Forum of Mathematics, Sigma (2022), **Vol. 10**:e87 1–36
doi:10.1017/fms.2022.74

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Computation of lattice isomorphisms and the integral matrix similarity problem

Werner Bley[1], Tommy Hofmann[2] and Henri Johnston[3]

[1]Ludwig-Maximilians-Universität München, Theresienstr. 39, D-80333 München, Germany; E-mail: bley@math.lmu.de.
[2]Universität Siegen, Naturwissenschaftlich-Technische Fakultät, Walter-Flex-Straße 3, 57068 Siegen, Germany; E-mail: tommy.hofmann@uni-siegen.de.
[3]Department of Mathematics, University of Exeter, EX4 4QF Exeter, United Kingdom; E-mail: H.Johnston@exeter.ac.uk.

Received: 16 March 2022; **Revised:** 3 August 2022; **Accepted:** 23 August 2022

2020 Mathematics subject classification: *Primary* – 11R33, 11Y40; *Secondary* – 16Z05, 20G30

Abstract

Let K be a number field, let A be a finite-dimensional K-algebra, let $\mathrm{J}(A)$ denote the Jacobson radical of A and let Λ be an $\mathcal{O}_K$-order in A. Suppose that each simple component of the semisimple K-algebra $A/\mathrm{J}(A)$ is isomorphic to a matrix ring over a field. Under this hypothesis on A, we give an algorithm that, given two Λ-lattices X and Y, determines whether X and Y are isomorphic and, if so, computes an explicit isomorphism $X \to Y$. This algorithm reduces the problem to standard problems in computational algebra and algorithmic algebraic number theory in polynomial time. As an application, we give an algorithm for the following long-standing problem: Given a number field K, a positive integer n and two matrices $A, B \in \mathrm{Mat}_n(\mathcal{O}_K)$, determine whether A and B are similar over $\mathcal{O}_K$, and if so, return a matrix $C \in \mathrm{GL}_n(\mathcal{O}_K)$ such that $B = CAC^{-1}$. We give explicit examples that show that the implementation of the latter algorithm for $\mathcal{O}_K = \mathbb{Z}$ vastly outperforms implementations of all previous algorithms, as predicted by our complexity analysis.

Contents

1. Introduction

Let K be a number field with ring of integers $\mathcal{O}_K$. Let A be a finite-dimensional K-algebra, and let Λ be an $\mathcal{O}_K$-order in A. A Λ-*lattice* is a (left) Λ-module that is finitely generated and torsion-free over $\mathcal{O}_K$. We will consider the following problem.

Problem (IsIsomorphic). Given two Λ-lattices X and Y, decide whether X and Y are isomorphic, and if so, return an isomorphism $X \to Y$.

A Λ-lattice contained in A is said to be *full* if it contains a K-basis of A. We will show that IsIsomorphic is polynomial-time reducible (see §5) to the following problem.

Problem (IsPrincipal). Given a full Λ-lattice X in A, decide whether there exists $\alpha \in X$ such that $X = \Lambda\alpha$, and if so, return such an element α.

Let $\mathrm{J}(A)$ denote the Jacobson radical of A. Note that the quotient algebra $\overline{A} := A/\mathrm{J}(A)$ is semisimple. Let $h : A \to \overline{A}$ denote the canonical projection map, and let $\overline{\Lambda} = h(\Lambda)$. We will show that the problem IsPrincipal for a full Λ-lattice X in A is polynomial-time reducible to the problem IsPrincipal for the full $\overline{\Lambda}$-lattice $\overline{X}$ in $\overline{A}$, where $\overline{X} = h(X)$.

Let

$$A/\mathrm{J}(A) \simeq \bigoplus_{i=1}^{r} A_i$$

be the Wedderburn decomposition. Each simple component A_i is isomorphic to a matrix ring $\mathrm{Mat}_{n_i}(D_i)$, where D_i is a skew field extension of K. Let K_i denote the centre of D_i. In order to make progress on the above problems, we impose the following hypothesis.

(H) Each component A_i of the Wedderburn decomposition $A/\mathrm{J}(A) \simeq \bigoplus_{i=1}^{r} A_i$ is isomorphic to a matrix ring over a field.

In the above notation, this is equivalent to the assertion that $D_i = K_i$ for each i.

Under hypothesis (H), we give algorithms that solve both IsIsomorphic and IsPrincipal. Moreover, we give the first complexity analysis of these problems and thus prove the following result. For precise definitions and statements, we refer the reader to §5 and §8.

Theorem. *The problem* IsIsomorphic *for lattices over orders in algebras satisfying hypothesis* (H) *reduces in probabilistic polynomial time to*

(a) Wedderburn*, the problem of computing explicitly the Wedderburn decomposition,*
(b) Factor*, the problem of factoring integers,*

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

(c) IsPrincipal *in the special case of rings of integers of number fields,*
(d) UnitGroup*, the computation of unit groups for rings of integers of number fields,*
(e) Primitive*, the computation of primitive elements in finite fields and*
(f) DLog*, the computation of discrete logarithms in finite fields.*

A number of articles have considered IsIsomorphic, IsPrincipal or closely related problems in special cases. In particular, [BE05] applies in the case that A is commutative and semisimple; [BW09] applies to group rings $\mathcal{O}_K[G]$, where G is a finite group, but only decides whether two lattices are both locally free and stably isomorphic; and [DD08, KV10, Pag14] apply to maximal or Eichler orders in quaternion algebras. The series of articles [Ble97, BJ08, BJ11, HJ20] consider progressively more general situations, culminating in a solution to IsIsomorphic when A is semisimple, but they all involve a very expensive enumeration step, which in many cases renders the algorithm impractical. We refer the reader to the introduction of [HJ20] for a more detailed overview. By contrast, Algorithm 8.3 replaces this enumeration step by a new method combining results of [BB06, BW09] with an idea of Husert [Hus17].

The original motivation for the study of these problems comes from the Galois module structure of rings of integers. Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. An interesting but difficult problem is to determine whether $\mathcal{O}_L$ is free over its so-called associated order $\mathcal{A}_{L/K} = \{\alpha \in K[G] \mid \alpha\mathcal{O}_L \subseteq \mathcal{O}_L\}$ and, if so, to determine an explicit generator. We refer the reader to §10 and to the introduction of [HJ20] for a more detailed overview of this question and related problems.

The main application of IsPrincipal in the present article is to the following problem.

Problem (IsSimilar). Given a number field K with ring of integers $\mathcal{O} = \mathcal{O}_K$, an integer $n \in \mathbb{Z}_{>0}$ and two matrices $A, B \in \mathrm{Mat}_n(\mathcal{O})$, determine whether A and B are similar over $\mathcal{O}$, and if so, return a conjugating matrix $C \in \mathrm{GL}_n(\mathcal{O})$ such that $B = CAC^{-1}$.

As a special case, this problem includes the so-called conjugacy problem for $\mathrm{GL}_n(\mathcal{O})$. A number of authors have considered the problem IsSimilar (or special cases), including Latimer–MacDuffee [LM33], Sarkisyan [Sar79], Grunewald [Gru80], Husert [Hus17] and Marseglia [Mar20]. Eick–O'Brien and the second named author of the present article gave the first practical algorithm that solves this problem in full generality [EHO19]. We refer the reader to §9.4 and §9.5 for a more detailed discussion of these results.

In §9, we give an efficient algorithm that solves IsSimilar in full generality and a complexity analysis showing that it is polynomial-time reducible to standard problems in algorithmic algebraic number theory, including the principal ideal problem in certain rings of integers and the computation of their unit groups (see Algorithm 9.13 and Theorem 9.14). As a corollary we obtain the following result (see Corollary 9.15 and Remark 5.1).

Theorem. *The problem* IsSimilar *reduces in probabilistic subexponential time to the problems* IsPrincipal *and* UnitGroup *for rings of integers of number fields.*

We first adapt ideas of Faddeev [Fad66] to recast IsSimilar in terms of lattices over orders in a certain K-algebra satisfying hypothesis (H). We then show how to explicitly compute the Jacobson radical of this K-algebra as well as the Wedderburn decomposition of the semisimple quotient from the rational canonical forms of the input matrices. Thus, we show that IsSimilar is reducible to IsPrincipal. In particular, Algorithm 9.13 avoids any expensive enumeration step. For a detailed comparison with other algorithms and implementations, including explicit examples and timings, we refer the reader to §9.5. As these comparisons and our complexity analysis suggest, the implementation of Algorithm 9.13 in the computer algebra package Hecke [FHHJ17] vastly outperforms implementations of other algorithms.

2. Preliminaries on lattices and orders

For further background on lattices and orders, we refer the reader to [Rei03, §4, §8]. Henceforth, all rings considered will be associative and unital.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Let R be an Noetherian 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. Since R is Noetherian, any R-submodule of an R-lattice is again an R-lattice. 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 $KM = V$. We may identify KM with $K \otimes_R M$.

Now, let A be a finite-dimensional K-algebra. Then A is both left and right Artinian and Noetherian. An *R-order* in A is a subring Λ of A (so in particular has the same unit element as A) such that Λ is a full R-lattice in A. Note that Λ is both left and right Noetherian, since Λ is finitely generated over R. A left *Λ-lattice X* is a left Λ-module that is also an R-lattice; in this case, KX may be viewed as a left A-module.

Henceforth, all modules (resp. lattices) will be assumed to be left modules (resp. lattices) unless otherwise stated. Two Λ-lattices are said to be *isomorphic* if they are isomorphic as Λ-modules. The following two lemmas generalise [HJ20, Lemma 2.1].

Lemma 2.1. *Let S be a Noetherian integral domain such that $R \subseteq S \subsetneq K$. Let Γ 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 Γ-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 ΓM is an S-lattice in V. Moreover, it is straightforward to see that ΓM is also a Γ-module and therefore is a Γ-lattice in V. □

Lemma 2.2. *Let S be a Noetherian integral domain such that $R \subseteq S \subsetneq K$. Let Λ be an R-order in A, let Γ be an S-order in A and suppose that $\Lambda \subseteq \Gamma$. Let $f : X \to Y$ be a homomorphism of Λ-lattices. Then the following hold.*

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

Proof. This is straightforward. The key points are to (a) extend f to KX using K-linearity; (b) restrict f^A to ΓX; (c) (injectivity) check that $\ker(f)$ is a full R-lattice in $\ker(f^A)$ and (c) (surjectivity) use the definitions of KY and ΓY. □

We will often use the following result without explicit mention.

Lemma 2.3. *Let Λ be an R-order in A, and let X be a Λ-lattice such that $\dim_K KX = \dim_K A$. Let $\alpha \in X$. Then $X = \Lambda\alpha$ if and only if α is a free generator of X over Λ.*

Proof. Suppose $X = \Lambda\alpha$. Then the map $f : \Lambda \to X$ given by $f(\lambda) = \lambda\alpha$ is a surjective homomorphism of Λ-lattices. By Lemma 2.2 f extends uniquely to a surjective map $f^A : A \to KX$. The hypotheses imply that f^A is injective, thus f is an isomorphism and so α is a free generator of X over Λ. The converse is trivial. □

3. Reduction steps for the lattice isomorphism problem

Let R be a Noetherian integral domain with field of fractions K and assume that $R \neq K$. Let Λ be an R-order in a finite-dimensional K-algebra A.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

3.1. Reduction to the free rank 1 *case via homomorphism groups*

Let X and Y be Λ-lattices. Let $V = KX$ and $W = KY$, which we regard as A-modules. We have

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

where $f|_X$ denotes the restriction of f to a map $f\colon X \to Y$. This follows from the fact that every element in $\mathrm{Hom}_\Lambda(X,Y)$ extends uniquely to an element in $\mathrm{Hom}_A(V,W)$ (see Lemma 2.2). Since a map $f \in \mathrm{Hom}_A(V,W)$ is also R-linear, we have $f(X) \subseteq Y$ if and only if $f \in \mathrm{Hom}_R(X,Y)$. Therefore,

$$\mathrm{Hom}_\Lambda(X,Y) = \mathrm{Hom}_A(V,W) \cap \mathrm{Hom}_R(X,Y).$$

Since X and Y are finitely generated over R, so is $\mathrm{Hom}_R(X,Y)$. Therefore, $\mathrm{Hom}_\Lambda(X,Y)$ is a full R-lattice in $\mathrm{Hom}_A(V,W)$. Similarly, $\mathrm{End}_\Lambda(Y)$ is a full R-lattice in $\mathrm{End}_A(W)$.

In fact, $\mathrm{End}_\Lambda(Y)$ is an R-order in $\mathrm{End}_A(W)$ and $\mathrm{Hom}_\Lambda(X,Y)$ is a (left) $\mathrm{End}_\Lambda(Y)$-lattice in $\mathrm{Hom}_A(V,W)$ via postcomposition. The following result underpins the main results of the present article; it is a straightforward generalisation of [HJ20, Proposition 3.7].

Proposition 3.1. *Two Λ-lattices X and Y are isomorphic if and only if*

(a) *the* $\mathrm{End}_\Lambda(Y)$*-lattice* $\mathrm{Hom}_\Lambda(X,Y)$ *is free of rank* 1*, and*
(b) *every (any) free generator of* $\mathrm{Hom}_\Lambda(X,Y)$ *over* $\mathrm{End}_\Lambda(Y)$ *is an isomorphism.*

Proof. If (a) and (b) hold, then it is clear that X and Y are isomorphic. Suppose conversely that X and Y are isomorphic. Fix an isomorphism $\varphi \in \mathrm{Hom}_\Lambda(X,Y)$. Then for any $g \in \mathrm{Hom}_\Lambda(X,Y)$, we have $h_g := g \circ \varphi^{-1} \in \mathrm{End}_\Lambda(Y)$ and so $g = h_g \circ \varphi$. Hence, φ is a generator of $\mathrm{Hom}_\Lambda(X,Y)$ over $\mathrm{End}_\Lambda(Y)$ and by Lemma 2.3 it is in fact a free generator. Thus, (a) holds. Now, let f be any free generator of $\mathrm{Hom}_\Lambda(X,Y)$ over $\mathrm{End}_\Lambda(Y)$. Then there exists $\theta \in \mathrm{Aut}_\Lambda(Y) = \mathrm{End}_\Lambda(Y)^\times$ such that $f = \theta \circ \varphi$, and hence f is an isomorphism. Thus, (b) holds. □

We now state and prove a closely related 'folklore' result that appears to be well known but whose proof is difficult to locate in the literature. We include this result for completeness, and it will not be applied in the present article. For any full R-lattice M in A, we define $\mathcal{O}_r(M) = \{\mu \in A \mid M\mu \subseteq M\}$. This is an R-order in A and is called the *right order* of M in A (see [Rei03, §8]). The following result may be viewed as a corollary of Proposition 3.1, but it is easier to give a direct proof.

Proposition 3.2. *Let X and Y be full Λ-lattices in A. Then $C := \{\lambda \in A \mid X\lambda \subseteq Y\}$ is a full $\mathcal{O}_r(X)$-lattice in A. Moreover, X and Y are isomorphic if and only if*

(a) *there exists $\alpha \in A^\times$ such that $C = \mathcal{O}_r(X)\alpha$, and*
(b) *we have $Y = XC$.*

Furthermore, when this is the case, $Y = X\alpha$.

Proof. Set $\mathcal{O} := \mathcal{O}_r(X)$. Clearly, C is both an R-module and an $\mathcal{O}$-module. Since X and Y are both full R-lattices in A, there exist nonzero $r, s \in R$ such that $Ys \subseteq X$ and $Xr \subseteq Y$ (see [Rei03, §4]). Thus, $\mathcal{O}r \subseteq C \subseteq \mathcal{O}s^{-1}$, where $\mathcal{O}r$ and $\mathcal{O}s^{-1}$ are both full R-lattices in A. Hence, C is a full R-lattice and therefore a full $\mathcal{O}$-lattice in A.

Suppose (a) and (b) hold. Then $Y = XC = X(\mathcal{O}\alpha) = (X\mathcal{O})\alpha = X\alpha$. Hence, X and Y are isomorphic since $\alpha \in A^\times$. Suppose conversely that $f : X \to Y$ is a Λ-isomorphism. Then by Lemma 2.2 f extends uniquely to an A-isomorphism $f^A : A \to A$ and hence is given by right multiplication by an element $\alpha \in A^\times$. Thus, $Y = X\alpha$. Moreover, $C = \{\lambda \in A \mid X\lambda \subseteq X\alpha\} = \mathcal{O}\alpha$ and $Y = X\alpha = (X\mathcal{O})\alpha = X(\mathcal{O}\alpha) = XC$. □

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

3.2. An alternative approach via localisation

We give an alternative version of Proposition 3.1 that uses localisation. This will be useful later for understanding the relation of some of our results to other results in the literature. For a nonzero prime ideal $\mathfrak{p}$ of R, we let $R_\mathfrak{p}$ denote the localisation (not completion) of R at $\mathfrak{p}$. We define the *localisation* $M_\mathfrak{p}$ of M at $\mathfrak{p}$ to be $R_\mathfrak{p}M$ and note that this is an $R_\mathfrak{p}$-lattice in KM. The localisation $\Lambda_\mathfrak{p}$ is an $R_\mathfrak{p}$-order in A, and localising a Λ-lattice X at $\mathfrak{p}$ yields a $\Lambda_\mathfrak{p}$-lattice $X_\mathfrak{p}$. Two Λ-lattices X and Y are said to be *locally isomorphic* if the $\Lambda_\mathfrak{p}$-lattices $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic for all maximal ideals $\mathfrak{p}$ of R.

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

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

Furthermore, when this is the case, every free generator of $\mathrm{Hom}_\Lambda(X,Y)$ over $\mathrm{End}_\Lambda(Y)$ is an isomorphism.

Proof. If X and Y are isomorphic, then (a) clearly holds and (b) holds by Proposition 3.1. Suppose conversely that (a) and (b) hold. Let f be a free generator of $\mathrm{Hom}_\Lambda(X,Y)$ over $\mathrm{End}_\Lambda(Y)$. Let $\mathfrak{p}$ be a maximal ideal of R. Then there exists an isomorphism $g_\mathfrak{p} \in \mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$. Moreover, f extends to a free generator $f_\mathfrak{p}$ of $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(X_\mathfrak{p}, Y_\mathfrak{p})$ over $\mathrm{End}_{\Lambda_\mathfrak{p}}(Y_\mathfrak{p})$, and so there exists $h_\mathfrak{p} \in \mathrm{End}_{\Lambda_\mathfrak{p}}(Y_\mathfrak{p})$ such that $g_\mathfrak{p} = h_\mathfrak{p} \circ f_\mathfrak{p}$. Note that $h_\mathfrak{p}$ is surjective and thus is in fact an automorphism of $Y_\mathfrak{p}$ by [CR81, (5.8)]. Therefore, $f_\mathfrak{p}$ is an isomorphism. Since this is true for all choices of $\mathfrak{p}$, we have that f itself is an isomorphism by [CR81, (4.2)(ii)]. □

3.3. Reduction to the case of lattices in semisimple algebras

Let $\mathrm{J}(A)$ denote the Jacobson radical of A, and note that $\overline{A} := A/\mathrm{J}(A)$ is a semisimple K-algebra by [CR81, (5.19)]. Let $h : A \to \overline{A}$ denote the canonical projection map. For an element $a \in A$, write $\overline{a}$ for $h(a)$, and for a subset $S \subseteq A$, write $\overline{S}$ for $h(S)$. Then $\overline{\Lambda}$ is an R-order in $\overline{A}$. The following result may be viewed as a variant of [Fad66, Theorem 3].

Theorem 3.4. *Let X be a full Λ-lattice in A. Then $\overline{X}$ is a full $\overline{\Lambda}$-lattice in $\overline{A}$. Moreover, the following statements hold for $\alpha \in X$.*

(a) *If $X = \Lambda\alpha$, then $\overline{X} = \overline{\Lambda}\overline{\alpha}$.*
(b) *If $\overline{X} = \overline{\Lambda}\overline{\alpha}$, then either $X = \Lambda\alpha$ or $X \neq \Lambda\beta$ for all $\beta \in X$.*

Proof. The first claim and part (a) are both clear. Suppose that $\overline{X} = \overline{\Lambda}\overline{\alpha}$ and that there exists $\beta \in X$ such that $X = \Lambda\beta$. Since $\alpha \in X = \Lambda\beta$, there exists $\varepsilon \in \Lambda$ such that $\alpha = \varepsilon\beta$. Hence, $\overline{\alpha} = \overline{\varepsilon}\overline{\beta}$, and since each of $\overline{\alpha}$ and $\overline{\beta}$ is a free generator of $\overline{X}$ over $\overline{\Lambda}$, we must have $\overline{\varepsilon} \in \overline{\Lambda}^\times$. Let $\eta \in \Lambda$ such that $\overline{\eta} = \overline{\varepsilon}^{-1}$. Then $\varepsilon\eta = 1 + \rho$, where $\rho \in \mathrm{J}(A)$. Moreover, $\rho = \varepsilon\eta - 1 \in \Lambda$. Since A is Artinian, $\mathrm{J}(A)$ is a nilpotent ideal (see [CR81, (5.15)]), and so ρ is a nilpotent element. Therefore,

$$\varepsilon^{-1} = \eta(1+\rho)^{-1} = \eta(1 - \rho + \rho^2 - \rho^3 + \cdots) \in \Lambda,$$

where the alternating sum is finite. Hence, $\varepsilon \in \Lambda^\times$ and so $\Lambda\alpha = \Lambda\varepsilon\beta = \Lambda\beta = X$. □

4. A necessary and sufficient condition for freeness

Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$, and let A be a finite-dimensional semisimple K-algebra. Let Λ be an $\mathcal{O}$-order in A. By [Rei03, (10.4)] there exists a (not necessarily unique) maximal $\mathcal{O}$-order $\mathcal{M}$ in A containing Λ.

