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 $\Lambda$ 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) $\Lambda$-lattice $X$ either computes a free basis of $X$ over $\Lambda$ or shows that $X$ is not free over $\Lambda$. In the present article, we generalise this by showing that, under weaker hypotheses on $A$, there exists an algorithm that for two given $\Lambda$-lattices $X$ and $Y$ either computes an isomorphism $X \rightarrow Y$ or determines that $X$ and $Y$ are not isomorphic. The algorithm is implemented in Magma for $A = \mathbb{Q}[G]$ and $\Lambda = \mathbb{Z}[G]$, 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 $\mathcal{O} = \mathcal{O}_K$. Let $A$ be a finite dimensional semisimple $K$-algebra and let $\Lambda$ be an $\mathcal{O}$-order in $A$. A $\Lambda$-lattice is a (left) $\Lambda$-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 $\Lambda$-lattice $X$ either computes a free basis of $X$ over $\Lambda$ or shows that $X$ is not free over $\Lambda$. In the present article, we generalise this by showing that, under the (weaker) hypotheses on $A$ discussed below, there exists an algorithm that for two given $\Lambda$-lattices $X$ and $Y$ either computes an isomorphism $X \rightarrow Y$ 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 $X \rightarrow Y$ between two given $\Lambda$-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 centre 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.

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

(H2) For each $i$, every maximal $\mathcal{O}$-order $\Delta_i$ in $D_i$ has the following properties:

(a) we can solve the principal ideal problem for fractional left $\Delta_i$-ideals, and

(b) $\Delta_i$ 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 localised 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.

Date: Version of 2nd August 2018.

2000 Mathematics Subject Classification. 11R33, 11Y40, 16Z05.
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 with Galois group \( \Gamma \). The classical Normal Basis Theorem says that \( L \) is free of rank 1 as a module over the group algebra \( K[\Gamma] \). A more difficult problem is that of determining the structure of the ring of integers \( \mathcal{O}_L \) over its associated order \( \mathcal{A}_{L/K}(\mathcal{O}_L) = \{ \lambda \in K[\Gamma] \mid \lambda \mathcal{O}_L \subseteq \mathcal{O}_L \} \). 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, focusing on the case of rings of integers.

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 \( \mathcal{A}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K[\Gamma] \) and that \( \mathcal{O}_L \) is a locally free \( \mathcal{O}_K[\Gamma] \)-lattice of rank 1 (see [Noe32, Frö83, I, §3] or [Kaw86]). Thus one can consider the class \( (\mathcal{O}_L) \) in the locally free class group \( \text{Cl}(\mathcal{O}_K[\Gamma]) \). If \( \Gamma \) is abelian then \( (\mathcal{O}_L) \) determines \( \mathcal{O}_L \) up to isomorphism, but for certain \( K \) and non-abelian \( \Gamma \), this class only determines \( \mathcal{O}_L \) up to stable isomorphism. If we restrict scalars and consider \( \mathcal{O}_L \) as a \( \mathbb{Z}[\Gamma] \)-module then striking work of Fröhlich and Taylor determines \( (\mathcal{O}_L) \) in terms of Artin root numbers of irreducible symplectic characters of \( \Gamma \) (see [Frö83, I] for an overview). In particular, if \( \Gamma \) is abelian then \( \mathcal{O}_L \) is always free over \( \mathbb{Z}[\Gamma] \) and if \( \Gamma \cong \mathbb{Q}_2 \) (the quaternion group of order 32) then \( \mathcal{O}_L \) is always stably free over \( \mathbb{Z}[\Gamma] \). Cougnard [Cou94] gave an example \( L/\mathbb{Q} \) with \( \Gamma \cong \mathbb{Q}_2 \) such that \( \mathcal{O}_L \) is stably free but not free over \( \mathbb{Z}[\Gamma] \).

If we relax the requirement that \( L/K \) is tamely ramified then the situation is much worse. In particular, if \( L/K \) is wildly ramified then \( \mathcal{O}_K[\Gamma] \) is strictly contained in \( \mathcal{A}_{L/K}(\mathcal{O}_L) \). 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 \( \mathcal{A}_{L/\mathbb{Q}}(\mathcal{O}_L) \) and, in addition, gives an explicit construction of a free generator (also see [Let90]). However, in general, \( \mathcal{O}_L \) need not even be locally free over \( \mathcal{A}_{L/K}(\mathcal{O}_L) \).

A different approach in the tame case is to study so-called ‘realisable classes’. Fix a number field \( K \) and an abstract finite group \( G \). Then every tamely ramified Galois extension \( L/K \) with \( \text{Gal}(L/K) \cong G \) defines a class \( (\mathcal{O}_L) \) in \( \text{Cl}(\mathcal{O}_K[G]) \) (this class may depend on the choice of isomorphism \( \text{Gal}(L/K) \cong G \), but we shall not dwell on this point here). Such classes are said to be realisable and the set of realisable classes is denoted \( R(\mathcal{O}_K[G]) \). When \( G \) is abelian, McCulloh [McC87] gave a complete description of \( R(\mathcal{O}_K[G]) \) and in particular showed that it is in fact a subgroup of \( \text{Cl}(\mathcal{O}_K[G]) \). This result has also been proven for particular non-abelian groups \( G \) (see [BS05], [BGS06] and [BS13], for example). Recently, Agboola and McCulloh have generalised these results to the case in which \( G \) belongs to a large class of soluble groups [AM]. Moreover, in the abelian case, Agboola [Agb12] has studied the distribution of realisable classes.

We now review previous work on algorithms that can be used to determine the structure of \( \mathcal{O}_L \) over \( \mathcal{A} = \mathcal{A}_{L/K}(\mathcal{O}_L) \), where again \( L/K \) is a finite Galois extension of number fields with Galois group \( \Gamma \). In the case that \( \Gamma \) is abelian, Bley [Ble97] gave algorithms for computing \( \mathcal{A} \), determining whether \( \mathcal{O}_L \) is locally free over \( \mathcal{A} \), and explicitly constructing a free generator for \( \mathcal{O}_L \) over \( \mathcal{A} \) or showing that no such generator exists. A non-abelian higher-rank generalisation was given by Bley and the second named author [BJ08, BJ11], and it is this work that is in turn generalised in the present article. In [BE05], Bley and Endres again considered the case in which \( \Gamma \) is abelian and gave algorithms for computing the Picard group \( \text{Pic}(\mathcal{A}) \) and solving the corresponding refined discrete logarithm problem (and thus for computing isomorphisms between invertible \( \mathcal{A} \)-submodules of \( K[\Gamma] \)). In the case that \( \Gamma \) is any finite group, Bley and Wilson [BW09] gave algorithms for computing the relative algebraic \( K \)-group \( K_0(\mathcal{A}, K) \) and solving the discrete logarithm problem in both \( K_0(\mathcal{A}, K) \) and the locally free class group \( \text{Cl}(\mathcal{A}) \) (note that this is a lot weaker than
the refined discrete logarithm problem and can only be used to determine whether two 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 it exists.

In §10, we discuss experimental results obtained by using a proof of concept implementation of Algorithm 4.1 in Magma [BCP97] for \( A = \mathbb{Q}[G] \) and \( \Lambda = \mathbb{Z}[G] \), 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 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 \( \text{Gal}(L/\mathbb{Q}) \cong G \) such that \( \mathcal{O}_L \) is stably free but not free over \( \mathbb{Z}[\text{Gal}(L/\mathbb{Q})] \). 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 \( \text{Gal}(L/\mathbb{Q}) \cong G \), we then examine the distribution of isomorphism classes of ambiguous ideals of \( \mathcal{O}_L \).

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; and Gunter Malle for numerous helpful comments. The first named 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 named author was supported by EPSRC First Grant EP/N005716/1 ‘Equivariant Conjectures in Arithmetic’.

2. Preliminaries on lattices and orders

For further background on lattices and orders, we refer the reader to [Rei03, §4 and §8]. Let \( R \) be an integral domain with field of fractions \( K \). To avoid trivialities, we assume that \( R \neq K \). An \( R \)-lattice is a finitely generated torsion free module over \( R \). For any finite dimensional \( K \)-vector space \( V \), an \( R \)-lattice in \( V \) is a finitely generated \( R \)-submodule \( M \) in \( V \). We define a \( K \)-vector subspace of \( V \) by

\[
KM := \{ \alpha_1 m_1 + \alpha_2 m_2 + \cdots + \alpha_r m_r \mid r \in \mathbb{Z}_{\geq 0}, \alpha_i \in K, m_i \in M \}
\]

and say that \( M \) is a full \( R \)-lattice in \( V \) if \( KM = V \).

Now further suppose that \( R \) is a noetherian integral domain and let \( A \) be a finite dimensional \( K \)-algebra. An \( R \)-order in \( A \) is a subring \( \Lambda \) of \( A \) (so in particular has the same unity element as \( A \)) such that \( \Lambda \) is a full \( R \)-lattice in \( A \). Note that \( \Lambda \) is both left and right noetherian, since \( A \) is finitely generated over \( R \). A left \( \Lambda \)-lattice \( X \) is a left \( \Lambda \)-module that is also an \( R \)-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 \( \Lambda \)-lattices are said to be isomorphic if they are isomorphic as \( \Lambda \)-modules.

Lemma 2.1. Let \( S \) be a noetherian integral domain such that \( R \subseteq S \subseteq K \). Let \( \Gamma \) be an \( S \)-order in \( A \). Let \( V \) be a finitely generated \( A \)-module. For any \( R \)-lattice \( M \) in \( V \), the set

\[
\Gamma M := \{ \gamma_1 m_1 + \gamma_2 m_2 + \cdots + \gamma_r m_r \mid r \in \mathbb{Z}_{\geq 0}, m_i \in M, \gamma_i \in \Gamma \}
\]

is a \( \Gamma \)-lattice in \( V \) containing \( M \).
Proof. That $M \subseteq \Gamma M$ is clear. Note that $K$ is the field of fractions of both $R$ and $S$. Write $M = \langle v_1, \ldots, v_l \rangle_R$ and $\Gamma = \langle w_1, \ldots, w_m \rangle_S$. An easy calculation shows that

$$\Gamma M = \langle w_i v_j \mid 1 \leq i \leq m, 1 \leq j \leq l \rangle_S$$

and hence $\Gamma M$ is an $S$-lattice in $V$. Moreover, it is straightforward to see that $\Gamma M$ is also a $\Gamma$-module and therefore is a $\Gamma$-lattice in $V$.

**Lemma 2.2.** Assume the setup and notation of Lemma 2.1. Let $\Lambda$ be an $R$-order in $A$ and let $f: X \to Y$ be a homomorphism of $\Lambda$-lattices. Then the following hold.

(a) There exists a unique homomorphism of $A$-modules $f^A: KX \to KY$ extending $f$.

If $f$ is injective (resp. surjective), then $f^A$ is injective (resp. surjective).

(b) There exists a unique homomorphism of $\Gamma$-lattices $f^\Gamma: \Gamma X \to \Gamma Y$ extending $f$.

If $f$ is injective (resp. surjective), then $f^\Gamma$ is injective (resp. surjective).

Proof. (a) Let $\{v_i\}_{1 \leq i \leq n}$ be a $K$-basis of $KX$ contained in $X$. For $i = 1, 2, \ldots, n$ we define $f^A(v_i) = f(v_i)$ and extend this to a $K$-linear map $f^A: KX \to KY$. We now check that $f^A$ is in fact $A$-linear. Since $KA = A$, for each $a \in A$ we can find $d \in R$ with $d \neq 0$ such that $da \in \Lambda$. Thus for $i = 1, 2, \ldots, n$ we have

$$df^A(av_i) = f^A(dav_i) = f(dav_i) = (da)f(v_i) = (da)f^A(v_i),$$

and hence $f^A(av_i) = af^A(v_i)$. Thus by $K$-linearity we have that $f^A$ is a homomorphism of $A$-modules. The statements about uniqueness, injectivity and surjectivity are clear.

