structure of ambiguous ideals of $\mathcal{O}_L$. There is a very large body of work on these problems, and we now mention only a small selection of results.

By far 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 $\mathcal{O}_L$ is a locally free $\mathcal{O}_K[G]$-lattice of rank 1 (see [Noe32] or [Frö83, I, §3]). Thus one can consider the class $(\mathcal{O}_L)$ in the locally free class group $\mathrm{Cl}(\mathcal{O}_K[G])$. If G is abelian or of odd order, then $(\mathcal{O}_L)$ determines $\mathcal{O}_L$ up to isomorphism, but for $K = \mathbb{Q}$ and certain nonabelian G of even order, this class only determines $\mathcal{O}_L$ up to stable isomorphism. If we restrict scalars and consider $\mathcal{O}_L$ as a $\mathbb{Z}[G]$-module, then we obtain a class $(\mathcal{O}_L)_{\mathbb{Z}[G]}$ in $\mathrm{Cl}(\mathbb{Z}[G])$. The root number class $W_{L/K}$ in $\mathrm{Cl}(\mathbb{Z}[G])$ was defined by Ph. Cassou-Noguès in terms of Artin root numbers of the irreducible symplectic characters of G, and Taylor's proof [Tay81] of a conjecture of Fröhlich shows that $(\mathcal{O}_L)_{\mathbb{Z}[G]} = W_{L/K}$ (see [Frö83, I] for an overview). In particular, if G is abelian or of odd order, then $W_{L/K}$ is trivial and $\mathcal{O}_L$ is always free over $\mathbb{Z}[G]$ (unfortunately, this approach does not give a description of a $\mathbb{Z}[G]$-basis). There are many examples of interesting behaviour when $G \cong Q_{4n}$, the quaternion group of order $4n$. For instance, when $K = \mathbb{Q}$ and $G \cong Q_8$, both possibilities for $W_{L/K}$ in $\mathrm{Cl}(\mathbb{Z}[Q_8]) \cong \{\pm 1\}$ occur infinitely often. Moreover, Cougnard [Cou94] gave an example with $K = \mathbb{Q}$ and $G \cong Q_{32}$ such that $\mathcal{O}_L$ is stably free but not free over $\mathbb{Z}[G]$.

If L/K is wildly ramified, then the situation becomes much more difficult because $\mathcal{O}_L$ is not even locally free over $\mathbb{Z}[G]$. One approach is to consider the structure of $\mathcal{O}_L$ over the so-called associated order $\mathfrak{A}_{L/K} = \{\lambda \in K[G] \mid \lambda \mathcal{O}_L \subseteq \mathcal{O}_L\}$, which is equal to $\mathcal{O}_K[G]$ if and only if L/K is tamely ramified. An important result in this setting is Leopoldt's Theorem [Leo59], which says that for any finite abelian extension $L/\mathbb{Q}$ the ring of integers $\mathcal{O}_L$ is always free over $\mathfrak{A}_{L/\mathbb{Q}}$ and, in addition, gives an explicit construction of a free generator (see also [Let90]). However, in general, $\mathcal{O}_L$ need not even be locally free over $\mathfrak{A}_{L/K}$. An alternative approach is to consider Chinburg's invariant $\Omega(L/K, 2)$ in $\mathrm{Cl}(\mathbb{Z}[G])$. This is equal to $(\mathcal{O}_L)_{\mathbb{Z}[G]}$ in the tamely ramified case, but is also defined when L/K is wildly ramified. Fröhlich [Frö78] generalized the definition of $W_{L/K}$ to the wildly ramified case. Chinburg's

"$\Omega(2)$ conjecture" [Chi85] asserts that $\Omega(L/K,2) = W_{L/K}$; in the tamely ramified case this is equivalent to the aforementioned theorem of Taylor.

Another interesting problem is the determination of the structure of the square root $\mathcal{A}_{L/K}$ of the inverse different $\mathcal{D}_{L/K}^{-1}$. The former exists (and is unique) precisely when the latter is a square, which can be tested using Hilbert's formula [Ser79, IV, Proposition 4]. In particular, $\mathcal{A}_{L/K}$ always exists when $|G|$ is odd. Erez showed that if $\mathcal{A}_{L/K}$ exists, then $\mathcal{A}_{L/K}$ is locally free over $\mathbb{Z}[G]$ if and only if L/K is weakly ramified, that is, the second ramification group of every prime is trivial (see [Ere91] and [CV16, footnote 1]). He also showed that if $|G|$ is odd and L/K is tamely ramified, then $\mathcal{A}_{L/K}$ is free over $\mathbb{Z}[G]$. This result was generalized by Caputo and Vinatier [CV16] and has been further extended in recent work of Agboola and Caputo [AC20] who showed that if L/K is tamely ramified and $\mathcal{A}_{L/K}$ exists, then $\Omega(L/K,2) = (\mathcal{O}_L)_{\mathbb{Z}[G]} = (\mathcal{A}_{L/K})_{\mathbb{Z}[G]}$ in $\mathrm{Cl}(\mathbb{Z}[G])$. Moreover, Erez has asked whether $\Omega(L/K,2) = (\mathcal{A}_{L/K})_{\mathbb{Z}[G]}$ for every weakly ramified extension L/K such that $\mathcal{A}_{L/K}$ exists (see [CV16, Question 2]); under the assumption of Chinburg's $\Omega(2)$ conjecture this may been seen as a generalization of a question of Vinatier [Vin03].

We now review previous work on related algorithms. Let K be a number field, let A be a finite-dimensional semisimple K-algebra, and let Λ be an $\mathcal{O}_K$-order in A. In the case that A is commutative and X is a Λ-lattice such that $K \otimes_{\mathcal{O}_K} X$ is free of rank 1 over A, Bley [Ble97] gave algorithms that determine whether X is locally free over Λ, and either explicitly construct a free generator for X over Λ or show that no such generator exists (though stated for a specific arithmetic case, it is straightforward to see that the algorithms work in this more general setting). A noncommutative higher-rank generalization was given by Bley and the second named author [BJ08, BJ11], and it is this work that is in turn generalized in the present paper. In [BE05], Bley and Endres again considered the case in which A is commutative and gave algorithms for computing the Picard group $\mathrm{Pic}(\Lambda)$ and solving the corresponding refined discrete logarithm problem (and thus for computing isomorphisms between invertible Λ-submodules of A). In the case that $A = K[G]$ for some finite group G, Bley and Wilson [BW09] gave algorithms for computing the relative algebraic K-group $K_0(\mathcal{O}_K[G], K)$ and solving the discrete logarithm problem in both $K_0(\mathcal{O}_K[G]), K)$ and the locally free class group $\mathrm{Cl}(\mathcal{O}_K[G])$ (note that this is a lot weaker than the *refined* discrete logarithm problem and can only be used to determine whether two locally free $\mathcal{O}_K[G]$-lattices are stably isomorphic).

The main algorithm of the present article (Algorithm 4.1) is very general: it is only subject to the hypotheses (H1) and (H2) and does not require the order Λ to be commutative or the lattices to be locally free, for example. Moreover, not only does it determine whether two lattices are isomorphic (rather than just stably isomorphic), but it also explicitly computes an isomorphism, if one exists.

In §10, we discuss experimental results obtained by using a proof of concept implementation of Algorithm 4.1 in Magma [BCP97] for $A = \mathbb{Q}[G]$, $\Lambda = \mathbb{Z}[G]$, and Λ-lattices X and Y contained in $\mathbb{Q}[G]$, where G is a finite group satisfying certain hypotheses. We now fix $G = Q_8 \times C_2$, the direct product of the quaternion group of order 8 and the cyclic group of order 2, and remark that this satisfies the hypotheses required by the implementation. Moreover, Swan [Swa83] showed that there exist $\mathbb{Z}[G]$-lattices that are stably free but not free, but that for any group H with $|H| < 16$, every stably free $\mathbb{Z}[H]$-lattice is, in fact, free. Using Swan's results,

Cougnard [Cou98] gave examples of tamely ramified Galois extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ such that $\mathcal{O}_L$ is stably free but not free over $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$. Using the implementation of Algorithm 4.1, we find the extension of smallest absolute discriminant with this property. For fixed tamely ramified Galois extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$, we then examine the distribution of isomorphism classes of ambiguous ideals of $\mathcal{O}_L$.

2. Preliminaries on lattices and orders

For further background, we refer the reader to [CR81, Rei03]. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. To avoid trivialities, we assume that $\mathcal{O} \neq K$.

2.1. **Lattices over Dedekind domains.** An $\mathcal{O}$-lattice M is a finitely generated torsion-free $\mathcal{O}$-module or, equivalently, a finitely generated projective $\mathcal{O}$-module. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, we let $\mathcal{O}_\mathfrak{p}$ denote the localization (not completion) of $\mathcal{O}$ at $\mathfrak{p}$. We define the localization of M at $\mathfrak{p}$ to be the $\mathcal{O}_\mathfrak{p}$-lattice $M_\mathfrak{p} := \mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} M$. We can identify M with its image $1 \otimes M$ in $\mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} M$ and thus may view M as embedded in $M_\mathfrak{p}$. In particular, we may view M as a finitely generated $\mathcal{O}$-submodule of the finite-dimensional K-vector space $K \otimes_\mathcal{O} M$, which we may write in the simpler form

$$KM := \{\alpha_1 m_1 + \cdots + \alpha_r m_r \mid r \in \mathbb{Z}_{\geq 0}, \alpha_i \in K, m_i \in M\}.$$

Then for any choice of $\mathfrak{p}$, we may identify $M_\mathfrak{p}$ with

$$\mathcal{O}_\mathfrak{p} M := \{\alpha_1 m_1 + \cdots + \alpha_r m_r \mid r \in \mathbb{Z}_{\geq 0}, \alpha_i \in \mathcal{O}_\mathfrak{p}, m_i \in M\}.$$

Alternatively, given a finite-dimensional K-vector space V, we can define an $\mathcal{O}$-lattice M in V to be a finitely generated $\mathcal{O}$-submodule of V. Then KM as defined above is a K-vector subspace of V and we say that M is a full $\mathcal{O}$-lattice in V if $KM = V$. Moreover, for each $\mathfrak{p}$ we define $M_\mathfrak{p}$ to be $\mathcal{O}_\mathfrak{p} M$ as above and note that this is an $\mathcal{O}_\mathfrak{p}$-lattice in V. We shall switch between the two ways of viewing $\mathcal{O}$-lattices as convenient.

2.2. **Lattices over orders.** Let A be a separable K-algebra, that is, a finite-dimensional semisimple K-algebra such that the center of each simple component of A is a separable field extension of K. An $\mathcal{O}$-order in A is a subring Λ of A (so, in particular, has the same unity element as A) such that Λ is a full $\mathcal{O}$-lattice in A. Note that Λ is both left and right noetherian, since Λ is finitely generated over $\mathcal{O}$. A left Λ-lattice X is a left Λ-module that is also an $\mathcal{O}$-lattice; in this case, KX may be viewed as a left A-module.

Henceforth all modules (resp., lattices) shall be assumed to be left modules (resp., lattices) unless otherwise stated. Two Λ-lattices are said to be isomorphic if they are isomorphic as Λ-modules. For any maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, the localization $\Lambda_\mathfrak{p}$ is an $\mathcal{O}_\mathfrak{p}$-order in A. Moreover, localizing a Λ-lattice X yields a $\Lambda_\mathfrak{p}$-lattice $X_\mathfrak{p}$. Two Λ-lattices X and Y are said to be locally isomorphic (or in the same genus) if and only if the $\Lambda_\mathfrak{p}$-lattices $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic for all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$.

Lemma 2.1. *Let $\Lambda \subseteq \Lambda'$ be $\mathcal{O}$-orders in A, and let Γ be either Λ' or $\Lambda'_\mathfrak{p}$ for some maximal ideal $\mathfrak{p}$ of $\mathcal{O}$. Let $f\colon X \to Y$ be a homomorphism of Λ-lattices. Then the following hold:*

(a) *The Γ-module ΓX generated by X is, in fact, a Γ-lattice. Similarly for ΓY.*

(b) *There exists a unique homomorphism of A-modules $f^A\colon KX \to KY$ extending f.*
(c) *There exists a unique homomorphism of Γ-lattices $f^\Gamma\colon \Gamma X \to \Gamma Y$ extending f.*
(d) *If f is injective (resp., surjective), then f^A and f^Γ are injective (resp., surjective).*

Proof. This is straightforward. The key points are to (a) check that ΓX is, in fact, finitely generated over either $\mathcal{O}$ or $\mathcal{O}_\mathfrak{p}$ as appropriate; (b) extend f to KX using K-linearity; (c) restrict f^A to ΓX; (d) (injectivity) check that $\ker(f)$ is an $\mathcal{O}$-lattice of full rank in $\ker(f^A)$; and (d) (surjectivity) use the definitions of KY and ΓY. □

3. Conditions for two lattices to be isomorphic

3.1. **Restricting isomorphisms over maximal orders.** Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, and assume that $\mathcal{O} \neq K$. Let Λ be an $\mathcal{O}$-order in a separable K-algebra A. By [Rei03, (10.4)] there exists a (not necessarily unique) maximal $\mathcal{O}$-order $\mathcal{M}$ such that $\Lambda \subseteq \mathcal{M} \subseteq A$. It is clear that if X and Y are isomorphic Λ-lattices, then they are locally isomorphic and $\mathcal{M}X$ and $\mathcal{M}Y$ are isomorphic $\mathcal{M}$-lattices. We now investigate the additional conditions under which a converse holds. In doing so, we generalize the results of [BJ08, §2], where necessary and sufficient conditions were given for a Λ-lattice to be free.

Theorem 3.1. *Let X and Y be locally isomorphic Λ-lattices such that there exists an isomorphism of $\mathcal{M}$-lattices $f\colon \mathcal{M}X \to \mathcal{M}Y$. Then f restricts to an isomorphism $f|_X\colon X \to Y$ of Λ-lattices if and only if $f(X) \subseteq Y$.*

Remark 3.2. The condition $f(X) \subseteq Y$ can be replaced with $Y \subseteq f(X)$ by making obvious changes to the proof below. The corollaries that follow can be rephrased analogously.

Proof of Theorem 3.1. One direction is trivial. For the other, suppose that $f(X) \subseteq Y$. The restriction $f|_X$ is clearly an injective Λ-lattice homomorphism, so it only remains to show that $f(X) = Y$.

Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$, and let $f_\mathfrak{p}\colon X_\mathfrak{p} \to Y_\mathfrak{p}$ be an isomorphism of $\Lambda_\mathfrak{p}$-lattices. By Lemma 2.1 there exist unique $\mathcal{M}_\mathfrak{p}$-lattice isomorphisms $f^{\mathcal{M}_\mathfrak{p}}\colon \mathcal{M}_\mathfrak{p}X \to \mathcal{M}_\mathfrak{p}Y$ and $f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}}\colon \mathcal{M}_\mathfrak{p}X_\mathfrak{p} \to \mathcal{M}_\mathfrak{p}Y_\mathfrak{p}$ extending f and $f_\mathfrak{p}$, respectively. Note that $\mathcal{M}_\mathfrak{p}X = \mathcal{M}_\mathfrak{p}X_\mathfrak{p}$ and $\mathcal{M}_\mathfrak{p}Y = \mathcal{M}_\mathfrak{p}Y_\mathfrak{p}$, and so we can and do consider $f^{\mathcal{M}_\mathfrak{p}}$ as a map $\mathcal{M}_\mathfrak{p}X_\mathfrak{p} \to \mathcal{M}_\mathfrak{p}Y_\mathfrak{p}$.

Observe that we have the following equalities and containment:

$$f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}}(X_\mathfrak{p}) = f_\mathfrak{p}(X_\mathfrak{p}) = Y_\mathfrak{p} \supseteq f(X)_\mathfrak{p} = \mathcal{O}_\mathfrak{p}f(X) = \mathcal{O}_\mathfrak{p}f^{\mathcal{M}_\mathfrak{p}}(X) = f^{\mathcal{M}_\mathfrak{p}}(\mathcal{O}_\mathfrak{p}X) = f^{\mathcal{M}_\mathfrak{p}}(X_\mathfrak{p}).$$

Thus if $[-:-]_{\mathcal{O}_\mathfrak{p}}$ denotes the module index (see [Frö67, §3] or [FT91, II.4]), then we have

$$[Y_\mathfrak{p} : f(X)_\mathfrak{p}]_{\mathcal{O}_\mathfrak{p}} = [Y_\mathfrak{p} : f^{\mathcal{M}_\mathfrak{p}}(X_\mathfrak{p})]_{\mathcal{O}_\mathfrak{p}} = [f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}}(X_\mathfrak{p}) : (f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}} \circ (f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}})^{-1} \circ f^{\mathcal{M}_\mathfrak{p}})(X_\mathfrak{p})]_{\mathcal{O}_\mathfrak{p}}$$
$$= [X_\mathfrak{p} : ((f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}})^{-1} \circ f^{\mathcal{M}_\mathfrak{p}})(X_\mathfrak{p})]_{\mathcal{O}_\mathfrak{p}} = \det_{\mathcal{O}_\mathfrak{p}}((f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}})^{-1} \circ f^{\mathcal{M}_\mathfrak{p}})\mathcal{O}_\mathfrak{p}.$$

Since $(f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}})^{-1} \circ f^{\mathcal{M}_\mathfrak{p}} : \mathcal{M}_\mathfrak{p}X_\mathfrak{p} \to \mathcal{M}_\mathfrak{p}X_\mathfrak{p}$ is an automorphism of $\mathcal{M}_\mathfrak{p}$-lattices and thus of $\mathcal{O}_\mathfrak{p}$-lattices, we must have $\det_{\mathcal{O}_\mathfrak{p}}((f_\mathfrak{p}^{\mathcal{M}_\mathfrak{p}})^{-1} \circ f^{\mathcal{M}_\mathfrak{p}}) \in \mathcal{O}_\mathfrak{p}^\times$, and hence

$[Y_{\mathfrak{p}} : f(X)_{\mathfrak{p}}]_{\mathcal{O}_{\mathfrak{p}}} = \mathcal{O}_{\mathfrak{p}}$. Since this holds for every maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ and $f(X) \subseteq Y$ by assumption, we must have $f(X) = Y$. Therefore $f|_X \colon X \to Y$ is an isomorphism of Λ-lattices. □

For an $\mathcal{M}$-lattice N, let $\mathrm{End}_{\mathcal{M}}(N)$ denote the ring of $\mathcal{M}$-endomorphisms of N, and let $\mathrm{Aut}_{\mathcal{M}}(N)$ be the group of $\mathcal{M}$-automorphisms of N. Note that $\mathrm{Aut}_{\mathcal{M}}(N) = \mathrm{End}_{\mathcal{M}}(N)^{\times}$.