Lemmas 4.1 and 4.2, as well as part of Proposition 4.3, are based on [Hus17, §1.6].

Lemma 4.1. *Let $\mathfrak{c}, \mathfrak{d}, \mathfrak{f}$ be left ideals of Λ such that $\mathfrak{c} \subseteq \mathfrak{d}$. Then $\mathfrak{d} \cap (\mathfrak{c} + \mathfrak{f}) = \mathfrak{c} + (\mathfrak{d} \cap \mathfrak{f})$.*

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Proof. We follow the proof of [Hus17, Lemma 1.37]. If $c \in \mathfrak{c}$ and $f \in \mathfrak{f}$ with $c + f \in \mathfrak{d}$, then $f \in \mathfrak{d}$ since $c \in \mathfrak{d}$. Hence, $c + f \in \mathfrak{c} + (\mathfrak{d} \cap \mathfrak{f})$. Therefore, $\mathfrak{d} \cap (\mathfrak{c} + \mathfrak{f}) \subseteq \mathfrak{c} + (\mathfrak{d} \cap \mathfrak{f})$. For the reverse inclusion, note that both $\mathfrak{c}$ and $\mathfrak{d} \cap \mathfrak{f}$ are contained in $\mathfrak{d} \cap (\mathfrak{c} + \mathfrak{f})$, and thus the same is true for their sum. □

An ideal of a ring will be said to be *proper* if the containment is strict. Henceforth, let $\mathfrak{f}$ be any proper full two-sided ideal of $\mathcal{M}$ that is contained in Λ. For $\eta \in \mathcal{M}$ we write $\overline{\eta}$ for its image in $\mathcal{M}/\mathfrak{f}$.

Lemma 4.2. *Let X be a left ideal of Λ. If $X + \mathfrak{f} = \Lambda$ and $\beta \in \mathcal{M}$ such that $\mathcal{M}X = \mathcal{M}\beta$, then $\overline{\beta} \in (\mathcal{M}/\mathfrak{f})^\times$ and $\mathcal{M}X \cap \Lambda = X$.*

Proof. We adapt the proof of [Hus17, Lemma 1.38]. Clearly, $\mathfrak{f}X \subseteq \mathcal{M}X \cap \mathfrak{f}$. We now show the reverse inclusion. Let $\gamma \in \mathcal{M}X \cap \mathfrak{f}$. Then we write $\gamma = \lambda\beta$ with $\lambda \in \mathcal{M}$ and we have

$$\begin{aligned} X + \mathfrak{f} = \Lambda &\implies \mathcal{M}(X + \mathfrak{f}) = \mathcal{M} \\ &\implies \mathcal{M}\beta + \mathfrak{f} = \mathcal{M} \\ &\implies \overline{\beta} \in (\mathcal{M}/\mathfrak{f})^\times \\ &\implies \overline{\lambda} = \overline{\gamma}\overline{\beta}^{-1} = \overline{0}(\overline{\beta})^{-1} = \overline{0} \text{ in } \mathcal{M}/\mathfrak{f} \\ &\implies \lambda \in \mathfrak{f} \\ &\implies \gamma = \lambda\beta \in \mathfrak{f}\beta = \mathfrak{f}\mathcal{M}\beta = \mathfrak{f}\mathcal{M}X = \mathfrak{f}X. \end{aligned}$$

Therefore, $\mathfrak{f}X = \mathcal{M}X \cap \mathfrak{f}$. Moreover, we have

$$\mathcal{M}X \cap \Lambda = \mathcal{M}X \cap (X + \mathfrak{f}) = X + (\mathcal{M}X \cap \mathfrak{f}) = X + \mathfrak{f}X = X,$$

where the second equality holds by Lemma 4.1. □

Define

$$\pi : (\mathcal{M}/\mathfrak{f})^\times \longrightarrow (\mathcal{M}/\mathfrak{f})^\times/(\Lambda/\mathfrak{f})^\times$$

to be the map induced by the canonical projection, where the codomain is the collection of left cosets of $(\Lambda/\mathfrak{f})^\times$ in $(\mathcal{M}/\mathfrak{f})^\times$. Note that $(\Lambda/\mathfrak{f})^\times$ is a subgroup of $(\mathcal{M}/\mathfrak{f})^\times$ but is not necessarily a normal subgroup, and so π is only a map of sets in general.

Part of the following result is a variant of [Hus17, Theorem 1.39].

Proposition 4.3. *Let X be a left ideal of Λ. Suppose that $X + \mathfrak{f} = \Lambda$ and that there exists $\beta \in \mathcal{M}$ such that $\mathcal{M}X = \mathcal{M}\beta$. Let $u \in \mathcal{M}^\times$, and let $\alpha = u\beta$. Then $\overline{\alpha}, \overline{\beta}, \overline{u} \in (\mathcal{M}/\mathfrak{f})^\times$ and the following are equivalent:*

(a) $X = \Lambda\alpha$,
(b) $\Lambda\alpha + \mathfrak{f} = \Lambda$,
(c) $\overline{\alpha} \in (\Lambda/\mathfrak{f})^\times$,
(d) $\pi(\overline{\beta}) = \pi(\overline{u^{-1}})$,
(e) $\alpha \in X$ *and X is locally free over* Λ.

Proof. Lemma 4.2 and the definitions of u and α imply that $\overline{\alpha}, \overline{\beta}, \overline{u} \in (\mathcal{M}/\mathfrak{f})^\times$. It is clear that (b) $\Leftrightarrow$ (c). Since $\beta = u^{-1}\alpha$, that (c) $\Leftrightarrow$ (d) follows from the definition of π. Since $X + \mathfrak{f} = \Lambda$, we also have (a) $\Rightarrow$ (b). Assume (b) holds. By two applications of Lemma 4.2, we have

$$X = \mathcal{M}X \cap \Lambda = \mathcal{M}\beta \cap \Lambda = \mathcal{M}\alpha \cap \Lambda = \mathcal{M}(\Lambda\alpha) \cap \Lambda = \Lambda\alpha,$$

where the first equality uses the hypothesis that $X + \mathfrak{f} = \Lambda$ and the last equality uses the assumption that (b) holds; thus (a) holds. Therefore, (a) $\Leftrightarrow$ (b). Finally, a special case of [BJ08, Proposition 2.1] shows that (a) $\Leftrightarrow$ (e). □

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Much of the following notation is adopted from [BB06] and [HJ20]. Denote the centre of a ring R by $Z(R)$. Let $C = Z(A)$, and let $\mathcal{O}_C$ be the integral closure of $\mathcal{O}$ in C. Let $\mathfrak{g} = \mathfrak{f} \cap C$, and note that this is a proper full ideal of $\mathcal{O}_C$. Let $e_1, \dots, e_r$ be the primitive idempotents of C and set $A_i = Ae_i$. Then

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

is a decomposition of A into indecomposable 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 $K \to K_i$, $\alpha \mapsto \alpha e_i$, and we have K-algebra isomorphisms $A_i \cong \mathrm{Mat}_{n_i}(D_i)$, where D_i is a skew field with $Z(D_i) \cong K_i$ (see [CR81, (3.28)]). The Wedderburn decomposition (1) induces decompositions

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

where $\mathcal{O}_{K_i}$ denotes the ring of algebraic integers of K_i. By [Rei03, (10.5)] we have $e_1, \dots, e_r \in \mathcal{M}$ and each $\mathcal{M}_i := \mathcal{M}e_i$ is a maximal $\mathcal{O}$-order (and thus a maximal $\mathcal{O}_{K_i}$-order) in A_i. Moreover, each $\mathfrak{f}_i := \mathfrak{f}e_i$ is a full two-sided ideal of $\mathcal{M}_i$, each $\mathfrak{g}_i := \mathfrak{g}e_i$ is a nonzero integral ideal of $\mathcal{O}_{K_i}$ and we have decompositions

$$\mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r, \quad \mathfrak{f} = \mathfrak{f}_1 \oplus \cdots \oplus \mathfrak{f}_r \quad \text{and} \quad \mathfrak{g} = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_r. \tag{3}$$

The reduced norm map $\mathrm{nr} : A \to C$ is defined componentwise (see [Rei03, §9]) and restricts to a group homomorphism $\mathrm{nr} : \mathcal{M}^\times \to \mathcal{O}_C^\times$.

Lemma 4.4. *There exists a surjective group homomorphism* $\overline{\mathrm{nr}} : (\mathcal{M}/\mathfrak{f})^\times \longrightarrow (\mathcal{O}_C/\mathfrak{g})^\times$ *that fits into the commutative diagram*

$$\begin{array}{ccc} \mathcal{M}^\times & \xrightarrow{\mathrm{nr}} & \mathcal{O}_C^\times \\ \downarrow & & \downarrow \\ (\mathcal{M}/\mathfrak{f})^\times & \xrightarrow{\overline{\mathrm{nr}}} & (\mathcal{O}_C/\mathfrak{g})^\times, \end{array}$$

where the vertical maps are induced by the canonical projections.

Proof. The decompositions (1), (2) and (3) and the componentwise definition of the reduced norm mean that we can and do assume without loss of generality that $r = 1$, that is, A is simple, $\mathcal{M} = \mathcal{M}_1$, $\mathfrak{f} = \mathfrak{f}_1$, $\mathfrak{g} = \mathfrak{g}_1$ and $C = K = K_1$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ dividing $\mathfrak{g}$, and let $K_\mathfrak{p}$ denote the completion (not localisation) of K at $\mathfrak{p}$. If M is an $\mathcal{O}_K$-module or an $\mathcal{O}_K$-algebra, then we write $\widehat{M}_\mathfrak{p} := M \otimes_{\mathcal{O}_K} \mathcal{O}_{K_\mathfrak{p}}$. By [Rei03, (7.6),(11.6)], $\widehat{\mathcal{M}}_\mathfrak{p}$ is a maximal $\mathcal{O}_{K_\mathfrak{p}}$-order in the central simple $K_\mathfrak{p}$-algebra $A \otimes_K K_\mathfrak{p}$. Let $\mathrm{nr}_\mathfrak{p} : \widehat{\mathcal{M}}_\mathfrak{p}^\times \to \mathcal{O}_{K_\mathfrak{p}}^\times$ denote the restriction of the reduced norm map. Then by [BB06, Corollary 2.4], we have that $\mathrm{nr}_\mathfrak{p}(1 + \widehat{\mathfrak{f}}_\mathfrak{p}) = 1 + \widehat{\mathfrak{g}}_\mathfrak{p}$ and $\mathrm{nr}_\mathfrak{p}(\widehat{\mathcal{M}}_\mathfrak{p}^\times) = \mathcal{O}_{K_\mathfrak{p}}^\times$. Hence, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1 + \widehat{\mathfrak{f}}_\mathfrak{p} & \longrightarrow & \widehat{\mathcal{M}}_\mathfrak{p}^\times & \longrightarrow & (\widehat{\mathcal{M}}_\mathfrak{p}/\widehat{\mathfrak{f}}_\mathfrak{p})^\times & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{nr}_\mathfrak{p}} & & \downarrow{\scriptstyle \mathrm{nr}_\mathfrak{p}} & & \downarrow{\scriptstyle \overline{\mathrm{nr}}_\mathfrak{p}} & & \\ 1 & \longrightarrow & 1 + \widehat{\mathfrak{g}}_\mathfrak{p} & \longrightarrow & \mathcal{O}_{K_\mathfrak{p}}^\times & \longrightarrow & (\mathcal{O}_{K_\mathfrak{p}}/\widehat{\mathfrak{g}}_\mathfrak{p})^\times & \longrightarrow & 1, \end{array}$$

where $\overline{\mathrm{nr}}_\mathfrak{p}$ is induced by the other two vertical maps and is surjective by the snake lemma.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

The Chinese remainder theorem gives canonical isomorphisms

$$(\mathcal{M}/\mathfrak{f})^\times \cong \prod_{\mathfrak{p}|\mathfrak{g}} (\widehat{\mathcal{M}}_\mathfrak{p}/\widehat{\mathfrak{f}}_\mathfrak{p})^\times \quad \text{and} \quad (\mathcal{O}_K/\mathfrak{g})^\times \cong \prod_{\mathfrak{p}|\mathfrak{g}} (\mathcal{O}_{K_\mathfrak{p}}/\widehat{\mathfrak{g}}_\mathfrak{p})^\times.$$

Let $\overline{\mathrm{nr}} = \prod_{\mathfrak{p}|\mathfrak{g}} \overline{\mathrm{nr}}_\mathfrak{p}$, and observe that the desired result now follows since the reduced norm map commutes with completion by [Rei03, (9.29)]. □

Let $\mathrm{SL}(\mathcal{M}) = \ker(\mathrm{nr} : \mathcal{M}^\times \to \mathcal{O}_C^\times)$ and $\mathrm{SL}(\mathcal{M}/\mathfrak{f}) = \ker(\overline{\mathrm{nr}})$. (Note that in the literature the set $\mathrm{SL}(\mathcal{M})$, which is the group of units of reduced norm one, is sometimes also denoted by $\mathcal{M}^1$.) Then by Lemma 4.4 and the definitions, we have the following commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{SL}(\mathcal{M}) & \longrightarrow & \mathcal{M}^\times & \xrightarrow{\mathrm{nr}} & \mathrm{nr}(\mathcal{M}^\times) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_2} & & \\
1 & \longrightarrow & \mathrm{SL}(\mathcal{M}/\mathfrak{f}) & \longrightarrow & (\mathcal{M}/\mathfrak{f})^\times & \xrightarrow{\overline{\mathrm{nr}}} & (\mathcal{O}_C/\mathfrak{g})^\times & \longrightarrow & 1 \\
 & & & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi_2} & & \\
 & & & & (\mathcal{M}/\mathfrak{f})^\times/(\Lambda/\mathfrak{f})^\times & & (\mathcal{O}_C/\mathfrak{g})^\times/\overline{\mathrm{nr}}((\Lambda/\mathfrak{f})^\times), & &
\end{array} \tag{4}$$

where the rows are exact and the vertical maps are induced by the canonical projections. Note that all the maps are group homomorphisms, apart from π, which is only a map of sets in general.

Theorem 4.5. *Let X be a left ideal of Λ such that $X + \mathfrak{f} = \Lambda$. Suppose that there exists $\beta \in \mathcal{M}$ such that $\mathcal{M}X = \mathcal{M}\beta$. Then the following statements hold.*

(a) *If X is free over Λ, then $\pi_2(\overline{\mathrm{nr}}(\overline{\beta}))$ is in the image of $\pi_2 \circ f_2$.*
(b) *If f_1 is surjective, then the converse of (a) holds. More precisely, if $u \in \mathcal{M}^\times$ and $\overline{a} \in (\Lambda/\mathfrak{f})^\times$ satisfy $\overline{\mathrm{nr}}(\overline{\beta}) = \overline{\mathrm{nr}}(\overline{u})\overline{\mathrm{nr}}(\overline{a})$, then for any $v \in \mathrm{SL}(\mathcal{M})$ with $f_1(v) = \overline{\beta}\overline{a}^{-1}\overline{u}^{-1}$, we have $X = \Lambda\alpha$, where $\alpha := (vu)^{-1}\beta$.*

Proof. (a) Suppose that X is free over Λ. Then there exists $\alpha \in X$ such that $X = \Lambda\alpha$. Thus, $\mathcal{M}\beta = \mathcal{M}X = \mathcal{M}(\Lambda\alpha) = \mathcal{M}\alpha$, and so there exists $u \in \mathcal{M}^\times$ such that $\alpha = u\beta$. Hence, $\pi(\overline{\beta}) = \pi(\overline{u^{-1}})$ by Proposition 4.3. In other words, there exists $a \in \Lambda$ such that $\overline{a} \in (\Lambda/\mathfrak{f})^\times$ and $\overline{\beta} = \overline{u^{-1}}\overline{a}$. Thus,

$$\overline{\mathrm{nr}}(\overline{\beta}) = \overline{\mathrm{nr}}(\overline{u^{-1}}\overline{a}) = \overline{\mathrm{nr}}(\overline{u^{-1}})\overline{\mathrm{nr}}(\overline{a}) = f_2(\mathrm{nr}(u^{-1}))\overline{\mathrm{nr}}(\overline{a}),$$

and so $\pi_2(\overline{\mathrm{nr}}(\overline{\beta})) = \pi_2(f_2(\mathrm{nr}(u^{-1})))$.

(b) Suppose that f_1 is surjective and $\pi_2(\overline{\mathrm{nr}}(\overline{\beta}))$ is in the image of $\pi_2 \circ f_2$. Then there exist u, a and v as in (b), and so $\pi(\overline{\beta}) = \pi(\overline{vu})$. Hence, by Proposition 4.3 we have $X = \Lambda\alpha$ where $\alpha := (vu)^{-1}\beta$. □

5. Preliminaries on complexity

We briefly recall the conventions that we will use for the complexity analysis of our algorithms. For details we refer the reader to Lenstra [Len92] or Cohen [Coh93, §1.1].

Let l be the size of the input data measured by the number of required bits. Then an algorithm is *polynomial time* if the running time is $O(P(l))$ for a polynomial P. An algorithm is *subexponential time* if there exists $0 \le a < 1$ and $b \in \mathbb{R}_{>0}$ such that the running time is $O(\exp(b \cdot l^a (\log l)^{a-1}))$.

A *probabilistic* algorithm may call a random number generator. In this case we say that the algorithm is *probabilistic polynomial time* if the expected running time is $O(P(l))$ for a polynomial P. We adopt the same convention for probabilistic subexponential time algorithms.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Given two computational problems A and B, a *(probabilistic) polynomial-time reduction* from A to B is an algorithm that solves A using a polynomial number of calls to an oracle solving B and is (probabilistic) polynomial time outside of those calls to the oracle.

Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$. We follow the convention of [Len92] for representing our input data. In some more detail, if $V = K^n$ is an n-dimensional vector space over K, we represent an $\mathcal{O}$-module $M \subseteq V$ by a pseudobasis of M, that is, by elements $v_1, \dots, v_k \in V$ and fractional $\mathcal{O}$-ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ such that $M = \mathfrak{a}_1 v_1 \oplus \cdots \oplus \mathfrak{a}_k v_k$ for some $k \leq n$. A K-algebra A of dimension d is represented as a d-dimensional vector space together with the K-linear multiplication map $A \otimes_K A \to A$, which is represented using d^3 elements of K. Given a finite-dimensional K-algebra A, an $\mathcal{O}$-order of A is represented using a pseudobasis. An n-dimensional A-module V is represented as a vector space over K together with d matrices in $\mathrm{Mat}_n(K)$, one for each basis element of A describing the action on elements of V. Given an $\mathcal{O}$-order Λ, a Λ-lattice is represented by an $\mathcal{O}$-submodule of a finite-dimensional A-module, invariant under the action of Λ.

We will be mainly interested in solving the following two problems.

Problem (IsIsomorphic). Given a finite-dimensional K-algebra A, an $\mathcal{O}$-order Λ in A and two Λ-lattices X and Y, decide whether X and Y are isomorphic, and if so, return an isomorphism $X \to Y$.

Problem (IsPrincipal). Given a finite-dimensional K-algebra A, an $\mathcal{O}$-order Λ in A and a full Λ-lattice X in A, decide whether there exists $\alpha \in X$ such that $X = \Lambda\alpha$, and if so, return such an element α.