(b) Let $f^A$ be the map from part (a) and define $f^\Gamma = f^A|_{\Gamma X}$, which is a priori a $\Gamma$-linear map $\Gamma X \to KY$. For $\sum_{i=1}^r \gamma_i x_i \in \Gamma X$ we have

$$f^A(\sum_{i=1}^r \gamma_i x_i) = \sum_{i=1}^r f^A(\gamma_i x_i) = \sum_{i=1}^r \gamma_i f(x_i) \in \Gamma f(X) \subseteq \Gamma Y.$$

Thus we can and do consider $f^\Gamma$ as a map $\Gamma X \to \Gamma Y$. If $f$ is injective, then $f^A$ is injective by part (a) and this implies that $f^\Gamma$ is also injective. Now suppose $f$ is surjective and let $\sum_{i=1}^r \gamma_i y_i \in \Gamma Y$. Then for $i = 1, 2, \ldots, r$ there exists $x_i \in X$ such that $f(x_i) = y_i$. Thus

$$\sum_{i=1}^r f(x_i) = \sum_{i=1}^r f(\gamma_i x_i) = \sum_{i=1}^r \gamma_i f(x_i) = f^A(\sum_{i=1}^r \gamma_i x_i) = f^\Gamma(\sum_{i=1}^r \gamma_i x_i),$$

and therefore $f^\Gamma$ is surjective. The uniqueness of $f^\Gamma$ follows from part (a).

3. Conditions for two lattices to be isomorphic

Let $\mathcal{O}$ be a Dedekind domain with quotient field $K$. To avoid trivialities, we assume that $\mathcal{O} \neq K$. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, we let $\mathcal{O}_\mathfrak{p}$ denote the localization (not completion) of $\mathcal{O}$ at $\mathfrak{p}$. If $M$ is an $\mathcal{O}$-lattice in a finite dimensional $K$-vector space $V$, then we write $X_\mathfrak{p} = \mathcal{O}_\mathfrak{p} \otimes_{\mathcal{O}} X$ for the localization of $X$ at $\mathfrak{p}$. Since $\mathcal{O}$ is a Dedekind domain, every $\mathcal{O}$-lattice is projective (see [CR81, §4D]) and so we can identify $X_\mathfrak{p}$ with the $\mathcal{O}_\mathfrak{p}$-submodule $\mathcal{O}_\mathfrak{p} X := \langle X \rangle_{\mathcal{O}_\mathfrak{p}} = \{\alpha_1 x_1 + \cdots + \alpha_r x_r \mid r \in \mathbb{Z}_{\geq 0}, \alpha_i \in \mathcal{O}_\mathfrak{p}, x_i \in X\}$ of $V$.

Let $A$ be a separable $K$-algebra, that is, a finite dimensional semisimple $K$-algebra such that the centre of each simple component of $A$ is a separable field extension of $K$ (see [Rei03, §7c]). Let $\Lambda$ be an $\mathcal{O}$-order in $A$. By localizing at a maximal ideal $\mathfrak{p}$, a $\Lambda$-lattice $X$ yields a $\Lambda_\mathfrak{p}$-lattice $X_\mathfrak{p}$. Two $\Lambda$-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 $\mathcal{O}$. For $R = \mathcal{O}$ or $\mathcal{O}_\mathfrak{p}$, we shall write $[-:-]_R$ for the $R$-module index (see [Frö67, §3] or [FT91, II.4]).
3.1. Restricting isomorphisms over maximal orders. 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 \( \Lambda \)-lattices then they are locally isomorphic and \( MX \) and \( MY \) are isomorphic \( \mathcal{M} \)-lattices. We now investigate the additional conditions under which a converse holds. In doing so, we generalise the results of [BJ08, §2], where necessary and sufficient conditions were given for a \( \Lambda \)-lattice to be free.

**Theorem 3.1.** Let \( X \) and \( Y \) be locally isomorphic \( \Lambda \)-lattices such that there exists an isomorphism of \( \mathcal{M} \)-lattices \( f : MX \to MY \). Then \( f \) restricts to an isomorphism \( f|_X : X \to Y \) of \( \Lambda \)-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 \( \Lambda \)-lattice homomorphism, so it only remains to show that \( f(X) = Y \).

Let \( p \) be a maximal ideal of \( \mathcal{O} \) and let \( f_p : X_p \to Y_p \) be an isomorphism of \( \Lambda_p \)-lattices. By Lemma 2.2 there exist unique \( \mathcal{M}_p \)-lattice isomorphisms \( f_{M_p} : \mathcal{M}_p X \to \mathcal{M}_p Y \) and \( f_{M_p}^*: \mathcal{M}_p X_p \to \mathcal{M}_p Y_p \) extending \( f \) and \( f_p \), respectively. Note that \( \mathcal{M}_p X = \mathcal{M}_p X_p \) and \( \mathcal{M}_p Y = \mathcal{M}_p Y_p \) and so we can and do consider \( f_{M_p} \) as a map \( \mathcal{M}_p X_p \to \mathcal{M}_p Y_p \).

Observe that we have the following equalities and containment:

\[
\begin{align*}
\mathcal{M}_p (X_p) &= \mathcal{M}_p (X) = \mathcal{O}_p f(X) = \mathcal{O}_p f_{M_p}^* (X) = f_{M_p}^* (\mathcal{O}_p X) = f_{M_p}^* (X_p).
\end{align*}
\]

Hence

\[
\begin{align*}
[Y_p : f(X)|_X \mathcal{O}_p] &= [Y_p : f_{M_p}^* (X)|_X \mathcal{O}_p] = [f_{M_p}^* (X)|_X : (f_{M_p}^* \circ (f_{M_p}^*)^{-1}) (X)|_X \mathcal{O}_p] \\
&= [X : ((f_{M_p}^*)^{-1} \circ f_{M_p}^*) (X)|_X \mathcal{O}_p] = \det \mathcal{O}_p ((f_{M_p}^*)^{-1} \circ f_{M_p}^*) \mathcal{O}_p.
\end{align*}
\]

Since \( (f_{M_p}^*)^{-1} \circ f_{M_p}^* : \mathcal{M}_p X_p \to \mathcal{M}_p X_p \) is an automorphism of \( \mathcal{M}_p \)-lattices and thus of \( \mathcal{O}_p \)-lattices, we must have \( \det \mathcal{O}_p ((f_{M_p}^*)^{-1} \circ f_{M_p}^*) \in \mathcal{O}_p^\times \) and hence \( [Y_p : f(X)|_X \mathcal{O}_p] = \mathcal{O}_p \). Since this holds for every maximal ideal \( p \) of \( \mathcal{O} \) and \( f(X) \subseteq Y \) by assumption, we must have \( f(X) = Y \). Therefore \( f|_X : X \to Y \) is an isomorphism of \( \Lambda \)-lattices. \( \square \)

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

**Corollary 3.3.** Two \( \Lambda \)-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 \( f : MX \to MY \), and

(c) there exists an automorphism \( g \in \text{Aut}_\mathcal{M}(MY) \) such that \( (g \circ f)(X) \subseteq Y \).

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

**Proof.** If (a), (b) and (c) hold then \( X \) and \( Y \) are isomorphic by Theorem 3.1. Suppose conversely that there exists a \( \Lambda \)-lattice isomorphism \( h : X \to Y \). Then (a) clearly holds, (b) holds with \( f := h^\mathcal{M} \) by Lemma 2.2 and (c) holds with \( g := \text{Id}_\mathcal{M}Y \) (the identity map on \( \mathcal{M}Y \)). \( \square \)

Most of the following notation is adopted from [BB06]. Denote the centre 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 \( e_1, \ldots, e_r \) be the primitive idempotents of \( C \) and set \( A_i = e_i A \). Then

\[
(1) \quad A = A_1 \oplus \cdots \oplus A_r.
\]
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 centres $K_i := Z(A_i)$ are finite field extensions of $K$ via $K \rightarrow K_i$, $\alpha \mapsto e_i \alpha$, and we have $K$-algebra isomorphisms $A_i \cong \text{Mat}_{n_i \times n_i}(D_i)$ where $D_i$ is a skew field with $Z(D_i) \cong K_i$ (see [CR81, (3.28)]). The Wedderburn decomposition (1) induces decompositions

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

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

\[ \text{End}_N(V) = \text{End}_{\mathcal{M}_i}(\mathcal{M}_i N) \oplus \cdots \oplus \text{End}_{\mathcal{M}_r}(\mathcal{M}_r N) \]
\[ \text{Aut}_N(V) = \text{Aut}_{\mathcal{M}_1}(\mathcal{M}_1 N) \times \cdots \times \text{Aut}_{\mathcal{M}_r}(\mathcal{M}_r N). \]

**Corollary 3.4.** Two $\Lambda$-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 $f_i : \mathcal{M}_i X \rightarrow \mathcal{M}_i Y$ for each $i$, and

(c) there exist $g_i \in \text{Aut}_{\mathcal{M}_i}(\mathcal{M}_i Y)$ 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 $(\sum_{i=1}^r (g_i \circ f_i)) : X \rightarrow Y$.

Now let $Y$ be a $\Lambda$-lattice. Define

\[ S = S_Y = \text{End}_\Lambda(MY) \quad \text{and} \quad T = T_Y = \text{End}_\Lambda(Y). \]

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 $S \rightarrow \overline{S}$ by $s \mapsto \overline{s}$. We have decompositions

\[ \mathfrak{I} = \mathfrak{I}_1 \oplus \cdots \oplus \mathfrak{I}_r, \quad S = S_1 \oplus \cdots \oplus S_r \quad \text{and} \quad \overline{S} = \overline{S}_1 \oplus \cdots \oplus \overline{S}_r, \]

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

**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 $\overline{g'_i} - \overline{g}_i \in \mathfrak{I}_i$. For each $i$, define

\[ h_i := g'_i \circ g_i^{-1} - \text{Id}_{\mathcal{M}_i Y} = (g'_i - g_i) \circ g_i^{-1} \in \mathfrak{I}_i g_i^{-1} = \mathfrak{I}_i, \]

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

\[ (\oplus_{i=1}^r (g'_i \circ f_i))(X) = (\oplus_{i=1}^r (\text{Id}_{\mathcal{M}_i Y} + h_i) \circ g_i \circ f_i))(X) \]
\[ = (\text{Id}_{\mathcal{M}_Y} + h) (\oplus_{i=1}^r (g_i \circ f_i))(X) \]
\[ \subseteq (\text{Id}_{\mathcal{M}_Y} + h)(Y) \]
\[ \subseteq Y, \]

that is, (c') holds. Therefore (c) and (c') are equivalent. \qed
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 non-zero 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 \( \mathcal{S} \), and thus the sets of representatives \( \mathcal{U}_i \), are finite; this is crucial for the development of any algorithm that relies on Corollary 3.5.

3.2. Reducing to the free rank 1 case via homomorphism groups. We now give an alternative approach to the one described in \( \S 3.1 \). Let \( X \) and \( Y \) be \( \Lambda \)-lattices. Then \( \text{End}_\Lambda(Y) \) is an \( \mathcal{O} \)-order in the separable \( K \)-algebra \( \text{End}_\Lambda(KY) \). Moreover, \( \text{Hom}_\Lambda(X,Y) \) is a \( (\text{left}) \text{End}_\Lambda(Y) \)-lattice in \( \text{Hom}_\Lambda(KX,KY) \) via post-composition. The following result is a generalisation of [Joh08, Proposition 3.2].