Corollary 3.3. *Two Λ-lattices X and Y are isomorphic if and only if*

(a) *X and Y are locally isomorphic,*
(b) *there exists an isomorphism of $\mathcal{M}$-lattices $f \colon \mathcal{M}X \to \mathcal{M}Y$, and*
(c) *there exists an automorphism $g \in \mathrm{Aut}_{\mathcal{M}}(\mathcal{M}Y)$ such that $(g \circ f)(X) \subseteq Y$.*

Further, when this is the case, an isomorphism is given by $(g \circ f) \colon X \to Y$.

Proof. If (a), (b), and (c) hold, then X and Y are isomorphic by Theorem 3.1. Suppose conversely that there exists a Λ-lattice isomorphism $h : X \to Y$. Then (a) clearly holds, (b) holds with $f := h^{\mathcal{M}}$ by Lemma 2.1, and (c) holds with $g := \mathrm{Id}_{\mathcal{M}Y}$ (the identity map on $\mathcal{M}Y$). □

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 $\mathcal{O}$ in C. Let $e_1, \dots, e_r$ be the primitive idempotents of C, and set $A_i = e_i A$. Then

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

is a decomposition of A into indecomposable two-sided ideals (see [CR81, (3.22)]). Each A_i is a simple K-algebra with identity element e_i. The centers $K_i := Z(A_i)$ are finite field extensions of K via $K \to K_i$, $\alpha \mapsto e_i\alpha$, and we have K-algebra isomorphisms $A_i \cong \mathrm{Mat}_{n_i \times n_i}(D_i)$ where D_i is a skew field with $Z(D_i) \cong K_i$ (see [CR81, (3.28)]). The Wedderburn decomposition (1) induces decompositions

$$C = K_1 \oplus \cdots \oplus K_r, \quad \mathcal{O}_C = \mathcal{O}_{K_1} \oplus \cdots \oplus \mathcal{O}_{K_r}, \quad \text{and} \quad \mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r, \tag{2}$$

where we have set $\mathcal{M}_i = e_i\mathcal{M}$. By [Rei03, (10.5)] each $\mathcal{M}_i$ is a maximal $\mathcal{O}$-order (and thus a maximal $\mathcal{O}_{K_i}$-order) in A_i.

For an $\mathcal{M}$-lattice N in a K-vector space V, we set $V_i = e_i V$ and $\mathcal{M}_i N = e_i(\mathcal{M}N)$. Then $\mathcal{M}_i N$ is a full $\mathcal{M}_i$-lattice in V_i. The decomposition (2) in turn induces decompositions

$$\mathrm{End}_{\mathcal{M}}(N) = \mathrm{End}_{\mathcal{M}_1}(\mathcal{M}_1 N) \oplus \cdots \oplus \mathrm{End}_{\mathcal{M}_r}(\mathcal{M}_r N) \text{ and} \tag{3}$$

$$\mathrm{Aut}_{\mathcal{M}}(N) = \mathrm{Aut}_{\mathcal{M}_1}(\mathcal{M}_1 N) \times \cdots \times \mathrm{Aut}_{\mathcal{M}_r}(\mathcal{M}_r N). \tag{4}$$

Corollary 3.4. *Two Λ-lattices X and Y are isomorphic if and only if*

(a) *X and Y are locally isomorphic,*
(b) *there exist isomorphisms of $\mathcal{M}_i$-lattices $f_i \colon \mathcal{M}_i X \to \mathcal{M}_i Y$ for each i, and*
(c) *there exist $g_i \in \mathrm{Aut}_{\mathcal{M}_i}(\mathcal{M}_i Y)$ for each i such that $(\sum_{i=1}^{r}(g_i \circ f_i))(X) \subseteq Y$.*

Further, when this is the case, an isomorphism is given by $(\sum_{i=1}^{r}(g_i \circ f_i)) \colon X \to Y$.

Now let Y be a Λ-lattice. Define

$$S = S_Y = \mathrm{End}_{\mathcal{M}}(\mathcal{M}Y) \quad \text{and} \quad T = T_Y = \mathrm{End}_{\Lambda}(Y).$$

Note that T identifies naturally with the subring $\{f \in S \mid f(Y) \subseteq Y\}$ of S. Let $\mathfrak{I}$ be any full two-sided ideal of S contained in T. Set $\overline{S} = S/\mathfrak{I}$ and $\overline{T} = T/\mathfrak{I}$ so

that $\overline{T}$ is a subring of $\overline{S}$, and denote the canonical map $S \to \overline{S}$ by $s \mapsto \overline{s}$. We have decompositions

$$\mathfrak{I} = \mathfrak{I}_1 \oplus \cdots \oplus \mathfrak{I}_r, \quad S = S_1 \oplus \cdots \oplus S_r, \quad \text{and} \quad \overline{S} = \overline{S_1} \oplus \cdots \oplus \overline{S_r}, \tag{5}$$

where each $\mathfrak{I}_i$ is a full two-sided ideal of $S_i := \mathrm{End}_{\mathcal{M}_i}(\mathcal{M}_i Y)$ and where $\overline{S_i} := S_i/\mathfrak{I}_i$. For each i, let $U_i \subseteq S_i^\times = \mathrm{Aut}_{\mathcal{M}_i}(\mathcal{M}_i Y)$ denote a set of representatives of the image of the natural projection $S_i^\times \to (\overline{S_i})^\times$.

Corollary 3.5. *Condition* (c) *in Corollary* 3.4 *can be weakened to*

(c′) *there exist automorphisms* $g_i' \in U_i$ *such that* $(\sum_{i=1}^r (g_i' \circ f_i))(X) \subseteq Y$.

Proof. Suppose throughout that (b) holds. If (c′) holds, then it is clear that (c) also holds. Suppose conversely that (c) holds. For each i, there exists $g_i' \in U_i$ such that $\overline{g_i'} = \overline{g_i}$. Note that $g_i' - g_i \in \mathfrak{I}_i$. For each i, define

$$h_i := g_i' \circ g_i^{-1} - \mathrm{Id}_{\mathcal{M}_i Y} = (g_i' - g_i) \circ g_i^{-1} \in \mathfrak{I}_i g_i^{-1} = \mathfrak{I}_i.$$

Observe that $g_i' = (\mathrm{Id}_{\mathcal{M}_i Y} + h_i) \circ g_i$ and that

$$h := h_1 + \cdots + h_r \in \mathfrak{I}_1 \oplus \cdots \oplus \mathfrak{I}_r = \mathfrak{I} \subseteq T = \{f \in S \mid f(Y) \subseteq Y\}.$$

Thus

$$\begin{aligned} \left(\bigoplus_{i=1}^r (g_i' \circ f_i)\right)(X) &= \left(\bigoplus_{i=1}^r (\mathrm{Id}_{\mathcal{M}_i Y} + h_i) \circ g_i \circ f_i)\right)(X) \\ &= (\mathrm{Id}_{\mathcal{M}Y} + h)\left(\bigoplus_{i=1}^r (g_i \circ f_i)(X)\right) \\ &\subseteq (\mathrm{Id}_{\mathcal{M}Y} + h)(Y) \\ &\subseteq Y, \end{aligned}$$

that is, (c′) holds. Therefore (c) and (c′) are equivalent. □

Remark 3.6. Corollary 3.5 is of particular interest when $\mathcal{O}$ is a residually finite Dedekind domain, that is, a Dedekind domain such that every quotient of $\mathcal{O}$ by a nonzero ideal is finite. For example, this condition is satisfied if $\mathcal{O}$ is the ring of integers of a number field. Moreover, it ensures that the ring $\overline{S}$, and thus the sets of representatives U_i, are finite; this is crucial for the development of any algorithm that relies on Corollary 3.5.

3.2. **Reduction to the free rank** 1 **case via homomorphism groups.** We now give an alternative approach to the one described in §3.1. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and assume that $\mathcal{O} \neq K$. Let Λ be an $\mathcal{O}$-order in a separable K-algebra A. Let X and Y be Λ-lattices. Then $\mathrm{End}_\Lambda(Y)$ is an $\mathcal{O}$-order in the separable K-algebra $\mathrm{End}_A(KY)$. Moreover, $\mathrm{Hom}_\Lambda(X, Y)$ is a (left) $\mathrm{End}_\Lambda(Y)$-lattice in $\mathrm{Hom}_A(KX, KY)$ via post-composition.

Proposition 3.7. *Two* Λ*-lattices* X *and* Y *are isomorphic if and only if*

(a) *the* $\mathrm{End}_\Lambda(Y)$*-lattice* $\mathrm{Hom}_\Lambda(X, Y)$ *is free of rank* 1*, and*

(b) *every free generator of* $\mathrm{Hom}_\Lambda(X, Y)$ *over* $\mathrm{End}_\Lambda(Y)$ *is an isomorphism.*

Proof. If (a) and (b) hold, then it is clear that X and Y are isomorphic. Suppose conversely that X and Y are isomorphic. Fix an isomorphism $\varphi \in \mathrm{Hom}_\Lambda(X, Y)$. Then for any $g \in \mathrm{Hom}_\Lambda(X, Y)$, we have $h_g := g \circ \varphi^{-1} \in \mathrm{End}_\Lambda(Y)$, and so $g = h_g \circ \varphi$.

Thus the map $\mathrm{End}_\Lambda(Y) \to \mathrm{Hom}_\Lambda(X,Y)$ defined by $h \mapsto h \circ \varphi$ is surjective; since it is a map of full $\mathcal{O}$-lattices in K-vector spaces of equal finite dimension, it is also injective. Hence φ is a free generator of $\mathrm{Hom}_\Lambda(X,Y)$ over $\mathrm{End}_\Lambda(Y)$, and thus (a) holds. Now let f be any free generator of $\mathrm{Hom}_\Lambda(X,Y)$ over $\mathrm{End}_\Lambda(Y)$. Then there exists $\theta \in \mathrm{Aut}_\Lambda(Y) = \mathrm{End}_\Lambda(Y)^\times$ such that $f = \theta \circ \varphi$, and hence f is an isomorphism. Thus (b) holds. □

Remark 3.8. Proposition 3.7 is used in the isomorphism test for localized lattices given in §8.4. In the case that $\mathcal{O}$ is the ring of integers of a number field K, necessary and sufficient conditions for the existence of a free generator of $\mathrm{Hom}_\Lambda(X,Y)$ over $\mathrm{End}_\Lambda(Y)$ are given by (special cases of) the results of [BJ08, §2], which are themselves special cases of those in §3.1.

4. The main algorithm

Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$, and let A be a finite-dimensional semisimple K-algebra. Note that these hypotheses ensure that A is a separable K-algebra. Let Λ be an $\mathcal{O}$-order in A. In this section, we outline an algorithm that takes two Λ-lattices X and Y and either returns an explicit isomorphism $X \to Y$ or determines that X and Y are not isomorphic. The key result on which the algorithm is based is Corollary 3.5 (also see Remark 3.6). We require that A satisfies the hypotheses (H1) and (H2) formulated in the introduction; we discuss the conditions under which these hold in §5.

Before sketching the individual steps of the algorithm, we briefly describe the presentation of the input data. We assume that A is given by a K-basis $a_1, \dots, a_s$ and structure constants $\alpha_{i,j,k} \in K$ for $1 \le i,j,k \le s$ such that $a_i \cdot a_j = \sum_{k=1}^{s} \alpha_{i,j,k} a_k$. From this, it is straightforward to construct an embedding of K-algebras $A \to \mathrm{Mat}_{s\times s}(K)$ (see [Ebe89, §2.2] for details). Moreover, we assume that Λ, X, and Y are given by $\mathcal{O}$-pseudobases as described, for example, in [Coh00, 1.4.1]. In other words,

$$X = \mathfrak{a}_1 v_1 \oplus \cdots \oplus \mathfrak{a}_m v_m \quad \text{and} \quad Y = \mathfrak{b}_1 w_1 \oplus \cdots \oplus \mathfrak{b}_n w_n,$$

where for each i both $\mathfrak{a}_i$ and $\mathfrak{b}_i$ are fractional ideals of $\mathcal{O}$ and $v_i \in V := KX$ and $w_i \in W := KY$. Similarly, $\Lambda = \mathfrak{c}_1\lambda_1 \oplus \cdots \oplus \mathfrak{c}_s\lambda_s$ with fractional $\mathcal{O}$-ideals $\mathfrak{c}_i$ and $\lambda_i \in A$. To describe the action of Λ on X (and of A on V), it suffices to assume that for each i there is a matrix $M_X(\lambda_i) \in \mathrm{GL}_m(K)$ describing the action of λ_i with respect to $v_1, \dots, v_m$. Finally, we assume that the action on Y is described similarly.

Algorithm 4.1. *Input: A, Λ, X, and Y as above.*

(a) *Check that X and Y have equal $\mathcal{O}$-rank, that is, check that $m = n$.*
(b) *Compute the central primitive idempotents e_i in A and the components $A_i := e_i A$, $1 \le i \le r$.*
(c) *Compute a maximal $\mathcal{O}$-order $\mathcal{M}$ in A containing Λ and set $\mathcal{M}_i := e_i\mathcal{M}$.*
(d) *Compute the set $\mathfrak{S}$ of maximal ideals $\mathfrak{p}$ of $\mathcal{O}$ dividing the module index $[\mathcal{M} : \Lambda]_\mathcal{O}$.*
(e) *For each i, compute an $\mathcal{M}_i$-lattice isomorphism $f_i \colon \mathcal{M}_i X \to \mathcal{M}_i Y$, if it exists.*
(f) *For each $\mathfrak{p} \in \mathfrak{S}$, check that $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices.*
(g) *Compute $S = S_Y := \mathrm{End}_\mathcal{M}(\mathcal{M}Y)$ and $T = T_Y := \mathrm{End}_\Lambda(Y)$ as well as the decomposition $S = \bigoplus_{i=1}^{r} S_i$ where $S_i := \mathrm{End}_{\mathcal{M}_i}(\mathcal{M}_i Y)$.*

(h) *Compute a full two-sided ideal* $\mathfrak{I} = \bigoplus_{i=1}^{r} \mathfrak{I}_i$ *of* S *contained in* T.
(i) *For each* i, *compute a finite set of representatives* $U_i \subset S_i^\times = \mathrm{Aut}_{\mathcal{M}_i}(\mathcal{M}_i Y)$ *of the image of the natural projection map* $S_i^\times \to (S_i/\mathfrak{I}_i)^\times$.
(j) *Test whether a tuple* $(g_i) \in \prod_{i=1}^{r} U_i$ *exists such that* $(\sum_{i=1}^{r}(g_i \circ f_i))(X) \subseteq Y$. *For such a tuple, an isomorphism is given by* $(\sum_{i=1}^{r}(g_i \circ f_i))\colon X \to Y$. *If no such tuple exists, then* X *and* Y *are not isomorphic.*

We now briefly comment on the individual steps of the algorithm.

(a) This is straightforward.
(b) Algorithms for the computation of primitive central idempotents have been given by Eberly [Ebe89, §2.4] and by Nebe and Steel [NS09, §2].
(c) The algorithms of Friedrichs [Fri00, Kapitel 3 and 4] can be used to compute a maximal order $\mathcal{M}$ with $\Lambda \subseteq \mathcal{M} \subseteq A$; it is then straightforward to compute each $\mathcal{M}_i$. Alternatively, for each i one can compute $\Lambda_i := e_i\Lambda$ and use the algorithm of Nebe and Steel [NS09, §3] (or the aforementioned algorithms of Friedrichs) to construct a maximal order $\mathcal{M}_i$ with $\Lambda_i \subseteq \mathcal{M}_i \subseteq A_i$; one can then set $\mathcal{M} := \bigoplus_i \mathcal{M}_i$.
(d) If the algorithms of Friedrichs are used for step (c), then $\mathfrak{S}$ can be determined along the way (there are additional complications if one first reduces to working in the simple components A_i because the containment $\Lambda \subseteq \bigoplus_i \Lambda_i$ is not necessarily an equality). However, even without this observation, since both Λ and $\mathcal{M}$ are both given by $\mathcal{O}$-pseudobases, $\mathfrak{S}$ can be determined using the Smith normal form algorithm (see [Coh00, 1.7.3]). Note that if G is a finite group and $\mathcal{O}[G] \subseteq \Lambda \subseteq K[G]$, then each $\mathfrak{p} \in \mathfrak{S}$ must divide $|G|$.
(e) This is the only step that requires the hypotheses (H1) and (H2). It is described in §6.
(f) The successful completion of step (e) gives an isomorphism of $\mathcal{M}$-lattices $f := \sum_i f_i : \mathcal{M}X \to \mathcal{M}Y$. If $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$ such that $\Lambda_\mathfrak{p} = \mathcal{M}_\mathfrak{p}$, then Lemma 2.1 shows that f extends to an isomorphism $f_\mathfrak{p} : X_\mathfrak{p} \to Y_\mathfrak{p}$ of $\Lambda_\mathfrak{p}$-lattices. Thus checking that X and Y are locally isomorphic reduces to checking that $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic $\Lambda_\mathfrak{p}$-lattices for each $\mathfrak{p} \in \mathfrak{S}$. Several algorithms to check this for a given maximal ideal $\mathfrak{p}$ are described in §8. In the special case that one wants to check that both $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are, in fact, free $\Lambda_\mathfrak{p}$-lattices, one can use the algorithm described in [BW09, §4.2] (see §8.4).
(g) The solution of the more general problem of computing homomorphism groups is described in §7.
(h) An algorithm of Friedrichs [Fri00, (2.16)] can be used to compute the left conductor $\mathfrak{c}_l = \{x \in \mathrm{End}_A(KY) \mid xS \subseteq T\}$ and the right conductor $\mathfrak{c}_r = \{x \in \mathrm{End}_A(KY) \mid Sx \subseteq T\}$ of S in T. As noted in [BB06, §3.2], one can then take $\mathfrak{I}$ to be either $\mathfrak{c}_r \cdot \mathfrak{c}_l$ or $\mathfrak{c}S$ where

$$\mathfrak{c} := \{x \in Z(\mathrm{End}_A(KY)) \mid xS \subseteq T\} = \mathfrak{c}_r \cap C = \mathfrak{c}_l \cap C$$

is the central conductor of S in T. To minimise the running time of step (j), one would like to take $\mathfrak{I}$ to be as large as possible; in many cases $\mathfrak{c}S$ is a better choice than $\mathfrak{c}_r \cdot \mathfrak{c}_l$, but in principle one could compute both to see which is better in a given situation. In the case that G is a finite group and Y is a locally free $\mathcal{O}[G]$-module of rank 1, we have canonical isomorphisms

$T \cong \mathcal{O}[G]^{\mathrm{op}} \cong \mathcal{O}[G]$ and $S \cong \mathcal{M}^{\mathrm{op}} \cong \mathcal{M}$, where R^{op} denotes the opposite ring of R; hence $\mathfrak{c}_r = \mathfrak{c}_l$ by [CR81, (27.13)] and so we can take $\mathfrak{I} = \mathfrak{c}_r = \mathfrak{c}_l$ and use Jacobinski's conductor formula (see loc. cit. or [Jac66]).