Under the assumption that A satisfies hypothesis (H), we will reduce these questions to well-studied problems in algorithmic number theory. These include IsPrincipal in the case where $A = K$ and $\Lambda = \mathcal{O}$, as well as the following problems:

- Factor: Given an ideal or element of the ring of integers $\mathcal{O}_F$ of a number field F, determine its factorisation into prime ideals.
- Primitive: Given a finite field $\mathbb{F}_q$, determine $\alpha \in \mathbb{F}_q^\times$ such that $\mathbb{F}_q^\times = \langle \alpha \rangle$.
- DLog: Given a finite field $\mathbb{F}_q$ and $\alpha, \beta \in \mathbb{F}_q^\times$ with $\mathbb{F}_q^\times = \langle \alpha \rangle$, determine $n \in \mathbb{Z}_{\geq 0}$ such that $\alpha^n = \beta$.
- UnitGroup: Given the ring of integers $\mathcal{O}_F$ of a number field F, determine a system of fundamental units for $\mathcal{O}_F^\times$.

We will use the following standard convention and notation to denote variations and instances of computational problems. For example, for an $\mathcal{O}$-order Λ, we denote by $\mathsf{IsIsomorphic}_\Lambda$ the set of instances of IsIsomorphic restricted to Λ-lattices. Similarly, we use $\mathsf{IsPrincipal}_\Lambda$ for the set of instances of IsPrincipal for Λ-lattices. Moreover, given a Λ-lattice X, we use $\mathsf{IsPrincipal}(X)$ to denote the instance of IsPrincipal for the lattice X. Note that in this case we still consider Λ part of the input.

Remark 5.1. Currently, the following complexity statements are known.

(a) The problem $\mathsf{Factor}_\mathbb{Z}$ can be solved in probabilistic subexponential time ([LP92, Theorem 10.5]). Given an ideal I of the ring of integers $\mathcal{O}_F$ of a number field F, the prime ideals of $\mathcal{O}_F$ lying above the rational prime factors of $\mathrm{Norm}_{F/\mathbb{Q}}(I)$ can be determined in probabilistic polynomial time ([Coh93, §6.2]); hence, there is a probabilistic polynomial-time reduction from Factor to $\mathsf{Factor}_\mathbb{Z}$. Since $\mathsf{Primitive}(\mathbb{F}_q)$ is probabilistic polynomial-time reducible to $\mathsf{Factor}(q-1)$, the same holds for Primitive. Moreover, DLog can be solved in subexponential time; see [Odl00] and the references therein. While it is conjectured that IsPrincipal and UnitGroup can also be solved in subexponential time, so far this has been established only under additional hypotheses and heuristics, including the generalised Riemann hypothesis (GRH); see [Buc90, Bia14, BF14].

(b) There exist quantum polynomial-time algorithms for solving each of the problems $\mathsf{Factor}_\mathbb{Z}$, DLog, Primitive ([Sho97, §5, §6]), UnitGroup ([EHKS14, Theorem 1.2]) and IsPrincipal for rings of integers of number fields ([BS16, Theorem 1.3]).

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Our approach to solving IsIsomorphic and IsPrincipal for noncommutative algebras A satisfying hypothesis (H) relies crucially on the solution of the following two subproblems.

Problem (Wedderburn). Given a number field K and a finite-dimensional semisimple K-algebra A satisfying hypothesis (H), determine number fields K_i, integers $r, n_i \in \mathbb{Z}_{>0}$ and an explicit isomorphism $A \cong \prod_{i=1}^{r} \mathrm{Mat}_{n_i}(K_i)$.

Problem (SplittingMatrixAlgebra). Given a number field K and a split central simple K-algebra A, determine an isomorphism $A \cong \mathrm{Mat}_n(K)$ for some $n \in \mathbb{Z}_{>0}$.

Remark 5.2. For a finite-dimensional semisimple K-algebra A, an explicit decomposition $A \cong \prod_{i=1}^{r} A_i$ into simple K-algebras A_i, as well as the centre K_i of each A_i, can be computed in polynomial time by [FR85, 1.5 B]. Thus, Wedderburn reduces to SplittingMatrixAlgebra. The decision problem of checking whether $A_i \cong \mathrm{Mat}_{n_i}(K_i)$ for some $n_i \in \mathbb{Z}_{>0}$ is polynomial-time reducible to the computation of (the discriminant of) a maximal order in A_i by [NS09, Corollary 3.4], hence to Factor by [IR93, Corollary 5.3]. The problem of finding an explicit isomorphism appears to be a much harder problem. In [IRS12, Theorem 1] it was shown that for algebras of bounded dimension over a fixed number field, SplittingMatrixAlgebra is probabilistic polynomial-time reducible to the problem of computing a maximal order, hence to Factor.

6. Complexity of algorithms related to orders and their lattices

Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$. The aim of this section is to establish the complexity of certain algorithms related to $\mathcal{O}$-orders and their lattices. These algorithms have already appeared in the literature, either implicitly or explicitly, but with either no or only partial analysis of their complexity.

6.1. Computing maximal orders

Let A be a finite-dimensional semisimple K-algebra, and let Λ be an $\mathcal{O}$-order in A. Let $d = \dim_K A$ and let $\mathrm{tr}\colon A \to K$ denote the reduced trace map (see [CR81, §7D]). Following [CR81, §26A], we define $\mathrm{Disc}(\Lambda)$ to be the ideal of $\mathcal{O}$ generated by all elements

$$\det\bigl(\mathrm{tr}(x_i x_j)_{1 \le i,j \le d}\bigr) \text{ with } x_1, \ldots, x_d \in \Lambda.$$

By applying a result of [FR85], the following is straightforward to deduce from the results of [Fri00].

Proposition 6.1. *Let Λ and A be as above. Then the problem of computing a maximal $\mathcal{O}$-order $\mathcal{M}$ in A containing Λ is probabilistic polynomial-time reducible to* Factor$(\mathrm{Disc}(\Lambda))$.

Proof. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$ dividing $\mathrm{Disc}(\Lambda)$, and write $v_{\mathfrak{p}}(-)$ for the $\mathfrak{p}$-adic valuation. It follows from [Fri00, (3.17)] that the computation of an order $\Lambda^{(\mathfrak{p})}$ such that $v_{\mathfrak{p}}([\Lambda^{(\mathfrak{p})} : \Lambda]_{\mathcal{O}})$ is maximal reduces in polynomial time to the problem of computing the maximal two-sided ideals of an order containing $\mathfrak{p}$. Now, fix an order Γ. Then the maximal two-sided ideals of Γ containing $\mathfrak{p}$ are the preimages of the maximal two-sided ideals under the canonical projection $\Gamma \to (\Gamma/\mathfrak{p}\Gamma)/\mathrm{J}(\Gamma/\mathfrak{p}\Gamma)$ (see [Fri00, (5.23)]). As a decomposition of this $(\mathcal{O}/\mathfrak{p})$-algebra into simple components and therefore the maximal two-sided ideals can be found in probabilistic polynomial time by [FR85, 1.5 B], an order $\Lambda^{(\mathfrak{p})}$ can be determined in probabilistic polynomial time. By [Fri00, (3.19)] the order $\sum_{\mathfrak{p}} \Lambda^{(\mathfrak{p})}$ is maximal, where $\mathfrak{p}$ runs over the maximal ideals of $\mathcal{O}$ dividing $\mathrm{Disc}(\Lambda)$. Therefore, the computation of a maximal order $\mathcal{M}$ containing Λ reduces in probabilistic polynomial time to Factor$(\mathrm{Disc}(\Lambda))$. □

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

6.2. Nice maximal orders

Let $n \in \mathbb{Z}_{>0}$, and let $A = \mathrm{Mat}_n(K)$ be a full matrix algebra. For a nonzero fractional ideal $\mathfrak{a}$ of $\mathcal{O}$, let

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

denote the $\mathcal{O}$-order in A consisting of all $n \times n$ matrices $(x_{ij})_{1 \le i,j \le n}$, where x_{11} ranges over all elements of $\mathcal{O}$, …, x_{1n} ranges over all elements of $\mathfrak{a}^{-1}$ and so on. (In the case $n = 1$, we take $\mathcal{M}_{\mathfrak{a},n} = \mathcal{O}$.) We say that a maximal $\mathcal{O}$-order in A is *nice* if it is equal to $\mathcal{M}_{\mathfrak{a},n}$ for some choice of $\mathfrak{a}$. By [Rei03, (27.6)] every maximal $\mathcal{O}$-order in A is conjugate to a nice maximal order.

Lemma 6.2. *There exists a probabilistic polynomial-time algorithm that, given a maximal $\mathcal{O}$-order $\mathcal{M}$ in $A = \mathrm{Mat}_n(K)$, determines a nonzero fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ and $S \in \mathrm{GL}_n(K)$ such that $S\mathcal{M}S^{-1} = \mathcal{M}_{\mathfrak{a},n}$.*

Proof. The algorithm is presented in [BJ08, §5] and works by reducing the problem to the computation of a Steinitz form of an $\mathcal{O}$-lattice of rank n, which can be performed in probabilistic polynomial time by Corollary A.3. □

6.3. Norm equations and principal ideals

Let $r \in \mathbb{Z}_{>0}$, and let $A = \prod_{i=1}^{r} \mathrm{Mat}_{n_i}(K_i)$, where K_i is a finite field extension of K and $n_i \in \mathbb{Z}_{>0}$ for each i. In particular, A is a finite-dimensional semisimple K-algebra satisfying hypothesis (H). Let C be the centre of A, which we can and do identify with $\prod_{i=1}^{r} K_i$. Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in A, and let $\mathcal{O}_C = \mathcal{M} \cap C = \prod_{i=1}^{r} \mathcal{O}_{K_i}$.

Lemma 6.3. *The reduced norm map* $\mathrm{nr}\colon \mathcal{M}^\times \to \mathcal{O}_C^\times$ *is surjective. Moreover, there exists a probabilistic polynomial-time algorithm that given $\mathcal{M}$ and $a \in \mathcal{O}_C^\times$ determines $\alpha \in \mathcal{M}^\times$ such that* $\mathrm{nr}(\alpha) = a$.

Proof. By decomposing $\mathcal{M}$ using the central primitive idempotents of A, it suffices to consider the case $A = \mathrm{Mat}_n(K)$, in which we must have $\mathcal{O}_C = \mathcal{O}$. Then the reduced norm map $\mathrm{nr} : A \to K$ is just the usual determinant map. Moreover, using Lemma 6.2, we can and do assume that $\mathcal{M} = \mathcal{M}_{\mathfrak{a},n}$ is a nice maximal order. Since $\alpha = \mathrm{diag}(a, 1, \dots, 1) \in \mathcal{M}_{\mathfrak{a},n}^\times$ satisfies $\mathrm{nr}(\alpha) = a$, the claim follows. □

An algorithm for solving the principal ideal problem for $\mathcal{M}$-lattices was given in [BJ08, §5]. We now analyse its complexity.

Proposition 6.4. *The problem* $\mathsf{IsPrincipal}_{\mathcal{M}}$ *is probabilistic polynomial-time reducible to one instance of* $\mathsf{IsPrincipal}_{\mathcal{O}_{K_i}}$ *for each $i = 1, \dots, r$.*

Proof. By decomposing $\mathcal{M}$ using the central primitive idempotents of A, it suffices to consider the case $A = \mathrm{Mat}_n(K)$, in which we must have $\mathcal{O}_C = \mathcal{O}$. Let X be a full $\mathcal{M}$-lattice in A. Let $e_{11} \in A$ be the matrix with the top-left entry equal to 1 and all other entries equal to 0. Using Lemma 6.2, we can and do assume that $\mathcal{M} = \mathcal{M}_{\mathfrak{a},n}$ is a nice maximal order. By [BJ08, Corollary 5.4], it is sufficient to check whether the Steinitz class of the $\mathcal{O}$-module $e_{11}X$ is equal to $[\mathfrak{a}^{-1}]$, which amounts to testing whether a certain ideal of $\mathcal{O}$ is principal. □

6.4. Computing isomorphisms between localised lattices

Let Λ be an $\mathcal{O}$-order in a finite-dimensional K-algebra A. Given two Λ-lattices X and Y and a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, we wish to determine whether there exists an isomorphism $X_\mathfrak{p} \cong Y_\mathfrak{p}$ of $\Lambda_\mathfrak{p}$-lattices and to compute such an isomorphism if so. By computing an isomorphism we mean computing a Λ-morphism $f\colon X \to Y$ such that its localisation $f_\mathfrak{p}\colon X_\mathfrak{p} \to Y_\mathfrak{p}$ is an isomorphism.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

We first consider the case where X is a full Λ-lattice in A and $Y = \Lambda$, for which an algorithm was presented in [BW09, §4.2] (although the algorithm was presented only in the context of semisimple algebras, the semisimplicity hypothesis is in fact unnecessary). We now outline the algorithm and analyse its complexity.

Proposition 6.5. *There exists a probabilistic polynomial-time algorithm that, given A, Λ and $\mathfrak{p}$ as above and a full Λ-lattice X in A, decides whether $X_\mathfrak{p}$ is free over $\Lambda_\mathfrak{p}$ and, if so, returns $\alpha \in X$ such that $X_\mathfrak{p} = \Lambda_\mathfrak{p}\alpha$.*

Proof. Consider the finitely generated $\mathcal{O}/\mathfrak{p}$-algebra $R_\mathfrak{p} := \Lambda/\mathfrak{p}\Lambda \cong \Lambda_\mathfrak{p}/\mathfrak{p}\Lambda_\mathfrak{p}$. It follows from [FR85, 1.5 A] that the Jacobson radical $J_\mathfrak{p} = \mathrm{J}(R_\mathfrak{p})$ can be determined in polynomial time. Let $\overline{R}_\mathfrak{p} = R_\mathfrak{p}/J_\mathfrak{p}$. By Lemma 2.3 and Nakayama's lemma, $X_\mathfrak{p}$ is free over $\Lambda_\mathfrak{p}$ if and only if $\overline{X}_\mathfrak{p} := (X/\mathfrak{p}X)/J_\mathfrak{p}(X/\mathfrak{p}X) \cong (X_\mathfrak{p}/\mathfrak{p}X_\mathfrak{p})/J_\mathfrak{p}(X_\mathfrak{p}/\mathfrak{p}X_\mathfrak{p})$ is free of rank 1 over $\overline{R}_\mathfrak{p}$. Using algorithms of Friedl–Rónyai [FR85, 1.5 B] and Ronyai [Ron87, Theorem 6.2], one can determine an isomorphism of $\overline{R}_\mathfrak{p}$ with a product of matrix algebras over finite fields k_i in probabilistic polynomial time. The final steps are just linear algebra over finite fields. □

The following algorithm without the complexity statement was given in [HJ20, §8.4].

Corollary 6.6. *There exists a probabilistic polynomial-time algorithm that, given A, Λ and $\mathfrak{p}$ as above and Λ-lattices X and Y, decides whether $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic as $\Lambda_\mathfrak{p}$-lattices and, if so, returns $f \in \mathrm{Hom}_\Lambda(X, Y)$ such that the localisation $f_\mathfrak{p}\colon X_\mathfrak{p} \to Y_\mathfrak{p}$ is an isomorphism.*

Proof. We use Proposition 6.5 together with the reduction to the free rank 1 case given by Proposition 3.1. Both $\mathrm{End}_\Lambda(Y)$ and $\mathrm{Hom}_\Lambda(X, Y)$ can be determined as described in [HJ20, §7.3] using pseudo-Hermite normal form and pseudo-Smith normal form computations, which are probabilistic polynomial time by [BFH17, Theorem 34, Proposition 43]. Using Proposition 6.5 one can determine in probabilistic polynomial time whether the $(\mathrm{End}_\Lambda(Y))_\mathfrak{p}$-lattice $(\mathrm{Hom}_\Lambda(X, Y))_\mathfrak{p}$ is free of rank 1. If not, then $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are not isomorphic over $\Lambda_\mathfrak{p}$. If so, then the algorithm returns a free generator $f \in \mathrm{Hom}_\Lambda(X, Y)$ of $(\mathrm{Hom}_\Lambda(X, Y))_\mathfrak{p}$ over $(\mathrm{End}_\Lambda(Y))_\mathfrak{p}$. Then $X_\mathfrak{p} \cong Y_\mathfrak{p}$ over $\Lambda_\mathfrak{p}$ if and only if the localisation $f_\mathfrak{p}\colon X_\mathfrak{p} \to Y_\mathfrak{p}$ is an isomorphism. □

Remark 6.7. Given two Λ-lattices X and Y, Corollary 6.6 can be used to decide if X and Y are in the same genus, that is, whether $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic $\Lambda_\mathfrak{p}$-lattices for every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$. Note that a necessary condition is that KX and KY are isomorphic as A-modules. By [CIK97, Corollary 3] there is a polynomial-time algorithm that decides whether KX and KY are isomorphic as A-modules and, if so, computes an isomorphism; hence, the problem reduces to the case $KX = KY$. In this situation, X and Y are in the same genus if and only if $X_\mathfrak{p}$ and $Y_\mathfrak{p}$ are isomorphic $\Lambda_\mathfrak{p}$-lattices for the finitely many prime ideals $\mathfrak{p}$ dividing the module index $[X : Y]_\mathcal{O}$ (see [Frö67, §3]). Hence, checking whether X and Y are in the same genus is polynomial-time reducible to $\mathsf{Factor}([X : Y]_\mathcal{O})$.

6.5. Finding a suitable choice of locally free left ideal

Let A be a finite-dimensional semisimple K-algebra, and let Λ be an $\mathcal{O}$-order in A. By [Rei03, (10.4)] there exists a (not necessarily unique) maximal $\mathcal{O}$-order $\mathcal{M}$ in A containing Λ. Let $\mathfrak{f}$ be any proper full two-sided ideal of $\mathcal{M}$ that is contained in Λ. The following result without the complexity statements is a consequence of a special case of the argument given in [BJ11, §5.1].

Proposition 6.8. *Given A, Λ and $\mathfrak{f}$ as above and a full Λ-lattice X in A, the problem of determining whether X is locally free over Λ and, if so, computing an element $\xi \in A^\times$ such that $X\xi \subseteq \Lambda$ and $X\xi + \mathfrak{f} = \Lambda$, is probabilistic polynomial-time reducible to $\mathsf{Factor}(\mathcal{O} \cap \mathfrak{f})$.*

Proof. Let $\mathrm{MaxSpec}(\mathcal{O})$ denote the set of all maximal ideals of $\mathcal{O}$. Let $\mathfrak{S} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ be the subset consisting of ideals that divide $\mathcal{O} \cap \mathfrak{f}$ (note that this is a proper nonzero ideal of $\mathcal{O}$), and let $\mathfrak{T} = \mathrm{MaxSpec}(\mathcal{O}) \setminus \mathfrak{S}$. Observe that, for every $\mathfrak{p} \in \mathfrak{T}$, we have $\mathfrak{f}_\mathfrak{p} = \Lambda_\mathfrak{p} = \mathcal{M}_\mathfrak{p}$, and so $X_\mathfrak{p}$ is free over $\Lambda_\mathfrak{p}$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

by [Rei03, (18.10)]. Moreover, for each i, checking whether $X_{\mathfrak{p}_i}$ is free over $\Lambda_{\mathfrak{p}_i}$ and, if so, computing $\omega_i \in X$ such that $X_{\mathfrak{p}_i} = \Lambda_{\mathfrak{p}_i}\omega_i$, can be performed in probabilistic polynomial time by Proposition 6.5. In particular, if this step is completed successfully, then X is locally free over Λ.

By [Coh00, Proposition 1.3.11], elements $\beta_1, \dots, \beta_n \in \mathcal{O}$ such that for each i, we have

$$\beta_i \equiv 1 \bmod \mathfrak{p}_i \quad \text{and} \quad \beta_i \equiv 0 \bmod \mathfrak{p}_j \text{ for } 1 \leq j \leq n, j \neq i$$

can be computed in polynomial time. For each i, let $\nu_i \in \mathcal{O} \setminus \mathfrak{p}_i$ be an element such that $X\omega_i^{-1}\nu_i \subseteq \Lambda$. Then $X\xi \subseteq \Lambda$, where $\xi := \sum_{i=1}^{n} \beta_i\omega_i^{-1}\nu_i$. By construction we have $(X\xi)_{\mathfrak{p}_i} = \Lambda_{\mathfrak{p}_i}$ for each i. Moreover, $\mathfrak{f}_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathfrak{T}$. Therefore, $(X\xi + \mathfrak{f})_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{MaxSpec}(\mathcal{O})$, and so $X\xi + \mathfrak{f} = \Lambda$ by [Rei03, (4.21)]. □

6.6. Computing generators of $(\Lambda/\mathfrak{f})^\times$ *and* $K_1(\Lambda/\mathfrak{f})$

We first recall some definitions from algebraic K-theory and refer the reader to [CR87, §40] for more details. For any ring R, the Whitehead group $K_1(R)$ is defined as $\mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)]$, where $\mathrm{GL}(R) = \varinjlim \mathrm{GL}_n(R)$ and $\mathrm{GL}_n(R)$ embeds into $\mathrm{GL}_{n+1}(R)$ via

$$\alpha \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}.$$

In particular, there is a canonical map $R^\times \to \mathrm{GL}(R) \to K_1(R)$.