Theorem 3.7. A homomorphism \( f \in \text{Hom}_\Lambda(X,Y) \) is an isomorphism if and only if

(a) \( X \) and \( Y \) are locally isomorphic, and
(b) \([Y : g(X)]_\mathcal{O} \subseteq [Y : f(X)]_\mathcal{O} \) for all \( g \in \text{Hom}_\Lambda(X,Y) \).

Proof. Let \( f \in \text{Hom}_\Lambda(X,Y) \). Suppose \( f \) is an isomorphism. Then (a) clearly holds and \([Y : f(X)]_\mathcal{O} = [Y : Y]_\mathcal{O} = \mathcal{O} \), giving (b). Suppose conversely that (a) and (b) hold. Suppose for a contradiction that \( f \) is not surjective. Then there exists a maximal ideal \( p \) of \( \mathcal{O} \) such that \([Y : f(X)]_\mathcal{O} \subseteq p \). Since \( X \) and \( Y \) are locally isomorphic there exists an isomorphism \( g \in \text{Hom}_\mathcal{O}_p(X,Y) \). Replacing \( g \) by \( \alpha g \) for some \( \alpha \in \mathcal{O} - p \), we can and do view \( g \) as an element of \( \text{Hom}_\mathcal{O}(X,Y) \). But then \( g(X)_p = Y \) and so \([Y : g(X)]_\mathcal{O} \nsubseteq p \), contradicting (b). Therefore \( f \) is surjective. Since \( X \) and \( Y \) are locally isomorphic, a rank argument shows that \( f \) is also injective and hence is an isomorphism. \( \square \)

Corollary 3.8. A homomorphism \( f \in \text{Hom}_\Lambda(X,Y) \) is an isomorphism if and only if

(a) \( X \) and \( Y \) are locally isomorphic, and
(b) \( f \) is a generator of \( \text{Hom}_\Lambda(X,Y) \) over \( \text{End}_\Lambda(Y) \).

Proof. Let \( f \in \text{Hom}_\Lambda(X,Y) \). Suppose \( f \) is an isomorphism. Then (a) clearly holds. Let \( g \in \text{Hom}_\Lambda(X,Y) \). Then \( h := g \circ f^{-1} \in \text{End}_\Lambda(Y) \) and \( g = h \circ f \). Hence (b) holds. Suppose conversely that (a) and (b) hold. Let \( g \in \text{Hom}_\Lambda(X,Y) \). Then there exists \( h \in \text{End}_\Lambda(Y) \) such that \( g = h \circ f \) and so

\[
[Y : g(X)]_\mathcal{O} = [Y : (h(f(X)))_\mathcal{O}] = [Y : f(X)]_\mathcal{O} \cdot [f(X) : (h(f(X)))_\mathcal{O}] = [Y : f(X)]_\mathcal{O} \cdot \det_\mathcal{O}(h) \subseteq [Y : f(X)]_\mathcal{O}.
\]

Hence \( f \) is an isomorphism by Theorem 3.7. \( \square \)

Corollary 3.9. Condition (b) in Corollary 3.8 can be strengthened to

(b') \( f \) is a free generator of \( \text{Hom}_\Lambda(X,Y) \) over \( \text{End}_\Lambda(Y) \).

Proof. Suppose that \( X \) and \( Y \) are (locally) isomorphic over \( \Lambda \). Then they have the same rank over \( \mathcal{O} \), and thus the same is true of \( \text{Hom}_\Lambda(X,Y) \) and \( \text{End}_\Lambda(Y) \). Hence any generator of \( \text{Hom}_\Lambda(X,Y) \) over \( \text{End}_\Lambda(Y) \) is in fact a free generator. \( \square \)

Remark 3.10. Necessary and sufficient conditions for the existence of a free generator of \( \text{Hom}_\Lambda(X,Y) \) over \( \text{End}_\Lambda(Y) \) are given by (special cases of) the results of [BJ08, \( \S 2 \)], which are themselves special cases of those in \( \S 3.1 \).

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 \( \Lambda \) be an \( \mathcal{O} \)-order in \( A \). In this section, we outline an algorithm that takes two \( \Lambda \)-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 \( \S 5 \).

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 \( a_1, \ldots, a_s \) and structure constants \( a_{i,j,k} \in K \) for \( 1 \leq i, j, k \leq s \) such that \( a_i \cdot a_j = \sum_{k=1}^{s} a_{i,j,k} a_k \). From this, it is straightforward to construct an embedding of \( K \)-algebras \( A \to \text{Mat}_{n \times n}(K) \) (see [Ebe89, §2.2] for details). Moreover, we assume that \( \Lambda, X \) and \( Y \) are given by \( \mathcal{O} \)-pseudo-bases as described, for example, in [Coh00, 1.4.1]. In other words,

\[
X = a_1 v_1 + \cdots + a_m v_m \quad \text{and} \quad Y = b_1 w_1 + \cdots + b_n w_n,
\]

where for each \( i \) both \( a_i \) and \( b_i \) are fractional ideals of \( \mathcal{O} \) and \( v_i \in V := KY \) and \( w_i \in W := KX \). Similarly, \( \Lambda = \mathbf{c}_1 \lambda_1 + \cdots + \mathbf{c}_s \lambda_s \) with fractional \( \mathcal{O} \)-ideals \( \mathbf{c}_i \) and \( \lambda_i \in A \). To describe the action of \( \Lambda \) on \( X \) (and of \( A \) on \( V \)), it suffices to assume that for each \( i \) there is a matrix \( M(X(\lambda_i)) \in \text{GL}_m(K) \) describing the action of \( \lambda_i \) with respect to \( v_1, \ldots, v_m \).

Finally, we assume that the action on \( Y \) is described similarly.

**Algorithm 4.1.** Input: \( A, \Lambda, X \) and \( Y \) as above.

1. Check that \( X \) and \( Y \) have equal \( \mathcal{O} \)-rank, that is, check that \( m = n \).
2. Compute the central primitive idempotents \( e_i \) in \( A \) and the components \( A_i := e_i A \), \( 1 \leq i \leq r \).
3. Compute a maximal \( \mathcal{O} \)-order \( \mathcal{M} \) in \( A \) containing \( \Lambda \) and set \( \mathcal{M}_i := e_i \mathcal{M} \).
4. Compute the set \( \mathcal{S} \) of maximal ideals \( \mathfrak{p} \) of \( \mathcal{O} \) dividing the module index \( [\mathcal{M} : \Lambda]_\mathcal{O} \).
5. For each \( i \), compute an \( \mathcal{M}_i \)-lattice isomorphism \( f_i: \mathcal{M}_i X \to \mathcal{M}_i Y \), if it exists.
6. For each \( \mathfrak{p} \in \mathcal{S} \), check that \( X_\mathfrak{p} \) and \( Y_\mathfrak{p} \) are isomorphic as \( \Lambda_\mathfrak{p} \)-lattices.
7. Compute \( S = S_Y := \text{End}_\mathcal{M}(\mathcal{M}Y) \) and \( T = T_Y := \text{End}_\mathcal{M}(\mathcal{M}Y) \) as well as the decomposition \( S = \oplus_{i=1}^r S_i \) where \( S_i := \text{End}_\mathcal{M}_i(\mathcal{M}_i Y) \).
8. Compute a full two-sided ideal \( \mathfrak{I} = \oplus_{i=1}^r \mathfrak{I}_i \) of \( S \) contained in \( T \).
9. For each \( i \), compute a finite set of representatives \( U_i \subset S_i^\times = \text{Aut}_\mathcal{M}_i(\mathcal{M}_i Y) \) of the image of the natural projection map \( S_i^\times \to (S_i/\mathfrak{I}_i)^\times \).
10. Test whether there exists a tuple \( (g_i) \in \prod_{i=1}^r U_i \) such that \( (\sum_{i=1}^r (g_i \circ f_i))(X) \subseteq Y \). For such a tuple, an isomorphism is given by \( (\sum_{i=1}^r (g_i \circ f_i)): X \to Y \). If no such tuple exists, then \( X \) and \( Y \) are not isomorphic.

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

1. (a) This is straightforward.
2. (b) Algorithms for the computation of primitive central idempotents have been given by Eberly [Ebe89, §2.4] and by Nebe and Steel [NS09, §2].
3. (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 \( \mathcal{M} := \bigoplus_i \mathcal{M}_i \).
4. (d) If the algorithms of Friedrichs are used for step (c), then \( \mathcal{S} \) 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 \( \Lambda \) and \( \mathcal{M} \) are both given by \( \mathcal{O} \)-pseudo-bases, \( \mathcal{S} \) can be determined using the Smith normal form.
algorithm (see [Coh00, 1.7.3]). Note that if $G$ is a finite group and $O[G] \subseteq \Lambda \subseteq K[G]$ then each $p \in \mathfrak{S}$ must divide $|G|$.

(e) This is the only step that requires the hypotheses (H1) and (H2). It is described in §6.

(f) Successful completion of step (e) gives an isomorphism $f := \sum_i f_i : M_X \to M_Y$ of $M$-lattices. If $p$ is a maximal ideal of $O$ such that $\Lambda_p = M_p$ then Lemma 2.2 shows that $f$ extends to an isomorphism $f_p : X_p \to Y_p$ of $M_p$-lattices. Thus checking that $X$ and $Y$ are locally isomorphic reduces to checking that $X_p$ and $Y_p$ are isomorphic $\Lambda_p$-lattices for each $p \in \mathfrak{S}$. Several algorithms to check this for a given maximal ideal $p$ are described in §8. In the special case that one wants to check that both $X_p$ and $Y_p$ are in fact free $\Lambda_p$-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 $c_i = \{x \in \text{End}_A(KY) \mid xS \subseteq T\}$ and right conductor $c_r = \{x \in \text{End}_A(KY) \mid Sx \subseteq T\}$ of $S$ in $T$. As noted in [BB06, §3.2], one can then take $\mathcal{J}$ to be either $c_r \cdot c_i$ or $cS$ where $c := \{x \in Z(\text{End}_A(KY)) \mid xS \subseteq T\} = c_r \cap C = c_i \cap C$ is the central conductor of $S$ in $T$. To minimise the running time of step (j), one would like to take $\mathcal{J}$ to be as large as possible; in many cases $cS$ is a better choice than $c_r \cdot c_i$, but in principle one could compute both to see which is better in a given situation.

The endomorphism ring $S_i = \text{End}_{\mathcal{M}}(\mathcal{M}_iY)$ is itself an $O$-order in the separable $K$-algebra $\text{End}_A(e_iKY)$. Viewing $S_i$ as a $\mathbb{Z}$-order, one can use the algorithm of Braun, Coulangeon, Nebe and Schönchenbek [BCNS15] to find generators $u_1, \ldots, u_r$ of $S_i^\times$. One can then compute $U_i$, the subgroup of $S_i^\times$ generated by $\overline{u}_1, \ldots, \overline{u}_r$ and write each element as a word of the form $\overline{u}_{i_1} \cdots \overline{u}_{i_s}$ where $r_i \in \mathbb{Z}$. For each such word, one can take $u_{i_1} \cdots u_{i_s}$ to be the corresponding element of $U_i$.

(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 generalisation 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 $\Lambda$-lattice $X$ is in fact free and, assuming it is, computing an explicit $\Lambda$-basis for $X$. Thanks to the algorithm of Braun, Coulangeon, Nebe and Schönchenbek [BCNS15] used in step (i) above, the hypotheses assumed in ibid. 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, which is (more or less) covered by the algorithms given in [BJ08, BJ11] (the hypotheses in ibid. can be weakened as described in Remark 4.2). However, algorithmically speaking, the reduction steps are far from trivial because they require methods to both compute homomorphism groups and test whether lattices are locally isomorphic; such methods are described in §7 and §8, respectively. Moreover, Algorithm
4.1 has the advantage of being more direct and thus more efficient. In particular, $\Lambda$ and $\text{End}_A(Y)$ are $\mathcal{O}$-orders in $A$ and $\text{End}_A(K|Y)$, respectively, but if $X$ and $Y$ are both locally free of rank $n$ then $\dim_K \text{End}_A(K|Y) = n^2 \dim_K(A)$.