(i) The endomorphism ring $S_i = \mathrm{End}_{\mathcal{M}_i}(\mathcal{M}_i Y)$ is itself an $\mathcal{O}$-order in the separable K-algebra $\mathrm{End}_{A_i}(e_i KY)$. Viewing S_i as a $\mathbb{Z}$-order, one can use the algorithm of Braun, Coulangeon, Nebe, and Schönnenbeck [BCNS15] to find generators $u_1, \ldots, u_t$ of $S_i^\times$. One can then compute $\overline{U}_i$, the subgroup of $\overline{S}_i^\times$ generated by $\overline{u}_1, \ldots, \overline{u}_t$, and write each element as a word of the form $\overline{u}_1^{r_1} \cdots \overline{u}_t^{r_t}$ where $r_i \in \mathbb{Z}$. For each such word, one can take $u_1^{r_1} \cdots u_t^{r_t}$ to be the corresponding element of U_i. Special cases of this problem are considered in [BJ08, §6] and [BJ11, §7].

(j) The number of tests for this step can be greatly reduced by using a generalization of the methods described in [Ble97, §2] and [BJ08, §7]. This is described in §9. Even with this improvement, this is the most time-consuming part of the whole algorithm.

Remark 4.2. The algorithms of Bley and the second-named author of the present article given in [BJ08, BJ11] can be viewed as Algorithm 4.1 specialised to the problem of determining whether a given Λ-lattice X is, in fact, free and, assuming it is, computing an explicit Λ-basis for X. Thanks to the algorithm of Braun, Coulangeon, Nebe, and Schönnenbeck [BCNS15] used in step (i) above, the hypotheses assumed in [BJ08, BJ11] can be weakened to those assumed in the present article (see §5).

Remark 4.3. There is an alternative to Algorithm 4.1 that uses the results of §3.2 to reduce to the "free rank 1" case. However, algorithmically speaking, the reduction steps are nontrivial because they require methods to both compute homomorphism groups (see §7) and test whether lattices are locally isomorphic (see §8); indeed, these methods are needed for both approaches.

5. Hypotheses

We recall and discuss the hypotheses (H1) and (H2) required for Algorithm 4.1. Let K be a number field with ring of integers $\mathcal{O}_K$, and let A be a finite-dimensional semisimple K-algebra. Let $A = A_1 \oplus \cdots \oplus A_r$ be the decomposition of A into indecomposable two-sided ideals, and let K_i denote the center of the simple algebra A_i.

(H1) For each i, we can compute an explicit isomorphism $A_i \cong \mathrm{Mat}_{n_i \times n_i}(D_i)$ of K-algebras, where D_i is a skew field with center K_i.

(H2) For each i, every maximal $\mathcal{O}_K$-order Δ_i in D_i has the following properties:
  (a) we can solve the principal ideal problem for fractional left Δ_i-ideals, and
  (b) Δ_i has the locally free cancellation property.

These hypotheses are only needed for step (e) of Algorithm 4.1, which is described in detail in §6. Note that (H2)(a) is independent of the choice of Δ_i in all cases in which it is known (see §5.2). Moreover, property (H2)(b) is independent of the choice of Δ_i, that is, if it holds for some choice of Δ_i, then it holds for all choices (see §5.3). A detailed discussion of working without (H2)(b) is given in §6.5.

5.1. **Explicit isomorphisms of simple algebras - (H1).** Note that (H1) is equivalent to explicitly finding a simple (left) A_i-module for each i. We list two situations in which this hypothesis is satisfied.

(a) In the case $K = \mathbb{Q}$, the problem in question is solved by an algorithm of Steel [Ste12, §2.3]. As described in §4, we may assume that we have an explicit embedding of $\mathbb{Q}$-algebras $A_i \to \mathrm{Mat}_{s_i}(\mathbb{Q})$ for some $s_i \in \mathbb{Z}_{\geq 1}$. Then A_i is a homogeneous module over itself, and Steel's algorithm returns simple submodules $S_1, \ldots, S_k$ of A_i such that $A_i = \bigoplus_{j=1}^{k} S_j$ and the S_j are all isomorphic.

(b) Let G be a finite group, let K be a finite Galois extension of $\mathbb{Q}$, and let $A = K[G]$. Then based on the character table algorithm of Unger [Ung06], Steel [Ste12, §3.10] describes how to compute all irreducible $K[G]$-modules up to isomorphism.

Remark 5.1. Let K be a number field, and let A be a finite-dimensional semisimple K-algebra. Then A is also a finite-dimensional semisimple $\mathbb{Q}$-algebra. Hence in principle (H1) is always satisfied by Steel's algorithm [Ste12, §2.3] as described in (a) above. However, viewing A as a $\mathbb{Q}$-algebra rather than a K-algebra means the loss of a certain amount of structural information that may considerably slow down computations.

5.2. **The principal ideal problem - (H2)(a).** Let D be a skew field that is central and finite-dimensional over a number field F. (In the above notation, we will consider $D = D_i$ and $F = K_i$ for each i.) Let $\Delta \subseteq D$ be a maximal $\mathcal{O}_F$-order, and let $\mathfrak{a}, \mathfrak{b}$ be fractional left Δ-ideals. Then it is straightforward to show that $\mathfrak{a} \cong \mathfrak{b}$ as left Δ-lattices if and only if there exists $\xi \in D^\times$ such that $\mathfrak{a} = \mathfrak{b}\xi$ (note that it is important that ξ appears on the right side of $\mathfrak{b}$). We say that we can solve the principal ideal problem for left ideals in Δ if for any choice of $\mathfrak{a}$, $\mathfrak{b}$ we have an algorithm to

(i) decide whether $\mathfrak{a} \cong \mathfrak{b}$ as left Δ-lattices, and
(ii) if so, compute $\xi \in D^\times$ such that $\mathfrak{a} = \mathfrak{b}\xi$.

If D is commutative (i.e., $D = F$), then the problem is solved by [Coh93, 6.5.10]. In the case that D is a totally definite quaternion algebra, Dembélé and Donnelly [DD08] described an algorithm and Kirschmer and Voight [KV10, §6] proved that this algorithm runs in polynomial time when the base field is fixed. In the case that D is an indefinite quaternion algebra Kirschmer and Voight [KV10, §4] described an algorithm that improves on naive enumeration, without analysing its complexity; Page [Pag14] has given an improved algorithm and heuristic bounds for its complexity. In summary, if D is either a number field or quaternion algebra, an algorithm to solve the principal ideal problem exists for all choices of Δ in D.

5.3. **Locally free cancellation - (H2)(b).** Let K be a number field, and let Λ be an $\mathcal{O}_K$-order in a finite-dimensional semisimple K-algebra A. Then Λ is said to have the locally free cancellation property if for any locally free finitely generated left Λ-lattices X and Y we have

$$X \oplus \Lambda^{(k)} \cong Y \oplus \Lambda^{(k)} \text{ for some } k \in \mathbb{Z}_{\geq 0} \implies X \cong Y.$$

Let $A = A_1 \oplus \cdots \oplus A_r$ be the decomposition of A into indecomposable two-sided ideals, and let K_i denote the center of the simple algebra A_i. We say that A_i is Eichler/$\mathcal{O}_{K_i}$ if and only if A_i is *not* a totally definite quaternion algebra (see

[CR87, (45.5)(i)] or [Rei03, (34.4)]). More generally, A is Eichler/$\mathcal{O}_K$ if and only if each A_i is Eichler/$\mathcal{O}_{K_i}$. The Jacobinski Cancellation Theorem [CR87, (51.24)] says that if A is Eichler/$\mathcal{O}_K$, then Λ has the locally free cancellation property.

We are concerned with the situation in which $\Lambda = \Delta$ is a maximal order in a skew field D. By the above discussion, we are reduced to the case that D is a totally definite quaternion algebra. Moreover, by [CR87, (51.25)], [Rei03, (17.3)(ii)], and the fact that any two orders in D have equal completions at all but finitely many places, we see that the locally free cancellation property is independent of the choice of Δ in D. A classification of maximal orders in totally definite quaternion algebras with locally free cancellation is given in [HM06] and corrected in [Sme15].

In principle, this classification means that one should be able to determine whether a given finite-dimensional semisimple K-algebra A satisfies (H2)(b), provided that one can explicitly identify the skew field D_i in the isomorphism $A_i \cong \mathrm{Mat}_{n_i \times n_i}(D_i)$. The case in which $A = K[G]$ for some finite group G is of particular interest, and this is discussed at length in [BJ11, §4.3]. We also have the following useful result.

Lemma 5.2. *Let K be a number field, and let G be a finite group. Then the group algebra $K[G]$ satisfies hypothesis* (H2)(b) *in each of the following cases:*

(i) *G is abelian, symmetric or dihedral;*
(ii) *G is of odd order;*
(iii) *K is* not *totally real;*
(iv) *$K = \mathbb{Q}$ and $|G| < 32$.*

Proof. Consider the Wedderburn decomposition $K[G] \cong \bigoplus_i \mathrm{Mat}_{n_i \times n_i}(D_i)$ where each D_i is a skew field with center K_i. Then by [CR81, (7.22)] for each i there exists $m_i \in \mathbb{Z}_{\geq 1}$ such that $[D_i : K_i] = m_i^2$. In case (i), it is well known that $m_i = 1$, i.e., that $D_i = K_i$ for each i. In case (ii), each m_i is odd as it must divide $|G|$ by [CR87, (74.8)(ii)]. In case (iii), no K_i is totally real as it is a field extension of K. Therefore, in cases (i), (ii), and (iii), no D_i is a totally real quaternion algebra (i.e., has $m_i = 2$ and K_i totally real), and so we are done by the Jacobinski Cancellation Theorem [CR87, (51.24)] as explained above. In case (iv), the desired result follows from the proof of [BJ11, Lemma 4.2]. □

6. Isomorphisms over maximal orders in simple algebras

The purpose of this section is to describe step (e) of Algorithm 4.1, which is the only step that requires the hypotheses (H1) and (H2). Thanks to hypothesis (H1), we are reduced to the following situation. Let D be a skew field that is central and finite-dimensional over a number field F. (In the notation of §5, we will consider $D = D_i$ and $F = K_i$ for each i.) Let $\mathcal{O} = \mathcal{O}_F$, and fix a choice Δ of maximal $\mathcal{O}$-order in D. Let $n \in \mathbb{Z}_{\geq 1}$, and let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in $\mathrm{Mat}_{n \times n}(D)$. Let M and N be $\mathcal{M}$-lattices. We require an algorithm that either computes an $\mathcal{M}$-lattice isomorphism $f : M \to N$ or determines that no such isomorphism exists. The basic idea is to reduce this to an analogous problem for certain Δ-lattices. To this end, we first transform $\mathcal{M}$ to a maximal order of a particular shape. We then use a "noncommutative Steinitz form" for Δ-lattices to further reduce to the principal ideal problem of (H2)(a).

6.1. **Maximal orders of a particular form.** We first briefly recall some facts and definitions from [Rei03]. Let $\mathfrak{a}$ be a fractional right Δ-ideal, that is, a full right Δ-lattice in D. The left and right orders of $\mathfrak{a}$ are defined to be

$$\mathcal{O}_l(\mathfrak{a}) := \{x \in D \mid x\mathfrak{a} \subseteq \mathfrak{a}\} \quad \text{and} \quad \mathcal{O}_r(\mathfrak{a}) := \{x \in D \mid \mathfrak{a}x \subseteq \mathfrak{a}\},$$

respectively. These are $\mathcal{O}$-orders in D. Since Δ is a maximal $\mathcal{O}$-order in D and $\mathfrak{a}$ is a right fractional Δ-ideal, we must have $\mathcal{O}_r(\mathfrak{a}) = \Delta$. We set $\Delta' := \mathcal{O}_l(\mathfrak{a})$ and note that this is also a maximal $\mathcal{O}$-order in D by [Rei03, (23.10)]. We define

$$\mathfrak{a}^{-1} := \{x \in D \mid \mathfrak{a}x\mathfrak{a} \subseteq \mathfrak{a}\},$$

and note that this is a fractional left Δ-ideal. Then by [Rei03, (22.7)] we have

$$\mathfrak{a}^{-1}\mathfrak{a} = \Delta, \quad \mathfrak{a}\mathfrak{a}^{-1} = \Delta', \quad (\mathfrak{a}^{-1})^{-1} = \mathfrak{a}.$$

Moreover, $\mathcal{O}_r(\mathfrak{a}^{-1}) = \Delta'$ and $\mathcal{O}_l(\mathfrak{a}^{-1}) = \Delta$ by [Rei03, (22.8)]. Let

$$\mathcal{M}_{\mathfrak{a},n} := \begin{pmatrix} \Delta & \dots & \Delta & \mathfrak{a}^{-1} \\ \vdots & \ddots & \vdots & \vdots \\ \Delta & \dots & \Delta & \mathfrak{a}^{-1} \\ \mathfrak{a} & \dots & \mathfrak{a} & \Delta' \end{pmatrix}$$

denote the ring of all $n \times n$ matrices $(x_{ij})_{1 \le i,j \le n}$ where x_{11} ranges over all elements of Δ, $\dots$, x_{1n} ranges over all elements of $\mathfrak{a}^{-1}$, and so on. (In the case $n = 1$, we take $\mathcal{M}_{\mathfrak{a},n} = \Delta'$.) By [Rei03, (27.6)] every maximal $\mathcal{O}$-order in $\mathrm{Mat}_{n\times n}(D)$ is isomorphic to $\mathcal{M}_{\mathfrak{a},n}$ for some right ideal $\mathfrak{a}$ of Δ.

Proposition 6.1 ([BJ11, §6.3])**.** *There exists an algorithm that, given a maximal $\mathcal{O}$-order $\mathcal{M}$ of $\mathrm{Mat}_{n\times n}(D)$, computes a right fractional ideal $\mathfrak{a}$ of Δ and an invertible matrix $S \in \mathrm{GL}_n(D)$ such that $\mathcal{M} = S\mathcal{M}_{\mathfrak{a},n}S^{-1}$.*

Hence by replacing $\mathcal{M}$ by $S^{-1}\mathcal{M}S$ and an $\mathcal{M}$-lattice M by $S^{-1}M$, we may assume without loss of generality that $\mathcal{M}$ is of the form $\mathcal{M}_{\mathfrak{a},n}$ for some right fractional Δ-ideal $\mathfrak{a}$.

6.2. **Reducing from $\mathcal{M}$-lattices to Δ-lattices.** We assume that $n \ge 2$ and that $\mathcal{M}$ is of the form $\mathcal{M}_{\mathfrak{a},n}$ for some right fractional Δ-ideal $\mathfrak{a}$. By [Rei03, (21.7)] $\mathcal{M}$ is Morita equivalent to Δ, that is, the category of left $\mathcal{M}$-modules is equivalent to the category of left Δ-modules. We now make this equivalence partially explicit in the case of lattices by generalizing [BJ11, §6.2] and adapting parts of [Lam99, §17].

We recall the convention that all modules are assumed to be left modules unless otherwise specified. For $1 \le i, j \le n$ let $e_{ij} \in \mathrm{Mat}_{n\times n}(D)$ be the matrix with 1 in position (i, j) and 0 everywhere else. Then

$$e_{ij}e_{kl} = \begin{cases} e_{il} & \text{if } j = k, \\ 0 & \text{otherwise.} \end{cases}$$

Recalling that $\mathcal{O}_l(\mathfrak{a}^{-1}) = \Delta$, we see that $e_{11}\mathcal{M}$ (i.e., the "first row" of $\mathcal{M}$) is a Δ-lattice. Thus the assignment $M \mapsto e_{11}M$ induces a functor between $\mathcal{M}$-lattices and Δ-lattices, where the corresponding map on morphisms is given by restriction,

$$\mathrm{Hom}_\Lambda(M, N) \longrightarrow \mathrm{Hom}_\Delta(e_{11}M, e_{11}N), \ f \longmapsto f|_{e_{11}M}.$$

One can show that this functor yields an equivalence of categories, but for our purposes the following result suffices.

Proposition 6.2. *Let M and N be $\mathcal{M}$-lattices. Then $M \cong N$ as $\mathcal{M}$-lattices if and only if $e_{11}M \cong e_{11}N$ as Δ-lattices. Moreover, given an isomorphism $g\colon e_{11}M \to e_{11}N$ of Δ-lattices, we can explicitly construct an isomorphism $f : M \to N$ of $\mathcal{M}$-lattices such that $f|_{e_{11}M} = g$.*

Proof. We note that all elements of D commute with e_{ij} for all $1 \leq i, j \leq n$. This, together with the assumption that $n \geq 2$, will be used throughout.

Suppose that $f\colon M \to N$ is an isomorphism of $\mathcal{M}$-lattices. Then it is clear that the restriction $f|_{e_{11}M} : e_{11}M \to e_{11}N$ is an isomorphism of Δ-lattices.