Now, assume the notation and setting of §6.5. Since $\Lambda/\mathfrak{f}$ is of finite cardinality, it is semilocal, and so the canonical map

$$(\Lambda/\mathfrak{f})^\times \longrightarrow K_1(\Lambda/\mathfrak{f})$$

is surjective by [CR87, (40.31)]. We consider the problems of computing generators of $(\Lambda/\mathfrak{f})^\times$ and of $K_1(\Lambda/\mathfrak{f})$, where the latter task means computing elements $x_1, \dots, x_n \in (\Lambda/\mathfrak{f})^\times$ such that their images generate $K_1(\Lambda/\mathfrak{f})$.

An algorithm for computing generators of $K_1(\Lambda/\mathfrak{f})$ is described in [BB06, §3.4–3.7]. With minor modifications, this algorithm also computes a generating set of $(\Lambda/\mathfrak{f})^\times$. In this subsection, we will analyse the complexity of both these algorithms. To treat both cases simultaneously, for a ring R we let $\mathrm{G}(R)$ denote either $K_1(R)$ or $R^\times$.

Let C denote the centre of A, and let $\mathcal{O}_C$ be the integral closure of $\mathcal{O}$ in C. Let $\mathfrak{g} = \mathfrak{f} \cap C$, and note that this is a proper full ideal of $\mathcal{O}_C$ and of $\Lambda \cap \mathcal{O}_C = \Lambda \cap C$. Let $\mathfrak{g} = \prod_{\mathfrak{P} \in \mathcal{P}} \mathfrak{P}^{e_{\mathfrak{P}}}$ be the prime ideal decomposition of $\mathfrak{g}$ in $\mathcal{O}_C$, where the set $\mathcal{P}$ of prime ideals of $\mathcal{O}_C$ is defined by the decomposition. Set $\mathcal{P}' := \{\mathfrak{P} \cap \Lambda \mid \mathfrak{P} \in \mathcal{P}\}$, a set of prime ideals of $\Lambda \cap \mathcal{O}_C$. For each $\mathfrak{p} \in \mathcal{P}'$ consider the ideal

$$\mathfrak{q} := \bigcap_{\substack{\mathfrak{P} \in \mathcal{P}, \\ \mathfrak{P} \cap \Lambda = \mathfrak{p}}} (\mathfrak{P}^{e_{\mathfrak{P}}} \cap \Lambda).$$

We write $\mathcal{Q}$ for the set of ideals $\mathfrak{q}$. Then by [BE05, Proposition 3.2]

$$\mathfrak{g} = \prod_{\mathfrak{q} \in \mathcal{Q}} \mathfrak{q} = \bigcap_{\mathfrak{q} \in \mathcal{Q}} \mathfrak{q}$$

is the unique primary decomposition of $\mathfrak{g}$ when considered as an ideal of $\Lambda \cap \mathcal{O}_C$. Moreover, by [BB06, Lemma 3.5], we have

$$\mathfrak{f} = \bigcap_{\mathfrak{q} \in \mathcal{Q}} (\mathfrak{q}\Lambda + \mathfrak{f}) = \prod_{\mathfrak{q} \in \mathcal{Q}} (\mathfrak{q}\Lambda + \mathfrak{f}),$$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

and by the Chinese remainder theorem we obtain an isomorphism

$$\Lambda/\mathfrak{f} \cong \prod_{\mathfrak{q}\in\mathcal{Q}} \Lambda/(\mathfrak{q}\Lambda+\mathfrak{f}).$$

This induces a decomposition

$$\mathrm{G}(\Lambda/\mathfrak{f}) \cong \prod_{\mathfrak{q}\in\mathcal{Q}} \mathrm{G}(\Lambda/(\mathfrak{q}\Lambda+\mathfrak{f})).$$

Thus, given $\mathcal{Q}$, it suffices to compute generators of $\mathrm{G}(\Lambda/(\mathfrak{q}\Lambda+\mathfrak{f}))$ for each $\mathfrak{q}\in\mathcal{Q}$.

Now, fix $\mathfrak{q}\in\mathcal{Q}$, and let $\mathfrak{p}=\mathfrak{P}\cap\Lambda\in\mathcal{P}'$ be the associated prime ideal of $\Lambda\cap\mathcal{O}_C$ for some $\mathfrak{P}\in\mathcal{P}$. As shown in [BB06, §3.7], we have an exact sequence

$$(1+\mathfrak{p}\Lambda+\mathfrak{f})/(1+\mathfrak{q}\Lambda+\mathfrak{f}) \longrightarrow \mathrm{G}(\Lambda/(\mathfrak{q}\Lambda+\mathfrak{f})) \longrightarrow \mathrm{G}(\Lambda/(\mathfrak{p}\Lambda+\mathfrak{f})) \longrightarrow 1. \tag{5}$$

We consider the problems of computing generators for the first and third terms in this sequence. Let $d := \dim_K A$.

Lemma 6.9. *Given Λ, $\mathfrak{f}$ and $\mathfrak{p}$ as above, the problem of computing generators of*

$$(\Lambda/(\mathfrak{p}\Lambda+\mathfrak{f}))^\times \text{ or } K_1(\Lambda/(\mathfrak{p}\Lambda+\mathfrak{f}))$$

is probabilistic polynomial-time reducible to at most d instances of the problem Primitive *for extensions of $\mathcal{O}/(\mathcal{O}\cap\mathfrak{P})$ of degree at most d. The number of generators is at most $d([K:\mathbb{Q}]+2)$.*

Proof. Let k denote the finite field $\mathcal{O}/(\mathfrak{p}\cap\mathcal{O})$. Let $R=\Lambda/(\mathfrak{p}\Lambda+\mathfrak{f})$, and note that this is annihilated by $\mathfrak{p}\cap\mathcal{O}$. Thus, R is a k-algebra such that $\dim_k R\le d$. In particular, R is Artinian, so its Jacobson radical $J=\mathrm{J}(R)$ is nilpotent by [CR81, (5.15)]. Since we have a decreasing filtration $J\supseteq J^2\supseteq\cdots\supseteq J^d$ and $\dim_k(J)\le d-1$, we obtain $J^d=0$. By [BB06, Lemma 3.6] and the same reasoning as in [BB06, §3.7], we have an exact sequence

$$1+J \longrightarrow \mathrm{G}(R) \longrightarrow \mathrm{G}(R/J) \longrightarrow 1.$$

We first discuss the computation of generators for $1+J$. To this end, let $l\in\mathbb{Z}_{\ge 0}$ be minimal subject to the condition $J^{2^l}=0$ and note that $2^l\le 2d$. Consider the filtration

$$1+J \supseteq 1+J^2 \supseteq \cdots \supseteq 1+J^{2^{l-1}} \supseteq 1.$$

Generators of J can be determined in polynomial time using the algorithms of [FR85, 1.5 A]. For each $i=0,\dots,l-1$, the map $\overline{x}\mapsto\overline{x-1}$ induces an isomorphism

$$(1+J^{2^i})/(1+J^{2^{i+1}}) \longrightarrow J^{2^i}/J^{2^{i+1}}$$

of abelian groups, and so it follows that we can find generators of $1+J$ in polynomial time. For each $i=0,\dots,l-1$ the number of generators of $J^{2^i}/J^{2^{i+1}}$ is bounded by $\dim_k(J^{2^i}/J^{2^{i+1}})[K:\mathbb{Q}]$. Now, summing over $i=0,\dots,l-1$ shows that $1+J$ is generated by at most $\dim_k(J)[K:\mathbb{Q}]\le(d-1)[K:\mathbb{Q}]$ elements.

Using algorithms of [FR85, 1.5 B] and [Ron87, Theorem 6.2], one can determine an isomorphism $R/J\cong\prod_{1\le i\le r}\mathrm{Mat}_{n_i}(k_i)$ with a product of matrix algebras over finite fields k_i in probabilistic polynomial time. Since

$$\mathrm{G}(R/J) \cong \prod_{1\le i\le r} \mathrm{G}(\mathrm{Mat}_{n_i}(k_i)),$$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

this problem reduces to the computation of each $\mathrm{G}(\mathrm{Mat}_{n_i}(k_i))$, which we claim is generated by at most 2 elements. If $\mathrm{G} = K_1$, then the claim follows from the fact that the canonical maps $k_i^\times \to K_1(k_i) \to K_1(\mathrm{Mat}_{n_i}(k_i))$ are isomorphisms. If $\mathrm{G} = (-)^\times$, then the claim follows from [Tay87], where it is shown that given a primitive element of k_i one can write down directly a two element generating set of $\mathrm{GL}_{n_i}(k_i)$. Since $\dim_k(R/J) \leq d$ we have $r \leq d$ and $[k_i : k] \leq d$ for each i. Finally, note that $\mathcal{O}/(\mathcal{O} \cap \mathfrak{p}) = \mathcal{O}/(\mathcal{O} \cap \mathfrak{P})$ since $\mathcal{O} \subseteq \Lambda$ implies $\mathcal{O} \cap \mathfrak{p} = \mathcal{O} \cap \mathfrak{P} \cap \Lambda = \mathcal{O} \cap \mathfrak{P}$. In particular, $G(R/J)$ is generated by at most $2r \leq 2d$ elements. □

Lemma 6.10. *Given Λ, $\mathfrak{f}$, $\mathfrak{p}$ and $\mathfrak{q}$ as above, we set*

$$e_\mathfrak{p} = \max\{e_\mathfrak{P} \mid \mathfrak{P} \in \mathcal{P},\ \mathfrak{P} \cap \Lambda = \mathfrak{p}\}.$$

Then there exists a polynomial-time algorithm that returns m elements of Λ whose classes generate $(1 + \mathfrak{p}\Lambda + \mathfrak{f})/(1 + \mathfrak{q}\Lambda + \mathfrak{f})$. If $e_\mathfrak{p} = 1$; we have $m = 0$. If $e_\mathfrak{p} > 1$, the number m of generators is bounded by $d(1 + \log_2(e_\mathfrak{p}))[K : \mathbb{Q}]$.

Proof. If $e_\mathfrak{p} = 1$, we clearly have $\mathfrak{p} = \mathfrak{q}$, and so $m = 0$. If $e_\mathfrak{p} > 1$, we let $l \in \mathbb{Z}_{>0}$ be minimal subject to the condition $\mathfrak{p}^{2^l} \subseteq \mathfrak{q}$. Then there exists a filtration

$$\mathfrak{p}\Lambda + \mathfrak{f} \supseteq (\mathfrak{q} + \mathfrak{p}^2)\Lambda + \mathfrak{f} \supseteq \cdots \supseteq (\mathfrak{q} + \mathfrak{p}^{2^{l-1}})\Lambda + \mathfrak{f} \supseteq \mathfrak{q}\Lambda + \mathfrak{f}.$$

For each $i = 0, \ldots, l-1$, the map $\overline{x} \mapsto \overline{x - 1}$ induces an isomorphism

$$\frac{1 + (\mathfrak{q} + \mathfrak{p}^{2^i})\Lambda + \mathfrak{f}}{1 + (\mathfrak{q} + \mathfrak{p}^{2^{i+1}})\Lambda + \mathfrak{f}} \longrightarrow \frac{(\mathfrak{q} + \mathfrak{p}^{2^i})\Lambda + \mathfrak{f}}{(\mathfrak{q} + \mathfrak{p}^{2^{i+1}})\Lambda + \mathfrak{f}}$$

of abelian groups. Hence, any $\mathbb{Z}$-basis of the right-hand side yields generators of the left-hand side. It remains to bound l. For every $\mathfrak{P} \in \mathcal{P}$ with $\mathfrak{P} \cap \Lambda = \mathfrak{p}$, the inclusion $\mathfrak{p}^{e_\mathfrak{p}} = (\mathfrak{P} \cap \Lambda)^{e_\mathfrak{p}} \subseteq \mathfrak{P}^{e_\mathfrak{p}} \cap \Lambda \subseteq \mathfrak{P}^{e_\mathfrak{P}} \cap \Lambda$ holds. Hence, $\mathfrak{p}^{e_\mathfrak{p}} \subseteq \mathfrak{q}$ and therefore $2^l \leq 2e_\mathfrak{p}$, which gives $l \leq 1 + \log_2(e_\mathfrak{p})$.

Since any quotient $((\mathfrak{q} + \mathfrak{p}^{2^i})\Lambda + \mathfrak{f})/((\mathfrak{q} + \mathfrak{p}^{2^{i+1}})\Lambda + \mathfrak{f})$ is generated by at most $d[K : \mathbb{Q}]$ elements, the quotient $(1 + \mathfrak{p}\Lambda + \mathfrak{f})/(1 + \mathfrak{q}\Lambda + \mathfrak{f})$ is generated by at most $(1 + \log_2(e_\mathfrak{p}))d[K : \mathbb{Q}]$ elements. □

Proposition 6.11. *Given Λ and $\mathfrak{f}$ as above, the problem of computing generators of $(\Lambda/\mathfrak{f})^\times$ and $K_1(\Lambda/\mathfrak{f})$ is probabilistic polynomial-time reducible to the factorisation of $\mathfrak{g} := \mathfrak{f} \cap \mathcal{O}_C$ as an ideal of $\mathcal{O}_C$ and, for each prime ideal divisor $\mathfrak{P}$ of $\mathfrak{g}$, at most d instances of* Primitive *for extensions of $\mathcal{O}/(\mathcal{O} \cap \mathfrak{P})$ of degree at most d. The number of generators is bounded by $5d[K : \mathbb{Q}] \log_2 |\mathcal{O}_C/\mathfrak{g}|$.*

Proof. Using the factorisation of $\mathfrak{g} = \mathfrak{f} \cap \mathcal{O}_C$, one can determine the sets of ideals $\mathcal{P}$, $\mathcal{P}'$ and $\mathcal{Q}$ in polynomial time. Since $|\mathcal{Q}| = |\mathcal{P}'| \leq |\mathcal{P}| \leq \log_2|\mathcal{O}_C/\mathfrak{g}|$, the claim follows from the reduction to the computation of $\mathrm{G}(\Lambda/(\mathfrak{q}\Lambda + \mathfrak{f}))$ for each $\mathfrak{q} \in \mathcal{Q}$ discussed at the beginning of the section, the exact sequence (5), Lemmas 6.9 and 6.10 and the following computation

$$\begin{aligned}
&d|\mathcal{P}'|([K : \mathbb{Q}] + 2) + d[K : \mathbb{Q}] \sum_{\mathfrak{p} \in \mathcal{P}', e_\mathfrak{p} > 1} (1 + \log_2(e_\mathfrak{p})) \\
&\leq d[K : \mathbb{Q}]\left(3|\mathcal{P}'| + \sum_{\mathfrak{p} \in \mathcal{P}', e_\mathfrak{p} > 1} 2\log_2(e_\mathfrak{p})\right) \\
&\leq d[K : \mathbb{Q}]\left(3|\mathcal{P}'| + 2\sum_{\mathfrak{P} \in \mathcal{P}} \log_2(e_\mathfrak{P})\right) \\
&\overset{(*)}{\leq} d[K : \mathbb{Q}]\left(3|\mathcal{P}'| + 2\log_2|\mathcal{O}_C/\mathfrak{g}|\right) \\
&\leq 5d[K : \mathbb{Q}] \log_2|\mathcal{O}_C/\mathfrak{g}|.
\end{aligned}$$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

The inequality $(*)$ is a consequence of

$$\sum_{\mathfrak{P}\in\mathcal{P}} \log_2(e_{\mathfrak{P}}) \le \sum_{\mathfrak{P}\in\mathcal{P}} e_{\mathfrak{P}} \le \sum_{\mathfrak{P}\in\mathcal{P}} e_{\mathfrak{P}} \log_2 |\mathcal{O}_C/\mathfrak{P}| = \log_2 |\mathcal{O}_C/\mathfrak{g}|,$$

which, in turn, is immediate from $\mathcal{O}_C/\mathfrak{g} \cong \prod_{\mathfrak{P}\in\mathcal{P}} \mathcal{O}_C/\mathfrak{P}^{e_{\mathfrak{P}}}$. □

Remark 6.12. In the setup above, we start with a proper full two-sided ideal $\mathfrak{f}$ of $\mathcal{M}$ contained in Λ and set $\mathfrak{g} := \mathfrak{f} \cap C$. Under hypothesis (H) on A, we may instead start with a proper full ideal $\mathfrak{g}$ of $\mathcal{O}_C$ such that $\mathfrak{g}\mathcal{M}$ is contained in Λ and then set $\mathfrak{f} := \mathfrak{g}\mathcal{M}$. In this situation, we then have $\mathfrak{g} = \mathfrak{f} \cap \mathcal{O}_C$ by [Rei03, (27.6)].

7. Lifting units of reduced norm one

Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$. Let $r \in \mathbb{Z}_{>0}$, and let $A = \prod_{i=1}^{r} \mathrm{Mat}_{n_i}(K_i)$, where K_i is a finite field extension of K and $n_i \in \mathbb{Z}_{>0}$ for each i. In particular, A is a finite-dimensional semisimple K-algebra satisfying hypothesis (H). Let C be the centre of A, which we can and do identify with $\prod_{i=1}^{r} K_i$. In this situation, the reduced norm map $\mathrm{nr}\colon A \to C$ is equal to the product of maps $\det : \mathrm{Mat}_{n_i}(K_i) \to K_i$.

Let $\mathcal{M}$ be a maximal $\mathcal{O}$-order in A, and let $\mathcal{O}_C = \mathcal{M} \cap C = \prod_{i=1}^{r} \mathcal{O}_{K_i}$. Then nr restricts to a group homomorphism $\mathrm{nr}\colon \mathcal{M}^\times \to \mathcal{O}_C^\times$, which is surjective since A satisfies the Eichler condition relative to $\mathcal{O}$ (see [CR87, (45.4), (45.6)]). Let $\mathfrak{g}$ be a proper full ideal of $\mathcal{O}_C$, and let $\mathfrak{f} = \mathfrak{g}\mathcal{M}$. Then by Lemma 4.4 there exists a commutative diagram of groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{SL}(\mathcal{M}) & \longrightarrow & \mathcal{M}^\times & \xrightarrow{\mathrm{nr}} & \mathcal{O}_C^\times & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_2} & & \\ 1 & \longrightarrow & \mathrm{SL}(\mathcal{M}/\mathfrak{f}) & \longrightarrow & (\mathcal{M}/\mathfrak{f})^\times & \xrightarrow{\overline{\mathrm{nr}}} & (\mathcal{O}_C/\mathfrak{g})^\times & \longrightarrow & 1, \end{array} \tag{6}$$

where the rows are exact, $\mathrm{SL}(\mathcal{M})$ and $\mathrm{SL}(\mathcal{M}/\mathfrak{f})$ are defined by the exactness of these rows, and the vertical maps are induced by the canonical projections. Note that this is consistent with diagram (4), but we do not require an order Λ for the above setup.

The aim of this section is to show that, under the above assumptions on A and $\mathfrak{f}$, the map f_1 is surjective, and there exists a polynomial-time algorithm that given an element of $\mathrm{SL}(\mathcal{M}/\mathfrak{f}) = \mathrm{SL}(\mathcal{M}/\mathfrak{g}\mathcal{M})$ returns a preimage under f_1.

7.1. Lifting unimodular matrices

We first consider the case where $A = \mathrm{Mat}_n(K)$ and $\mathcal{M} = \mathrm{Mat}_n(\mathcal{O})$ for some $n \in \mathbb{Z}_{>0}$. In this situation, we have $\mathcal{O} = \mathcal{O}_C$ and $\mathcal{M}/\mathfrak{f} = \mathrm{Mat}_n(\mathcal{O}/\mathfrak{g})$. Moreover, both the maps nr and $\overline{\mathrm{nr}}$ in diagram (6) are just the usual determinant maps, $\mathrm{SL}(\mathcal{M}) = \mathrm{SL}_n(\mathcal{O})$, and $\mathrm{SL}(\mathcal{M}/\mathfrak{f}) = \mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$. Thus, f_1 is the canonical map $f_1 : \mathrm{SL}_n(\mathcal{O}) \to \mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$. Note that this map is trivial when $n = 1$, so we henceforth suppose that $n \ge 2$.

We use the following notation for a commutative ring R. Given $1 \le i, j \le n$ with $i \ne j$, and $r \in R$, we denote by $e_{ij}(r) \in \mathrm{SL}_n(R)$ the matrix with ones on the diagonal and entry r at position (i, j). We refer to these matrices as *elementary matrices*. Let $\mathrm{E}_n(R)$ denote the subgroup of $\mathrm{SL}_n(R)$ generated by all elementary matrices.