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 $\mathcal{O} = \mathcal{O}_K$ 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 centre of the simple algebra $A_i$.

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

(H2) For each $i$, every maximal $\mathcal{O}$-order $\Delta_i$ in $D_i$ has the following properties:

(a) we can solve the principal ideal problem for fractional left $\Delta_i$-ideals, and

(b) $\Delta_i$ 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 $\Delta_i$ in all cases in which it is known (see §5.2). Moreover, property (H2)(b) is independent of the choice of $\Delta_i$, that is, if it holds for some choice of $\Delta_i$ 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 $A_i \rightarrow \text{Mat}_{s_i}(\mathbb{Q})$ 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 slow down computations considerably.

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

(i) decide whether $a \cong b$ as left $\Delta$-lattices, and

(ii) if so, compute $\xi \in D^\times$ such that $a = b\xi$.

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 $\Delta$ in $D$.

5.3. **Locally free cancellation - (H2)(b).** Let $K$ be a number field and let $\Lambda$ be an $\mathcal{O}_K$-order in a finite dimensional semisimple $K$-algebra $A$. Then $\Lambda$ is said to have the locally free cancellation property if for any locally free finitely generated left $\Lambda$-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 centre of the simple algebra $A_i$. We say that $A_i$ is Eichler/$\mathcal{O}_K$ 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/$\mathcal{O}_K$. The Jacobinski Cancellation Theorem [CR87, (51.24)] says that if $A$ is Eichler/$\mathcal{O}_K$ then $\Lambda$ 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 $\Delta$ 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 $A_i \cong \text{Mat}_{n_i \times n_i}(D_i)$. 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 $K[G] \cong \bigoplus_i \text{Mat}_{n_i \times n_i}(D_i)$ where each $D_i$ is a skew field with centre $K_i$. Then by [CR81, (7.22)] for each $i$ there exists $m_i \in \mathbb{Z}_{>1}$ 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 \( F \). Let \( \mathcal{O} = \mathcal{O}_F \) and fix a choice \( \Delta \) 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 \( \text{Mat}_{n \times n}(D) \). Let \( \mathcal{M} \) and \( N \) be \( \mathcal{M} \)-lattices. We require an algorithm that either computes an \( \mathcal{M} \)-lattice isomorphism \( f : \mathcal{M} \to N \) or determines that no such isomorphism exists. The basic idea is to reduce this to an analogous problem for certain \( \Delta \)-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 \( \Delta \)-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 \( a \) be a fractional right \( \Delta \)-ideal, that is, a full right \( \Delta \)-lattice in \( D \). The left and right orders of \( a \) are defined to be

\[
\mathcal{O}_l(a) := \{ x \in D \mid xa \subseteq a \} \quad \text{and} \quad \mathcal{O}_r(a) := \{ x \in D \mid ax \subseteq a \},
\]

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

\[
a^{-1} := \{ x \in D \mid axa \subseteq a \},
\]

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

\[
a^{-1}a = \Delta, \quad aa^{-1} = \Delta', \quad (a^{-1})^{-1} = a.
\]

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

\[
\mathcal{M}_{a,n} := \begin{pmatrix}
\Delta & \ldots & \Delta & a^{-1} \\
\vdots & \ddots & \vdots & \vdots \\
\Delta & \ldots & \Delta & a^{-1} \\
a & \ldots & a & \Delta'
\end{pmatrix}
\]

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

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

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 \( \mathcal{M}_{a,n} \) for some right fractional \( \Delta \)-ideal \( a \).

6.2. Reducing from \( \mathcal{M} \)-lattices to \( \Delta \)-lattices. We assume that \( n \geq 2 \) and that \( \mathcal{M} \) is of the form \( \mathcal{M}_{a,n} \) for some right fractional \( \Delta \)-ideal \( a \). By [Rei03, (21.7)] \( \mathcal{M} \) is Morita equivalent to \( \Delta \), that is, the category of left \( \mathcal{M} \)-modules is equivalent to the category of left \( \Delta \)-modules. We now make this equivalence partially explicit in the case of lattices by generalising [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 \( 1 \leq i, j \leq n \) let \( e_{ij} \in \text{Mat}_{n \times n}(D) \) 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 $O_l(a^{-1}) = \Delta$, we see that $e_{11}M$ (i.e. the ‘first row’ of $M$) is a $\Delta$-lattice. Thus the assignment $M \mapsto e_{11}M$ induces a functor between $\text{M}$-lattices and $\Delta$-lattices, where the corresponding map on morphisms is given by restriction,

$$\text{Hom}_{\text{M}}(M, N) \rightarrow \text{Hom}_{\Delta}(e_{11}M, e_{11}N), \ f \mapsto f|_{e_{11}M}.$$ 

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 $\text{M}$-lattices. Then $M \cong N$ as $\text{M}$-lattices if and only if $e_{11}M \cong e_{11}N$ as $\Delta$-lattices. Moreover, given an isomorphism $g : e_{11}M \rightarrow e_{11}N$ of $\Delta$-lattices, we can explicitly construct an isomorphism $f : M \rightarrow N$ of $\text{M}$-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 $f : M \rightarrow N$ is an isomorphism of $\text{M}$-lattices. Then it is clear that restriction $f|_{e_{11}M} : e_{11}M \rightarrow e_{11}N$ is an isomorphism of $\Delta$-lattices.

Suppose conversely that we are given an isomorphism $g : e_{11}M \rightarrow e_{11}N$ of $\Delta$-lattices. Let $g' : e_{11}FM \rightarrow e_{11}FN$ be the unique extension of $g$ to an isomorphism of $\text{D}$-modules, which exists by Lemma 2.2(a). For $i = 1, \ldots, n$ we define

$$f'_i : e_{ii}FM \rightarrow e_{ii}FN, \quad e_{ii}x \mapsto e_{ii}g'(e_{ii}x) = e_{ii}e_{ii}g'(e_{11}e_{ii}e_{ii}x),$$

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

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

$$f'_i(e_{ii}M) = e_{ii}e_{ii}g'(e_{11}e_{ii}e_{ii}M) \subseteq e_{ii}e_{ii}g'(e_{11}M) = e_{ii}e_{ii}e_{11}N \subseteq e_{ii}N.$$

Similarly, we have

$$e_{ii}N = e_{ii}e_{11}e_{ii}N \subseteq e_{ii}e_{ii}N = e_{ii}g'(e_{11}M) = e_{ii}g'(e_{11}e_{ii}M) \subseteq e_{ii}g'(e_{11}M) = f'_i(e_{ii}M).$$

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

Now consider the case $i = n$. In the following we use that $e_{nn}M$ (i.e. the ‘last row’ of $\text{M}$) is a left $\Delta'$-lattice and that $\text{a}a^{-1} = \Delta'$. Since $a^{-1}e_{nn} \subseteq \text{M}$ and $e_{nn}a \subseteq \text{M}$ we have

$$f'_n(e_{nn}M) = e_{nn}g'(e_{11}M) = e_{nn}g'(e_{11}e_{nn}M) = e_{nn}g'(e_{11}a^{-1}e_{11}M) \subseteq e_{nn}g'(e_{11}aM) = e_{nn}e_{11}aN = e_{nn}e_{nn}aN \subseteq e_{nn}N.$$

Similarly, we have

$$e_{nn}N = e_{nn}e_{11}e_{nn}N = e_{nn}e_{11}a^{-1}e_{nn}N \subseteq e_{nn}e_{11}aN = e_{nn}g'(e_{11}aM) = e_{nn}g'(e_{nn}e_{nn}aN) \subseteq e_{nn}g'(e_{nn}M) = f'_n(e_{nn}M).$$

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 $f_i : e_{ii}N \rightarrow e_{ii}M$. 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

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

and note that this is a homomorphism of $\text{M}$-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 $e_{i1}g'(e_{i1}x) = f_i(e_{i1}x) = 0$ for each $i$. Multiplying on the left by $e_{i1}$ gives
\[ 0 = e_{i1}e_{i1}g'(e_{i1}x) = e_{i1}g'(e_{i1}x) = g'(e_{i1}x). \]
Since $g'$ is injective this implies that $e_{i1}x = 0$, and multiplying on the left by $e_{i1}$ then gives $e_{i1}x = e_{i}x = 0$. Hence $x = e_{i1}x + \cdots + e_{ni}x = 0$. \hfill \qed 

Remark 6.3. If $\mathcal{M} = \text{Mat}_{n\times n}(\Delta)$ then the construction given in the proof of Proposition 6.2 simplifies considerably (also see [Lam99, §6.1]) for a discussion of the explicit Morita equivalence of $\mathcal{M}$ and $\Delta$ in this case). Moreover, if $\mathcal{M}$ is a principal fractional right ideal of $\Delta$ (i.e. $\mathcal{M} = \xi \Delta$ for some $\xi \in D^\times$) then there exists $S \in \text{GL}_n(D)$ such that $SM_{\mathcal{M},n}S^{-1} = \text{Mat}_{n\times n}(\Delta)$ 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 generalised to the case $D \neq F$ by using [CR87, (49.32)])

6.3. Noncommutative Steinitz form for $\Delta$-lattices. Let $M$ be a $\Delta$-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 $\Delta$-ideal $b$ such that
\[ M = \Delta m_1 + \cdots + \Delta m_{r-1} + bm_r. \]
Such a decomposition is known as noncommutative Steinitz form of $M$. An algorithm for computing it is described in [BJ11, §5.3, §5.4]. Moreover, $M$ is a locally free $\Delta$-lattice by [Rei03, (18.10)]. Thus if $\Delta$ has the locally free cancellation property of (H2)(b) (described in §5.3) then $r$ and the isomorphism class of $b$ uniquely determine the isomorphism class of $M$. We therefore have the following result.

Lemma 6.4. Let $M$ and $N$ be two $\Delta$-lattices of equal rank $r \in \mathbb{Z}_{\geq 1}$. Let $b$ and $c$ be left fractional $\Delta$-ideals such that
\[ M \cong \Delta^{(r-1)} \oplus b \quad \text{and} \quad N \cong \Delta^{(r-1)} \oplus c. \]
If $b \cong c$ as left fractional $\Delta$-ideals, then $M$ and $N$ are isomorphic. Moreover, if $\Delta$ 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 $f : \mathcal{M}_iX \rightarrow \mathcal{M}_iY$ of $\mathcal{M}_i$-lattices or determines that no such isomorphism exists.

(i) Using (H1) we can suppose without loss of generality that $A_i = \text{Mat}_{n_i \times n_i}(D_i)$ for some $n_i \in \mathbb{Z}_{\geq 1}$ and some skew field $D_i$ with centre $K_i$. 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 $\Delta$ in $D$. Set
\[ M := \mathcal{M}_iX = e_{i1}\mathcal{M}_iX \quad \text{and} \quad N := \mathcal{M}_iY = e_{i1}\mathcal{M}_iY, \]
and skip to step (iv) below.