Suppose conversely that we are given an isomorphism $g : e_{11}M \to e_{11}N$ of Δ-lattices. Let $g' : e_{11}FM \to e_{11}FN$ be the unique extension of g to an isomorphism of D-modules, which exists by Lemma 2.1. For $i = 1, \dots, n$ we define

$$f_i' : e_{ii}FM \longrightarrow e_{ii}FN, \quad e_{ii}x \longmapsto e_{i1}g'(e_{1i}x) = e_{ii}e_{i1}g'(e_{11}e_{1i}e_{ii}x),$$

where the last equality shows that these maps are well defined.

Suppose that $1 \leq i < n$. Then $e_{1i} = e_{1i}e_{ii}$ and $e_{i1} = e_{i1}e_{11}$ are both elements of $\mathcal{M}$, and so we have

$$f_i'(e_{ii}M) = e_{ii}e_{i1}g'(e_{11}e_{1i}e_{ii}M) \subseteq e_{ii}e_{i1}g'(e_{11}M) = e_{ii}e_{i1}e_{11}N \subseteq e_{ii}N.$$

Similarly, we have

$$\begin{aligned} e_{ii}N = e_{i1}e_{11}e_{1i}N &\subseteq e_{i1}e_{11}N = e_{i1}g'(e_{11}M) = e_{i1}g'(e_{1i}e_{i1}M) \\ &\subseteq e_{i1}g'(e_{1i}M) = f_i'(e_{ii}M). \end{aligned}$$

Hence $f_i'(e_{ii}M) = e_{ii}N$.

Now consider the case $i = n$. Since $1 \in \Delta' = \mathfrak{a}\mathfrak{a}^{-1}$ and both $\mathfrak{a}^{-1}e_{1n}$ and $e_{n1}\mathfrak{a}$ are contained in $\mathcal{M}$, we have

$$\begin{aligned} f_n'(e_{nn}M) = e_{n1}g'(e_{1n}M) &= e_{n1}g'(e_{11}e_{1n}M) \\ &\subseteq e_{n1}g'(e_{11}\mathfrak{a}\mathfrak{a}^{-1}e_{1n}M) \\ &\subseteq e_{n1}g'(e_{11}\mathfrak{a}M) = e_{n1}e_{11}\mathfrak{a}N = e_{nn}e_{n1}\mathfrak{a}N \\ &\subseteq e_{nn}N. \end{aligned}$$

Similarly, we have

$$\begin{aligned} e_{nn}N &= e_{n1}e_{11}e_{1n}N \\ &\subseteq e_{n1}e_{11}\mathfrak{a}\mathfrak{a}^{-1}e_{1n}N \\ &\subseteq e_{n1}e_{11}\mathfrak{a}N = e_{n1}g'(e_{11}\mathfrak{a}M) = e_{n1}g'(e_{1n}e_{n1}\mathfrak{a}M) \\ &\subseteq e_{n1}g'(e_{1n}M) = f_n'(e_{nn}M). \end{aligned}$$

Hence $f_n'(e_{nn}M) = e_{nn}N$.

We have shown that for each i, the map f_i' restricts to a well-defined surjective map $f_i : e_{ii}N \to e_{ii}M$. Since $e_{11} + \cdots + e_{nn}$ is the $n \times n$ identity matrix, we have a decomposition $M = e_{11}M \oplus \cdots \oplus e_{nn}M$. Define

$$f : M \longrightarrow N, \quad x \mapsto f_1(e_{11}x) + \cdots + f_n(e_{nn}x),$$

and note that this is a homomorphism of $\mathcal{M}$-lattices by construction. Since each f_i is surjective and $N = e_{11}N \oplus \cdots \oplus e_{nn}N$, we see that f is also surjective. It remains to show that f is injective. Let $x \in M$ and suppose that $f(x) = 0$. Since

the elements e_{ii} are pairwise orthogonal, this implies that $e_{i1}g'(e_{1i}x) = f_i(e_{ii}x) = 0$ for each i. Multiplying on the left by e_{1i} gives

$$0 = e_{1i}e_{i1}g'(e_{1i}x) = e_{11}g'(e_{1i}x) = g'(e_{1i}x).$$

Since g' is injective this implies that $e_{1i}x = 0$, and multiplying on the left by e_{i1} then gives $e_{i1}e_{1i}x = e_{ii}x = 0$. Hence $x = e_{11}x + \cdots + e_{nn}x = 0$. □

Remark 6.3. If $\mathcal{M} = \mathrm{Mat}_{n\times n}(\Delta)$, then the construction given in the proof of Proposition 6.2 simplifies considerably (see also [Lam99, §17] for a discussion of the explicit Morita equivalence of $\mathcal{M}$ and Δ in this case). Moreover, if $\mathfrak{a}$ is a principal fractional right ideal of Δ (i.e., $\mathfrak{a} = \xi\Delta$ for some $\xi \in D^\times$), then there exists $S \in \mathrm{GL}_n(D)$ such that $S\mathcal{M}_{\mathfrak{a},n}S^{-1} = \mathrm{Mat}_{n\times n}(\Delta)$, and so we are reduced to the aforementioned situation. In particular, if $D = F$ and F has class number 1, then every fractional right ideal of $\mathcal{O} = \Delta$ is principal (this statement can be generalized to the case $D \neq F$ by using [CR87, (49.32)]).

6.3. **Noncommutative Steinitz form for Δ-lattices.** Let M be a Δ-lattice. Then there exists $r \in \mathbb{Z}_{\geq 1}$ such that $FM \cong D^{(r)}$. Moreover, by [Rei03, (27.8)] there exist elements $m_1, \ldots, m_r \in FM$ and a fractional left Δ-ideal $\mathfrak{b}$ such that

$$M = \Delta m_1 \oplus \cdots \oplus \Delta m_{r-1} \oplus \mathfrak{b}m_r.$$

Such a decomposition is known as a noncommutative Steinitz form of M. An algorithm for computing it is described in [BJ11, §5.3, §5.4]. Moreover, M is a locally free Δ-lattice by [Rei03, (18.10)]. Thus if Δ has the locally free cancellation property of (H2)(b) (described in §5.3), then r and the isomorphism class of $\mathfrak{b}$ uniquely determine the isomorphism class of M. We therefore have the following result.

Lemma 6.4. *Let M and N be two Δ-lattices of equal rank $r \in \mathbb{Z}_{\geq 1}$. Let $\mathfrak{b}$ and $\mathfrak{c}$ be left fractional Δ-ideals such that*

$$M \cong \Delta^{(r-1)} \oplus \mathfrak{b} \quad \textit{and} \quad N \cong \Delta^{(r-1)} \oplus \mathfrak{c}.$$

If $\mathfrak{b} \cong \mathfrak{c}$ as left fractional Δ-ideals, then M and N are isomorphic. Moreover, if Δ has the locally free cancellation property of (H2)(b)*, then the converse is also true.*

6.4. **Step (e) of Algorithm 4.1.** As input, we take a maximal order $\mathcal{M}_i$ in A_i and $\mathcal{M}_i$-lattices $\mathcal{M}_iX$ and $\mathcal{M}_iY$ (i fixed). We describe an algorithm that either computes an isomorphism $f : \mathcal{M}_iX \to \mathcal{M}_iY$ of $\mathcal{M}_i$-lattices or determines that no such isomorphism exists.

(i) Using (H1) we can suppose without loss of generality that $A_i = \mathrm{Mat}_{n_i\times n_i}(D_i)$ for some $n_i \in \mathbb{Z}_{\geq 1}$ and some skew field D_i with center K_i. We henceforth drop the subscripts from D_i and n_i and write F in place of K_i. Let $\mathcal{O} = \mathcal{O}_F$.

(ii) Suppose $n = 1$. Then $\mathcal{M}_i = \Delta$ for some maximal $\mathcal{O}$-order Δ in D. Set

$$M := \mathcal{M}_iX = e_{11}\mathcal{M}_iX \quad \text{and} \quad N := \mathcal{M}_iY = e_{11}\mathcal{M}_iY,$$

and skip to step (iv) below.

(iii) Suppose $n \geq 2$. Fix any maximal $\mathcal{O}$-order Δ in D. Compute $S \in \mathrm{GL}_n(D)$ as in Proposition 6.1. Set

$$\mathcal{M}_i' := S^{-1}\mathcal{M}_iS, \quad M := S^{-1}\mathcal{M}_iX, \quad \text{and} \quad N := S^{-1}\mathcal{M}_iY.$$

The problem is reduced to either computing an isomorphism $M \to N$ of $\mathcal{M}_i'$-lattices or determining that no such isomorphism exists.

(iv) Use [BJ11, §5.3, §5.4] to compute decompositions

$$e_{11}M = \Delta m_1 \oplus \cdots \oplus \Delta m_{r-1} \oplus \mathfrak{b} m_r \quad \text{and} \quad e_{11}N = \Delta n_1 \oplus \cdots \oplus \Delta n_{s-1} \oplus \mathfrak{c} n_s.$$

If $r \neq s$, then the algorithm terminates with the conclusion that $\mathcal{M}_i X$ and $\mathcal{M}_i Y$ are not isomorphic as $\mathcal{M}_i$-lattices.

(v) Use (H2)(a) to check whether $\mathfrak{b} \cong \mathfrak{c}$ as fractional left Δ-ideals, and, if so, return $\xi \in D$ such that $\mathfrak{b} = \mathfrak{c}\xi$. Otherwise, (H2)(b) shows that $e_{11}M$ and $e_{11}N$ are not isomorphic as Δ-lattices, and so the algorithm terminates with the conclusion that $\mathcal{M}_i X$ and $\mathcal{M}_i Y$ are not isomorphic as $\mathcal{M}_i$-lattices. (In the case $n = 1$ this is true because $e_{11}M = \mathcal{M}_i X$ and $e_{11}N = \mathcal{M}_i Y$, and in the case $n \geq 2$ this follows from step (iii), Proposition 6.2, and Lemma 6.4.)

(vi) If a suitable $\xi \in D$ is found in step (v), then, together with the decompositions of $e_{11}M$ and $e_{11}N$ found in step (iv), it can be used to compute an explicit isomorphism $e_{11}M \cong e_{11}N$ of Δ-lattices.

(vii) If $n = 1$, then we are already done since $\mathcal{M}_i = \Delta$, $e_{11}M = \mathcal{M}_i X$, and $e_{11}N = \mathcal{M}_i Y$. If $n \geq 2$, then use Proposition 6.2 to construct an isomorphism $M \to N$ of $\mathcal{M}_i'$-lattices; using step (iii), we thus obtain an isomorphism $\mathcal{M}_i X \to \mathcal{M}_i Y$ of $\mathcal{M}_i$-lattices.

Remark 6.5. If $n = 1$, then Δ is uniquely determined by $\mathcal{M}_i$. Moreover, the choice of $\mathcal{M}_i$ may be limited by the requirement that $\Lambda \subseteq \bigoplus_i \mathcal{M}_i$. However, if $n \geq 2$, then we can make any choice of Δ.

6.5. **Working without the locally free cancellation property (H2)(b).**

Remark 6.6. Suppose that $KM \cong KN \cong D \cong A_i$, that is, $n = r = s = 1$ and $\mathcal{M}_i = \Delta$ in the notation above. Then the problem of determining whether $e_{11}N \cong e_{11}M$ as Δ-lattices is equivalent to checking whether $\mathfrak{b} \cong \mathfrak{c}$ as fractional left Δ-ideals. This can be done with (H2)(a) alone, and so (H2)(b) is not necessary in this case. Thus (H2)(b) can be replaced with a weaker but more complicated to state hypothesis, which corresponds to (H2′)(a) of [BJ11].

Example 6.7. Let Q_{32} be the quaternion group of order 32, and let $A = \mathbb{Q}[Q_{32}]$. Let Λ be any order in A, and let $\mathcal{M}$ be a maximal order such that $\Lambda \subseteq \mathcal{M} \subseteq A$. Then [Swa83, Theorem II] shows that $\mathcal{M}$ does not have the locally free cancellation property. Each simple component A_i of A is isomorphic to either (i) a matrix ring over a number field or (ii) a totally definite quaternion algebra. By the discussion in §5.3, each $\mathcal{M}_i$ in a component A_i of case (i) does have the locally free cancellation property. The remaining $\mathcal{M}_i$ in components A_i of case (ii) do not have the locally free cancellation property. However, if X and Y are Λ-lattices such that $\mathbb{Q}X \cong \mathbb{Q}Y \cong A$, then Remark 6.6 shows that Algorithm 4.1 will always correctly determine whether $\mathcal{M}X$ and $\mathcal{M}Y$ are isomorphic as $\mathcal{M}$-lattices in step (e); the other steps will run as usual as they do not depend on (H2).

Remark 6.8. The algorithm described in §6.4 can still be run without (H2)(b), but it may not come to a conclusion. If it is found that $\mathfrak{b} \cong \mathfrak{c}$ as fractional left Δ-ideals in step (v), then the algorithm will go on to construct an isomorphism $\mathcal{M}_i X \to \mathcal{M}_i Y$ of $\mathcal{M}_i$-lattices, whether or not Δ has the locally free cancellation property. However, if $\mathfrak{b} \ncong \mathfrak{c}$ and Δ does not have the locally free cancellation property, then it is not possible to conclude that $e_{11}M \ncong e_{11}N$, and thus the algorithm cannot determine whether $\mathcal{M}_i X$ and $\mathcal{M}_i Y$ are isomorphic as $\mathcal{M}_i$-lattices.

7. Saturation of lattices and computation of homomorphism groups

We describe how to compute homomorphism groups between lattices over orders, and along the way we give algorithms to compute saturations of lattices. Thus, in particular, we can compute endomorphism rings of lattices over orders, as required for step (g) of Algorithm 4.1. Some of the results presented here were already given in the first-named author's Ph.D. thesis [Hof16, §1, §11].

7.1. **Saturations of lattices over integral domains.** Let R be an integral domain with field of fractions K. To avoid trivialities, we assume that $R \neq K$. Let M be an R-lattice, that is, a finitely generated torsion-free R-module. Let N be an R-sublattice of M. We say that N is saturated (in M) if M/N is torsion-free as an R-module (note that the term "R-pure sublattice" is used in [Rei03, p. 45]). Equivalently, N is saturated in M if for each $r \in R$ we have $N \cap rM = rN$. The unique minimal R-lattice L that is saturated in M and satisfies $N \subseteq L \subseteq M$ is called the saturation of N in M.

Lemma 7.1. *The saturation of N in M is $KN \cap M$.*

Proof. This follows directly from [Rei03, (4.0)]; see also [Hof16, Lemma 1.33(ii)]. □

7.2. **Computation of saturations of lattices over rings of integers.** Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$. We now give a result that can be used to compute saturations of $\mathcal{O}$-lattices. A key ingredient is the pseudo-Hermite normal form as described in [Coh00, 1.4.6]. A similar result that uses the pseudo-Smith normal form [Coh00, 1.7.2] instead is given in the first-named author's Ph.D. thesis [Hof16, Lemma 1.35]. In the special case $\mathcal{O} = \mathbb{Z}$, both results are contained in Steel's Ph.D. thesis [Ste12, 1.7.9]. While the result below is folklore, to the best of the authors' knowledge no proof has been published until now.

Lemma 7.2. *Let M and N be $\mathcal{O}$-lattices with pseudobases $((\alpha_i)_{1\le i\le m}, (\mathfrak{a}_i)_{1\le i\le m})$ and $((\beta_i)_{1\le i\le n}, (\mathfrak{b}_i)_{1\le i\le n})$, respectively. Suppose that N is a sublattice of M (so $n \le m$). Let $A \in \mathrm{Mat}_{m\times n}(K)$ be the unique matrix satisfying*

$$(\beta_1, \beta_2, \dots, \beta_n) = (\alpha_1, \alpha_2, \dots, \alpha_m)A.$$

Let $((\mathfrak{h}_i)_{1\le i\le m}, H)$ be a pseudo-Hermite normal form of $((\mathfrak{a}_i^{-1})_{1\le i\le m}, A^t)$, and let $U \in \mathrm{GL}_m(K)$ be the corresponding transformation matrix. Define

$$(\omega_1, \omega_2, \dots, \omega_m) := (\alpha_1, \alpha_2, \dots, \alpha_m)U^{-t}.$$

Then $((\mathfrak{h}_i^{-1})_{m-n+1\le i\le m}, (\omega_i)_{m-n+1\le i\le m})$ is a pseudobasis of the saturation of N in M.

Proof. For a matrix P we will denote the entry at position (i, j) with $P_{i,j}$. By definition of pseudo-Hermite normal form (see [Coh00, 1.4.6]) the following hold:

(a) For all i and j we have $U_{i,j} \in \mathfrak{a}_i^{-1}\mathfrak{h}_j^{-1}$.
(b) We have $\prod_{i=1}^m \mathfrak{a}_i^{-1} = \det(U)\prod_{i=1}^m \mathfrak{h}_i$.
(c) The matrix $H = A^tU$ is of the form

$$H = A^tU = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 & * & \cdots & * \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

where the first $m-n$ columns are zero (we will write this in abbreviated form as $H = A^tU = (0 \mid \tilde{H})$, where $\tilde{H} \in \mathrm{Mat}_{n\times n}(K)$).

We first show that $((\mathfrak{h}_i^{-1})_{1\le i\le m}, (\omega_i)_{1\le i\le m})$ is a pseudobasis of M. By [Coh00, 1.4.2] it suffices to show that

$$\prod_{i=1}^{m} \mathfrak{a}_i = \det(U^{-t}) \prod_{i=1}^{m} \mathfrak{h}_i^{-1} \quad \text{and} \quad (U^{-t})_{i,j} \in \mathfrak{a}_i(\mathfrak{h}_j^{-1})^{-1} = \mathfrak{a}_i\mathfrak{h}_j \text{ for } 1 \le i,j \le m.$$

The first claim follows directly from property (b). The second claim is equivalent to $(U^{-1})_{i,j} \in \mathfrak{a}_j\mathfrak{h}_i$ for $1 \le i,j \le m$, which can be shown by expressing $(U^{-1})_{i,j}$ in terms of the adjugate matrix and using properties (a) and (b).

Let $S = \bigoplus_{i=m-n+1}^{m} \mathfrak{h}_i^{-1}\omega_i$. Then $M/S \cong \bigoplus_{i=1}^{m-n} \mathfrak{h}_i^{-1}\omega_i$ is torsion-free, and so S is saturated in M. Moreover, since S and N are both of rank n, to prove that S is the saturation of N in M it suffices to show that $N \subseteq S$.