Since $\mathcal{O}/\mathfrak{g}$ is semilocal, $\mathrm{SL}_n(\mathcal{O}/\mathfrak{g}) = \mathrm{E}_n(\mathcal{O}/\mathfrak{g})$ by [Bas68, Chapter V, Corollary 9.2]. Thus, every element of $\mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$ can be expressed as a product of elementary matrices, and every such matrix can easily be lifted to an elementary matrix in $\mathrm{SL}_n(\mathcal{O})$. This immediately implies the theoretical part of Corollary 7.6 below. However, we will need a constructive proof that then translates into an efficient algorithm.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

We will show that, given the factorisation of $\mathfrak{g}$, there exists a polynomial-time algorithm for lifting unimodular matrices over $\mathcal{O}/\mathfrak{g}$ to $\mathcal{O}$. The idea is to reduce to the local case and then apply the Chinese remainder theorem.

For any matrix M, let M^t denote its transpose. A vector $\mathbf{v} = (v_1, \dots, v_n)^t$ of elements of a commutative ring R is said to be *unimodular* if $\sum_{i=1}^n Rv_i = R$. In the following we denote by $\mathfrak{q} = \mathfrak{p}^l$, $l \in \mathbb{Z}_{>0}$, the power of a nonzero prime ideal of $\mathcal{O}$. Note that $\mathcal{O}/\mathfrak{q}$ is a local ring.

Lemma 7.1. *There exists a polynomial-time algorithm that given a unimodular vector $\mathbf{v} \in (\mathcal{O}/\mathfrak{q})^n$ returns elementary matrices $E_1, \dots, E_k \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{q})$ such that $E_1 \cdots E_k \mathbf{v} = (x, 0, \dots, 0)^t$ for some $x \in (\mathcal{O}/\mathfrak{q})^\times$.*

Proof. Write $\mathbf{v} = (v_1, \dots, v_n)^t$. Note that as $\mathcal{O}/\mathfrak{q}$ is local; $\mathbf{v}$ being unimodular implies that there exists $1 \leq i \leq n$ such that $v_i \in (\mathcal{O}/\mathfrak{q})^\times$.

Case 1: If $v_1 \in (\mathcal{O}/\mathfrak{q})^\times$, then $e_{21}(-v_1^{-1}v_2) \cdots e_{n1}(-v_1^{-1}v_n)\mathbf{v}$ has the required form.

Case 2: If $v_i \in (\mathcal{O}/\mathfrak{q})^\times$ with $1 < i \leq n$, then after multiplying $\mathbf{v}$ by $e_{1i}(1)e_{i1}(-1)e_{1i}(1)$ on the left, the first entry will be invertible and we are in the first case. □

Lemma 7.2. *There exists a polynomial-time algorithm that given a matrix $V \in \mathrm{SL}_n(\mathcal{O}/\mathfrak{q})$ returns elementary matrices $E_1, \dots, E_k \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{q})$ such that $E_1 \cdots E_k V$ is upper triangular. If V is lower triangular, then $E_1 \cdots E_k V$ is diagonal.*

Proof. The first part follows by repeatedly applying Lemma 7.1 to V and submatrices of V. If V is lower triangular, then we are always in Case 1 of the proof of Lemma 7.1 and thus easily see that the resulting matrix is diagonal. □

As we will see below, the previous results allow us to transform unimodular matrices into diagonal matrices. Thus, it remains to consider unimodular diagonal matrices.

Lemma 7.3. *There exists a polynomial-time algorithm that given $V = \mathrm{diag}(v_1, \dots, v_n) \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{q})$ with $\prod_{1 \leq i \leq n} v_i = 1$ returns elementary matrices $E_1, \dots, E_k \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{q})$ such that $E_1 \cdots E_k V$ is the $n \times n$ identity matrix.*

Proof. From [Ros94, 2.1.3 Corollary] it follows that a diagonal matrix with diagonal $(1, \dots, 1, v, v^{-1}, 1, \dots, 1)$ with $v \in (\mathcal{O}/\mathfrak{q})^\times$ is the product of six elementary matrices since

$$\begin{pmatrix} v & 0 \\ 0 & v^{-1} \end{pmatrix} = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -v^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Hence, we can left-multiply V with $6(n-1)$ elementary matrices to obtain $(1, 1, \dots, 1)^t$. □

Proposition 7.4. *There exists a polynomial-time algorithm that given a matrix $V \in \mathrm{SL}_n(\mathcal{O}/\mathfrak{q})$ returns elementary matrices $E_1, \dots, E_k, F_1, \dots, F_l \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{q})$ such that $E_1 \cdots E_k V F_1 \dots F_l$ is the $n \times n$ identity matrix.*

Proof. Using Lemma 7.2 there exist elementary matrices $E_1, \dots, E_{k'}$ such that $U := E_1 \cdots E_{k'} V$ is an upper triangular matrix. Using Lemma 7.2 again, this time applied to the lower diagonal matrix U^t, we can find elementary matrices $F_1, \dots, F_l$ such that $D = UF_1 \cdots F_l$ is a diagonal matrix. Finally, invoking Lemma 7.3 yields elementary matrices $\tilde{E}_1, \dots, \tilde{E}_{\tilde{k}}$ such that $\tilde{E}_1 \cdots \tilde{E}_{\tilde{k}} D$ is the $n \times n$ identity matrix. □

Corollary 7.5. *There exists a polynomial-time algorithm that given the factorisation of $\mathfrak{g}$ and a matrix $V \in \mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$ returns elementary matrices $E_1, \dots, E_k \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{g})$ such that $V = E_1 \cdots E_k$.*

Proof. In the case that $\mathfrak{g}$ is a prime ideal power, this follows from Proposition 7.4. Now, let $\mathfrak{g} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ be the product of m coprime prime ideal powers, and consider a matrix $V \in \mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$. For each

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

$1 \le i \le m$ we can determine in polynomial time a factorisation of $V \in \mathrm{SL}_n(\mathcal{O}/\mathfrak{q}_i)$ into elementary matrices. The result follows by observing that the canonical map

$$\mathrm{E}_n(\mathcal{O}/\mathfrak{g}) \to \prod_{i=1}^{m} \mathrm{E}_n(\mathcal{O}/\mathfrak{q}_i)$$

is an isomorphism by the Chinese remainder theorem which can be made effective in polynomial time ([Coh00, Proposition 1.3.11]). □

Since we can trivially lift elementary matrices along the canonical map $f_1 : \mathrm{SL}_n(\mathcal{O}) \to \mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$, the same is true for arbitrary matrices in $\mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$.

Corollary 7.6. *There exists a polynomial-time algorithm that given the factorisation of* $\mathfrak{g}$ *and a matrix* $V \in \mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$ *returns* $U \in \mathrm{SL}_n(\mathcal{O})$ *such that* $f_1(U) = V$.

7.2. Lifting norm one units for nice maximal orders

We now consider the case in which $A = \mathrm{Mat}_n(K)$ and $\mathcal{M} = \mathcal{M}_{\mathfrak{a},n}$ is a nice maximal order as defined in §6.2, where $\mathfrak{a}$ is a nonzero fractional ideal of $\mathcal{O}$ and $n \in \mathbb{Z}_{\ge 2}$. (As in §7.1, the case $n = 1$ is trivial.) Some of the ideas used here are based on [BJ08, §6].

Let $\mathfrak{b}$ be an integral ideal of $\mathcal{O}$ such that $\mathfrak{b} + \mathfrak{g} = \mathcal{O}$ and $\mathfrak{a} = \xi\mathfrak{b}$ for some $\xi \in K^\times$. Such an ideal $\mathfrak{b}$ and element ξ can be computed in probabilistic polynomial time, as shown in Corollary A.2. Let $b \in \mathfrak{b}$, $y \in \mathfrak{g}$ such that $b + y = 1$, and let $R = \mathcal{O}/\mathfrak{g}$. Then we have an isomorphism $\mathcal{O}/\mathfrak{g} \to \mathfrak{a}/\mathfrak{a}\mathfrak{g}$ of R-modules defined by $z + \mathfrak{g} \mapsto zb\xi + \mathfrak{a}\mathfrak{g}$, with the inverse map given by $x + \mathfrak{a}\mathfrak{g} \mapsto \xi^{-1}x + \mathfrak{g}$. The first of these maps induces an isomorphism $\theta_1 : R^{\oplus n} \to R^{\oplus n-1} \oplus \mathfrak{a}/\mathfrak{a}\mathfrak{g}$ of R-modules, and the second map induces an inverse θ_2. Define $n \times n$ diagonal matrices $\Phi_1 = \mathrm{diag}(1, \dots, 1, \xi^{-1})$ and $\Phi_2 = \mathrm{diag}(1, \dots, 1, b\xi)$. Then we have maps

$$\psi_1 \colon \mathrm{Mat}_n(\mathcal{O}) \longrightarrow \mathcal{M},\ X \mapsto \Phi_2 X \Phi_1 \quad \text{and} \quad \psi_2 \colon \mathcal{M} \longrightarrow \mathrm{Mat}_n(\mathcal{O}),\ Y \mapsto \Phi_1 Y \Phi_2.$$

These maps are not multiplicative in general. However, since θ_1 and θ_2 are mutually inverse isomorphisms, we see that ψ_1 and ψ_2 induce mutually inverse isomorphisms

$$\overline{\psi}_1 \colon \mathrm{GL}_n(\mathcal{O}/\mathfrak{g}) \to (\mathcal{M}/\mathfrak{g}\mathcal{M})^\times \quad \text{and} \quad \overline{\psi}_2 \colon (\mathcal{M}/\mathfrak{g}\mathcal{M})^\times \to \mathrm{GL}_n(\mathcal{O}/\mathfrak{g}).$$

Lemma 7.7. *Let* $\overline{E} \in \mathrm{SL}_n(\mathcal{O}/\mathfrak{g})$ *be an elementary matrix. Then* $\overline{\psi}_1(\overline{E})$ *can be lifted to an element* $U \in \mathcal{M}^\times$ *with* $\mathrm{nr}(U) = 1$.

Proof. For $V \in \mathrm{Mat}_n(\mathcal{O})$ we write

$$V = \left(\begin{array}{c|c} V_1 & x \\ \hline y & d \end{array}\right)$$

with $V_1 \in \mathrm{Mat}_{n-1}(\mathcal{O}), x, y^t \in \mathcal{O}^{n-1}$ and $d \in \mathcal{O}$. Then

$$\psi_1(V) = \left(\begin{array}{c|c} V_1 & \xi^{-1}x \\ \hline \xi b y & bd \end{array}\right).$$

Let $I_m \in \mathrm{Mat}_m(\mathcal{O})$ denote the identity matrix.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Case 1: If $\overline{E} = \left(\begin{array}{c|c} e_{ij}(\bar{a}) & 0 \\ \hline 0 & 1 \end{array}\right)$ with $a \in \mathcal{O}$, then $\overline{\psi}_1(\overline{E}) = \left(\begin{array}{c|c} e_{ij}(\bar{a}) & 0 \\ \hline 0 & \bar{b} \end{array}\right)$ and a lift is given by

$$\left(\begin{array}{c|c} e_{ij}(a) & 0 \\ \hline 0 & 1 \end{array}\right).$$

Case 2: If $\overline{E} = \left(\begin{array}{c|c} \overline{I}_{n-1} & \bar{x} \\ \hline 0 & 1 \end{array}\right)$ with $\bar{x}^t = (0, \ldots, 0, \bar{a}, 0, \ldots, 0), a \in \mathcal{O}$, then $\overline{\psi}_1(\overline{E}) = \left(\begin{array}{c|c} \overline{I}_{n-1} & \overline{\xi^{-1}x} \\ \hline 0 & \bar{b} \end{array}\right)$ and a lift is given by

$$\left(\begin{array}{c|c} I_{n-1} & \xi^{-1}x \\ \hline 0 & 1 \end{array}\right).$$

Note that in this case $\xi^{-1}a \in \mathfrak{b}\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$.

Case 3: If $\overline{E} = \left(\begin{array}{c|c} \overline{I}_{n-1} & 0 \\ \hline \bar{y} & 1 \end{array}\right)$ with $\bar{y} = (0, \ldots, 0, \bar{a}, 0, \ldots, 0), a \in \mathcal{O}$, then $\psi_1(\overline{E}) = \left(\begin{array}{c|c} \overline{I}_{n-1} & 0 \\ \hline \overline{\xi b y} & \bar{b} \end{array}\right)$ and a lift is given by

$$\left(\begin{array}{c|c} I_{n-1} & 0 \\ \hline \xi b y & 1 \end{array}\right).$$

Here we note that $\xi b a \in \xi\mathfrak{b} = \mathfrak{a}$. □

Proposition 7.8. *For $A = \mathrm{Mat}_n(K)$ let $\mathcal{M} = \mathcal{M}_{\mathfrak{a},n} \subseteq A$ be a nice maximal order. Then there exists a probabilistic polynomial-time algorithm that given the factorisation of $\mathfrak{g}$ and $V \in \mathrm{SL}(\mathcal{M}/\mathfrak{g}\mathcal{M})$ returns $U \in \mathrm{SL}(\mathcal{M})$ with $f_1(U) = V$.*

Proof. By Corollary 7.5 we can find elementary matrices $E_1, \ldots, E_r \in \mathrm{Mat}_n(\mathcal{O}/\mathfrak{g})$ with $\overline{\psi}_2(V) = E_1 \cdots E_r$. Applying $\overline{\psi}_1$ we obtain $V = \overline{\psi}_1(E_1) \cdots \overline{\psi}_1(E_r)$. Moreover, by Lemma 7.7, each of the matrices $\overline{\psi}_1(E_i)$ can be lifted to a matrix $U_i \in \mathcal{M}^\times$ with $\mathrm{nr}(U_i) = 1$. Thus, we can and do take $U := \prod_i U_i$. □

7.3. Lifting norm one units in maximal orders

We now consider an arbitrary maximal order $\mathcal{M}$ of $A = \prod_{i=1}^r \mathrm{Mat}_{n_i}(K_i)$.

Theorem 7.9. *The map $f_1 \colon \mathrm{SL}(\mathcal{M}) \to \mathrm{SL}(\mathcal{M}/\mathfrak{g}\mathcal{M})$ is surjective. Moreover, there exists a probabilistic polynomial-time algorithm that given the factorisation of $\mathfrak{g}$ and $V \in \mathrm{SL}(\mathcal{M}/\mathfrak{g}\mathcal{M})$ returns an element $U \in \mathrm{SL}(\mathcal{M})$ with $f_1(U) = V$.*

Proof. By decomposing $\mathcal{M}$ using the central primitive idempotents, it is sufficient to consider the case $A = \mathrm{Mat}_n(K)$. By Lemma 6.2, we can and do assume that $\mathcal{M} = \mathcal{M}_{\mathfrak{a},n}$ is a nice maximal order. Thus, the result follows from Proposition 7.8. □

8. Isomorphism testing and the principal ideal problem

Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$, and let A be a finite-dimensional K-algebra satisfying hypothesis (H). Let Λ be an $\mathcal{O}$-order in A. In this section, we present the main algorithm for solving the isomorphism problem IsIsomorphic for lattices over Λ.

We begin with two straightforward reductions which together show that it suffices to consider the problem IsPrincipal in the case that A is semisimple. Note that these reductions are valid when A is an arbitrary finite-dimensional K-algebra that does not necessarily satisfy hypothesis (H).

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Proposition 8.1. *The problem* IsIsomorphic *is polynomial-time reducible to* IsPrincipal. *More precisely, for Λ-lattices X and Y, the problem* IsIsomorphic *is polynomial-time reducible to* IsPrincipal *for an $\mathrm{End}_\Lambda(Y)$-lattice in $\mathrm{End}_A(KY)$.*

Proof. Let X and Y be two Λ-lattices. By [CIK97, Corollary 3] we can check in polynomial time whether the A-modules KX and KY are isomorphic and, if so, compute an isomorphism $f\colon KY \to KX$. Then $\Phi\colon \mathrm{Hom}_A(KX, KY) \to \mathrm{End}_A(KY)$, $g \mapsto g \circ f$ is an isomorphism of $\mathrm{End}_A(KY)$-modules. Recall from §3.1 that we consider $\mathrm{Hom}_\Lambda(X, Y)$ as a subset of $\mathrm{Hom}_A(KX, KY)$. Thus, by Proposition 3.1, the Λ-lattices X and Y are isomorphic if and only if the full $\mathrm{End}_\Lambda(Y)$-lattice $\Phi(\mathrm{Hom}_\Lambda(X, Y))$ in $\mathrm{End}_A(KY)$ is free of rank 1 and for every (any) free generator α the morphism $\alpha \circ f^{-1}\colon X \to Y$ is an isomorphism. □

Let $\mathrm{J}(A)$ denote the Jacobson radical of A, and recall that $\overline{A} := A/\mathrm{J}(A)$ is a semisimple K-algebra by [CR81, (5.19)]. For any full Λ-lattice X in A, let $\overline{X}$ denote its image under the canonical projection map $A \to \overline{A}$. Note that $\overline{\Lambda}$ is an $\mathcal{O}$-order in $\overline{A}$.

Proposition 8.2. *The problem* IsPrincipal *for an arbitrary finite-dimensional K-algebra is polynomial-time reducible to* IsPrincipal *for a finite-dimensional semisimple K-algebra. More precisely, for a full Λ-lattice X in A, the problem* IsPrincipal *is polynomial-time reducible to the problem* IsPrincipal *for the full $\overline{\Lambda}$-lattice $\overline{X}$ in $\overline{A}$.*

Proof. The Jacobson radical of A can be computed in polynomial time by [FR85, 1.5 A]. The result then follows from Theorem 3.4. □

The main algorithm of the present article is as follows.

Algorithm 8.3. Suppose that A is semisimple and satisfies hypothesis (H). Let X be a full Λ-lattice in A. The following steps solve IsPrincipal(X), that is, they determine whether there exists $\alpha \in X$ such that $X = \Lambda\alpha$ and, if so, return such an element α.

(1) Determine the centre C of A, the decomposition $A = \prod_i A_i$ into simple K-algebras A_i and, for each i, an isomorphism $A_i \cong \mathrm{Mat}_{n_i}(K_i)$.
(2) Compute a maximal $\mathcal{O}$-order $\mathcal{M}$ in A containing Λ and its centre $\mathcal{O}_C := \mathcal{M} \cap C$.
(3) Compute the central primitive idempotents e_i and the components $\mathcal{M}_i := \mathcal{M}e_i$.
(4) Compute the central conductor $\mathfrak{g} := \{x \in C \mid x\mathcal{M} \subseteq \Lambda\}$ of Λ in $\mathcal{M}$ and $\mathfrak{f} := \mathfrak{g}\mathcal{M}$.
(5) Check whether $\mathcal{M}X$ is free over $\mathcal{M}$, and if so, compute β such that $\mathcal{M}X = \mathcal{M}\beta$.
(6) Check whether X is locally free over Λ.
(7) Replace X by $X\xi$, where $\xi \in A^\times$ is such that $X\xi \subseteq \Lambda$ and $X\xi + \mathfrak{f} = \Lambda$.
(8) Compute a set of generators for $(\Lambda/\mathfrak{f})^\times$.
(9) Let $\overline{\mathrm{nr}}\colon (\mathcal{M}/\mathfrak{f})^\times \longrightarrow (\mathcal{O}_C/\mathfrak{g})^\times$ be the map of Lemma 4.4. Compute $(\mathcal{O}_C/\mathfrak{g})^\times$ as an abstract abelian group and compute $\overline{\mathrm{nr}}((\Lambda/\mathfrak{f})^\times)$ as a subgroup of $(\mathcal{O}_C/\mathfrak{g})^\times$.
(10) Let π_2 and f_2 be the maps defined in the commutative diagram (4). Decide whether $\overline{\mathrm{nr}}(\overline{\beta})$ is in the image of $\pi_2 \circ f_2$, and if so, compute $\bar{a} \in (\Lambda/\mathfrak{f})^\times$ and $u \in \mathcal{M}^\times$ such that $\overline{\mathrm{nr}}(\overline{\beta a}) = \overline{\mathrm{nr}}(\bar{u})$.
(11) Compute $v \in \mathrm{SL}(\mathcal{M})$ such that $\overline{\beta a u^{-1}} = \overline{v}$.

If any of steps (5), (6) or (10) fail, then X is not free over Λ. If all these steps succeed, then $X = \Lambda\alpha$ where $\alpha := (vu)^{-1}\beta$.