(iii) Suppose $n \geq 2$. Fix any maximal $\mathcal{O}$-order $\Delta$ in $D$. Compute $S \in \text{GL}_n(D)$ 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 $M \rightarrow N$ of $\mathcal{M}_i'$-lattices or determining that no such isomorphism exists.
Let $\Lambda$ be any order in $\mathbb{Q}[Q_{32}]$. Let $A$ be any order in $A$ and let $M$ be a maximal order such that $\Lambda \subseteq M \subseteq A$. Then $\text{[Swa83, Theorem II]}$ shows that $M$ 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 $M_i$ in a component $A_i$ of case (i) does have the locally free cancellation property. The remaining $M_i$ in components $A_i$ of case (ii) do not have the locally free cancellation property. However, if $X$ and $Y$ are $\Lambda$-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 $MX$ and $MY$ are isomorphic as $M$-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 $b \cong c$ as fractional left $\Delta$-ideals in step (v), then the algorithm will go on to construct an isomorphism $M_iX \to M_iY$ of $M_i$-lattices, whether or not $\Delta$ has the locally free cancellation property. However, if $b \not\cong c$ and $\Delta$ does not have the locally free cancellation property, then it is not possible to conclude that $e_{11}M \not\cong e_{11}N$ and thus the algorithm cannot determine whether $M_iX$ and $M_iY$ are isomorphic as $M_i$-lattices.

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

$$e_{11}M = \Delta m_1 \oplus \cdots \oplus \Delta m_{r-1} \oplus bm_r \quad \text{and} \quad e_{11}N = \Delta n_1 \oplus \cdots \oplus \Delta n_{s-1} \oplus cn_s.$$  

If $r \neq s$ then the algorithm terminates with the conclusion that $M_iX$ and $M_iY$ are not isomorphic as $M_i$-lattices.

(v) Use (H2)(a) to check whether $b \cong c$ as fractional left $\Delta$-ideals, and if so, return $\xi \in D$ such that $b = c\xi$. Otherwise, (H2)(b) shows that $e_{11}M$ and $e_{11}N$ are not isomorphic as $\Delta$-lattices and so the algorithm terminates with the conclusion that $M_iX$ and $M_iY$ are not isomorphic as $M_i$-lattices. (In the case $n = 1$ this is true because $e_{11}M = M_iX$ and $e_{11}N = M_iY$ 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 $\Delta$-lattices.

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

Remark 6.5. If $n = 1$ then $\Delta$ is uniquely determined by $M_i$. Moreover, the choice of $M_i$ may be limited by the requirement that $\Lambda \subseteq \oplus_i M_i$. However, if $n \geq 2$ then we can make any choice of $\Delta$.  

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 $M_i = \Delta$ in the notation above. Then the problem of determining whether $e_{11}N \cong e_{11}M$ as $\Delta$-lattices is equivalent to checking whether $b \cong c$ as fractional left $\Delta$-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].
7. Saturation of Lattices and Computation of Homomorphism Groups

We describe how to compute homomorphism groups between lattices over orders and along the way 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. Let $M$ be an $R$-lattice and let $N$ be a sublattice of $M$. We shall 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.** Let $R$ be an integral domain with field of fractions $K$. Let $M$ be an $R$-lattice and let $N$ be a sublattice of $M$. Then the saturation of $N$ in $M$ is $KN \cap M$.

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

7.2. Computation of Saturations of Lattices over Rings of Integers. Let $K$ be a number field with ring of integers $O = \mathcal{O}_K$. We now give a result that can be used to compute saturations of $O$-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 $O = \mathbb{Z}$, 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 $O$-lattices with pseudo-bases $((\alpha_1)_{1 \leq i \leq m}, (\alpha_i)_{1 \leq i \leq m})$ and $((\beta_1)_{1 \leq i \leq n}, (\beta_i)_{1 \leq i \leq n})$, respectively. Suppose that $N$ is a sublattice of $M$ (so $n \leq m$). Let $A \in \text{Mat}_{m \times n}(K)$ be the unique matrix satisfying

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

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

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

Then $((\beta_i^{-1})_{m-n+1 \leq i \leq m}, (\omega_i)_{m-n+1 \leq i \leq m})$ is a pseudo-basis 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 $U_{i,j} \in \alpha_i^{-1}b_j^{-1}$.
(b) We have $\prod_{i=1}^n \alpha_i^{-1} = \det(U) \prod_{i=1}^m b_j$.
(c) The matrix $H = A^tU$ is of the following form

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

where the first $m-n$ columns are zero (we will write this in abbreviated form as $H = A^tU = (0 | \bar{H})$, where $\bar{H} \in \text{Mat}_{n \times m}(K)$).
We first show that \(((b_i^{-1})_{1 \leq i \leq m}, (\omega_i)_{1 \leq i \leq m})\) is a pseudo-basis of \(M\). By [Coh00, 1.4.2] it suffices to show that
\[
\prod_{i=1}^{m} a_i = \det(U^{-t}) \prod_{i=1}^{m} b_i^{-1} \quad \text{and} \quad (U^{-t})_{i,j} \in a_i(b_j^{-1})^{-1} = a_i b_j \text{ for } 1 \leq i, j \leq m.
\]
The first claim follows directly from property (b). The second claim is equivalent to \((U^{-1})_{i,j} \in a_j b_i\) for \(1 \leq i, j \leq m\), which can be shown by expressing \((U^{-1})_{i,j}\) in terms of the adjugate matrix and using properties (a) and (b).

Let \(S = \bigoplus_{i=m-n+1}^{m} b_i^{-1}\omega_i\). Then \(M/S \cong \bigoplus_{i=m-n}^{m} b_i^{-1}\omega_i\) 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
\[
(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_m)A = (\alpha_1, \ldots, \alpha_m)U^{-t}H^t
\]
\[
= (\omega_1, \ldots, \omega_m)H^t = (\omega_1, \ldots, \omega_m) \begin{pmatrix} 0 \\ \hat{H}^t \end{pmatrix}
\]
\[
= (\omega_{m-n+1}, \ldots, \omega_m) \hat{H}^t.
\]
By our hypotheses, we have \(b_i \sum_{j=1}^{m} \alpha_j A_{ji} = b_i \beta_i \subseteq N \subseteq M = \bigoplus_{j=1}^{m} a_j \alpha_j\) for \(1 \leq i \leq n\). Hence for \(1 \leq i \leq n\) and \(1 \leq j \leq m\) we have \(b_i A_{ji} \subseteq a_j\), that is, \(A_{ji} \in a_j b_i^{-1}\). Together with property (a), this shows that for \(1 \leq i, j \leq n\), we have
\[
\hat{H}_{i,j} = H_{i,m-n+j} = \sum_{k=1}^{m} (A^t)_{i,k} U_{k,m-n+j} = \sum_{k=1}^{m} A_{k,i} U_{k,m-n+j}
\]
\[
\in \sum_{k=1}^{m} a_k b_i^{-1} a_k^{-1} h_{m-n+j}^{-1} = b_i^{-1} h_{m-n+j}^{-1}.
\]
In particular, for \(1 \leq j \leq n\) we have
\[
b_j \beta_j = b_j \left( \sum_{i=1}^{n} (\hat{H}^t)_{i,j} \cdot \omega_{m-n+i} \right) \subseteq b_j \sum_{i=1}^{n} b_j^{-1} h_{m-n+i}^{-1} \omega_{m-n+i} = b_j^{-1} \omega_{m-n+i} = S.
\]
This shows that \(N = \sum_{j=1}^{n} b_j \beta_j \subseteq S\), as required. \(\square\)

**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 \(\Lambda\) be an \(\mathcal{O}\)-order in \(A\). We give an algorithm that takes two \(\Lambda\)-lattices \(X\) and \(Y\) and returns the \(\Lambda\)-lattice \(\text{Hom}_\Lambda(X, Y)\). 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,

\[
\text{Hom}_\Lambda(X, Y) = \{ f|_X^Y \mid f \in \text{Hom}_A(V, W) \text{ such that } f(X) \subseteq Y \},
\]
where \(f|_X^Y\) denotes the restriction of \(f\) to a map \(f: X \to Y\). Note that this follows from the fact that every element in \(\text{Hom}_\Lambda(X, Y)\) extends uniquely to an element in \(\text{Hom}_A(V, W)\) (see Lemma 2.2). Since there exists an algorithm for computing a \(K\)-basis of \(\text{Hom}_A(V, W)\) 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 pseudo-bases, that is,

\[
X = a_1 \alpha_1 \oplus a_2 \alpha_2 \oplus \cdots \oplus a_m \alpha_m \quad \text{and} \quad Y = b_1 \beta_1 \oplus b_2 \beta_2 \oplus \cdots \oplus b_n \beta_n,
\]
with $\alpha_i \in V, \beta_j \in W$ and $a_i, b_j$ fractional ideals of $K$. Since $(\alpha_i)_{1 \leq i \leq m}$ and $(\beta_j)_{1 \leq j \leq n}$ are $K$-bases of $V$ and $W$ respectively, we use them to identify $\text{Hom}_K(V, W)$ with $\text{Mat}_{m \times n}(K)$ (we treat vectors as row vectors). Under this identification we have

$$
\text{Hom}_\mathcal{O}(X, Y) = \bigoplus_{1 \leq i \leq n} a_i^{-1}b_j e_{ij} = \begin{pmatrix}
(a_1^{-1}b_1 & \ldots & a_1^{-1}b_n) \\
\vdots & \ddots & \vdots \\
a_m^{-1}b_1 & \ldots & a_m^{-1}b_n
\end{pmatrix} \subseteq \text{Mat}_{m \times n}(K),
$$

where $e_{ij} \in \text{Mat}_{m \times n}(K)$ 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 $\text{Hom}_A(X, Y) = \text{Hom}_A(V, W) \cap \text{Hom}_\mathcal{O}(X, Y)$.

(b) Let $B_1, \ldots, B_r$ be a $K$-basis of $\text{Hom}_A(V, W)$ with $B_i \in \text{Hom}_\mathcal{O}(X, Y)$. Then $\text{Hom}_A(X, Y) = K(\langle B_1, \ldots, B_r \rangle_\mathcal{O}) \cap \text{Hom}_\mathcal{O}(X, Y)$.

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

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

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

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

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

Let $G$ be any finite group. The algorithm above has been implemented for $\mathbb{Z}[G]$-lattices $M, N$ contained in any finitely generated $\mathbb{Q}[G]$-modules $V$ and $W$. The MAGMA [BCP97] code is available on the webpage of the first named author.

8. Isomorphism testing for localised 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 $\Lambda$ 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 $\Lambda$-lattices of equal $\mathcal{O}$-rank $n$ and let $p$ be a maximal ideal of $\mathcal{O}$. We give three algorithms that determine whether or not the localizations $X_p$ and $Y_p$ are isomorphic as $\Lambda_p$-lattices. The first algorithm makes use of reduced lattices and does not give an isomorphism if it exists. By contrast, the second algorithm, which uses the results of §7, will find an isomorphism if it exists. The third algorithm is a fast probabilistic algorithm of Monte Carlo type. Variants of these results are contained in the first named author’s Ph.D. thesis [Hof16, §12], but we caution that here the subscript $p$ denotes localization, whereas in ibid. it denotes completion. Finally, we remark on the special case of testing for local freeness.

8.1. Using reduced lattices.

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

(a) $X_p$ and $Y_p$ are isomorphic as $\Lambda_p$-lattices.