Observe that

$$\begin{aligned}(\beta_1,\dots,\beta_n) &= (\alpha_1,\dots,\alpha_m)A = (\alpha_1,\dots,\alpha_m)U^{-t}H^t \\ &= (\omega_1,\dots,\omega_m)H^t = (\omega_1,\dots,\omega_m)\begin{pmatrix}0\\ \tilde{H}^t\end{pmatrix} \\ &= (\omega_{m-n+1},\dots,\omega_m)\tilde{H}^t.\end{aligned}$$

By our hypotheses, we have $\mathfrak{b}_i \sum_{j=1}^{m} \alpha_j A_{j,i} = \mathfrak{b}_i\beta_i \subseteq N \subseteq M = \bigoplus_{j=1}^{m} \mathfrak{a}_j\alpha_j$ for $1 \le i \le n$. Hence for $1 \le i \le n$ and $1 \le j \le m$ we have $\mathfrak{b}_i A_{j,i} \subseteq \mathfrak{a}_j$, that is, $A_{j,i} \in \mathfrak{a}_j\mathfrak{b}_i^{-1}$. Together with property (a), this shows that for $1 \le i,j \le n$, we have

$$\begin{aligned}\tilde{H}_{i,j} = H_{i,m-n+j} &= \sum_{k=1}^{m} (A^t)_{i,k}U_{k,m-n+j} = \sum_{k=1}^{m} A_{k,i}U_{k,m-n+j} \\ &\in \sum_{k=1}^{m} \mathfrak{a}_k\mathfrak{b}_i^{-1}\mathfrak{a}_k^{-1}\mathfrak{h}_{m-n+j}^{-1} = \mathfrak{b}_i^{-1}\mathfrak{h}_{m-n+j}^{-1}.\end{aligned}$$

In particular, for $1 \le j \le n$ we have

$$\begin{aligned}\mathfrak{b}_j\beta_j = \mathfrak{b}_j\left(\sum_{i=1}^{n} (\tilde{H}^t)_{i,j}\cdot\omega_{m-n+i}\right) &\subseteq \mathfrak{b}_j \sum_{i=1}^{n} \mathfrak{b}_j^{-1}\mathfrak{h}_{m-n+i}^{-1}\omega_{m-n+i} \\ &= \sum_{i=1}^{n} \mathfrak{h}_{m-n+i}^{-1}\omega_{m-n+i} \\ &= S.\end{aligned}$$

This shows that $N = \sum_{j=1}^{n} \mathfrak{b}_j\beta_j \subseteq S$, as required. □

Remark 7.3. An algorithm to compute pseudo-Hermite normal forms is given by [Coh00, Algorithm 1.4.7] and has been improved upon in [FH14, BFH17].

7.3. **Computation of homomorphism groups.** Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$, and let A be a finite-dimensional semisimple K-algebra. Let Λ be an $\mathcal{O}$-order in A. We give an algorithm that takes two Λ-lattices X and Y and returns the Λ-lattice $\mathrm{Hom}_\Lambda(X,Y)$. Let $V = KX$ and $W = KY$, which may be regarded as A-modules. A key ingredient in computing the homomorphism group

is the following characterization:

$$\mathrm{Hom}_\Lambda(X,Y) = \{f|_X \mid f \in \mathrm{Hom}_A(V,W) \text{ such that } f(X) \subseteq Y\}, \tag{6}$$

where $f|_X$ denotes the restriction of f to a map $f\colon X \to Y$. Note that this follows from the fact that every element in $\mathrm{Hom}_\Lambda(X,Y)$ extends uniquely to an element in $\mathrm{Hom}_A(V,W)$ (see Lemma 2.1). Since there exists an algorithm for computing a K-basis of $\mathrm{Hom}_A(V,W)$ due to Steel [Ste12, 1.9.3], it remains to single out the morphisms that map X to Y. This will be done by employing the algorithm for computing saturations given in §7.2. We assume that X and Y are given by pseudobases, that is,

$$X = \mathfrak{a}_1\alpha_1 \oplus \mathfrak{a}_2\alpha_2 \oplus \cdots \oplus \mathfrak{a}_m\alpha_m \quad \text{and} \quad Y = \mathfrak{b}_1\beta_1 \oplus \mathfrak{b}_2\beta_2 \oplus \cdots \oplus \mathfrak{b}_n\beta_n,$$

with $\alpha_i \in V, \beta_j \in W$ and $\mathfrak{a}_i, \mathfrak{b}_j$ fractional ideals of K. Since $(\alpha_i)_{1\le i\le m}$ and $(\beta_j)_{1\le j\le n}$ are K-bases of V and W, respectively, we will use them to identify $\mathrm{Hom}_K(V,W)$ with $\mathrm{Mat}_{m\times n}(K)$ (we treat vectors as row vectors). Under this identification we have

$$\mathrm{Hom}_\mathcal{O}(X,Y) = \bigoplus_{\substack{1\le i\le n\\ 1\le j\le m}} \mathfrak{a}_i^{-1}\mathfrak{b}_j e_{ij} = \begin{pmatrix} \mathfrak{a}_1^{-1}\mathfrak{b}_1 & \dots & \mathfrak{a}_1^{-1}\mathfrak{b}_n \\ \vdots & \ddots & \vdots \\ \mathfrak{a}_m^{-1}\mathfrak{b}_1 & \dots & \mathfrak{a}_m^{-1}\mathfrak{b}_n \end{pmatrix} \subseteq \mathrm{Mat}_{m\times n}(K), \tag{7}$$

where $e_{ij} \in \mathrm{Mat}_{m\times n}(K)$ is the matrix with 1 in position (i,j) and 0 everywhere else. The following result is a special case of [Hof16, Lemma 11.2].

Lemma 7.4.

(a) *We have* $\mathrm{Hom}_\Lambda(X,Y) = \mathrm{Hom}_A(V,W) \cap \mathrm{Hom}_\mathcal{O}(X,Y)$.

(b) *Let* $B_1,\dots,B_r$ *be a* K*-basis of* $\mathrm{Hom}_A(V,W)$ *with* $B_i \in \mathrm{Hom}_\mathcal{O}(X,Y)$. *Then*

$$\mathrm{Hom}_\Lambda(X,Y) = K(\langle B_1,\dots,B_r\rangle_\mathcal{O}) \cap \mathrm{Hom}_\mathcal{O}(X,Y).$$

Proof. Since a map $f \in \mathrm{Hom}_A(V,W)$ is also $\mathcal{O}$-linear we have $f(X) \subseteq Y$ if and only if $f \in \mathrm{Hom}_\mathcal{O}(X,Y)$. Thus part (a) follows from (6). Part (b) follows from (a) since $K(\langle B_1,\dots,B_r\rangle_\mathcal{O}) = \mathrm{Hom}_A(V,W)$. □

Using Lemma 7.1 we see that Lemma 7.4(b) says that the $\mathcal{O}$-lattice $\mathrm{Hom}_\Lambda(X,Y)$ is the saturation of $\langle B_1,\dots,B_r\rangle_\mathcal{O}$ in $\mathrm{Hom}_\mathcal{O}(X,Y)$. Hence the computation of $\mathrm{Hom}_\Lambda(X,Y)$ is reduced to the computation of a saturation of $\mathcal{O}$-lattices. Therefore to compute $\mathrm{Hom}_\Lambda(X,Y)$, we proceed as follows:

(i) Compute a K-basis $B_1,\dots,B_r$ of $\mathrm{Hom}_A(V,W)$ using the algorithm of Steel [Ste12, 1.9.3].

(ii) Scale the B_i's such that $B_i \in \mathrm{Hom}_\mathcal{O}(X,Y)$ for all $i = 1,\dots,r$.

(iii) Compute the saturation S of $\langle B_1,\dots,B_r\rangle_\mathcal{O}$ in $\mathrm{Hom}_\mathcal{O}(X,Y)$ using Lemma 7.2 and one of the algorithms referenced in Remark 7.3, and return S.

8. Isomorphism testing for localized lattices

Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$, and let A be a finite-dimensional semisimple K-algebra. Let Λ be an $\mathcal{O}$-order in A, and let $\mathcal{M}$ be a maximal $\mathcal{O}$-order such that $\Lambda \subseteq \mathcal{M} \subseteq A$. Let X and Y be Λ-lattices of equal $\mathcal{O}$-rank n, and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$. We give four algorithms that determine whether or not the localizations $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices. The first algorithm makes use of reduced lattices, the second uses the results of §7, the third

is a probabilistic algorithm of Monte Carlo type, and the fourth reduces to the case of testing whether a lattice localized at $\mathfrak{p}$ is free. Of these, only the second and the fourth algorithms explicitly compute an isomorphism, if one exists. Variants of the first three algorithms are contained in the first-named author's Ph.D. thesis [Hof16, §12], but we caution that here the subscript $\mathfrak{p}$ denotes localization, whereas in loc. cit. it denotes completion. Finally, we discuss implementations and running times of the last three algorithms in the case that G is a finite group and $\Lambda = \mathbb{Z}[G]$.

8.1. **Using reduced lattices.**

Proposition 8.1. *Let* $k_0 := \min\{k \in \mathbb{Z}_{\geq 0} \mid \mathfrak{p}^k \mathcal{M}_\mathfrak{p} \subseteq \Lambda_\mathfrak{p}\}$, *and let* $k \geq k_0 + 1$. *Then the following are equivalent:*

(a) $X_\mathfrak{p}$ *and* $Y_\mathfrak{p}$ *are isomorphic as* $\Lambda_\mathfrak{p}$*-lattices.*
(b) $X/\mathfrak{p}^k X$ *and* $Y/\mathfrak{p}^k Y$ *are isomorphic as* $\Lambda/\mathfrak{p}^k\Lambda$*-modules.*
(c) *The* $\mathcal{O}/\mathfrak{p}^k$*-module* $\mathrm{Hom}_{\Lambda/\mathfrak{p}^k\Lambda}(X/\mathfrak{p}^k X, Y/\mathfrak{p}^k Y)$ *contains an invertible element.*

Proof. The equivalence of (b) and (c) is clear. Since $\mathfrak{p}^{k_0}\mathcal{M}_\mathfrak{p} \subseteq \Lambda_\mathfrak{p}$ we see that $\mathfrak{p}^{k_0}\mathcal{O}_\mathfrak{p}$ is contained in the central conductor of $\Lambda_\mathfrak{p}$ in $\mathcal{M}_\mathfrak{p}$. From [CR81, (29.4)] it follows that $\mathfrak{p}^{k_0}\mathcal{O}_\mathfrak{p} \cdot \mathrm{Ext}^1_{\Lambda_\mathfrak{p}}(M, N) = 0$ for all $\Lambda_\mathfrak{p}$-lattices M and N. Now a theorem of Higman [Hig60, Theorem 3] (see also [CR81, (30.14)]) implies that $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic $\Lambda_\mathfrak{p}$-lattices if and only if $X_\mathfrak{p}/\mathfrak{p}^k X_\mathfrak{p}$ and $Y_\mathfrak{p}/\mathfrak{p}^k Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}/\mathfrak{p}^k\Lambda_\mathfrak{p}$-modules. The equivalence of (a) and (b) now follows from the canonical isomorphisms

$$\Lambda_\mathfrak{p}/\mathfrak{p}^k\Lambda_\mathfrak{p} \cong \Lambda/\mathfrak{p}^k\Lambda, \quad X/\mathfrak{p}^k X \cong X_\mathfrak{p}/\mathfrak{p}^k X_\mathfrak{p}, \quad \text{and} \quad Y/\mathfrak{p}^k Y \cong Y_\mathfrak{p}/\mathfrak{p}^k Y_\mathfrak{p}. \qquad \square$$

To exploit this result algorithmically, we first have to explain how to determine the homomorphism group of reduced modules in part (c). Note that $X/\mathfrak{p}^k X$ and $Y/\mathfrak{p}^k Y$ are both free of rank n over $\mathcal{O}/\mathfrak{p}^k$. Thus we may fix $\mathcal{O}/\mathfrak{p}^k$-bases of $X/\mathfrak{p}^k X$ and $Y/\mathfrak{p}^k Y$, which we use to describe the action of Λ on these modules via ring homomorphisms

$$\rho_1 \colon \Lambda \longrightarrow \mathrm{End}_{\Lambda/\mathfrak{p}^k\Lambda}(X/\mathfrak{p}^k X) \longrightarrow \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p}^k),$$
$$\rho_2 \colon \Lambda \longrightarrow \mathrm{End}_{\Lambda/\mathfrak{p}^k\Lambda}(Y/\mathfrak{p}^k Y) \longrightarrow \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p}^k).$$

Then for a set $\mathcal{G} \subseteq \Lambda$ generating Λ as an $\mathcal{O}$-algebra we obtain

$$\mathrm{Hom}_{\Lambda/\mathfrak{p}^k\Lambda}(X/\mathfrak{p}^k X, Y/\mathfrak{p}^k Y) = \{M \in \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p}^k) \mid \rho_1(g)M = M\rho_2(g)\, \forall g \in \mathcal{G}\}.$$

Consider the $\mathcal{O}/\mathfrak{p}^k$-linear map

$$h \colon \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p}^k) \to \prod_{g\in\mathcal{G}} \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p}^k), \quad M \mapsto ((\rho_1(g)M - M\rho_2(g))_{g\in\mathcal{G}}), \tag{8}$$

and observe that $\ker(h) = \mathrm{Hom}_{\Lambda/\mathfrak{p}^k\Lambda}(X/\mathfrak{p}^k X, Y/\mathfrak{p}^k Y)$. Since the quotient ring $\mathcal{O}/\mathfrak{p}^k$ is an Euclidean ring in the sense of [Fle71], an $\mathcal{O}/\mathfrak{p}^k$-spanning set of $\ker(h)$ can be computed using techniques related to the Howell normal form (see [SM98, FH14]).

Let $M \mapsto \overline{M}$ denote the canonical projection map $\mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p}^k) \to \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p})$.

Lemma 8.2. *Let* k *be as in Proposition* 8.1, *and let* $A_1, \ldots, A_r \in \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p}^k)$ *be an* $\mathcal{O}/\mathfrak{p}^k$*-spanning set of* $\mathrm{Hom}_{\Lambda/\mathfrak{p}^k\Lambda}(X/\mathfrak{p}^k X, Y/\mathfrak{p}^k Y)$. *Then both* $X_\mathfrak{p}$ *and* $Y_\mathfrak{p}$ *are isomorphic as* $\Lambda_\mathfrak{p}$*-lattices if and only if there exist* $a_1, \ldots, a_r \in \mathcal{O}/\mathfrak{p}$ *with* $\det_{\mathcal{O}/\mathfrak{p}}(a_1\overline{A}_1 + \cdots + a_r\overline{A}_r) \neq 0$.

Proof. By Proposition 8.1, $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices if and only if there exist elements $a_1, \dots, a_r \in \mathcal{O}/\mathfrak{p}^k$ such that $a_1A_1 + \cdots + a_rA_r$ is invertible, or, equivalently, $\det_{\mathcal{O}/\mathfrak{p}^k}(a_1A_1 + \cdots + a_rA_r) \neq 0$. The claim now follows since reduction mod $\mathfrak{p}$ commutes with taking determinants and an element $a \in \mathcal{O}/\mathfrak{p}^k$ is a unit if and only if $(a \bmod \mathfrak{p})$ is a unit in $\mathcal{O}/\mathfrak{p}$. □

To test whether $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices, we can thus proceed as follows:

(i) Use an algorithm of Friedrichs [Fri00, (2.16)] to compute k_0. Set $k := k_0 + 1$.
(ii) Construct the $\mathcal{O}/\mathfrak{p}^k$-linear map h of (8) as a matrix.
(iii) Compute an $\mathcal{O}/\mathfrak{p}^k$-spanning set $A_1, \dots, A_r$ of $\ker(h)$.
(iv) For every tuple $(a_1, \dots, a_r) \in (\mathcal{O}/\mathfrak{p})^r$ test whether $\det_{\mathcal{O}/\mathfrak{p}}(a_1\overline{A}_1 + \cdots + a_r\overline{A}_r) \neq 0$. The $\Lambda_\mathfrak{p}$-lattices $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic if and only if such a tuple exists.

8.2. **Using global homomorphism groups.** The second approach is based on the ability to compute the global homomorphism group $\mathrm{Hom}_\Lambda(X, Y)$. We follow the notation and setup of §7.3, but specialize to the case $m = n$. Hence we let $V = KX$ and $W = KY$ and assume that X and Y are given by pseudobases, that is,

$$X = \mathfrak{a}_1\alpha_1 \oplus \mathfrak{a}_2\alpha_2 \oplus \cdots \oplus \mathfrak{a}_n\alpha_n \quad \text{and} \quad Y = \mathfrak{b}_1\beta_1 \oplus \mathfrak{b}_2\beta_2 \oplus \cdots \oplus \mathfrak{b}_n\beta_n,$$

with $\alpha_i \in V, \beta_j \in W$, and $\mathfrak{a}_i, \mathfrak{b}_j$ fractional ideals of K. As in §7.3, we use the K-bases $(\alpha_i)_i$, $(\beta_i)_i$ to identify homomorphism spaces as subsets of $\mathrm{Mat}_{n\times n}(K)$. Thus we have

$$\mathrm{Hom}_\Lambda(X, Y) \subseteq \mathrm{Hom}_A(V, W) \subseteq \mathrm{Hom}_K(V, W) = \mathrm{Mat}_{n\times n}(K). \tag{9}$$

Let $M \mapsto \overline{M}$ denote the canonical projection map $\mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p}) \to \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p})$.

Lemma 8.3. *Suppose $v_\mathfrak{p}(\mathfrak{a}_i) = v_\mathfrak{p}(\mathfrak{b}_i) = 0$ for $1 \leq i \leq n$. Then the following hold:*

(a) *The $\Lambda_\mathfrak{p}$-lattices $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are $\mathcal{O}_\mathfrak{p}$-free with $\mathcal{O}_\mathfrak{p}$-bases $(\alpha_i)_i$ and $(\beta_j)_j$, respectively.*
(b) *We have $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p}) = \mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p}) \cap \mathrm{Hom}_A(V, W)$.*
(c) *There exists a pseudobasis $((\mathfrak{c}_i)_i, (A_i)_{1\leq i\leq r})$ of $\mathrm{Hom}_\Lambda(X, Y)$ with $v_\mathfrak{p}(\mathfrak{c}_i) = 0$ and $A_i \in \mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p})$ for $1 \leq i \leq r$.*
(d) *The matrices $A_1, \dots, A_r$ form an $\mathcal{O}_\mathfrak{p}$-basis of $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$.*
(e) *Let $B_1, \dots, B_r \in \mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p})$ be any $\mathcal{O}_\mathfrak{p}$-basis of $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$. The $\Lambda_\mathfrak{p}$-lattices $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic if and only if there exists a tuple $(b_1, \dots, b_r) \in (\mathcal{O}/\mathfrak{p})^r$ such that $\det_{\mathcal{O}/\mathfrak{p}}(b_1\overline{B}_1 + \cdots + b_r\overline{B}_r) \neq 0$. Moreover, if such a tuple exists, then an isomorphism is given by $b_1B_1 + \cdots + b_rB_r$.*

Proof.