Proof of correctness of Algorithm 8.3. Failure of steps (5) or (6) immediately implies that X is not free over Λ. Otherwise, we use the local bases computed in step (6) to replace X by $X\xi$ in step (7), as described in Proposition 6.8 and its proof. After successful completion of steps (1) to (7), we then can and do assume that X is a locally free full Λ-lattice in A such that $X + \mathfrak{f} = \Lambda$ and $\mathcal{M}X = \mathcal{M}\beta$. These are the assumptions needed for Theorem 4.5. Moreover, since A is semisimple and satisfies hypothesis (H), the map f_1 in diagram (4) is surjective by Theorem 7.9, and so Theorem 4.5 (b) can be applied. Hence, X is free over Λ if and only if $\overline{\mathrm{nr}}(\overline{\beta})$ is contained in the image of $\pi_2 \circ f_2$. This is precisely what is checked in step (10). In addition, the second part of Theorem 4.5 (b) implies that $X = \Lambda\alpha$ with α as at the end of Algorithm 8.3. □

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

The following result analyses the complexity of Algorithm 8.3, and further details on each step are given in the proof.

Theorem 8.4. *Let Λ be an $\mathcal{O}$-order in a finite-dimensional semisimple K-algebra A satisfying hypothesis* (H)*, and let $K_1, \dots, K_r$ be the simple components of the centre of A. Let $\mathcal{M}$ be any choice of maximal $\mathcal{O}$-order in A containing Λ, and let $\mathfrak{h} = [\mathcal{M} : \Lambda]_{\mathcal{O}}$ be the module index of Λ in $\mathcal{M}$. Then for a full Λ-lattice X in A, Algorithm 8.3 reduces the problem* IsPrincipal(X) *in probabilistic polynomial time to*

(a) Wedderburn(A)*, the computation of the Wedderburn decomposition of A,*
(b) Factor(Disc(Λ))*, the factorisation of the discriminant of Λ,*
(c) *for each i with $1 \le i \le r$, one instance of* IsPrincipal$_{\mathcal{O}_{K_i}}$*,*
(d) *for each i with $1 \le i \le r$,* UnitGroup$(\mathcal{O}_{K_i})$*,*
(e) *for each prime ideal divisor $\mathfrak{p}$ of $\mathfrak{h}$, the problem* DLog *for extensions of $\mathcal{O}/\mathfrak{p}$ and*
(f) *for each prime ideal divisor $\mathfrak{p}$ of $\mathfrak{h}$, the problem* Primitive *for extensions of $\mathcal{O}/\mathfrak{p}$.*

Note that $\mathcal{M}$ and $\mathfrak{h}$ are not part of the input and $\mathfrak{h}$ is only needed for the above complexity statement. Moreover, $\mathfrak{h}$ does not depend on the choice of $\mathcal{M}$.

Proof. In the following, the steps refer to those of Algorithm 8.3. Let $\mathcal{M}$ be the maximal order computed in step (2), and let $\mathfrak{f}$ be the ideal computed in step (4). Before analysing the steps, we make the following observations. By [Rei03, (25.3)], Disc$(\mathcal{M})$ is independent of the choice of $\mathcal{M}$. Moreover, by [CR81, (26.3)(iii)], we have Disc$(\Lambda) = \mathfrak{h}^2$Disc$(\mathcal{M})$, and so Disc$(\Lambda)$ and $\mathfrak{h}$ are also independent of the choice of $\mathcal{M}$. Since $\mathfrak{h}\mathcal{M} \subseteq \Lambda$, we have $\mathfrak{h} \subseteq \mathfrak{g}$ for any choice of $\mathcal{M}$. Therefore, Disc$(\Lambda) \subseteq \mathfrak{h} \subseteq \mathfrak{g}$ and $\mathfrak{h}\Lambda \subseteq \mathfrak{f}$. In particular, Factor$(\mathcal{O} \cap \mathfrak{f})$ and Factor$(\mathfrak{g})$ reduce in polynomial time to Factor(Disc(Λ)).

Step (1) is an instance of Wedderburn. In step (2), the problem of computing a maximal $\mathcal{O}$-order $\mathcal{M}$ in A containing Λ reduces in probabilistic polynomial time to Factor(Disc(Λ)) by Proposition 6.1. It is then trivial to determine $\mathcal{O}_C = \mathcal{M} \cap C$. Step (3) can be easily performed using the isomorphisms $A_i \cong \mathrm{Mat}_{n_i}(K_i)$ from step (1). In step (4), the central conductor $\mathfrak{g}$ can be computed as the intersection $(\mathcal{M} : \Lambda)_l \cap C$, where $(\mathcal{M} : \Lambda)_l := \{x \in \mathcal{M} \mid x\mathcal{M} \subseteq \Lambda\}$ is the left conductor of Λ into $\mathcal{M}$. As the left conductor can be determined using a pseudo-Hermite normal form computation (see [Fri00, (2.16)]), this step can also be performed in polynomial time. Step (5) is probabilistic polynomial-time reducible to one instance of IsPrincipal$_{\mathcal{O}_{K_i}}$ for each $1 \le i \le r$, by Proposition 6.4. Steps (6) and (7) are probabilistic polynomial-time reducible to Factor$(\mathcal{O} \cap \mathfrak{f})$ by Proposition 6.8.

Step (8): Proposition 6.11 shows that this is probabilistic polynomial-time reducible to Factor$(\mathfrak{g})$ and for each prime ideal divisor $\mathfrak{P}$ of $\mathfrak{g}$ at most d instances of Primitive in extensions of $\mathcal{O}/(\mathcal{O} \cap \mathfrak{P})$ of degree at most d. Now, for each prime ideal $\mathfrak{p}$ dividing $\mathfrak{g} \cap \mathcal{O}$, there are at most d prime ideals $\mathfrak{P}$ of $\mathcal{O}_C$ satisfying $\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$. Finally, note that $\mathfrak{g} \cap \mathcal{O}$ divides $\mathfrak{h}$.

Step (9): It follows from [Coh00, Algorithms 4.2.2 and 4.2.17] that the computation of generators and the structure of $(\mathcal{O}_C/\mathfrak{g})^\times$ as an abelian group is polynomial-time reducible to Factor$(\mathfrak{g})$ and for each prime ideal divisor $\mathfrak{P}$ of $\mathfrak{g}$ one instance of Primitive in an extension $\mathcal{O}/(\mathcal{O} \cap \mathfrak{P})$ of degree at most d. Estimating the number of prime ideal divisors as in the previous paragraph shows that this part contributes d instances of Primitive in (e). Let $V = \{\bar{a}_1, \dots, \bar{a}_m\}$ be a set of generators of $(\Lambda/\mathfrak{f})^\times$. Let e denote the exponent of $(\mathcal{O}_C/\mathfrak{g})^\times$, and let $\mathcal{G} := \prod_{i=1}^m \mathbb{Z}/e\mathbb{Z} \cdot \bar{a}_i$ be the $\mathbb{Z}/e\mathbb{Z}$-free abelian group on V. Let $\bar{\nu}\colon \mathcal{G} \to (\mathcal{O}_C/\mathfrak{g})^\times$ be the homomorphism induced by $\bar{a}_i \mapsto \overline{\mathrm{nr}}(\bar{a}_i)$. Then $\mathrm{im}(\bar{\nu}) = \overline{\mathrm{nr}}((\Lambda/\mathfrak{f})^\times)$ and we apply algorithms for finite abelian groups (see [Coh00, §4.1]) to compute the image. For this we have to solve the discrete logarithm in $(\mathcal{O}_C/\mathfrak{g})^\times$ for each of the m generators $\bar{a}_1, \dots, \bar{a}_m$. By Proposition 6.11, the number m is bounded by $5d[K : \mathbb{Q}] \log_2 |\mathcal{O}_C/\mathfrak{g}|$. Thus, the claim in part (f) follows from

$$|\mathcal{O}_C/\mathfrak{g}| \le |\mathcal{O}_C/\mathfrak{h}\mathcal{O}_C| = \prod_{i=1}^{r} |\mathcal{O}_{K_i}/\mathfrak{h}\mathcal{O}_{K_i}| = \prod_{i=1}^{r} \mathrm{N}_{K_i/\mathbb{Q}}(\mathfrak{h}\mathcal{O}_{K_i}) = \prod_{i=1}^{r} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{h})^{[K_i:K]}$$
$$= \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{h})^{[C:K]} \le \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{h})^d.$$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Note that solving the discrete logarithm in $(\mathcal{O}_C/\mathfrak{g})^\times$ requires solving the discrete logarithm problem in $(\mathcal{O}_C/\mathfrak{P})^\times$ for all prime ideals $\mathfrak{P}$ dividing $\mathfrak{g}$. As in step (8), for each prime ideal $\mathfrak{p}$ dividing $\mathfrak{g} \cap \mathcal{O}$ there are at most d prime ideals $\mathfrak{P}$ of $\mathcal{O}_C$ with $\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$ and for each of those prime ideals $\mathcal{O}_C/\mathfrak{P}$ is an extension of $\mathcal{O}/\mathfrak{p}$ of degree at most d.

Step (10): The reduced norm map $\mathrm{nr}\colon \mathcal{M}^\times \to \mathcal{O}_C^\times$ is surjective by Lemma 6.3. The computation of $\mathcal{O}_C^\times$ is performed componentwise and thus reduces to $\mathsf{UnitGroup}(\mathcal{O}_{K_i})$ for $1 \le i \le r$. We then determine the image of the canonical projection $\mathcal{O}_C^\times \to (\mathcal{O}_C/\mathfrak{g})^\times/\mathrm{im}(\bar{\nu})$ as an abstract subgroup of $(\mathcal{O}_C/\mathfrak{g})^\times/\mathrm{im}(\bar{\nu})$. This again requires an instance of solving the discrete logarithm in $(\mathcal{O}_C/\mathfrak{g})^\times$ for each of the generators of $\mathcal{O}_C^\times$. By Dirichlet's unit theorem the number of these generators can be bounded by d. Applying standard algorithms for finite abelian groups it is then straightforward to decide whether $\overline{\mathrm{nr}}(\bar{\beta})$ is contained in the image of $\mathcal{O}_C^\times \to (\mathcal{O}_C/\mathfrak{g})^\times/\mathrm{im}(\bar{\nu})$ and, if so, to compute $\epsilon \in \mathcal{O}_C^\times$, $a \in (\Lambda/\mathfrak{f})^\times$ such that $\bar{\epsilon} \equiv \overline{\beta a} \pmod{\mathfrak{g}}$. An element $u \in \mathcal{M}^\times$ such that $\mathrm{nr}(u) = \epsilon$ can be found using Lemma 6.3 in probabilistic polynomial time. Note that this step requires one more instance of solving the discrete logarithm in $(\mathcal{O}_C/\mathfrak{g})^\times$, which was already analysed in step (9).

Step (11): As the factorisation of $\mathfrak{g}$ is known, this can be done in probabilistic polynomial time by Theorem 7.9. □

We now consider the case in which we allow certain precomputations that only depend on the order Λ and not on the Λ-lattice X.

Corollary 8.5. *Fix an $\mathcal{O}$-order Λ in a finite-dimensional semisimple K-algebra A satisfying hypothesis* (H)*, and let $K_1, \dots, K_r$ be the simple components of the centre of A. Then for a full Λ-lattice X in A, the problem* $\mathsf{IsPrincipal}(X)$ *reduces in probabilistic polynomial to* $\mathsf{IsPrincipal}$ *for $\mathcal{O}_{K_i}$, $1 \le i \le r$, and* DLog.

Proof. In Algorithm 8.3 we may consider all steps which do not depend on X as precomputations. Then for each lattice X only steps (5), (6), (7), (10) and (11) have to be performed. The claim follows as in the proof of Theorem 8.4. □

Remark 8.6. In Theorem 8.4 better results can be obtained by describing the complexity in terms of the central conductor $\mathfrak{g}$ (which depends not only on the order Λ but also on the maximal order computed during the algorithm) instead of $\mathfrak{h}$. More precisely, (e) and (f) can be replaced by

(e′) for each prime ideal divisor $\mathfrak{P}$ of $\mathfrak{g}$, the problem DLog for extensions of $\mathcal{O}/(\mathcal{O} \cap \mathfrak{P})$,
(f′) for each prime ideal divisor $\mathfrak{P}$ of $\mathfrak{g}$, the problem $\mathsf{Primitive}$ for extensions of $\mathcal{O}/(\mathcal{O} \cap \mathfrak{P})$.

Remark 8.7. By Remark 5.2, in Theorem 8.4, (a) can be replaced by

(a′) $\mathsf{SplittingMatrixAlgebra}(A_i)$ for $1 \le i \le r$, where $A = \bigoplus_{i=1}^r A_i$ is the decomposition into simple K-algebras.

Note that we have formulated Theorem 8.4 using $\mathsf{Wedderburn}$ since for certain families of algebras, one can directly solve $\mathsf{Wedderburn}$ in polynomial time (which would not necessarily be true after passing to the simple components). This happens, for example, for certain algebras of the form $A/\mathrm{J}(A)$ that appear in the similarity problem for matrices over rings of integers of number fields (see §9.3).

Remark 8.8. In view of Remarks 5.1 and 5.2, as well as the reductions of Propositions 8.1 and 8.2, the problems $\mathsf{IsPrincipal}_\Lambda$ and $\mathsf{IsIsomorphic}_\Lambda$ for orders Λ in finite-dimensional K-algebras A satisfying hypothesis (H) reduces

(a) in probabilistic subexponential time to $\mathsf{UnitGroup}$ and $\mathsf{IsPrincipal}$ for rings of integers of number fields, and $\mathsf{Wedderburn}$ or $\mathsf{SplittingMatrixAlgebra}$,
(b) in quantum polynomial time to $\mathsf{Wedderburn}$ or $\mathsf{SplittingMatrixAlgebra}$.

9. Application: similarity of matrices over rings of integers

After proving some general results on the similarity of matrices over commutative rings, we will give an application of Algorithm 8.3 to the similarity problem for matrices over rings of integers of number fields.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

9.1. Similarity of matrices over commutative rings

Let R be a commutative ring, and let $n \in \mathbb{Z}_{>0}$. Recall that two matrices $A, B \in \mathrm{Mat}_n(R)$ are said to be *similar over* R if there exists a *conjugating matrix* $C \in \mathrm{GL}_n(R)$ such that $B = CAC^{-1}$.

We will adopt the setup of Faddeev [Fad66]. For $A, B \in \mathrm{Mat}_n(R)$ we define

$$C_R(A, B) = \{X \in \mathrm{Mat}_n(R) \mid XA = BX\} \quad \text{and} \quad C_R(B) = C_R(B, B).$$

Note that $C_R(B)$ is an R-algebra and that $C_R(A, B)$ is a (left) $C_R(B)$-module.

Lemma 9.1. *Suppose there exists $C \in \mathrm{GL}_n(R)$ such that $B = CAC^{-1}$. Then the maps*

$$\theta_C : C_R(B) \longrightarrow C_R(A, B), \quad X \longmapsto XC,$$
$$\theta_{C^{-1}} : C_R(A, B) \longrightarrow C_R(B), \quad X \longmapsto XC^{-1},$$

are mutually inverse $C_R(B)$-module isomorphisms.

Proof. If $X \in C_R(B)$, then $B(XC) = XBC = X(CAC^{-1})C = (XC)A$ and so $XC \in C_R(A, B)$. Hence, the map θ_C is well defined. Similarly, the map θ_C^{-1} is also well defined and it is clear that θ_C and $\theta_{C^{-1}}$ are mutually inverse. □

Proposition 9.2. *Two matrices $A, B \in \mathrm{Mat}_n(R)$ are similar over R if and only if*

(a) *the $C_R(B)$-module $C_R(A, B)$ is free of rank* 1*, and*
(b) *every (any) free generator C of $C_R(A, B)$ over $C_R(B)$ is in $\mathrm{GL}_n(R)$.*

Furthermore, when this is the case, C as in part (b) satisfies $B = CAC^{-1}$.

Proof. Suppose that (a) and (b) hold, and let C be a free generator of $C_R(A, B)$ over $C_R(B)$. In particular, $C \in C_R(A, B) \cap \mathrm{GL}_n(R)$, and it easily follows that $B = CAC^{-1}$. Suppose conversely that there exists $C \in \mathrm{GL}_n(R)$ such that $B = CAC^{-1}$. Then θ_C is an isomorphism by Lemma 9.1, and so C is a free generator of $C_R(A, B)$ over $C_R(B)$. Thus, (a) holds. Now, let D be any free generator of $C_R(A, B)$ over $C_R(B)$. Then there exists $E \in C_R(B)^\times \subseteq \mathrm{GL}_n(R)$ such that $D = EC$ and so $D \in \mathrm{GL}_n(R)$. Thus, (b) holds. □

The following result was proven by Faddeev [Fad66, Theorem 2] in the case $R = \mathbb{Z}$, though it was expressed in terms of ideals rather than modules. Moreover, Guralnick [Gur80, Theorem 6] observed that the proof works for any integral domain. We include a short proof for the convenience of the reader and for comparison as per Remark 9.4.

Proposition 9.3. *Suppose that R is an integral domain. Two matrices $A, B \in \mathrm{Mat}_n(R)$ are similar over R if and only if*

(a) *the $C_R(B)$-module $C_R(A, B)$ is free of rank* 1*, and*
(b) *for every maximal ideal $\mathfrak{p}$ of R, the matrices A and B are similar over $R_\mathfrak{p}$.*

Furthermore, when this is the case, any free generator C of $C_R(A, B)$ over $C_R(B)$ satisfies $B = CAC^{-1}$.

Proof. Suppose that $A, B \in \mathrm{Mat}_n(R)$ are similar over R. Then (b) clearly holds and (a) holds by Proposition 9.2. Suppose conversely that (a) and (b) hold. Let C be a free generator of $C_R(A, B)$ over $C_R(B)$. Let $\mathfrak{p}$ be a maximal ideal of R. Then there exists $C_\mathfrak{p} \in \mathrm{GL}_n(R_\mathfrak{p})$ such that $B = C_\mathfrak{p} A C_\mathfrak{p}^{-1}$ and so $C_\mathfrak{p} \in C_{R_\mathfrak{p}}(A, B)$. Since C is also a free generator of $C_{R_\mathfrak{p}}(A, B)$ over $C_{R_\mathfrak{p}}(B)$, there exists $D_\mathfrak{p} \in C_{R_\mathfrak{p}}(B)$ such that $C_\mathfrak{p} = D_\mathfrak{p} C$. Then $\det(D_\mathfrak{p}) \det(C) = \det(C_\mathfrak{p}) \in R_\mathfrak{p}^\times$ and so $\det(C) \in R_\mathfrak{p}^\times$. Moreover, by [CR81, (4.2)(iv)], we have $R = \cap_\mathfrak{p} R_\mathfrak{p}$ which implies that $R^\times = \cap_\mathfrak{p} R_\mathfrak{p}^\times$, where in both cases the intersection ranges over all maximal ideals $\mathfrak{p}$ of R. Therefore, $\det(C) \in R^\times$ and so $C \in \mathrm{GL}_n(R)$. In particular, $C \in C_R(A, B) \cap \mathrm{GL}_n(R)$, and it easily follows that $B = CAC^{-1}$. □

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Remark 9.4. Propositions 9.2 and 9.3 and their proofs are analogues of Propositions 3.1 and 3.3, respectively. Indeed, in the case that R is a Noetherian integral domain, the former can be deduced from the latter, though it is easier to give more direct proofs of more general results. Moreover, as well as having weaker hypotheses, Proposition 9.2 is better suited to algorithmic applications than Proposition 9.3.

9.2. The similarity problem in terms of modules over polynomial rings

Let R be a commutative ring, and let $n \in \mathbb{Z}_{>0}$. Let $R[x]$ be a polynomial ring in one variable over R. For $A \in \mathrm{Mat}_n(R)$, we define $T_R(A)$ to be the $R[x]$-module R^n with the action $xv = Av$ for $v \in R^n$.

Lemma 9.5. *Let $A, B, C \in \mathrm{Mat}_n(R)$. Define $\psi_{A,B,C} : T_R(A) \to T_R(B)$ by $v \mapsto Cv$. Then $C \in C_R(A, B)$ if and only if $\psi_{A,B,C}$ is an $R[x]$-module homomorphism. In particular, we have canonical isomorphisms*

(a) *$C_R(A, B) \cong \mathrm{Hom}_{R[x]}(T_R(A), T_R(B))$ of R-modules;*
(b) *$C_R(A) \cong \mathrm{End}_{R[x]}(T_R(A))$ of R-algebras.*

Proof. The function $\psi_{A,B,C}$ is an $R[x]$-module homomorphism if and only if $C(Av) = B(Cv)$ for all $v \in R^n$, which in turn is equivalent to $C \in C_R(A, B)$. This gives the first claim; the remaining claims now follow easily. □

The following result is well known and is an easy consequence of Lemma 9.5.

Lemma 9.6. *Let $A, B, C \in \mathrm{Mat}_n(R)$. Then the following are equivalent:*

(a) *$C \in C_R(A, B) \cap \mathrm{GL}_n(R)$,*
(b) *$C \in \mathrm{GL}_n(R)$ and $B = CAC^{-1}$,*
(c) *$\psi_{A,B,C}$ is an $R[x]$-module isomorphism.*

In particular, A and B are similar over R if and only if $T_R(A) \cong T_R(B)$ as $R[x]$-modules.