(b) $X/p^kX$ and $Y/p^kY$ are isomorphic as $\Lambda/p^k\Lambda$-modules.
Theorem 7.3. Let $X, Y$ be as in Proposition 7.1 and assume that $X$ and $Y$ are isomorphic as $\mathcal{O}$-modules.

\[ X \oplus \cdots \oplus X \cong Y \oplus \cdots \oplus Y. \]

Proof. By Proposition 7.1, $X_p$ and $Y_p$ are isomorphic as $\Lambda_p$-modules if and only if there exist $\Lambda_p$-bases of $X_p$ and $Y_p$ such that 

\[ \det_{\mathcal{O}/p}(a_1A_1 + \cdots + a_rA_r) \neq 0. \]

The claim now follows since reduction mod $p$ commutes with taking determinants and an element $a \in \mathcal{O}/p$ is a unit if and only if $(a \mod p)$ is a unit in $\mathcal{O}/p$. \qed

Lemma 8.2. Let $k$ be as in Proposition 8.1 and let $A_1, \ldots, A_r \in \operatorname{Mat}_{n \times n}(\mathcal{O}/p)$ be an $\mathcal{O}/p$-spanning set of $\operatorname{Hom}_{\mathcal{O}/p}(X/p^kX, Y/p^kY)$. Then $X_p$ and $Y_p$ are isomorphic as $\Lambda_p$-modules if and only if there exist elements $a_1, \ldots, a_r \in \mathcal{O}/p$ with 

\[ \det_{\mathcal{O}/p}(a_1A_1 + \cdots + a_rA_r) \neq 0. \]

Proof. By Proposition 8.1, $X_p$ and $Y_p$ are isomorphic as $\Lambda_p$-modules if and only if there exist elements $a_1, \ldots, a_r \in \mathcal{O}/p$ such that 

\[ a_1A_1 + \cdots + a_rA_r \text{ is invertible, or equivalently, } \det_{\mathcal{O}/p}(a_1A_1 + \cdots + a_rA_r) \neq 0. \]

The claim now follows since reduction mod $p$ commutes with taking determinants and an element $a \in \mathcal{O}/p$ is a unit if and only if $(a \mod p)$ is a unit in $\mathcal{O}/p$. \qed

To test whether $X_p$ and $Y_p$ are isomorphic as $\Lambda_p$-modules, we can thus proceed as follows:

\begin{enumerate}
  \item Use an algorithm of Friedrichs [Fri00, (2.16)] to compute $k_0$. Set $k := k_0 + 1$.
  \item Construct the $\mathcal{O}/p$-linear map $h$ of (8) as a matrix.
  \item Compute an $\mathcal{O}/p$-spanning set $A_1, \ldots, A_r$ of $\ker(h)$.
  \item For every tuple $(a_1, \ldots, a_r) \in \mathcal{O}/p$ test whether 

    \[ \det_{\mathcal{O}/p}(a_1A_1 + \cdots + a_rA_r) \neq 0. \]

The $\Lambda_p$-lattices $X_p$ and $Y_p$ 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 $\operatorname{Hom}_{\mathcal{O}}(X, Y)$. 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 pseudo-bases, that is,

\[ X = a_1\alpha_1 \oplus a_2\alpha_2 \oplus \cdots \oplus a_n\alpha_n \quad \text{and} \quad Y = b_1\beta_1 \oplus b_2\beta_2 \oplus \cdots \oplus b_n\beta_n, \]
with \( \alpha_i \in V, \beta_j \in W \) and \( a_i, b_j \) fractional ideals of \( K \). As in \S7.3, we use the \( K \)-bases \( (\alpha_i)_i, (\beta_j)_j \) to identify homomorphism spaces as subsets of \( \text{Mat}_{n \times n}(K) \). Thus we have

\[
\text{Hom}_A(X, Y) \subseteq \text{Hom}_A(V, W) \subseteq \text{Hom}_K(V, W) = \text{Mat}_{n \times n}(K).
\]

Let \( M \to \overline{M} \) denote the canonical projection map \( \text{Mat}_{n \times n}(\mathcal{O}_p) \to \text{Mat}_{n \times n}(\mathcal{O}/p) \).

**Lemma 8.3.** Suppose \( v_p(a_i) = v_p(b_i) = 0 \) for \( 1 \leq i \leq n \). Then the following hold:

(a) The \( \Lambda_p \)-lattices \( X_p \) and \( Y_p \) are \( \mathcal{O}_p \)-free with \( \mathcal{O}_p \)-bases \( (a_i)_i \) and \( (b_j)_j \), respectively.

(b) We have \( \text{Hom}_{\Lambda_p}(X_p, Y_p) = \text{Mat}_{n \times n}(\mathcal{O}_p) \cap \text{Hom}_A(V, W) \).

(c) There exists a pseudo-basis \( ((\epsilon_i), (A_i))_{1 \leq i \leq r} \) of \( \text{Hom}_A(X, Y) \) with \( v_p(\epsilon_i) = 0 \) and \( A_i \in \text{Mat}_{n \times n}(\mathcal{O}_p) \) for \( 1 \leq i \leq r \).

(d) The matrices \( A_1, \ldots, A_r \) form an \( \mathcal{O}_p \)-basis of \( \text{Hom}_{\Lambda_p}(X_p, Y_p) \).

(e) Let \( B_1, \ldots, B_r \in \text{Mat}_{n \times n}(\mathcal{O}_p) \) be any \( \mathcal{O}_p \)-basis of \( \text{Hom}_{\Lambda_p}(X_p, Y_p) \). The \( \Lambda_p \)-lattices \( X_p \) and \( Y_p \) are isomorphic if and only if there exists a tuple \( (b_1, \ldots, b_r) \in (\mathcal{O}/p)^r \) such that \( \det_{\mathcal{O}/p}(b_1B_1 + \cdots + b_rB_r) \neq 0 \). 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 \( \mathcal{O}_p a_i = \mathcal{O}_p b_i = \mathcal{O}_p \). Thus

\[
X_p = \mathcal{O}_p X = \bigoplus_i \mathcal{O}_p a_i \quad \text{and} \quad Y_p = \mathcal{O}_p Y = \bigoplus_i \mathcal{O}_p b_i.
\]

(b) Note that \( f \in \text{Hom}_A(V, W) \) satisfies \( f \in \text{Hom}_{\Lambda_p}(X_p, Y_p) \) if and only if \( f(X_p) \subseteq Y_p \). By part (a) and the identification (9), this is in turn equivalent to \( f \in \text{Mat}_{n \times n}(\mathcal{O}_p) \).

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

\[
\text{Hom}_A(X, Y) = \text{Hom}_A(V, W) \cap \text{Hom}_\mathcal{O}(X, Y) \subseteq \text{Hom}_\mathcal{O}(X, Y) = \bigoplus_{1 \leq i, j \leq n} a_i^{-1}b_j e_{ij}.
\]

Hence by the assumptions on the coefficient ideals and the identification (9) we have that \( \text{Hom}_A(X, Y) \) is a subset of \( \text{Mat}_{n \times n}(\mathcal{O}_p) \). Let \( ((\epsilon_i), (A_i))_{1 \leq i \leq r} \) be any pseudo-basis of \( \text{Hom}_A(X, Y) \) and let \( \pi \in \mathfrak{p} \setminus \mathfrak{p}^2 \) be any uniformizer. Then

\[
c_i A_i = (\epsilon_i/\pi^{v_p(\epsilon_i)})(\pi^{v_p(\epsilon_i)} A_i) \subseteq \text{Hom}_A(X, Y) \subseteq \text{Mat}_{n \times n}(\mathcal{O}_p).
\]

Since \( c_i/\pi^{v_p(\epsilon_i)} \) has \( \mathfrak{p} \)-adic valuation 0, we thus have that every entry of \( \pi^{v_p(\epsilon_i)} A_i \) has \( \mathfrak{p} \)-adic valuation \( \geq 0 \), that is, \( \pi^{v_p(\epsilon_i)} A_i \in \text{Mat}_{n \times n}(\mathcal{O}_p) \). Moreover, \( ((\epsilon_i/\pi^{v_p(\epsilon_i)}), (\pi^{v_p(\epsilon_i)} A_i))_{1 \leq i \leq r} \) is also a pseudo-basis of \( \text{Hom}_A(X, Y) \). Hence by making the appropriate substitution, we can and do assume without loss of generality that the pseudo-basis \( ((\epsilon_i), (A_i))_{1 \leq i \leq r} \) has the desired properties.

(d) By [Rei03, (3.18)] and the identification of \( \mathcal{O}_p \text{Hom}_A(X, Y) \) with \( \mathcal{O}_p \otimes \mathcal{O} \text{Hom}_A(X, Y) \), we have

\[
\text{Hom}_{\Lambda_p}(X_p, Y_p) = \mathcal{O}_p \text{Hom}_A(X, Y) = \bigoplus_{i=1}^r \mathcal{O}_p c_i A_i = \bigoplus_{i=1}^r \mathcal{O}_p A_i.
\]

(e) The two \( \Lambda_p \)-lattices \( X_p \) and \( Y_p \) are isomorphic if and only if \( \text{Hom}_{\Lambda_p}(X_p, Y_p) \) contains an invertible element. By part (b), \( M \in \text{Hom}_{\Lambda_p}(X_p, Y_p) \) is invertible if and only if \( \det_{\mathcal{O}_p}(M) \in \mathcal{O}_p^\times \). This is in turn equivalent to \( \det_{\mathcal{O}_p}(M) \mod \mathfrak{p} \neq 0 \) in \( \mathcal{O}_p/p\mathcal{O}_p \cong \mathcal{O}/\mathfrak{p} \).

The claim now follows from the observation that \( \det_{\mathcal{O}_p}(M) \mod \mathfrak{p} = \det_{\mathcal{O}/\mathfrak{p}}(\overline{M}) \) together with the hypothesis on \( B_1, \ldots, B_r \).

To test whether \( X_p \) and \( Y_p \) are isomorphic as \( \Lambda_p \)-lattices, and to compute an isomorphism if it exists, we can thus proceed as follows:
\( (i) \) Adjust the pseudo-bases of \( X \) and \( Y \) such that the coefficient ideals have zero \( p \)-adic valuation. For example, if \( \pi \in p \setminus p^2 \) is any uniformizer, then
\[
((\pi^{v_0}(a_i))_{1 \leq i \leq n}, (a_i/\pi^{v_0}(a_i))_{1 \leq i \leq n})
\]
is a pseudo-basis of \( X \) of the required form (similarly for \( Y \)).

\( (ii) \) Compute a pseudo-basis \( ((c_i), (A_i))_{1 \leq i \leq r} \) of \( \text{Hom}_A(X, Y) \) using the algorithm of §7.3 and adjust it such that the coefficient ideals have zero \( p \)-adic valuation (as in the proof of Lemma 8.3(c)).

\( (iii) \) Reduce the matrices \( A_1, \ldots, A_r \) modulo \( p \) to obtain \( \overline{A}_1, \ldots, \overline{A}_r \in \text{Mat}_{n \times n}(\mathcal{O}/p) \). For every tuple \( (a_1, \ldots, a_r) \in \mathcal{O}/p \) test whether \( \det_{\mathcal{O}/p}(a_1\overline{A}_1 + \cdots + a_r\overline{A}_r) \neq 0 \). If there exists such a tuple, then \( X_p \) and \( Y_p \) are isomorphic as \( \Lambda_p \)-lattices and an isomorphism is given by \( a_1A_1 + \cdots + a_rA_r \). Otherwise \( X_p \) and \( Y_p \) are not isomorphic as \( \Lambda_p \)-lattices.

Let \( G \) be any finite group and let \( p \) be a rational prime. The algorithm above has been implemented for \( \mathbb{Z}[G] \)-lattices \( M, N \) contained in any finitely generated \( \mathbb{Q}[G] \)-modules \( V \) and \( W \). The Magma [BCP97] code is available on the webpage of the first named author.

### 8.3. Probabilistic isomorphism testing

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

Let \( A_1, \ldots, A_r \in \text{Mat}_{n \times n}(\mathcal{O}_p) \) be an \( \mathcal{O}_p \)-basis of \( \text{Hom}_{\Lambda_p}(X_p, Y_p) \) as given by Lemma 8.3. Let \( M \mapsto \overline{M} \) denote the canonical projection map \( \text{Mat}_{n \times n}(\mathcal{O}_p) \to \text{Mat}_{n \times n}(\mathcal{O}/p) \). Let \( T_1, \ldots, T_r \) be indeterminates and consider the polynomial
\[
f := \det(T_1\overline{A}_1 + \cdots + T_r\overline{A}_r) \in (\mathcal{O}/p)[T_1, \ldots, T_r],
\]
which is of total degree \( \leq n \).