(a) By assumption we have $\mathcal{O}_\mathfrak{p}\mathfrak{a}_i = \mathcal{O}_\mathfrak{p}\mathfrak{b}_i = \mathcal{O}_\mathfrak{p}$. Thus

$$X_\mathfrak{p} = \mathcal{O}_\mathfrak{p}X = \bigoplus_i \mathcal{O}_\mathfrak{p}\alpha_i \quad \text{and} \quad Y_\mathfrak{p} = \mathcal{O}_\mathfrak{p}Y = \bigoplus_i \mathcal{O}_\mathfrak{p}\beta_i.$$

(b) Note that $f \in \mathrm{Hom}_A(V, W)$ satisfies $f \in \mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ if and only if $f(X_\mathfrak{p}) \subseteq Y_\mathfrak{p}$. By part (a) and the identification (9), this is in turn equivalent to $f \in \mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p})$.

(c) From Lemma 7.4(a) and (7) (with $m = n$) we have

$$\mathrm{Hom}_\Lambda(X,Y) = \mathrm{Hom}_A(V,W) \cap \mathrm{Hom}_\mathcal{O}(X,Y) \subseteq \mathrm{Hom}_\mathcal{O}(X,Y) = \bigoplus_{1\le i,j\le n} \mathfrak{a}_i^{-1}\mathfrak{b}_j e_{ij}.$$

Hence by the assumptions on the coefficient ideals and the identification (9) we have that $\mathrm{Hom}_\Lambda(X,Y)$ is a subset of $\mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p})$. Let $((\mathfrak{c}_i),(A_i))_{1\le i\le r}$ be any pseudobasis of $\mathrm{Hom}_\Lambda(X,Y)$, and let $\pi \in \mathfrak{p}\setminus\mathfrak{p}^2$ be any uniformizer. Then

$$\mathfrak{c}_i A_i = (\mathfrak{c}_i/\pi^{v_\mathfrak{p}(\mathfrak{c}_i)})(\pi^{v_\mathfrak{p}(\mathfrak{c}_i)}A_i) \subseteq \mathrm{Hom}_\Lambda(X,Y) \subseteq \mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p}).$$

Since $\mathfrak{c}_i/\pi^{v_\mathfrak{p}(\mathfrak{c}_i)}$ has $\mathfrak{p}$-adic valuation 0, we thus have that every entry of $\pi^{v_\mathfrak{p}(\mathfrak{c}_i)}A_i$ has $\mathfrak{p}$-adic valuation ≥ 0, that is, $\pi^{v_\mathfrak{p}(\mathfrak{c}_i)}A_i \in \mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p})$. Moreover, the family $((\mathfrak{c}_i/\pi^{v_\mathfrak{p}(\mathfrak{c}_i)}),(\pi^{v_\mathfrak{p}(\mathfrak{c}_i)}A_i))_{1\le i\le r}$ is also a pseudobasis of $\mathrm{Hom}_\Lambda(X,Y)$. Hence by making the appropriate substitution, we can and do assume without loss of generality that the pseudobasis $((\mathfrak{c}_i)_i,(A_i)_i)_{1\le i\le r}$ has the desired properties.

(d) By [Rei03, (3.18)] and the identification of $\mathcal{O}_\mathfrak{p}\otimes_\mathcal{O}\mathrm{Hom}_\Lambda(X,Y)$ with $\mathcal{O}_\mathfrak{p}\mathrm{Hom}_\Lambda(X,Y)$, we have

$$\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p},Y_\mathfrak{p}) = \mathcal{O}_\mathfrak{p}\mathrm{Hom}_\Lambda(X,Y) = \bigoplus_{i=1}^r \mathcal{O}_\mathfrak{p}\mathfrak{c}_i A_i = \bigoplus_{i=1}^r \mathcal{O}_\mathfrak{p} A_i.$$

(e) The two $\Lambda_\mathfrak{p}$-lattices $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic if and only if $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p},Y_\mathfrak{p})$ contains an invertible element. By part (b), $M \in \mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p},Y_\mathfrak{p})$ is invertible if and only if $\det_{\mathcal{O}_\mathfrak{p}}(M) \in \mathcal{O}_\mathfrak{p}^\times$. This is in turn equivalent to $\det_{\mathcal{O}_\mathfrak{p}}(M) \bmod \mathfrak{p} \ne 0$ in $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} \cong \mathcal{O}/\mathfrak{p}$. The claim follows from the observation that $\det_{\mathcal{O}_\mathfrak{p}}(M) \bmod \mathfrak{p} = \det_{\mathcal{O}/\mathfrak{p}}(\overline{M})$ together with the hypothesis on $B_1,\dots,B_r$. □

To test whether $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices, and to compute an isomorphism if it exists, we can thus proceed as follows:

(i) Adjust the pseudobases of X and Y such that the coefficient ideals have zero $\mathfrak{p}$-adic valuation. For example, if $\pi \in \mathfrak{p}\setminus\mathfrak{p}^2$ is any uniformizer, then
$$((\pi^{v_\mathfrak{p}(\mathfrak{a}_i)}\alpha_i)_{1\le i\le n},(\mathfrak{a}_i/\pi^{v_\mathfrak{p}(\mathfrak{a}_i)})_{1\le i\le n})$$
is a pseudobasis of X of the required form (similarly for Y).

(ii) Compute a pseudobasis $((\mathfrak{c}_i),(A_i))_{1\le i\le r}$ of $\mathrm{Hom}_\Lambda(X,Y)$ using the algorithm of §7.3 and adjust it such that the coefficient ideals have zero $\mathfrak{p}$-adic valuation (as in the proof of Lemma 8.3(c)).

(iii) Reduce the matrices $A_1,\dots,A_r$ modulo $\mathfrak{p}$ to obtain matrices $\overline{A}_1,\dots,\overline{A}_r \in \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p})$. Then for every tuple $(a_1,\dots,a_r) \in (\mathcal{O}/\mathfrak{p})^r$ test whether $\det_{\mathcal{O}/\mathfrak{p}}(a_1\overline{A}_1+\cdots+a_r\overline{A}_r) \ne 0$. If such a tuple exists, then $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices and an isomorphism is given by $a_1A_1+\cdots+a_rA_r$. Otherwise $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are not isomorphic as $\Lambda_\mathfrak{p}$-lattices.

8.3. **Probabilistic isomorphism testing.** The previous two approaches to isomorphism testing have reduced the problem to testing the vanishing of potentially $\#(\mathcal{O}/\mathfrak{p})^r$ determinants of elements in $\mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p})$ (if $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are not isomorphic as $\Lambda_\mathfrak{p}$-lattices, then one really needs $\#(\mathcal{O}/\mathfrak{p})^r$ determinant computations). In particular, if either r or $\#(\mathcal{O}/\mathfrak{p})$ is large, this is a rather time-consuming step. We now connect the problem to polynomial identity testing, which allows us to lower the number of determinant computations in certain situations (see also Remark 8.6).

Let $A_1, \dots, A_r \in \mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p})$ be an $\mathcal{O}_\mathfrak{p}$-basis of $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ as given by Lemma 8.3. Let $M \mapsto \overline{M}$ denote the canonical projection map $\mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p}) \to \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p})$. Let $T_1, \dots, T_r$ be indeterminates and consider the polynomial

$$f := \det(T_1\overline{A}_1 + \cdots + T_r\overline{A}_r) \in (\mathcal{O}/\mathfrak{p})[T_1, \dots, T_r],$$

which is of total degree $\le n$.

Lemma 8.4. *The two $\Lambda_\mathfrak{p}$-lattices $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic if and only if f as defined above is not the zero-polynomial.*

Proof. Suppose that $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices. Then by Lemma 8.3(e) there exist $a_1, \dots, a_r \in \mathcal{O}/\mathfrak{p}$ such that $f(a_1, \dots, a_r) \neq 0$, and so, in particular f, is not the zero-polynomial. Suppose conversely that f is not the zero-polynomial. Then there exists a finite extension $\mathbb{F}$ of $\mathcal{O}/\mathfrak{p}$ and $b_1, \dots, b_r \in \mathbb{F}$ such that $f(b_1, \dots, b_r) \neq 0$. Let S be a discrete valuation ring with maximal ideal $\mathfrak{P}$ such that $\mathcal{O}_\mathfrak{p} \subseteq S$ and $S/\mathfrak{P} \cong \mathbb{F}$. Since $A_1, \dots, A_r$ is also an S-basis of $\mathrm{Hom}_{S\Lambda_\mathfrak{p}}(SX_\mathfrak{p}, SY_\mathfrak{p})$, Lemma 8.3(e) applied to $SX_\mathfrak{p}$ and $SY_\mathfrak{p}$ shows that $b_1A_1 + \cdots + b_rA_r$ is an $S\Lambda$-isomorphism $SX_\mathfrak{p} \to SY_\mathfrak{p}$. Hence $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices by [CR81, (30.25)]. □

To test whether or not f is the zero-polynomial, we shall make use of the following classical result (see [Sch80, Zip79]).

Theorem 8.5 (Schwartz–Zippel lemma)**.** *Let $\mathbb{F}$ be a finite field. For a nonzero polynomial $g \in \mathbb{F}[T_1, \dots, T_r]$ of total degree $n < \#\mathbb{F}$ we have*

$$\frac{\#\{(a_1, \dots, a_r) \in \mathbb{F}^r \mid g(a_1, \dots, a_r) = 0\}}{\#\mathbb{F}^r} \le \frac{n}{\#\mathbb{F}}.$$

Since $f = 0$ in $\mathbb{F}[T_1, \dots, T_r]$ is equivalent to $f = 0$ in $\mathbb{F}'[T_1, \dots, T_r]$ for every extension $\mathbb{F}'$ of $\mathbb{F}$, the condition on the total degree is not an actual restriction, as we can just extend scalars if necessary. We now formulate a probabilistic version of the isomorphism test given in §8.2. Let $1 > \varepsilon > 0$ be some chosen error bound. The following algorithm to test whether $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices is of Monte Carlo type, in the sense described in step (iv):

(i) Compute an $\mathcal{O}_\mathfrak{p}$-basis $A_1, \dots, A_r$ of $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ as in §8.2.
(ii) Set $f := \det(T_1\overline{A}_1 + \cdots + T_r\overline{A}_r) \in (\mathcal{O}/\mathfrak{p})[T_1, \dots, T_r]$.
(iii) Choose $l, k \in \mathbb{Z}_{\ge 1}$ such that $\#(\mathcal{O}/\mathfrak{p})^l > n$ and $(n/\#(\mathcal{O}/\mathfrak{p})^l)^k < \varepsilon$. Let $\mathbb{F}$ be the degree l extension of $\mathcal{O}/\mathfrak{p}$.
(iv) Choose $v_1, \dots, v_k \in \mathbb{F}^r$ uniformly distributed. For every i in the range $1 \le i \le k$ test whether $f(v_i) \neq 0$. If such an i exists, then $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices. Otherwise, the probability that $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are not isomorphic as $\Lambda_\mathfrak{p}$-lattices is at least $1 - \varepsilon$.

Remark 8.6. While the Monte Carlo nature of this algorithm makes it useless if it needs to be shown that $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are not isomorphic, there are applications where it can significantly speed up computations. Assume that we are given Λ-lattices $X, Y_1, \dots, Y_m$ and we know that $X_\mathfrak{p}$ must be isomorphic to one of $Y_{1,\mathfrak{p}}, \dots, Y_{m,\mathfrak{p}}$ (for example, these could be representatives for the isomorphism classes of $\Lambda_\mathfrak{p}$-lattices). Then using the probabilistic algorithm to test $X_\mathfrak{p} \cong Y_{i,\mathfrak{p}}$, $1 \le i \le m$, with some small ε, we can quickly find the $Y_{i,\mathfrak{p}}$ that is isomorphic to $X_\mathfrak{p}$ (it will not be necessary to prove directly that $X_\mathfrak{p}$ is not isomorphic to some specific $Y_{j,\mathfrak{p}}$).

8.4. **Reduction to testing whether a lattice localized at $\mathfrak{p}$ is free.** If $Y = \Lambda^{(k)}$ for some $k \in \mathbb{Z}_{\geq 1}$, then testing whether $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices is, of course, equivalent to testing whether $X_\mathfrak{p}$ is free of rank k over $\Lambda_\mathfrak{p}$. An algorithm for computing a $\Lambda_\mathfrak{p}$-basis of $X_\mathfrak{p}$ (if one exists) is given by Bley and Wilson in [BW09, §4.2]. The basic idea is to reduce modulo $\mathfrak{p}$ and then reduce again modulo the Jacobson radical of $\Lambda_\mathfrak{p}/\mathfrak{p}\Lambda_\mathfrak{p}$, find a basis over the resulting associative algebra over a finite field (if one exists), and then lift this basis using Nakayama's lemma (twice). If $X_\mathfrak{p}$ is free over $\Lambda_\mathfrak{p}$, then the lifted elements form a basis. Otherwise, either it was not possible to find a basis modulo the Jacobson radical of $\Lambda_\mathfrak{p}/\mathfrak{p}\Lambda_\mathfrak{p}$, or the lifted elements do not form a basis. Since it is straightforward to check whether a given set of elements forms a basis, this gives an algorithm to test whether $X_\mathfrak{p}$ is free and compute a basis if so. This method is in general faster than the others presented in this section because it does not require an expensive search step.

We now describe how to use this algorithm to give a general isomorphism testing algorithm for localized lattices. If one of $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ is free over $\Lambda_\mathfrak{p}$ and the other is not, then the above algorithm can be used to show that they are not isomorphic as $\Lambda_\mathfrak{p}$-lattices. For the general case we use Proposition 3.7 with $\Lambda = \Lambda_\mathfrak{p}$, $X = X_\mathfrak{p}$ and $Y = Y_\mathfrak{p}$. This says that $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic over $\Lambda_\mathfrak{p}$ if and only if the $\mathrm{End}_{\Lambda_\mathfrak{p}}(Y_\mathfrak{p})$-lattice $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ is free of rank 1 and every free generator of $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ over $\mathrm{End}_{\Lambda_\mathfrak{p}}(Y_\mathfrak{p})$ is an isomorphism. Also note that any $f \in \mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ is an $\Lambda_\mathfrak{p}$-isomorphism if and only if it is an $\mathcal{O}_\mathfrak{p}$-isomorphism. To test whether $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices, and to compute an isomorphism if it exists, we can thus proceed as follows:

(i) Compute $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ and $\mathrm{End}_{\Lambda_\mathfrak{p}}(Y_\mathfrak{p})$ using the methods described in §8.2.

(ii) Use the algorithm of [BW09, §4.2] outlined above to check if $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ is free over $\mathrm{End}_{\Lambda_\mathfrak{p}}(Y_\mathfrak{p})$; compute a free generator f if so. If $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ is not free over $\mathrm{End}_{\Lambda_\mathfrak{p}}(Y_\mathfrak{p})$, then $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are not isomorphic as $\Lambda_\mathfrak{p}$-lattices.

(iii) Check whether $f : X_\mathfrak{p} \to Y_\mathfrak{p}$ is an $\mathcal{O}_\mathfrak{p}$-isomorphism. If so, then it is an isomorphism of $\Lambda_\mathfrak{p}$-lattices. Otherwise, $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are not isomorphic as $\Lambda_\mathfrak{p}$-lattices.

8.5. **Implementation of algorithms.** Let G be any finite group. The algorithms of §8.2, §8.3, and §8.4 have been implemented for $\mathbb{Z}[G]$-lattices X and Y contained in any finitely generated $\mathbb{Q}[G]$-modules V and W. Explicitly, for a given rational prime p, these implementations check whether the localizations X_p and Y_p are isomorphic over $\mathbb{Z}_{(p)}[G]$. Moreover, the implementations of the algorithms of §8.2 and §8.4 compute an isomorphism if one exists. The Magma [BCP97] code is available on the webpage of the first-named author.

Remark 8.7. Isomorphism testing for localized lattices is one of the main ingredients needed to compute a set of representatives of the isomorphism classes of full rank $\Lambda_\mathfrak{p}$-lattices of a fixed A-module V, or equivalently, of full rank $\Lambda_\mathfrak{p}$-sublattices of a fixed $\Lambda_\mathfrak{p}$-lattice. The basic idea is to recursively compute maximal sublattices until no new isomorphism class is found; this goes back to Plesken [Ple74] (see also [Hof16, Algorithm 13.7]). We have used this algorithm together with the algorithms described in this section to determine a set of representatives of the isomorphism classes of full rank $\mathbb{Z}_{(2)}[A_4]$-lattices of $\mathbb{Q}[A_4]$, where A_4 is the alternating group on 4 letters. In total there are 163 isomorphism classes, for which the algorithm requires

approximately 84 000 isomorphism tests. The average running times for a single isomorphism test using the algorithms from §8.2, §8.3 (with error bound $\varepsilon = 2^{-20}$), and §8.4 are 0.0500 seconds, 0.0087 seconds, and 0.0063 seconds, respectively. All computations were performed using MAGMA [BCP97] V2.22-3 and a single core of a Intel Xeon CPU E5-2643 v3 @ 3.40GHz.

9. Reducing the number of final tests

The number of tests in step (j) of Algorithm 4.1 can be enormous. We now describe an ad hoc method similar to those outlined in [Ble97, §2] and [BJ08, §7] to reduce the number of tests required. For simplicity, we assume that we are in the case $K = \mathbb{Q}$ and $\mathcal{O} = \mathbb{Z}$. The method described here generalizes to other cases, and besides, we can reduce to the case $K = \mathbb{Q}$ without loss of generality because determining whether X and Y are isomorphic as Λ-lattices does not depend on whether we view A as a K-algebra or a $\mathbb{Q}$-algebra (though there may be a trade-off in computational cost).