9.3. Jacobson radicals of certain endomorphism algebras

Let F be a field. We now explicitly compute the Jacobson radical $\mathrm{J}(\mathrm{End}_{F[x]}(V))$ of $\mathrm{End}_{F[x]}(V)$ for a finitely generated $F[x]$-module V. The motivating application is Proposition 9.11 below.

Lemma 9.7. *Let $f \in F[x]$ be an irreducible polynomial, and let $j, k \in \mathbb{Z}_{>0}$. Let*

$$\lambda \in \mathrm{Hom}_{F[x]}(F[x]/(f^j), F[x]/(f^k)) \quad \text{and} \quad \mu \in \mathrm{Hom}_{F[x]}(F[x]/(f^k), F[x]/(f^j)).$$

(a) *If $j \le k$ then $\mathrm{im}(\lambda) \subseteq f^{k-j} \cdot \big(F[x]/(f^k)\big)$.*
(b) *For any choice of j, k we have $\mathrm{im}(\lambda \circ \mu) \subseteq f^{|k-j|} \cdot \big(F[x]/(f^k)\big)$.*

Proof. Suppose $j \le k$. We have $\lambda(x + (f^j)) = y + (f^k)$ for some $y \in F[x]$. Then

$$f^j y + (f^k) = f^j(y + (f^k)) = f^j \lambda(x + f^j) = \lambda(f^j x + (f^j)) = \lambda(0) = 0,$$

so $f^j y \in (f^k)$ and hence $y \in (f^{k-j})$. Thus, (a) follows from the fact that the image of λ is uniquely determined by the image of $x + (f^j)$. Part (b) follows easily from (a). □

Proposition 9.8. *Let $f \in F[x]$ be an irreducible polynomial. Let $m \in \mathbb{Z}_{>0}$, let $d_1, \dots, d_m \in \mathbb{Z}_{\ge 0}$ and let $V = \bigoplus_{j=1}^m (F[x]/(f^j))^{d_j}$. Then we have a canonical isomorphism*

$$\mathrm{End}_{F[x]}(V) \cong E := \bigoplus_{j=1}^m \bigoplus_{k=1}^m e_{jk} \mathrm{Hom}_{F[x]}((F[x]/(f^k))^{d_k}, (F[x]/(f^j))^{d_j}), \tag{7}$$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

where the right-hand side denotes the $m \times m$ 'matrix ring' with (j,k)-th entries in $\mathrm{Hom}_{F[x]}((F[x]/(f^k))^{d_k}, (F[x]/(f^j))^{d_j})$. *For $1 \leq j,k \leq m$, define $\gamma_{jk} = f$ if $j = k$ and $\gamma_{jk} = 1$ otherwise. Then the isomorphism $\mathrm{End}_{F[x]}(V) \cong E$ induces isomorphisms*

$$\mathrm{J}(\mathrm{End}_{F[x]}(V)) \cong I := \bigoplus_{j=1}^{m} \bigoplus_{k=1}^{m} e_{jk}\gamma_{jk}\mathrm{Hom}_{F[x]}((F[x]/(f^k))^{d_k}, (F[x]/(f^j))^{d_j}), \text{ and} \tag{8}$$

$$\mathrm{End}_{F[x]}(V)/\mathrm{J}(\mathrm{End}_{F[x]}(V)) \cong E/I \cong \prod_{j=1}^{m} \mathrm{Mat}_{d_j}(F[x]/(f)). \tag{9}$$

Proof. The decomposition (7) follows from standard properties of Homs and direct sums. It follows from Lemma 9.7 (b) that I is a two-sided ideal of E. Moreover, it is straightforward to check that E/I is canonically isomorphic to the right-hand side of equation (9). Thus, E/I is Artinian semisimple and so $\mathrm{J}(E/I) = 0$ by [CR81, (5.18)]. Hence, $\mathrm{J}(E) \subseteq I$ by [CR81, (5.6)(ii)]. Lemma 9.7 (a) and the definition of γ_{jk} implies that each element $\lambda = (\lambda_{jk}) \in I$ is an upper triangular matrix in the sense that for $j \geq k$ the image of λ_{jk} is contained in $f \cdot F[x]/(f^j)$. Hence, for $\mu = (\mu_{jk}) \in I^m$ the image of each μ_{jk} is contained in $f \cdot F[x]/(f^j)$. It follows that $I^{m^2} = 0$, and thus I is nilpotent. Thus, since E is Artinian, $I \subseteq \mathrm{J}(E)$ by [CR81, (5.15)]. Therefore, $\mathrm{J}(E) = I$, as claimed. □

Corollary 9.9. *Let $r \in \mathbb{Z}_{>0}$, and let $V = \bigoplus_{i=1}^{r} V_i$, where $V_i = \bigoplus_{j=1}^{m_i} (F[x]/(f_i^j))^{d_{i,j}}$ for some $m_i \in \mathbb{Z}_{>0}$, $d_{i,j} \in \mathbb{Z}_{\geq 0}$, and some distinct monic irreducible polynomials $f_i \in F[x]$. Then there are canonical isomorphisms*

$$\mathrm{End}_{F[x]}(V) \cong \prod_{i=1}^{r} \mathrm{End}_{F[x]}(V_i) \cong \prod_{i=1}^{r} \bigoplus_{j=1}^{m_i} \bigoplus_{k=1}^{m_i} e_{jk}\mathrm{Hom}_{F[x]}((F[x]/(f_i^k))^{d_{i,k}}, (F[x]/(f_i^j))^{d_{i,j}})$$

and

$$\mathrm{End}_{F[x]}(V)/\mathrm{J}(\mathrm{End}_{F[x]}(V)) \cong \prod_{i=1}^{r} \prod_{j=1}^{m_i} \mathrm{Mat}_{d_{i,j}}(F[x]/(f_i)).$$

In particular, if F is a number field, then $\mathrm{End}_{F[x]}(V)$ satisfies hypothesis (H).

Proof. The desired result follows from Proposition 9.8 together with the observation that $\mathrm{Hom}_{F[x]}(V_i, V_j) = 0$ for $i \neq j$. □

Proposition 9.10. *Let $n \in \mathbb{Z}_{>0}$, and let $A \in \mathrm{Mat}_n(F)$.*

(a) *The minimal polynomial of A is squarefree if and only if $C_F(A)$ is semisimple.*
(b) *The minimal polynomial of A is equal to the characteristic polynomial of A if and only if $C_F(A)/\mathrm{J}(C_F(A))$ is isomorphic to a finite product of fields.*
(c) *The characteristic polynomial of A is squarefree if and only if $C_F(A)$ is isomorphic to a finite product of fields.*
(d) *If A is nilpotent, then $C_F(A)/\mathrm{J}(C_F(A))$ is isomorphic to $\prod_{j=1}^{m} \mathrm{Mat}_{d_j}(F)$ for some $m, d_1, \ldots, d_m \in \mathbb{Z}_{>0}$.*

Proof. Let $f \in F[x]$ denote the characteristic polynomial of A. It is a standard result in linear algebra that there is an isomorphism of $F[x]$-modules

$$T_F(A) \cong F[x]/(g_1) \oplus \cdots \oplus F[x]/(g_s), \tag{10}$$

where $g_1, \ldots, g_s \in F[x]$ are the invariant factors of A and $g_1 \mid g_2 \mid \cdots \mid g_s$. Thus, g_s is the minimal polynomial of A and $f = g_1 \cdots g_s$. Moreover, by Lemma 9.5 (b), there is a canonical isomorphism

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

$C_F(A) \cong \mathrm{End}_{F[x]}(V)$ of F-algebras, where $V := T_F(A)$. Let $f_1, \dots, f_r \in F[x]$ denote the distinct monic irreducible factors of f. Then there exists a decomposition $V = \bigoplus_{i=1}^{r} V_i$ and isomorphisms $V_i \cong \bigoplus_{j=1}^{m_i} F[x]/(f_i^j)^{d_{i,j}}$ for some $m_i \in \mathbb{Z}_{>0}$ and $d_{i,j} \in \mathbb{Z}_{\geq 0}$. (a) Observe that g_s is squarefree if and only if each g_k is squarefree if and only if $m_i = 1$ for $i = 1, \dots, r$. By Corollary 9.9, this in turn is equivalent to the triviality of $\mathrm{J}(\mathrm{End}_{F[x]}(V))$, which is equivalent to the semisimplicity of $\mathrm{End}_{F[x]}(V)$ by [CR81, (5.18)]. (b) Observe that $g_s = f$ if and only if $s = 1$ if and only if $d_{i,1} = 1$ for $i = 1, \dots, r$. By Corollary 9.9, this in turn holds if and only if $\mathrm{End}_{F[x]}(V)/\mathrm{J}(\mathrm{End}_{F[x]}(V))$ is isomorphic to a finite product of fields. (c) This follows from the previous two parts, once one obverses that if f is squarefree then it must be equal to g_s. (d) If A is nilpotent, then f is some power of x, and so $r = 1$ and $f_1 = x$. Thus the claim follows from Proposition 9.8 and the canonical isomorphism $F[x]/(x) \cong F$. □

Proposition 9.11. *Let K be a number field, let $n \in \mathbb{Z}_{>0}$, and let $A \in \mathrm{Mat}_n(K)$. Let f be the characteristic polynomial of A, and let $f = f_1^{n_1} \cdots f_r^{n_r}$ be its factorisation, where $f_1, \dots, f_r \in K[x]$ are distinct monic irreducible polynomials and $n_i \in \mathbb{Z}_{>0}$ for each i. Let $K_i = K[x]/(f_i)$ for $i = 1, \dots, r$. Then there exists a polynomial-time algorithm that computes the factorisation of f, computes $C_K(A)$ and $\mathrm{J}(C_K(A))$ and computes an explicit homomorphism of K-algebras*

$$\rho \colon C_K(A) \longrightarrow C_K(A)/\mathrm{J}(C_K(A)) \xrightarrow{\cong} \prod_{i=1}^{r} \prod_{j=1}^{m_i} \mathrm{Mat}_{d_{i,j}}(K_i)$$

for some $m_i \in \mathbb{Z}_{>0}$ and $d_{i,j} \in \mathbb{Z}_{\geq 0}$ such that $\sum_{j=1}^{m_i} j d_{i,j} = n_i$ for each i. In particular, this solves Wedderburn *for $C_K(A)/\mathrm{J}(C_K(A))$, which satisfies hypothesis* (H).

Proof. Assume the setup and notation of the proof of Proposition 9.10 with $F = K$. The isomorphism of (10) is obtained when computing the rational canonical form, which can be performed in polynomial time (see [Vil93, Theorem 4]). Moreover, polynomials in $K[x]$ can be factored in polynomial time by the algorithm of [Len83, (4.5) Theorem]. Thus, we can explicitly compute a decomposition $T_K(A) = \bigoplus_{i=1}^{r} V_i$ and isomorphisms $V_i \cong \bigoplus_{j=1}^{m_i} (K[x]/(f_i^j))^{d_{i,j}}$ for some $m_i \in \mathbb{Z}_{>0}$ and $d_{i,j} \in \mathbb{Z}_{\geq 0}$. Note that, for each i, we have $\sum_{j=1}^{m_i} j d_{i,j} = n_i$ since $f = g_1 \cdots g_s$. Since $C_K(A)$ is canonically isomorphic to $\mathrm{End}_{K[x]}(T_K(A))$ by Lemma 9.5 (b), the desired result now follows from Corollary 9.9. □

9.4. An algorithm for determining similarity and computing a conjugating matrix

We now consider the following problem.

Problem (IsSimilar). Given a number field K with ring of integers $\mathcal{O} = \mathcal{O}_K$, an integer $n \in \mathbb{Z}_{>0}$ and two matrices $A, B \in \mathrm{Mat}_n(\mathcal{O})$, determine whether A and B are similar over $\mathcal{O}$, and if so, return a conjugating matrix $C \in \mathrm{GL}_n(\mathcal{O})$ such that $B = CAC^{-1}$.

Let $n \in \mathbb{Z}_{>0}$, and let $A, B \in \mathrm{Mat}_n(\mathbb{Z})$. Assume that there exists $D \in \mathrm{GL}_n(\mathbb{Q})$ such that $B = DAD^{-1}$. Thus, A and B have the same minimal polynomial $f \in \mathbb{Z}[x]$, and so the $\mathbb{Z}[x]$-modules $T_{\mathbb{Z}}(A)$ and $T_{\mathbb{Z}}(B)$ are in fact $\mathbb{Z}[x]/(f)$-lattices. In view of Lemma 9.6, this implies that IsSimilar over $\mathbb{Z}$ can be reduced to the problem of determining whether the $\mathbb{Z}[x]/(f)$-lattices $T_{\mathbb{Z}}(A)$ and $T_{\mathbb{Z}}(B)$ are isomorphic and, if so, of computing an isomorphism between them.

Using this observation, Sarkisyan [Sar79] and Grunewald [Gru80] independently showed that the conjugacy problem over $\mathbb{Z}$ for arbitrary pairs of matrices is decidable. Moreover, Applegate and Onishi [AO81, AO82] considered the cases of 2×2 and 3×3 matrices, and Behn and Van der Merwe [BVdM02] also considered the 2×2 case.

In the case that the characteristic polynomial of A (and B) is squarefree (and thus the minimal and characteristic polynomials coincide), the above approach via $\mathbb{Z}[x]/(f)$-lattices is equivalent to a classical result of Latimer–MacDuffee [LM33]. This last result was recently generalised in the dissertation of Husert [Hus17] to the case where the minimal polynomial is squarefree but the characteristic polynomial is arbitrary. See Proposition 9.10 for properties of the $\mathbb{Q}$-algebra $C_{\mathbb{Q}}(A)$ in both of these special cases.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

For a discussion of practical algorithms that have been implemented on a computer, see §9.5.

Proposition 9.12. *Let R be a Noetherian integral domain with field of fractions $K \neq R$. Let $n \in \mathbb{Z}_{>0}$, and let $A, B \in \mathrm{Mat}_n(R)$. Suppose that $D \in \mathrm{GL}_n(K)$ satisfies $B = DAD^{-1}$. Then A and B are similar over R if and only if*

(a) *the $C_R(B)$-lattice $C_R(A,B)D^{-1}$ in $C_K(B)$ is free of rank 1, and*
(b) *every (any) free generator C' of $C_R(A,B)D^{-1}$ over $C_R(B)$ satisfies $C'D \in \mathrm{GL}_n(R)$.*

Furthermore, when this is the case, $B = CAC^{-1}$, where $C := C'D$.

Proof. By Lemma 9.1 the map $\theta_{D^{-1}} : C_K(A,B) \to C_K(B)$, $X \mapsto XD^{-1}$ is an isomorphism of $C_K(B)$-modules. Hence, the desired result follows from Proposition 9.2. □

The main algorithm of this section is as follows.

Algorithm 9.13. Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$, let $n \in \mathbb{Z}_{>0}$ and let $A, B \in \mathrm{Mat}_n(\mathcal{O})$. The following steps solve IsSimilar for A and B, that is, they determine whether A and B are similar over $\mathcal{O}$, and if so, return an element $C \in \mathrm{GL}_n(\mathcal{O})$ such that $B = CAC^{-1}$.

(1) Check whether A and B are similar over K, and if so, compute $D \in \mathrm{GL}_n(K)$ such that $B = DAD^{-1}$. If not, then A and B are not similar over $\mathcal{O}$.
(2) Compute $C_K(B)$, $\mathrm{J}(C_K(B))$ and an explicit homomorphism of K-algebras

$$\rho : C_K(B) \longrightarrow C_K(B)/\mathrm{J}(C_K(B)) \xrightarrow{\cong} \prod_{i=1}^{t} \mathrm{Mat}_{d_i}(K_i),$$

where the K_i's are (not necessarily distinct) finite field extensions of K.
(3) Check whether $\rho(C_{\mathcal{O}}(A,B)D^{-1})$ is a free $\rho(C_{\mathcal{O}}(B))$-lattice, and if so, compute a generator $E \in \rho(C_{\mathcal{O}}(A,B)D^{-1})$. If not, then A and B are not similar over $\mathcal{O}$.
(4) Compute $C' \in C_{\mathcal{O}}(A,B)D^{-1}$ such that $\rho(C') = E$.
(5) Check whether $C := C'D \in \mathrm{GL}_n(\mathcal{O})$. If so, then $B = CAC^{-1}$. If not, then A and B are not similar over $\mathcal{O}$.

Proof of correctness of Algorithm 9.13. If all steps succeed, then $C \in C_{\mathcal{O}}(A,B) \cap \mathrm{GL}_n(\mathcal{O})$ and it easily follows that $B = CAC^{-1}$. It remains to show that if any of steps (1), (3) or (5) fail, then A and B are not similar over $\mathcal{O}$. If step (1) fails, then this is clear. If step (3) fails, then Theorem 3.4 (a) implies that $C_{\mathcal{O}}(A,B)D^{-1}$ is not free over $C_{\mathcal{O}}(B)$, and the result follows from Proposition 9.12 (a). Finally, suppose that step (5) fails, that is, $C \notin \mathrm{GL}_n(\mathcal{O})$. If C' is not a free generator of $C_{\mathcal{O}}(A,B)D^{-1}$ over $C_{\mathcal{O}}(B)$, then Theorem 3.4 (b) implies that $C_{\mathcal{O}}(A,B)D^{-1}$ is not free over $C_{\mathcal{O}}(B)$, and again the result follows from Proposition 9.12 (a). If C' is a free generator of $C_{\mathcal{O}}(A,B)D^{-1}$ over $C_{\mathcal{O}}(B)$, then the result follows from Proposition 9.12 (b). □

The following result analyses the complexity of Algorithm 9.13, and further details on each step are given in the proof.

Theorem 9.14. *Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$, let $n \in \mathbb{Z}_{>0}$ and let $A, B \in \mathrm{Mat}_n(\mathcal{O})$. Let $f_1, \ldots, f_r \in K[x]$ be the distinct monic irreducible factors of the characteristic polynomial of B. For $i = 1, \ldots, r$ let $K_i = K[x]/(f_i)$. Let Λ be the image of $C_{\mathcal{O}}(B)$ under the projection $C_K(B) \to C_K(B)/\mathrm{J}(C_K(B))$. Let $\mathcal{M}$ be any choice of maximal $\mathcal{O}$-order in $C_K(B)/\mathrm{J}(C_K(B))$ containing Λ, and let $\mathfrak{h} = [\mathcal{M} : \Lambda]_{\mathcal{O}}$ be the module index of Λ in $\mathcal{M}$. Then Algorithm 9.13 reduces the problem* IsSimilar *for A and B in probabilistic polynomial time to*

(a) $\mathsf{Factor}(\mathrm{Disc}(\Lambda))$, *the factorisation of the discriminant of Λ,*
(b) *for each i with $1 \leq i \leq r$, one instance of* $\mathsf{IsPrincipal}_{\mathcal{O}_{K_i}}$,
(c) *for each i with $1 \leq i \leq r$,* $\mathsf{UnitGroup}(\mathcal{O}_{K_i})$,
(d) *for each prime ideal divisor $\mathfrak{p}$ of $\mathfrak{h}$, the problem* DLog *for extensions of $\mathcal{O}/\mathfrak{p}$ and*
(e) *for each prime ideal divisor $\mathfrak{p}$ of $\mathfrak{h}$, the problem* Primitive *for extensions of $\mathcal{O}/\mathfrak{p}$.*

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

Note that $\mathcal{M}$ and $\mathfrak{h}$ are not part of the input and $\mathfrak{h}$ is only needed for the above complexity statement. Moreover, $\mathfrak{h}$ does not depend on the choice of $\mathcal{M}$.

Proof. In the following, the steps refer to those of Algorithm 9.13. Step (1) can be performed in polynomial time by [CIK97, Theorem 2], and step (2) can be performed in polynomial time by Proposition 9.11. Steps (4) and (5) are straightforward and can both be performed in polynomial time. Step (3) can be performed using Algorithm 8.3, and so the desired result now follows from Theorem 8.4 after noting that $\mathsf{Wedderburn}(C_K(B)/\mathsf{J}(C_K(B)))$ was already performed in step (2). □

We also record the following two consequences of Remark 8.8.

Corollary 9.15. *The problem* IsSimilar *reduces in probabilistic subexponential time to the problems* IsPrincipal *and* UnitGroup *for rings of integers of number fields.*

Corollary 9.16. *There exists a polynomial quantum algorithm for solving* IsSimilar.