**Lemma 8.4.** The two \( \Lambda_p \)-lattices \( X_p \) and \( Y_p \) are isomorphic if and only if \( f \) as defined above is not the zero-polynomial.

**Proof.** Suppose that \( X_p \) and \( Y_p \) are isomorphic as \( \Lambda_p \)-lattices. Then by Lemma 8.3(e) there exist \( a_1, \ldots, a_r \in \mathcal{O}/p \) such that \( f(a_1, \ldots, a_r) \neq 0 \) 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 \( F \) of \( \mathcal{O}/p \) and \( b_1, \ldots, b_r \in F \) such that \( f(b_1, \ldots, b_r) \neq 0 \). Let \( S \) be a discrete valuation ring with maximal ideal \( \mathfrak{m} \) such that \( \mathcal{O}_p \subseteq S \) and \( S/\mathfrak{m} \cong F \). Since \( A_1, \ldots, A_r \) is also an \( S \)-basis of \( \text{Hom}_{\Lambda_p}(SX_p, SY_p) \), Lemma 8.3(e) applied to \( SX_p \) and \( SY_p \) shows that \( b_1A_1 + \cdots + b_rA_r \) is an \( S \)-isomorphism \( SX_p \to SY_p \). Hence \( X_p \) and \( Y_p \) are isomorphic as \( \Lambda_p \)-lattices by [CR81, (30.25)]. \( \square \)

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

**Theorem 8.5** (Schwartz–Zippel lemma). Let \( F \) be a finite field. For a non-zero polynomial \( g \in F[T_1, \ldots, T_r] \) of total degree \( n < \#F \) we have
\[
\frac{\#\{ (a_1, \ldots, a_r) \in F^r \mid g(a_1, \ldots, a_r) = 0 \}}{\#F^r} \leq \frac{n}{\#F^r}.
\]
In particular, if \( v_1, \ldots, v_r \in F^r \) are chosen uniformly and \( f(v_i) = 0 \) for \( 1 \leq i \leq r \), then the probability that \( f \) is non-zero is at most \( (n/\#F^r)^r \).
Since \( f = 0 \) in \( \mathbb{F}[T_1, \ldots, T_r] \) is equivalent to \( f = 0 \) in \( \mathbb{F}'[T_1, \ldots, T_r] \) 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. This algorithm is of Monte Carlo type, which means that if it is executed with parameter \( 1 > \varepsilon > 0 \) and returns that \( X_p \) and \( Y_p \) are not isomorphic as \( \Lambda_p \)-lattices, then the probability that \( X_p \) and \( Y_p \) are in fact isomorphic is less than \( \varepsilon \). However, if the algorithm returns that \( X_p \) and \( Y_p \) are isomorphic as \( \Lambda_p \)-lattices, then this is indeed the case. We now describe the algorithm, where \( 1 > \varepsilon > 0 \) is some chosen error bound.

(i) Compute an \( \mathcal{O}_p \)-basis \( A_1, \ldots, A_r \) of \( \text{Hom}_{\Lambda_p}(X_p, Y_p) \) as in §8.2.
(ii) Set \( f := \det(T_1 \overline{A}_1 + \cdots + T_r \overline{A}_r) \in (\mathcal{O}/p)[T_1, \ldots, T_r] \).
(iii) Choose \( l, m \in \mathbb{Z}_{\geq 1} \) such that \( \#(\mathcal{O}/p)^l > n \) and \( (n/\#(\mathcal{O}/p))^m < \varepsilon \). Let \( \mathbb{F} \) be the degree \( l \) extension of \( (\mathcal{O}/p) \).
(iv) Choose \( v_1, \ldots, v_m \in \mathbb{F}^r \) uniformly distributed. If \( f(v_i) \neq 0 \) for some \( 1 \leq i \leq m \), return true. If not, return false.

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

Let \( G \) be any finite group and let \( p \) be a rational prime. The algorithm above has been implemented for \( \mathbb{Z}[G] \)-lattices \( M, N \) contained in any finitely generated \( \mathbb{Q}[G] \)-modules \( V \) and \( W \). The MAGMA [BCP97] code is available on the webpage of the first named author.

8.4. Local freeness. An important special case is that in which we wish to check whether \( X_p \) and \( Y_p \) are free as \( \Lambda_p \)-lattices. For example, in the case \( Y = \Lambda^{(k)} \) for some \( k \in \mathbb{Z}_{\geq 1} \), the problem is reduced to testing whether \( X_p \) is free of rank \( k \) over \( \Lambda_p \). An algorithm for computing a \( \Lambda_p \)-basis (and thus for checking freeness over \( \Lambda_p \)) is given by Bley and Wilson in [BW09, §4.2]. The basic idea is to reduce modulo \( p \) and then reduce again modulo the Jacobson radical of \( \Lambda_p/p\Lambda_p \), find a basis over the resulting associative algebra over a finite field, and then lift this basis using Nakayama's lemma (twice). This method is much faster than the others presented in this section since it does not require an expensive search step. We also remark that if one of \( X_p \) and \( Y_p \) is free over \( \Lambda_p \) and the other is not, this algorithm gives a fast way to show that they are not isomorphic as \( \Lambda_p \)-lattices.

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 \( \Lambda \)-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 \( \Omega_X \) and \( \Omega_Y \) be \( \mathbb{Z} \)-bases of \( M_X \) and \( M_Y \), respectively. Denote by \( M_X, M_Y \in \text{Mat}_{d \times d}(\mathbb{Z}) \) basis matrices of \( X \) and \( Y \) with respect to \( \Omega_X \) and \( \Omega_Y \). Now if
$h : \mathcal{M}X \to \mathcal{M}Y$ is any \( \mathbb{Z} \)-linear map with basis matrix \( M \) with respect to \( \Omega_X \) and \( \Omega_Y \), then \( h(X) \subseteq Y \) if and only if \( M_X M_Y^{-1} \in \text{Mat}_{d \times d}(\mathbb{Z}) \). 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

\begin{equation}
\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.
\end{equation}

From the previous steps of Algorithm 4.1, we have isomorphisms \( f_i : \mathcal{M}_iX \to \mathcal{M}_iY \) of \( \mathcal{M}_i \)-lattices and finite subsets \( U_i \subseteq \text{Aut}_{M_i}(\mathcal{M}_iY) \) 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 \( \Omega_X \) and \( \Omega_Y \) of \( \mathcal{M}X \) and \( \mathcal{M}Y \) adapted to the decompositions in (10). For isomorphisms \( f_i : \mathcal{M}_iX \to \mathcal{M}_iY \) the matrix representing \( \sum_{i=1}^r f_i \) is a block matrix of the form \( \text{diag}(M(f_1), \ldots, M(f_r)) \) with \( M(f_i) \in \text{Mat}_{d_i \times d_i}(\mathbb{Z}) \). Similarly, for automorphisms \( g_i : \mathcal{M}_iY \to \mathcal{M}_iY \) the matrix representing \( \sum_{i=1}^r g_i \) is a block diagonal matrix of the form \( \text{diag}(M(g_1), \ldots, M(g_r)) \) with \( M(g_i) \in \text{GL}_{d_i}(\mathbb{Z}) \). Hence with respect to \( \Omega_X \) and \( \Omega_Y \), the morphism \( h := \sum_{i=1}^r g_i \circ f_i \) is given by

\[ M = \text{diag}(M(g_1)M(f_1), \ldots, M(g_r)M(f_r)). \]

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

\[
\begin{pmatrix}
M_X^{(1)} & \cdots & 0 \\
0 & M_X^{(r)} & \ddots \\
0 & 0 & \ddots & 0 \\
M_Y^{(1)} & \cdots & 0 \\
\end{pmatrix}
\begin{pmatrix}
M(g_1)M(f_1) & \cdots & 0 \\
0 & M(g_r)M(f_r) & \ddots \\
0 & 0 & \ddots & 0 \\
M_Y^{(1)} & \cdots & 0 \\
\end{pmatrix}
\begin{pmatrix}
M_Y^{(1)} & \cdots & 0 \\
0 & M_Y^{(r)} & \ddots \\
0 & 0 & \ddots & 0 \\
M_Y^{(1)} & \cdots & 0 \\
\end{pmatrix},
\]

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

\[
\begin{pmatrix}
M_X^{(1)}M(g_1)M(f_1)M_Y^{(1)} & \cdots & 0 \\
0 & M_X^{(r)}M(g_r)M(f_r)M_Y^{(r)} & \ddots \\
0 & 0 & \ddots & 0 \\
M_X^{(1)}M(g_1)M(f_1)M_Y^{(1)} & \cdots & 0 \\
\end{pmatrix},
\]

we see that the \( i \)th 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

\[ M_X^{(1)}M(g_1)M(f_1)M_Y^{(1)} \notin \text{Mat}_{d_1 \times d_1}(\mathbb{Z}), \]

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 centre of the simple algebra \( A_i \). For each \( i \) there is an isomorphism \( A_i \cong \text{Mat}_{n_i \times n_i}(D_i) \) of \( \mathbb{Q} \)-algebras, where \( D_i \) is a skew field with centre \( K_i \).

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) \( G = \mathbb{F}_q \times \mathbb{F}_q^x \), 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 non-linear 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 locally free \( \mathbb{Z}[G] \)-lattices 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 tamely ramified Galois extensions \( K/Q \) with \( \text{Gal}(K/Q) \cong G \). We note that it is straightforward to realise these lattices as lattices in \( \mathbb{Q}[G] \) by finding a normal basis generator of \( K/Q \), which can be done in several ways; for example, one can use the algorithm of Girstmair [Gr99]. Moreover, as discussed below, these lattices are always locally free.

10.1. \textbf{Galois }\( G \)-\textbf{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 \( (L, \varphi) \) consisting of a Galois extension \( L/K \) together with a group isomorphism \( \varphi : G \to \text{Gal}(L/K) \). 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 \( O_L \) is a \( \text{Gal}(L/K) \)-invariant finitely generated torsion-free \( O_K \)-module, the pair \( (O_L, \varphi) \) uniquely defines a \( O_K[G] \)-lattice in \( L \). It is straightforward to see that if \( (O_L, \varphi) \) is free (resp. stably free, locally free) then \( (O_L, \psi) \) is also free (resp. stably free, locally free) for any choice of isomorphism \( \psi : G \to \text{Gal}(L/K) \).

Henceforth assume that \( L/K \) is (at most) tamely ramified. Then it is well-known that \( (O_L, \varphi) \) is a locally free \( O_K[G] \)-lattice of rank 1 (see [Noe32], [Fr83, I, §3] or [Kaw86]). Let \( LF_1(O_K[G]) \) denote the set of isomorphism classes of locally free \( O_K[G] \)-lattices of rank 1 and let \( [O_L^\varphi] \in LF_1(O_K[G]) \) denote the isomorphism class of \( (O_L, \varphi) \). An automorphism \( \theta \in \text{Aut}(G) \) induces an action on \( LF_1(O_K[G]) \) such that in particular \( \theta : [O_L^\varphi] = [O_L^{\varphi \theta}] \).