The idea is based on the following simple observation. Let $d \in \mathbb{Z}_{\geq 1}$ be the $\mathbb{Z}$-rank of X and Y, and let Ω_X and Ω_Y be $\mathbb{Z}$-bases of $\mathcal{M}X$ and $\mathcal{M}Y$, respectively. Denote by $M_X, M_Y \in \mathrm{Mat}_{d\times d}(\mathbb{Z})$ basis matrices of X and Y with respect to Ω_X and Ω_Y. Now if $h\colon \mathcal{M}X \to \mathcal{M}Y$ is any $\mathbb{Z}$-linear map with basis matrix M with respect to Ω_X and Ω_Y, then $h(X) \subseteq Y$ if and only if $M_X M M_Y^{-1} \in \mathrm{Mat}_{d\times d}(\mathbb{Z})$. We will show how appropriate choices of bases and basis matrices can help us to reduce the number of tests in step (j).

Recall from §3.1 that we have a decomposition $\mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r$ which induces decompositions

$$\mathcal{M}X = \mathcal{M}_1X \oplus \cdots \oplus \mathcal{M}_rX \quad \text{and} \quad \mathcal{M}Y = \mathcal{M}_1Y \oplus \cdots \oplus \mathcal{M}_rY. \tag{10}$$

From the previous steps of Algorithm 4.1, we have isomorphisms $f_i\colon \mathcal{M}_iX \to \mathcal{M}_iY$ of $\mathcal{M}_i$-lattices and finite subsets $U_i \subseteq \mathrm{Aut}_{\mathcal{M}_i}(\mathcal{M}_iY)$ for $1 \leq i \leq r$. We need to check whether there exists $(g_1, \ldots, g_r) \in U_1 \times \cdots \times U_r$ such that $(\sum_{i=1}^r (g_i \circ f_i))(X) \subseteq Y$.

Let $d_i \in \mathbb{Z}_{\geq 1}$ denote the $\mathbb{Z}$-rank of $\mathcal{M}_iX$, which is also equal to the $\mathbb{Z}$-rank of $\mathcal{M}_iY$. Now we choose $\mathbb{Z}$-bases Ω_X and Ω_Y of $\mathcal{M}X$ and $\mathcal{M}Y$ adapted to the decompositions in (10). For isomorphisms $f_i\colon \mathcal{M}_iX \to \mathcal{M}_iY$ the matrix representing $\sum_{i=1}^r f_i$ is a block matrix of the form $\mathrm{diag}(M(f_1), \ldots, M(f_r))$ with $M(f_i) \in \mathrm{Mat}_{d_i\times d_i}(\mathbb{Z})$. Similarly, for automorphisms $g_i\colon \mathcal{M}_iY \to \mathcal{M}_iY$ the matrix representing $\sum_{i=1}^r g_i$ is a block diagonal matrix of the form $\mathrm{diag}(M(g_1), \ldots, M(g_r))$ with $M(g_i) \in \mathrm{GL}_{d_i}(\mathbb{Z})$. Hence with respect to Ω_X and Ω_Y, the morphism $h := \sum_{i=1}^r g_i \circ f_i$ is given by

$$M = \mathrm{diag}(M(g_1)M(f_1), \ldots, M(g_r)M(f_r)).$$

Now let M_X and M_Y be upper triangular basis matrices of X and Y with respect to Ω_X and Ω_Y. Then h satisfies $h(X) \subseteq Y$ if and only if $M_X M M_Y^{-1} \in \mathrm{Mat}_{d\times d}(\mathbb{Z})$. Setting $\tilde{M}_Y := M_Y^{-1} \in \mathrm{GL}_d(\mathbb{Q})$, the matrix $M_X M M_Y^{-1}$ is equal to

$$\begin{pmatrix} M_X^{(1)} & & * \\ & \ddots & \\ 0 & & M_X^{(r)} \end{pmatrix} \begin{pmatrix} M(g_1)M(f_1) & & 0 \\ & \ddots & \\ 0 & & M(g_r)M(f_r) \end{pmatrix} \begin{pmatrix} \tilde{M}_Y^{(1)} & & * \\ & \ddots & \\ 0 & & \tilde{M}_Y^{(r)} \end{pmatrix},$$

with $M_X^{(i)} \in \mathrm{Mat}_{d_i \times d_i}(\mathbb{Z})$, $\tilde{M}_Y^{(i)} \in \mathrm{GL}_{d_i}(\mathbb{Q})$ for $i = 1, \ldots, r$. As this product of matrices is equal to

$$\begin{pmatrix} \boxed{M_X^{(1)} M(g_1) M(f_1) \tilde{M}_Y^{(1)}} & & * \\ & \ddots & \\ 0 & & \boxed{M_X^{(r)} M(g_r) M(f_r) \tilde{M}_Y^{(r)}} \end{pmatrix},$$

we see that the ith block on the diagonal depends only on g_i and is independent of g_j for $j \neq i$. In particular, if for example we find $g_1 \in U_1$ such that

$$M_X^{(1)} M(g_1) M(f_1) \tilde{M}_Y^{(1)} \notin \mathrm{Mat}_{d_1 \times d_1}(\mathbb{Z}),$$

then we can remove all elements $\{g_1\} \times U_2 \times \cdots \times U_r$ from the search space.

10. Computational results

We have a proof of concept implementation of Algorithm 4.1 in Magma [BCP97], which works in the following situation. Let G be a finite group, let $A = \mathbb{Q}[G]$, and let $\Lambda = \mathbb{Z}[G]$. Let $A = A_1 \oplus \cdots \oplus A_r$ be the decomposition of A into indecomposable two-sided ideals, and let K_i denote the center of the simple algebra A_i. For each i there is an isomorphism $A_i \cong \mathrm{Mat}_{n_i \times n_i}(D_i)$ of $\mathbb{Q}$-algebras, where D_i is a skew field with center K_i. Suppose that for each i, at least one of the following holds: (a) $D_i = \mathbb{Q}$, (b) $A_i = D_i = K_i$ (so, in particular, $n_i = 1$), or (c) D_i is a quaternion algebra and $n_i = 1$ (that is, $A_i = D_i$ is a skew field and $[D_i : \mathbb{Q}] = 4$). This condition holds in each of the following cases:

(i) G is abelian;
(ii) $G = S_n$, the symmetric group on n letters;
(iii) $G = \mathbb{F}_q \rtimes \mathbb{F}_q^\times$, where $\mathbb{F}_q$ is the finite field with $q \geq 3$ elements and the semidirect product is defined by the natural action (such a group has a unique nonlinear irreducible character, which is rationally represented);
(iv) $G = Q_8, Q_{12}, Q_8 \times C_2$ or $Q_{12} \times C_2$, where Q_{4n} is the quaternion group of order $4n$ and C_2 is the cyclic group of order 2.

The implementation can decide whether two $\mathbb{Z}[G]$-lattices contained in $\mathbb{Q}[G]$ are isomorphic and, if so, give an explicit isomorphism. In practice, the number of final tests required for step (j) of Algorithm 4.1 is too high in many cases (when $G = Q_{12} \times C_2$, for example), even if the methods of §9 are employed. The code is available on the webpage of the first-named author.

The implementation can be used to investigate the Galois module structure of arithmetic objects such as the rings of integers and ambiguous ideals of Galois extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$. We note that it is straightforward to realise these lattices as lattices in $\mathbb{Q}[G]$ by finding a normal basis generator of $K/\mathbb{Q}$, which can be done in several ways; for example, one can use the algorithm of Girstmair [Gir99].

10.1. **Galois G-extensions.** Let K be a number field and, let G be a finite group. We fix a G-extension of K, that is, a pair (L, φ) consisting of a Galois extension L/K together with a group isomorphism $\varphi\colon G \to \mathrm{Gal}(L/K)$. In this way one obtains an action of G on L. The classical Normal Basis Theorem implies that $(L, \varphi) \cong K[G]$ as $K[G]$-modules. Since $\mathcal{O}_L$ is a $\mathrm{Gal}(L/K)$-invariant finitely generated torsion-free $\mathcal{O}_K$-module, the pair $(\mathcal{O}_L, \varphi)$ uniquely defines a $\mathcal{O}_K[G]$-lattice in L. It is straightforward to see that if $(\mathcal{O}_L, \varphi)$ is free (resp., stably free, locally free), then

$(\mathcal{O}_L, \psi)$ is also free (resp., stably free, locally free) for any choice of isomorphism $\psi : G \to \mathrm{Gal}(L/K)$.

Henceforth, assume that L/K is (at most) tamely ramified. Then it is well known that $(\mathcal{O}_L, \varphi)$ is a locally free $\mathcal{O}_K[G]$-lattice of rank 1 (see [Noe32], [Frö83, I, §3], or [Kaw86]). Let $LF_1(\mathcal{O}_K[G])$ denote the set of isomorphism classes of locally free $\mathcal{O}_K[G]$-lattices of rank 1, and let $[\mathcal{O}_L^\varphi] \in LF_1(\mathcal{O}_K[G])$ denote the isomorphism class of $(\mathcal{O}_L, \varphi)$. An automorphism $\theta \in \mathrm{Aut}(G)$ induces an action on $LF_1(\mathcal{O}_K[G])$ such that, in particular, $\theta \cdot [\mathcal{O}_L^\varphi] = [\mathcal{O}_L^{\varphi\circ\theta}]$. We define

$$\{[\mathcal{O}_L]\} := \{[\mathcal{O}_L^\psi] \in LF_1(\mathcal{O}_K[G]) \mid \psi : G \to \mathrm{Gal}(L/K) \text{ is an isomorphism}\}.$$

Since any two isomorphisms $G \to \mathrm{Gal}(L/K)$ differ by an element of $\mathrm{Aut}(G)$, we see that $\{[\mathcal{O}_L]\}$ is the $\mathrm{Aut}(G)$-orbit of $[\mathcal{O}_L^\varphi]$ in $LF_1(\mathcal{O}_K[G])$, and this is independent of the choice of φ. For $\sigma \in \mathrm{Gal}(L/K)$ let ι_σ denote the inner automorphism of $\mathrm{Gal}(L/K)$ defined by $\tau \mapsto \sigma\tau\sigma^{-1}$. Then it is straightforward to check that the map $\sigma : (\mathcal{O}_L, \varphi) \to (\mathcal{O}_L, \iota_\sigma \circ \varphi)$ is an isomorphism of $\mathcal{O}_K[G]$-lattices. Thus the action of $\mathrm{Aut}(G)$ on $\{[\mathcal{O}_L]\}$ factors through $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$, where $\mathrm{Inn}(G)$ is the normal subgroup of $\mathrm{Aut}(G)$ consisting of inner automorphisms.

10.2. **Rings of integers of $Q_8 \times C_2$-extensions.** Let $G = Q_8 \times C_2$, the direct product of the quaternion group of order 8 and the cyclic group of order 2. Swan [Swa83] showed that there exist $\mathbb{Z}[G]$-lattices that are stably free but not free, but that for any group H with $|H| < 16$, every stably free $\mathbb{Z}[H]$-lattice is, in fact, free. He also showed that $|LF_1(\mathbb{Z}[G])| = 40$ and that there are 4 classes in $LF_1(\mathbb{Z}[G])$ that are stably free. We label these classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$, where $\mathcal{C}_1$ is the class of free $\mathbb{Z}[G]$-lattices of rank 1 and the lattices contained in the other classes are stably free but not free. (Note that the labelling of $\mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_4$ is arbitrary, but the key point is that it will be fixed for the rest of this discussion.) Based upon these results, Cougnard [Cou98] showed that for each $1 \le i \le 4$, there exist infinitely many G-extensions (L, φ) of $\mathbb{Q}$ with $[\mathcal{O}_L^\varphi] = \mathcal{C}_i$. The group of automorphisms $\mathrm{Aut}(G)$ has order 192 and the quotient group of outer automorphisms $\mathrm{Out}(G)$ has order 48. Using either our implementation of Algorithm 4.1 or the description and discussion of $LF_1(\mathbb{Z}[G])$ in [Swa83, §16], it can be shown that the action of $\mathrm{Aut}(G)$ on $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4\}$ has two orbits, namely $\{\mathcal{C}_1\}$ and $\{\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4\}$.

We now describe how we used our implementation of Algorithm 4.1 to verify the numerical examples considered by Cougnard. Let $N/\mathbb{Q}$ be a finite Galois extension with $\mathrm{Gal}(N/\mathbb{Q}) \cong Q_8$, and fix a choice of isomorphism $\varphi\colon Q_8 \to \mathrm{Gal}(N/\mathbb{Q})$. Let $d \in \mathbb{Q}$ such that $\sqrt{d} \notin N$. Then $N(\sqrt{d})/\mathbb{Q}$ is Galois and there is a canonical identification

$$\mathrm{Gal}(N(\sqrt{d})/\mathbb{Q}) = \mathrm{Gal}(N/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}). \tag{11}$$

Also, since $\mathrm{Aut}(C_2)$ is trivial there is a unique isomorphism $\theta_d\colon C_2 \to \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Using (11) we define an isomorphism $\varphi_d\colon Q_8 \times C_2 \longrightarrow \mathrm{Gal}(N(\sqrt{d})/\mathbb{Q})$ by $\varphi_d = \varphi \times \theta_d$ (this is the unique isomorphism whose restriction back to the first factor recovers φ). Let $[\mathcal{O}_{N(\sqrt{d})}]$ denote the $\mathbb{Z}[G]$-isomorphism class of $(\mathcal{O}_{N(\sqrt{d})}, \varphi_d)$. It is interesting to compare such isomorphism classes as d varies while keeping N and φ fixed.

In [Cou98, VIII], Cougnard considered the number field N_1 with defining polynomial

$$\mathtt{x}^8 - \mathtt{x}^7 + 62126\mathtt{x}^6 - 565081\mathtt{x}^5 + 1060385071\mathtt{x}^4 - 16366741325\mathtt{x}^3 + 465279400700\mathtt{x}^2 + 7092550941085\mathtt{x} + 160472449673155 \in \mathbb{Q}[\mathtt{x}].$$

We were able to compute the following isomorphism classes of rings of integers:

(i) $\mathcal{C}_1 = [\mathcal{O}_{N_1(\sqrt{5})}] = [\mathcal{O}_{N_1(\sqrt{221})}]$,
(ii) $\mathcal{C}_2 = [\mathcal{O}_{N_1(\sqrt{17})}]$,
(iii) $\mathcal{C}_3 = [\mathcal{O}_{N_1(\sqrt{13})}] = [\mathcal{O}_{N_1(\sqrt{21})}] = [\mathcal{O}_{N_1(\sqrt{65})}]$,
(iv) $\mathcal{C}_4 = [\mathcal{O}_{N_1(\sqrt{85})}]$.

In case (i), our implementation of Algorithm 4.1 yielded explicit $\mathbb{Z}[G]$-isomorphisms of the rings of integers with $\mathbb{Z}[G]$, and so we obtained explicit normal integral bases (as the coefficients of the elements generating the normal integral bases are quite large, we do not reproduce them here). The implementation was also used to check whether any two of the rings of integers listed above are isomorphic or not as $\mathbb{Z}[G]$-lattices, and thus verified that the isomorphism classes listed above are indeed distinct. We used two independent methods to check that all the rings of integers above are stably free and thus do, in fact, belong to the isomorphism classes $\mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_4$ in cases (ii), (iii), and (iv) (recall the labelling of these classes is arbitrary but fixed). Note that a locally free $\mathbb{Z}[G]$-lattice of rank 1 is stably free if and only if it has trivial class in the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$. The first method was to use an algorithm of Bley and Wilson [BW09] that solves the discrete logarithm problem in $\mathrm{Cl}(\mathbb{Z}[G])$. This algorithm was implemented in Magma [BCP97] by Bley and the code is available on his website. The second method was to use the remarkable work of Fröhlich and Taylor that determines the class in $\mathrm{Cl}(\mathbb{Z}[G])$ of the ring of integers of a tamely ramified G-extension in terms of the Artin root numbers of the irreducible symplectic characters of G (see [Frö83, I, §6]). We used the Magma command `RootNumber` to show that these root numbers are 1 in all the cases above, which implies that the classes in $\mathrm{Cl}(\mathbb{Z}[G])$ are trivial. Therefore the results above are in agreement with those of Cougnard (he also considered similar situations starting with fields other than N_1, but we do not consider these here).

Note that once a single representative of each isomorphism class has been found, our implementation of Algorithm 4.1 can be used to check whether any given locally free $\mathbb{Z}[G]$-lattice of rank 1 is stably free or not and so one does not need to apply either of the two methods described above when investigating further examples. Moreover, in principle one can use Algorithm 4.1 to check whether a ring of integers is stably free over $\mathbb{Z}[G]$ without using the above methods at all. Let (L, φ) be a G-extension of $\mathbb{Q}$. Then the Bass Cancellation Theorem [CR87, (41.20)] shows that $(\mathcal{O}_L, \varphi)$ is stably free over $\mathbb{Z}[G]$ if and only if $(\mathcal{O}_L, \varphi) \oplus \mathbb{Z}[G] \cong \mathbb{Z}[G] \oplus \mathbb{Z}[G]$ as $\mathbb{Z}[G]$-modules (this is independent of the choice of φ). This, of course, can be checked by Algorithm 4.1, but unfortunately our implementation is restricted to locally free $\mathbb{Z}[G]$-lattices in $\mathbb{Q}[G]$.