We define
\[
\{[O_L] \} := \{[O_L^{\varphi}] \in LF_1(O_K[G]) \mid \psi : G \to \text{Gal}(L/K) \text{ is an isomorphism}\}.
\]

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

10.2. \textbf{Rings of integers of }\( Q_8 \times C_2 \)-\textbf{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 [Sw83] showed 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 \( C_1, C_2, C_3, C_4 \), where \( C_1 \) 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 \( C_2, C_3 \) and \( C_4 \) 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 \( 1 \leq i \leq 4 \), there exist
infinitely many $G$-extensions $(L, \varphi)$ of $\mathbb{Q}$ with $[O_L^G] = C_i$. The group of automorphisms $\text{Aut}(G)$ has order 192 and the quotient group of outer automorphisms $\text{Out}(G)$ 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 $\text{Aut}(G)$ on $\{C_1, C_2, C_3, C_4\}$ has two orbits, namely $\{C_1\}$ and $\{C_2, C_3, C_4\}$.

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 $\text{Gal}(N/\mathbb{Q}) \cong Q_8$ and fix a choice of isomorphism $\varphi: Q_8 \to \text{Gal}(N/\mathbb{Q})$. 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

\begin{equation}
\text{Gal}(N(\sqrt{d})/\mathbb{Q}) = \text{Gal}(N/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}).
\end{equation}

Moreover, since $\text{Aut}(C_2)$ is trivial there is a unique isomorphism $\theta_d: C_2 \to \text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.

Using (11) we define an isomorphism $\varphi_d: Q_8 \times C_2 \to \text{Gal}(N(\sqrt{d})/\mathbb{Q})$ by $\varphi_d = \varphi \times \theta_d$ (this is the unique isomorphism whose restriction back to the first factor recovers $\varphi$). Let $[O_{N(\sqrt{d})}]$ denote the $\mathbb{Z}[G]$-isomorphism class of $(O_{N(\sqrt{d})}, \varphi_d)$. It is interesting to compare such isomorphism classes as $d$ varies while keeping $N$ and $\varphi$ fixed.

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

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

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

\begin{enumerate}
    \item $C_1 = [O_{N_1(\sqrt{5})}] = [O_{N_1(\sqrt{227})}]$;
    \item $C_2 = [O_{N_1(\sqrt{7})}]$;
    \item $C_3 = [O_{N_1(\sqrt{15})}] = [O_{N_1(\sqrt{73})}] = [O_{N_1(\sqrt{89})}]$;
    \item $C_4 = [O_{N_1(\sqrt{83})}]$.
\end{enumerate}

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 $C_2, C_3$ and $C_4$ 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 $\text{Cl}(\mathbb{Z}[G])$. The first method was to use an algorithm of Bley and Wilson [BW09] that solves the discrete logarithm problem in $\text{Cl}(\mathbb{Z}[G])$. 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 $\text{Cl}(\mathbb{Z}[G])$ 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 $\text{RootNumber}$ to show that these root numbers are 1 in all the cases above, which implies that the classes in $\text{Cl}(\mathbb{Z}[G])$ 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 \((L, \varphi)\) be a \( G \)-extension of \( \mathbb{Q} \). Then the BassCancellation 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 \( \varphi \)). 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 \( \text{Gal}(L/\mathbb{Q}) \cong G \) and \( |\text{Disc}(\mathcal{O}_L)| \leq 10^{40} \). (Note that the fields considered in the previous paragraph all satisfy \( |\text{Disc}(\mathcal{O}_L)| \geq 10^{64} \) because \( |\text{Disc}(\mathcal{O}_L)| \geq 10^{62} \).) Since any such field \( L \) is a tamely ramified quadratic extension of a tamely ramified Galois extension \( L_0/\mathbb{Q} \) with \( \text{Gal}(L_0/\mathbb{Q}) \cong Q_8 \) and \( |\text{Disc}(\mathcal{O}_{L_0})| \leq 10^{20} \), we first used algorithms based on class field theory provided by Fieker in [Fie01] 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 \( \varphi : G \to \text{Gal}(L/\mathbb{Q}) \), we only determine whether \([\mathcal{O}_L]_G\) lies in \( C_1 \), in \( C_2 \cup C_3 \cup C_4 \), 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 \( \mathbb{Z}[\text{Gal}(L/\mathbb{Q})] \). 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

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

and discriminant

\[
94869706773115698998939510744199462890625 = 3^{12} \cdot 5^{12} \cdot 11^{12} \cdot 13^{12}.
\]

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 \( \text{Gal}(L/\mathbb{Q}) \cong G \) and that \( \mathcal{O}_L \) is stably free but not free over \( \mathbb{Z}[\text{Gal}(L/\mathbb{Q})] \) (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 \((L, \varphi)\) be a tamely ramified \( G \)-extension of \( K \) and let \( a \) 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 \( \varphi \)). Then \((a, \varphi)\) uniquely defines an \( \mathcal{O}_K[G] \)-lattice in \( L \). Since \( L/K \) is tamely ramified, \((a, \varphi)\) is locally free and the observations made in §10.1 also apply in this setting. For a maximal ideal \( p \) of \( \mathcal{O}_K \) decomposing as \( p\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e \) we set \( \psi(p) = \mathfrak{P}_1 \cdots \mathfrak{P}_g \). We have the following classification.

- The ideal \( \psi(p) \) is ambiguous and the set \( \{\psi(p) \mid p \text{ a maximal ideal of } \mathcal{O}_K\} \) is a free \( \mathbb{Z} \)-basis of the abelian group of ambiguous ideals of \( \mathcal{O}_L \).
- Every ambiguous ideal \( a \) of \( \mathcal{O}_L \) can be uniquely written in the form \( a = a_0 b \), with \( b \) an ideal of \( \mathcal{O}_K \) and

\[
a_0 = \psi(p_1)^{a_1} \cdots \psi(p_g)^{a_g}, \quad 0 \leq a_i < e_i,
\]
where $e_i > 1$ is the ramification index of a maximal ideal of $\mathcal{O}_L$ dividing $p_i$. The ideal $a_0$ 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 $a_0b$ with $a_0$ primitive and $b$ an ideal of $\mathbb{Z}$ is isomorphic to $a_0$ as a $\mathbb{Z}[\text{Gal}(L/\mathbb{Q})]$-module. Thus when investigating the possible Galois module structure of ambiguous ideals in this situation, we can restrict to primitive ambiguous ideals.

In the sequel, we extend $\psi$ to all non-zero fractional ideals of $\mathcal{O}_K$ so that if $a_1, \ldots, a_t \in \mathbb{Z}$ and $p_1, \ldots, p_t$ are maximal ideals of $\mathcal{O}_K$ then $\psi(p_1^{a_1} \cdots p_t^{a_t}) = \psi(p_1)^{a_1} \cdots \psi(p_t)^{a_t}$.

10.4. Ambiguous ideals for a fixed $\mathbb{Q}_8 \times C_2$-extension. We now specialise to the case $G = \mathbb{Q}_8 \times C_2$ 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 $\text{Gal}(L_1/\mathbb{Q}) \cong G$. 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 $\mathbb{Z}[\text{Gal}(L_1/\mathbb{Q})]$-lattice. We verified this result with our implementation of Algorithm 4.1 and also investigated the $\mathbb{Z}[\text{Gal}(L_1/\mathbb{Q})]$-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 $\varphi: G \rightarrow \text{Gal}(L_1/\mathbb{Q})$, 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 $\psi(2^2\mathbb{Z})$, respectively.

Now let $L_2 = N_1(\sqrt{221})$. Again, the extension $L_2/\mathbb{Q}$ is Galois with $\text{Gal}(L_2/\mathbb{Q}) \cong G$. 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 $\mathbb{Z}[\text{Gal}(L_2/\mathbb{Q})]$-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 $\varphi: G \rightarrow \text{Gal}(L_2/\mathbb{Q})$, the 1536 = 3 · 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 $\psi(5^217^2\mathbb{Z})$, $\psi(5^2\mathbb{Z})$ and $\psi(7^211^2\mathbb{Z})$ are pairwise non-isomorphic (for a fixed $\varphi$) 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 $\mathcal{O}_{L_1}$.

REFERENCES

[Agb12] A. Agboola, On counting rings of integers as Galois modules, J. Reine Angew. Math. 663 (2012), 1–31.

[AM] A. Agboola and L. R. McCulloh, On the relative Galois module structure of rings of integers in tame extensions, to appear in Algebra and Number Theory.

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

[BCNS15] O. Braun, R. Coulangeon, G. Nebe, and S. Schönnenbeck, Computing in arithmetic groups with Voroool's algorithm, J. Algebra 435 (2015), 263–285.

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

[BE05] W. Bley and W. Endres, Picard groups and refined discrete logarithms, LMS J. Comput. Math. 8 (2005), 1–16.
[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, J. Symbolic Comput. 80 (2017), no. 3, 581–615.

[BGS06] N. P. Byott, C. Greither, and B. Sodaigui, Classes réalisables d'extensions non abéliennes, J. Reine Angew. Math. 601 (2006), 1–27.

[BJ08] W. Bley and H. Johnston, Computing generators of free modules over orders in group algebras, J. Algebra 320 (2008), no. 2, 836–852.

[BJ11] ———, Computing generators of free modules over orders in group algebras II, Math. Comp. 80 (2011), no. 276, 2411–2434.

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

[BS05] N. P. Byott and B. Sodaigui, Realizable Galois module classes for tetrahedral extensions, Compos. Math. 141 (2005), no. 3, 573–582.

[BS13] ———, Realizable Galois module classes over the group ring for non abelian extensions, Ann. Inst. Fourier (Grenoble) 63 (2013), no. 1, 303–371.

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

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

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

[Cou94] J. Cougnard, Un anneau d'entiers stablement libre et non libre, Experiment. Math. 3 (1994), no. 2, 129–136.

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

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

[CR87] ———, Methods of representation theory. Vol. II, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1987, With applications to finite groups and orders, A Wiley-Interscience Publication.

[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.

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

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

[Fie01] C. Fieker, Computing class fields via the Artin map, Math. Comp. 70 (2001), no. 235, 1293–1303 (electronic).

[Fle71] C. R. Fletcher, Euclidean rings, J. London Math. Soc. (2) 4 (1971), 79–82.

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

[Frö67] A. Fröhlich, Local fields, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 1–41.

[Frö83] ———, Galois module structure of algebraic integers, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 1, Springer-Verlag, Berlin, 1983.

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

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

[Hig60] D. G. Higman, On representations of orders over Dedekind domains, Canad. J. Math. 12 (1960), 107–125.

[HM06] E. Hallouin and C. Maire, Cancellation in totally definite quaternion algebras, J. Reine Angew. Math. 595 (2006), 189–213.

[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.
[Joh08] H. Johnston, *Relative Galois module structure of rings of integers of absolutely abelian number fields*, J. Reine Angew. Math. **620** (2008), 85–103.

[Kaw86] F. Kawamoto, *On normal integral bases of local fields*, J. Algebra **98** (1986), no. 1, 197–199.

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

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

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

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

[McC87] L. R. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375/376** (1987), 259–306.

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

[NS09] G. Nebe and A. Steel, *Recognition of division algebras*, J. Algebra **322** (2009), no. 3, 903–909.

[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.

[Rei03] I. Reiner, *Maximal orders*, London Mathematical Society Monographs, vol. 28, The Clarendon Press Oxford University Press, Oxford, 2003.

[Sch80] J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. ACM **27** (1980), no. 4, 701–717.

[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.

[Sme15] D. Smertnig, *A note on cancellation in totally definite quaternion algebras*, J. Reine Angew. Math. **707** (2015), 209–216.

[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.

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

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

[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.

Fachbereich Mathematik, Technische Universität Kaiserslautern, 67663 Kaiserslautern, Germany

*E-mail address:* thofmann@mathematik.uni-kl.de

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

Department of Mathematics, University of Exeter, Exeter, EX4 4QF, U.K.

*E-mail address:* H.Johnston@exeter.ac.uk

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