We have used our implementation of Algorithm 4.1 to investigate the distribution of the Galois module structure of the rings of integers among all tamely ramified Galois extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ and $|\mathrm{Disc}(\mathcal{O}_L)| \leq 10^{40}$. (Note that the fields considered in the previous paragraph all satisfy $|\mathrm{Disc}(\mathcal{O}_{N_1(\sqrt{d})})| \geq 10^{64}$ because $|\mathrm{Disc}(\mathcal{O}_{N_1})| \geq 10^{32}$.) Since any such field L is a tamely ramified quadratic

extension of a tamely ramified Galois extension $L_0/\mathbb{Q}$ with $\mathrm{Gal}(L_0/\mathbb{Q}) \cong Q_8$ and $|\mathrm{Disc}(\mathcal{O}_{L_0})| \leq 10^{20}$, we first used algorithms based on class field theory described in [FHS19] and implemented in Hecke [FHHJ17] to construct all the possible L_0 (there are 235 such fields). We then used the same techniques to build appropriate quadratic extensions of these fields. In total there are 315 extensions $L/\mathbb{Q}$ with the desired properties (one needs to take care to discard duplicates). In order to avoid the dependence on the choice of isomorphism $\varphi : G \to \mathrm{Gal}(L/\mathbb{Q})$, we only determine whether $[\mathcal{O}_L^{\varphi}]$ lies in $\mathcal{C}_1$, in $\mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$, or in neither of these. In other words, we determine whether $\mathcal{O}_L$ is free, stably free but not free, or not stably free over $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$. Of the 315 rings of integers $\mathcal{O}_L$ under consideration, 80 are free, 1 is stably free but not free, and 234 are not stably free. The one stably free but not free example is the ring of integers of the number field L with defining polynomial

$$\begin{aligned}\mathtt{x}^{16} + 11\mathtt{x}^{15} - 603\mathtt{x}^{14} - 3827\mathtt{x}^{13} + 145692\mathtt{x}^{12} + 266691\mathtt{x}^{11} - 16993778\mathtt{x}^{10}\\ +30104389\mathtt{x}^{9} + 898058760\mathtt{x}^{8} - 4356130039\mathtt{x}^{7} - 11656785671\mathtt{x}^{6}\\ +135624739908\mathtt{x}^{5} - 369009691593\mathtt{x}^{4} + 364395270692\mathtt{x}^{3} + 8335437012\mathtt{x}^{2}\\ -166048630160\mathtt{x} + 22344148336 \in \mathbb{Q}[\mathtt{x}]\end{aligned}$$

and discriminant

$$948697067731156989893951074419946289062 5 = 3^{12} \cdot 5^{12} \cdot 11^{12} \cdot 13^{12}.$$

Since our table of number fields is complete with respect to the given absolute discriminant bound, L is, in fact, the number field of smallest absolute discriminant with the property that $L/\mathbb{Q}$ is Galois with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ and that $\mathcal{O}_L$ is stably free but not free over $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ (note that this forces $L/\mathbb{Q}$ to be tamely ramified).

10.3. **Ambiguous ideals.** We first recall some general properties of ambiguous ideals following Ullom [Ull69, Chapter I]. Let K be a number field, and let G be a finite group. Let (L, φ) be a tamely ramified G-extension of K, and let $\mathfrak{a}$ be an ambiguous ideal of $\mathcal{O}_L$, that is, an ideal that is invariant under the action of G (note that this property does not depend on the choice of φ). Then $(\mathfrak{a}, \varphi)$ uniquely defines an $\mathcal{O}_K[G]$-lattice in L. Since L/K is tamely ramified, $(\mathfrak{a}, \varphi)$ is locally free and the observations made in §10.1 also apply in this setting. For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ decomposing as $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ we set $\psi(\mathfrak{p}) = \mathfrak{P}_1 \cdots \mathfrak{P}_g$. We have the following classification:

- The ideal $\psi(\mathfrak{p})$ is ambiguous and the set $\{\psi(\mathfrak{p}) \mid \mathfrak{p} \text{ a maximal ideal of } \mathcal{O}_K\}$ is a free $\mathbb{Z}$-basis of the abelian group of ambiguous ideals of $\mathcal{O}_L$.
- Every ambiguous ideal $\mathfrak{a}$ of $\mathcal{O}_L$ can be uniquely written in the form $\mathfrak{a} = \mathfrak{a}_0\mathfrak{b}$, with $\mathfrak{b}$ an ideal of $\mathcal{O}_K$ and

$$\mathfrak{a}_0 = \psi(\mathfrak{p}_1)^{a_1} \cdots \psi(\mathfrak{p}_t)^{a_t}, \quad 0 \leq a_i < e_i,$$

  where $e_i > 1$ is the ramification index of a maximal ideal of $\mathcal{O}_L$ dividing $\mathfrak{p}_i$. The ideal $\mathfrak{a}_0$ is called a primitive ambiguous ideal.

If $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$ is a principal ideal domain, and so every ambiguous ideal $\mathfrak{a}_0\mathfrak{b}$ with $\mathfrak{a}_0$ primitive and $\mathfrak{b}$ an ideal of $\mathbb{Z}$ is isomorphic to $\mathfrak{a}_0$ as a $\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$-module. Thus when investigating the possible Galois module structure of ambiguous ideals in this situation, we can restrict ourselves to primitive ambiguous ideals.

In the sequel, we extend ψ to all nonzero fractional ideals of $\mathcal{O}_K$ so that if $a_1, \dots, a_t \in \mathbb{Z}$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ are maximal ideals of $\mathcal{O}_K$, then $\psi(\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}) = \psi(\mathfrak{p}_1)^{a_1} \cdots \psi(\mathfrak{p}_t)^{a_t}$.

10.4. **Ambiguous ideals for a fixed $Q_8 \times C_2$-extension.** We now specialise to the case $G = Q_8 \times C_2$ and $K = \mathbb{Q}$ as in §10.2. Let N_1 denote the extension of $\mathbb{Q}$ defined in §10.2. Let $L_1 = N_1(\sqrt{5})$, and note that $L_1/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(L_1/\mathbb{Q}) \cong G$. Since the discriminant of $\mathcal{O}_{L_1}$ is

$$3^{12} \cdot 5^{12} \cdot 7^{12} \cdot 11^{12} \cdot 13^{12} \cdot 17^{12},$$

the extension $L_1/\mathbb{Q}$ is tamely ramified and thus every ambiguous ideal of $\mathcal{O}_{L_1}$ is a locally free $\mathbb{Z}[G]$-lattice. Moreover, as the ramification indices of the rational primes dividing the discriminant are all equal to 4, there are $4^6 = 4096$ primitive ambiguous ideals. In [Cou98, VIII], Cougnard showed that $\mathcal{O}_{L_1}$ is a free $\mathbb{Z}[\mathrm{Gal}(L_1/\mathbb{Q})]$-lattice. We verified this result with our implementation of Algorithm 4.1 and also investigated the $\mathbb{Z}[\mathrm{Gal}(L_1/\mathbb{Q})]$-structure of all the primitive ambiguous ideals: 1024 are free, 1024 are stably free but not free, and 2048 are not stably free. More precisely, for a fixed choice of isomorphism $\varphi\colon G \to \mathrm{Gal}(L_1/\mathbb{Q})$, all 1024 stably free but not free primitive ambiguous ideals lie in the same $\mathbb{Z}[G]$-isomorphism class. Examples of free, stably free but not free, and not stably free ambiguous ideals are $\psi(17\mathbb{Z})$, $\psi(17^2\mathbb{Z})$, and $\psi(11^2\mathbb{Z})$, respectively.

Now let $L_2 = N_1(\sqrt{221})$. Again, the extension $L_2/\mathbb{Q}$ is Galois with $\mathrm{Gal}(L_2/\mathbb{Q}) \cong G$. Since $\mathcal{O}_{L_2}$ has the same discriminant as $\mathcal{O}_{L_1}$, the extension $L_2/\mathbb{Q}$ is also tamely ramified and there are 4096 primitive ambiguous ideals whose $\mathbb{Z}[\mathrm{Gal}(L_2/\mathbb{Q})]$-structure is as follows: 512 are free, 1536 are stably free but not free, and 2048 are not stably free (in particular, $\mathcal{O}_{L_2}$ is free, as was first shown by Cougnard [Cou98, VIII]). Moreover, for a fixed choice of isomorphism $\varphi\colon G \to \mathrm{Gal}(L_2/\mathbb{Q})$, the $1536 = 3 \cdot 512$ stably free but not free primitive ambiguous ideals are equally distributed among the three isomorphism classes of stably free but not free $\mathbb{Z}[G]$-lattices of rank 1. The ambiguous primitive ideals $\psi(5^2 17^2\mathbb{Z})$, $\psi(5^2\mathbb{Z})$, and $\psi(7^2 11^2\mathbb{Z})$ are pairwise nonisomorphic (for a fixed φ) and stably free but not free. Moreover, $\psi(11^2\mathbb{Z})$ is not stably free and $\psi(17\mathbb{Z})$ is free but not equal to $\mathcal{O}_{L_1}$.

Acknowledgments

The authors are indebted to Werner Bley for suggesting this project and for his help in drafting an early version of §3.1. The authors also wish to thank Alex Bartel for pointing out a mistake in an earlier version of this article, Nigel Byott for several helpful conversations and comments, Gunter Malle for numerous helpful comments, and the referee for a thorough and thoughtful report.

References

[AC20] A. Agboola and L. Caputo, *On the square root of the inverse different*, `arXiv:1803.09392` (2020).

[BB06] W. Bley and R. Boltje, *Computation of Locally Free Class Groups*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 72–86, DOI 10.1007/11792086_6. MR2282916

[BCNS15] O. Braun, R. Coulangeon, G. Nebe, and S. Schönnenbeck, *Computing in arithmetic groups with Voronoi's algorithm*, J. Algebra **435** (2015), 263–285, DOI 10.1016/j.jalgebra.2015.01.022. MR3343219

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. MR1484478

[BE05] W. Bley and M. Endres, *Picard groups and refined discrete logarithms*, LMS J. Comput. Math. **8** (2005), 1–16, DOI 10.1112/S1461157000000875. MR2123128

[BFH17] J.-F. Biasse, C. Fieker, and T. Hofmann, *On the computation of the HNF of a module over the ring of integers of a number field*. part 3, J. Symbolic Comput. **80** (2017), no. part 3, 581–615, DOI 10.1016/j.jsc.2016.07.027. MR3574529

[BJ08] W. Bley and H. Johnston, *Computing generators of free modules over orders in group algebras*, J. Algebra **320** (2008), no. 2, 836–852, DOI 10.1016/j.jalgebra.2008.01.042. MR2422318

[BJ11] W. Bley and H. Johnston, *Computing generators of free modules over orders in group algebras II*, Math. Comp. **80** (2011), no. 276, 2411–2434, DOI 10.1090/S0025-5718-2011-02488-9. MR2813368

[Ble97] W. Bley, *Computing associated orders and Galois generating elements of unit lattices*, J. Number Theory **62** (1997), no. 2, 242–256, DOI 10.1006/jnth.1997.2050. MR1432772

[BW09] W. Bley and S. M. J. Wilson, *Computations in relative algebraic K-groups*, LMS J. Comput. Math. **12** (2009), 166–194, DOI 10.1112/S1461157000001480. MR2564571

[Chi85] T. Chinburg, *Exact sequences and Galois module structure*, Ann. of Math. (2) **121** (1985), no. 2, 351–376, DOI 10.2307/1971177. MR786352

[Coh93] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206

[Coh00] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR1728313

[Cou94] J. Cougnard, *Un anneau d'entiers stablement libre et non libre* (French, with English and French summaries), Experiment. Math. **3** (1994), no. 2, 129–136. MR1313877

[Cou98] J. Cougnard, *Anneaux d'entiers stablement libres sur $\mathbb{Z}[H_8 \times C_2]$* (French, with English and French summaries), J. Théor. Nombres Bordeaux **10** (1998), no. 1, 163–201. MR1827291

[CR81] C. W. Curtis and I. Reiner, *Methods of Representation Theory. Vol. I*, With applications to finite groups and orders; Pure and Applied Mathematics; A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1981. MR632548

[CR87] C. W. Curtis and I. Reiner, *Methods of Representation Theory. Vol. II*, With applications to finite groups and orders; A Wiley-Interscience Publication, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1987. MR892316

[CV16] L. Caputo and S. Vinatier, *Galois module structure of the square root of the inverse different in even degree tame extensions of number fields*, J. Algebra **468** (2016), 103–154, DOI 10.1016/j.jalgebra.2016.06.035. MR3550860

[DD08] L. Dembélé and S. Donnelly, *Computing Hilbert Modular Forms over Fields with Nontrivial Class Group*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 371–386, DOI 10.1007/978-3-540-79456-1_25. MR2467859

[Ebe89] W. M. Eberly, *Computations for algebras and group representations*, Ph.D. thesis, University of Toronto, 1989.

[Ere91] B. Erez, *The Galois structure of the square root of the inverse different*, Math. Z. **208** (1991), no. 2, 239–255, DOI 10.1007/BF02571523. MR1128708

[FH14] C. Fieker and T. Hofmann, *Computing in quotients of rings of integers*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 349–365, DOI 10.1112/S1461157014000291. MR3240814

[FHHJ17] C. Fieker, W. Hart, T. Hofmann, and F. Johansson, *Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language*, ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2017, pp. 157–164, DOI 10.1145/3087604.3087611. MR3703682

[FHS19] C. Fieker, T. Hofmann, and C. Sircana, *On the Construction of Class Fields*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 239–255. MR3952015

[Fle71] C. R. Fletcher, *Euclidean rings*, J. London Math. Soc. (2) **4** (1971), 79–82, DOI 10.1112/jlms/s2-4.1.79. MR292809

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

[Frö67] J. W. S. Cassels and A Fröhlich (eds.), *Algebraic number theory*, Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union, Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967. MR0215665

[Frö78] A. Fröhlich, *Some problems of Galois module structure for wild extensions*, Proc. London Math. Soc. (3) **37** (1978), no. 2, 193–212.

[Frö83] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 1, Springer-Verlag, Berlin, 1983. MR717033

[FT91] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR1215934

[Gir99] K. Girstmair, *An algorithm for the construction of a normal basis*, J. Number Theory **78** (1999), no. 1, 36–45, DOI 10.1006/jnth.1999.2388. MR1706933

[Hig60] D. G. Higman, *On representations of orders over Dedekind domains*, Canadian J. Math. **12** (1960), 107–125, DOI 10.4153/CJM-1960-010-1. MR109175

[HM06] E. Hallouin and C. Maire, *Cancellation in totally definite quaternion algebras*, J. Reine Angew. Math. **595** (2006), 189–213, DOI 10.1515/CRELLE.2006.048. MR2244802

[Hof16] T. Hofmann, *Integrality of representations of finite groups*, Ph.D. thesis, Technische Universität Kaiserslautern, 2016.

[Jac66] H. Jacobinski, *On extensions of lattices*, Michigan Math. J. **13** (1966), 471–475. MR204538

[Kaw86] F. Kawamoto, *On normal integral bases of local fields*, J. Algebra **98** (1986), no. 1, 197–199, DOI 10.1016/0021-8693(86)90022-0. MR825142

[KV10] M. Kirschmer and J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. **39** (2010), no. 5, 1714–1747, DOI 10.1137/080734467. MR2592031

[Lam99] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999. MR1653294

[Leo59] H.-W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers* (German), J. Reine Angew. Math. **201** (1959), 119–149, DOI 10.1515/crll.1959.201.119. MR108479

[Let90] G. Lettl, *The ring of integers of an abelian number field*, J. Reine Angew. Math. **404** (1990), 162–170, DOI 10.1515/crll.1990.404.162. MR1037435

[Noe32] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung* (German), J. Reine Angew. Math. **167** (1932), 147–152, DOI 10.1515/crll.1932.167.147. MR1581331

[NS09] G. Nebe and A. Steel, *Recognition of division algebras*, J. Algebra **322** (2009), no. 3, 903–909, DOI 10.1016/j.jalgebra.2009.04.026. MR2531228

[Pag14] A. Page, *An algorithm for the principal ideal problem in indefinite quaternion algebras*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 366–384, DOI 10.1112/S1461157014000321. MR3240815

[Ple74] W. G. Plesken, *Beiträge zur Bestimmung der endlichen irreduziblen Untergruppen von* $\mathrm{GL}(n,\mathbb{Z})$ *und ihrer ganzzahligen Darstellungen*, Ph.D. thesis, RWTH Aachen, 1974.

[Rei03] I. Reiner, *Maximal Orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original; With a foreword by M. J. Taylor. MR1972204

[Sch80] J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. Assoc. Comput. Mach. **27** (1980), no. 4, 701–717, DOI 10.1145/322217.322225. MR594695

[Ser79] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237

[SM98] A. Storjohann and T. Mulders, *Fast Algorithms for Linear Algebra Modulo N*, Algorithms—ESA '98 (Venice), Lecture Notes in Comput. Sci., vol. 1461, Springer, Berlin, 1998, pp. 139–150, DOI 10.1007/3-540-68530-8_12. MR1683348

[Sme15] D. Smertnig, *A note on cancellation in totally definite quaternion algebras*, J. Reine Angew. Math. **707** (2015), 209–216, DOI 10.1515/crelle-2013-0069. MR3403458

[Ste12] A. K. Steel, *Construction of ordinary irreducible representations of finite groups*, Ph.D. thesis, Pure Mathematics, University of Sydney, 2012.

[Swa83] R. G. Swan, *Projective modules over binary polyhedral groups*, J. Reine Angew. Math. **342** (1983), 66–172, DOI 10.1515/crll.1983.342.66. MR703486

[Tay81] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), no. 1, 41–79, DOI 10.1007/BF01389193. MR608528

[Ull69] S. Ullom, *Normal bases in Galois extensions of number fields*, Nagoya Math. J. **34** (1969), 153–167. MR240082

[Ung06] W. R. Unger, *Computing the character table of a finite group*, J. Symbolic Comput. **41** (2006), no. 8, 847–862, DOI 10.1016/j.jsc.2006.04.002. MR2246713

[Vin03] S. Vinatier, *Sur la racine carrée de la codifférente* (French, with English and French summaries), J. Théor. Nombres Bordeaux **15** (2003), no. 1, 393–410. Les XXIIèmes Journées Arithmetiques (Lille, 2001). MR2019023

[Zip79] R. Zippel, *Probabilistic Algorithms for Sparse Polynomials*, Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), Lecture Notes in Comput. Sci., vol. 72, Springer, Berlin-New York, 1979, pp. 216–226. MR575692

Fachbereich Mathematik, Technische Universität Kaiserslautern, 67663 Kaiserslautern, Germany

Email address: thofmann@mathematik.uni-kl.de

URL: http://www.mathematik.uni-kl.de/∼thofmann

Department of Mathematics, University of Exeter, Exeter, EX4 4QF United Kingdom

Email address: H.Johnston@exeter.ac.uk

URL: http://emps.exeter.ac.uk/mathematics/staff/hj241