9.5. Implementation of the algorithm

The algorithm for solving the principal ideal problem for orders in algebras satisfying hypothesis (H), and its application to the similarity problem has been implemented using the computer algebra package Hecke [FHHJ17] (also available in Oscar [OSC22]) and is included from version 0.13 onwards. The implementation works for arbitrary pairs of matrices in $\mathrm{Mat}_n(\mathbb{Z})$. We now give a brief comparison with other algorithms and implementations, all of which are for pairs of matrices in $\mathrm{Mat}_n(\mathbb{Z})$, subject to certain further restrictions in cases (a)–(c). Recall that in Proposition 9.10 the restrictions in (b) and (c) are rephrased in terms of the algebra $C_{\mathbb{Q}}(A)$.

(a) The algorithm of Opgenorth–Plesken–Schulz [OPS98] solves the similarity problem for pairs of matrices of finite order.
(b) The algorithm of Husert [Hus17] solves the similarity problem for pairs of matrices, both of which are either nilpotent or have squarefree minimal polynomial. However, the implementation is restricted to nilpotent matrices and matrices with irreducible minimal polynomial.
(c) The algorithm of Marseglia [Mar20] solves the similarity problem for pairs of matrices with squarefree characteristic polynomial (this condition implies that the minimal and characteristic polynomials coincide).
(d) The algorithm of Eick–O'Brien and the second named author of the present article [EHO19] is based on ideas of Grunewald [Gru80] and solves the similarity problem for arbitrary pairs of matrices.

All of the above algorithms (a)–(d) have been implemented in Magma [BCP97], but no formal complexity analysis has been given for any of them. However, we can compare these with our algorithm using timings and heuristic reasoning. All timings in the examples below were performed using a single core of a 3.40 GHz Intel E5-2643 processor and under the assumption of GRH. Magma V2.23-3 was used to run algorithms (a)–(d).

For random pairs of matrices of a given rational canonical form, our algorithm dramatically outperforms (a) and the algorithm for nilpotent matrices of (b). In the latter case this is not surprising since the algorithm in question requires an exhaustive search among candidates within a large search space. In the case of matrices with squarefree minimal polynomial, the bottleneck of algorithm (b) is a final enumeration over a set $\Lambda/\mathfrak{f}$, which our algorithm avoids by means of the results of §6.6 (in particular, see Proposition 6.11). In cases where the set $\Lambda/\mathfrak{f}$ is large, our algorithm dramatically outperforms that of (b).

Example 9.17. Consider the two matrices

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -5336100 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -5336100 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -5336100 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 5 & 0 & 53361000 & 0 \\ -5336100 & 0 & 40 & -5 & 0 & -53361000 \\ 0 & 0 & -8 & 1 & 0 & 0 \\ 0 & 0 & -5336164 & 8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -5336100 & 0 \end{pmatrix},$$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

both with irreducible minimal polynomial $f = x^2 + 5336100$ and characteristic polynomial f^3. The algorithm of (b) requires an enumeration over a set of size $2357947691 \approx 10^9$, thus rendering it impractical for this example. However, the implementation of our algorithm requires 6 seconds to recognise that A and B are similar over $\mathbb{Z}$ and to find a conjugating matrix. Note that $C_{\mathbb{Q}}(A) \cong \mathrm{Mat}_3(K)$, where $K = \mathbb{Q}[x]/(x^2 + 5336100)$.

Algorithm (c) is more restricted than (b) in that it requires the matrices in question to have squarefree characteristic polynomial. However, in contrast to the squarefree minimal polynomial case of (b), it avoids a final enumeration step, and thus it performs as well as our algorithm in this special case.

We have compared the implementation of our algorithm with that of algorithm (d) for a variety of different examples and found that in all cases the former outperformed the latter, often dramatically. However, we should mention that as a by-product, given a matrix $A \in \mathrm{Mat}_n(\mathbb{Z})$, algorithm (d) can be used to determine generators of the arithmetic group $C_{\mathbb{Z}}(A)^\times = \{X \in \mathrm{GL}_n(\mathbb{Z}) \mid XA = AX\}$. Various examples in [EHO19] as well as the overall strategy of finding candidates in large search spaces suggest that algorithm (d) has at least exponential complexity. We now review some of these examples from [EHO19] and show how our algorithm fares in comparison.

Example 9.18 [EHO19, 6.3.2]. Consider the two matrices

$$A = \begin{pmatrix} -3 & -1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -3 & -1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -5 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -3 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -5 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 13 & -15 & 16 & 24 & -16 & -7 & -35 & 15 & 0 \\ -3 & 44 & -40 & -71 & 62 & 28 & 157 & -76 & 16 \\ 18 & -15 & -3 & -7 & -31 & 6 & -226 & 129 & -52 \\ -69 & 72 & -55 & -78 & 86 & 18 & 355 & -186 & 48 \\ -75 & 98 & -82 & -124 & 117 & 35 & 406 & -206 & 46 \\ -45 & 19 & -21 & -22 & 10 & 1 & 49 & -25 & -3 \\ 24 & -66 & 53 & 89 & -89 & -31 & -289 & 147 & -37 \\ 30 & -78 & 61 & 102 & -104 & -35 & -348 & 178 & -45 \\ 24 & 11 & -8 & -23 & 26 & 14 & 58 & -29 & 11 \end{pmatrix},$$

both with irreducible minimal polynomial $f = x^3 + 2x^2 + 13x - 1$ and characteristic polynomial f^3. As these are not equal, algorithm (c) cannot be applied in this situation. Moreover, algorithm (d) fails to run in reasonable time because the search space is too large. However, the implementation of our algorithm requires 10 seconds to recognise that A and B are similar over $\mathbb{Z}$ and to find a conjugating matrix. Note that $C_{\mathbb{Q}}(A) \cong \mathrm{Mat}_3(K)$, where $K = \mathbb{Q}[x]/(f)$.

Example 9.19 [EHO19, 6.3.3]. Consider the two matrices

$$A = \begin{pmatrix} 13 & 67 & 6 & 0 & 0 & -1 \\ 0 & 1 & 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ -270 & -1350 & 0 & 1 & 2 & 20 \\ -135 & -675 & 0 & 0 & 1 & 10 \\ -27 & -135 & 0 & 0 & 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 13 & 79 & 0 & 0 & 1 & -76 \\ 0 & 1 & 0 & 0 & 0 & 3 \\ -270 & -1620 & 1 & 2 & -20 & 1620 \\ -135 & -810 & 0 & 1 & -10 & 810 \\ 27 & 162 & 0 & 0 & 2 & -162 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

both with minimal and characteristic polynomial equal to $(x-1)^4(x^2-15x-1)$. As this is not squarefree, algorithms (b) and (c) cannot be applied in this situation. Again, the search space for a certain subproblem is too large, making the computation infeasible for algorithm (d). However, the implementation of our algorithm finds a conjugating matrix in less than one second. Note that $\dim_{\mathbb{Q}}(C_{\mathbb{Q}}(A)) = 6$ and

$$C_{\mathbb{Q}}(A)/\mathrm{J}(C_{\mathbb{Q}}(A)) \cong \mathbb{Q} \times K,$$

where $K = \mathbb{Q}[x]/(x^2 - 15x - 1)$.

Example 9.20. Consider the two matrices

$$A = \begin{pmatrix} 1 & -4 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 & -6 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 \\ -4 & 16 & -3 & 0 & -5 & -6 \\ 0 & 0 & -37 & 0 & -9 & -55 \end{pmatrix}, \quad B = \begin{pmatrix} -88 & -4 & 0 & -66 & -51 & 32 \\ -2683 & 225 & 326 & -2670 & 1755 & 634 \\ -2607 & -666 & -332 & -525 & -6747 & 2835 \\ 14 & 0 & 0 & 13 & 2 & 0 \\ 523 & 38 & -3 & 330 & 440 & -325 \\ 285 & 74 & 37 & 54 & 749 & -314 \end{pmatrix},$$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

both with minimal and characteristic polynomial $(x-1)^2(x^4+58x^3+88x^2+176x+1)$. As this is not squarefree, algorithms (b) and (c) cannot be applied in this situation. Moreover, the implementation of algorithm (d) requires approximately one hour to find a conjugating matrix. By contrast, the implementation of our algorithm finds such a matrix in less than one second. Note that $\dim_{\mathbb{Q}}(C_{\mathbb{Q}}(A)) = 6$ and

$$C_{\mathbb{Q}}(A)/\mathrm{J}(C_{\mathbb{Q}}(A)) \cong \mathbb{Q} \times K,$$

where $K = \mathbb{Q}[x]/(x^4+58x^3+88x^2+176x+1)$.

10. Application: Galois module structure of rings of integers

An important motivation for Algorithm 8.3 and its predecessors is the investigation of the Galois module structure of rings of integers. We only briefly recall the problem here and refer the reader to the introduction of [HJ20] for a more detailed overview.

Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. The classical normal basis theorem says that $L \cong K[G]$ as $K[G]$-modules. A much more difficult problem is that of determining whether the ring of integers $\mathcal{O}_L$ is free over its so-called associated order $\mathcal{A}_{L/K} = \{\alpha \in K[G] \mid \alpha\mathcal{O}_L \subseteq \mathcal{O}_L\}$. Note that if a prime $\mathfrak{p}$ of K is (at most) tamely ramified in L/K or is such that the localised associated order $\mathcal{A}_{L/K,\mathfrak{p}}$ is maximal, then the localisation $\mathcal{O}_{L,\mathfrak{p}}$ is necessarily free over $\mathcal{A}_{L/K,\mathfrak{p}}$. In particular, $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}$ if and only if $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathcal{A}_{L/K,\mathfrak{p}}$ for every prime $\mathfrak{p}$ of K that is wildly ramified in L/K. In this situation, one can consider the class $[\mathcal{O}_L]$ in the locally free class group $\mathrm{Cl}(\mathcal{A}_{L/K})$. Moreover, if $K[G]$ satisfies hypothesis (H), then every order in $K[G]$ has the so-called locally free cancellation property (this follows from Jacobinski's cancellation theorem [CR87, (51.24)]), and so $\mathcal{O}_L$ is free over $\mathcal{A}_{L/K}$ if and only if it is locally free and the class $[\mathcal{O}_L]$ is the trivial element of $\mathrm{Cl}(\mathcal{A}_{L/K})$.

For an abstract finite group Γ, we say that L/K is a Γ-extension if it is a Galois extension such that $\mathrm{Gal}(L/K) \cong \Gamma$. Let $\Gamma = S_4 \times C_2$, the direct product of the symmetric group on 4 letters and the cyclic group of order 2. Since

$$\mathbb{Q}[\Gamma] \cong \prod_{i=1}^{4} \mathbb{Q} \times \prod_{j=1}^{2} \mathrm{Mat}_2(\mathbb{Q}) \times \prod_{k=1}^{4} \mathrm{Mat}_3(\mathbb{Q}),$$

the algebra $\mathbb{Q}[\Gamma]$ satisfies hypothesis (H). Using the methods of [FHS19], we have constructed wildly ramified Γ-extensions of $\mathbb{Q}$ of small discriminant. The wildly ramified Γ-extension of minimal discriminant is $L_1 := K_1(\sqrt{92})$, where K_1 is the S_4-extension of $\mathbb{Q}$ defined by

$$x^{24}+2x^{22}+27x^{20}+112x^{18}+585x^{16}+338x^{14}+5767x^{12} \\ +4362x^{10}+1417x^8-76x^6-29x^4-6x^2+1 \in \mathbb{Q}[x].$$

The field L_1 has discriminant $2^{84} \cdot 23^{24}$ and is wildly ramified at 2. Moreover, the associated order $\mathcal{A}_{L_1/\mathbb{Q}}$ has index $2^{43} \cdot 3^3$ in a maximal order $\mathcal{M}$ satisfying $\mathcal{A}_{L_1/\mathbb{Q}} \subseteq \mathcal{M} \subseteq \mathbb{Q}[\mathrm{Gal}(L_1/\mathbb{Q})]$ (note that this index is independent of the choice of $\mathcal{M}$). Using Algorithm 8.3 we have checked that $\mathcal{O}_{L_1}$ is free over $\mathcal{A}_{L_1/\mathbb{Q}}$ and have also obtained an explicit generator (unfortunately, the coefficients are too large to reproduce in print). The algorithms of [BB06, BW09] show that $\mathrm{Cl}(\mathcal{A}_{L_1/\mathbb{Q}}) \cong C_2$. However, the algorithm of [BW09] for solving the discrete logarithm problem in a locally free class group is restricted to the case in which the order in question is a group ring or a maximal order, and so this approach does not allow us to determine $[\mathcal{O}_{L_1}]$ in $\mathrm{Cl}(\mathcal{A}_{L_1/\mathbb{Q}})$.

We have performed the same computation using Algorithm 8.3 described above for all wildly ramified Γ-extensions $L/\mathbb{Q}$ with $|\mathrm{Disc}(L)| \leq 60^{48}$. For 686 out of these 2600 extensions, $\mathcal{O}_L$ is locally free

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

over $\mathcal{A}_{L/\mathbb{Q}}$, and in all of these cases, $\mathcal{O}_L$ is in fact free over $\mathcal{A}_{L/\mathbb{Q}}$. It would be interesting to find a proof of, or counterexample to, the assertion that the same phenomenon holds without the restriction on $|\mathrm{Disc}(L)|$.

A. Weak approximation in probabilistic polynomial time

Let K be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero integral ideals of $\mathcal{O}$. A classical result (see [Coh00, Corollary 1.3.9]) asserts that there exists a deterministic algorithm for computing $x \in K^\times$ such that $x\mathfrak{a}$ is integral and coprime to $\mathfrak{b}$. If the factorisation of $\mathfrak{b}$, or equivalently, of $\mathrm{N}(\mathfrak{b})$, is given, the algorithm runs in polynomial time. There also exists a probabilistic algorithm [Coh00, Algorithm 1.3.14], which does not require the factorisation of $\mathfrak{b}$ or $\mathrm{N}(\mathfrak{b})$, but is not polynomial time. The aim of this section is to combine the deterministic and probabilistic variants to obtain a probabilistic polynomial-time algorithm. The approach is based on the following general form of the constructive weak approximation theorem, which relies on ideas of [Bel04, Algorithm 6.15]. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, let $v_\mathfrak{p}(-)$ denote the $\mathfrak{p}$-adic valuation.

Proposition A.1. *There exists a probabilistic polynomial-time algorithm that given nonzero integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$ returns an element $x \in \mathfrak{a}$ with $v_\mathfrak{p}(x) = v_\mathfrak{p}(\mathfrak{a})$ for all prime ideals $\mathfrak{p}$ dividing $\mathfrak{b}$.*

Proof. We adapt the proofs of [Bel04, Lemmas 6.14, 6.16], taking into account [Bel04, Remark 6.17 (2)]. For the rest of the proof, we fix a positive constant $0 < C < 1$. Let $a = \min(\mathfrak{a} \cap \mathbb{Z}_{>0})$, let $b = \min(\mathfrak{b} \cap \mathbb{Z}_{>0})$ and let $d = [K : \mathbb{Q}]$. Note that if $a = 1$ or $b = 1$ or $d = 1$, then we can just take $x = a$. Thus, we can and do assume that $a, b, d \geq 2$. We define $y \in \mathbb{R}$ by the equality $Cy\log(y) = d\log(b)$. Then $y > 2$ and we observe that y is polynomially bounded in terms of d and $\log(b)$. Hence, we can determine the set

$$S := \{\mathfrak{p} \subseteq \mathcal{O} \text{ prime such that } \mathfrak{p} \cap \mathbb{Z} = (p) \text{ with a rational prime } p < y\}$$

in polynomial time. We define ideals

$$\mathfrak{a}_0 = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}, \qquad \mathfrak{b}_0 = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})}.$$

Then $\mathfrak{a} = \mathfrak{a}_0\mathfrak{a}_1$ and $\mathfrak{b} = \mathfrak{b}_0\mathfrak{b}_1$ with integral ideals $\mathfrak{a}_1, \mathfrak{b}_1$ such that

$$\mathfrak{a}_0 + \mathfrak{a}_1 = \mathfrak{b}_0 + \mathfrak{b}_1 = \mathcal{O},$$

which can be computed in polynomial time. We write $b = b_0b_1$ with

$$b_0 = \prod_{p < y} p^{v_p(b)}.$$

Since the factorisations of $\mathfrak{a}_0$ and $\mathfrak{b}_0$ are known, using the deterministic polynomial-time algorithm [Coh00, Proposition 1.3.8] we can find $x_0 \in \mathcal{O}$ with $x_0 \in \mathfrak{a}_0$ and $v_\mathfrak{p}(x_0) = v_\mathfrak{p}(\mathfrak{a}_0)$ for all $\mathfrak{p}$ dividing $\mathfrak{b}_0$.

We now show that we can find an element $x_1 \in \mathfrak{a}_1$ with $v_\mathfrak{p}(x_1) = v_\mathfrak{p}(\mathfrak{a}_1)$ for all $\mathfrak{p}$ dividing $\mathfrak{b}_1$ in probabilistic polynomial time. For the rest of the proof, we will refer to such elements as *good* elements. We will prove that a positive proportion (independent of $\mathfrak{a}$ and $\mathfrak{b}$) of elements of the finite abelian group $\mathfrak{a}_1/\mathfrak{a}_1\mathfrak{b}_1$ are good. For a prime ideal $\mathfrak{p}$ dividing $\mathfrak{b}_1$, let $A_\mathfrak{p}$ denote the set $\mathfrak{a}_1\mathfrak{p}/\mathfrak{a}_1\mathfrak{b}_1$. Then, for a set of prime ideals T dividing $\mathfrak{b}_1$, we have

$$\left|\bigcap_{\mathfrak{p} \in T} A_\mathfrak{p}\right| = \mathrm{N}(\mathfrak{b}_1)/\prod_{\mathfrak{p} \in T} \mathrm{N}(\mathfrak{p}).$$

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

From the inclusion-exclusion principle it follows that

$$\left|\bigcup_{\mathfrak{p}|\mathfrak{b}_1} A_{\mathfrak{p}}\right| = \mathrm{N}(\mathfrak{b}_1)\left(1 - \prod_{\mathfrak{p}|\mathfrak{b}_1}\left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right)\right).$$

By definition, the lift of $x \in \mathfrak{a}_1/\mathfrak{a}_1\mathfrak{b}_1$ is good if and only if $x \notin \bigcup_{\mathfrak{p}|\mathfrak{b}_1} A_{\mathfrak{p}}$. Hence, the probability that (the lift) of a random element of $\mathfrak{a}_1/\mathfrak{a}_1\mathfrak{b}_1$ is good is

$$\prod_{\mathfrak{p}|\mathfrak{b}_1}\left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right).$$

Now, set $C_1 := d\log(b_1)/(y\log(y)) \leq C$. Since there are at most $d\log_y(b_1)$ prime ideals $\mathfrak{p}$ dividing $\mathfrak{b}_1$, each satisfying $\mathrm{N}(\mathfrak{p}) \geq y$, we have

$$\begin{aligned}\textstyle\prod_{\mathfrak{p}|\mathfrak{b}_1}(1 - 1/\mathrm{N}(\mathfrak{p})) \geq (1-1/y)^{d\log_y(b_1)} &\geq \exp(-1/y - 1/y^2)^{d\log_y(b_1)} = \exp(-C_1 - C_1/y)\\ &\geq \exp(-C(1+1/y)) \geq \exp(-3C/2).\end{aligned}$$

Here the second inequality follows from $1 - x \geq \exp(-x - x^2)$ for $0 \leq x \leq 1/2$. Thus, we can find a good element in probabilistic polynomial time.

Now, given $x_i \in \mathfrak{a}_i$ with $v_{\mathfrak{p}}(x_i) = v_{\mathfrak{p}}(\mathfrak{a}_i)$ for all primes $\mathfrak{p}$ dividing $\mathfrak{b}_i$, we proceed as follows. For $i = 0, 1$ let $\mathfrak{c}_i$ be the largest divisor of $\mathfrak{b}_i$ which is coprime to $\mathfrak{a}$. Note that each $\mathfrak{c}_i$ can be determined in polynomial time by using only ideal sums and ideal division. Moreover, if $\mathfrak{p}$ is a prime ideal with $\mathfrak{p} \mid \mathfrak{b}_i$ and $\mathfrak{p} \nmid \mathfrak{a}$, then $\mathfrak{p} \mid \mathfrak{c}_i$. Since $\mathfrak{a}_0^2\mathfrak{c}_0 + \mathfrak{a}_1^2\mathfrak{c}_1 = \mathcal{O}$, we can determine elements $e_i \in \mathfrak{a}_i^2\mathfrak{c}_i$ with $e_0 + e_1 = 1$ in polynomial time. We now prove that the element

$$x := e_0x_1 + e_1x_0 \in \mathfrak{a}$$

satisfies $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(\mathfrak{a})$ for all $\mathfrak{p}$ dividing $\mathfrak{b}$.

Case 1: $\mathfrak{p} \nmid \mathfrak{a}$. Assume that $\mathfrak{p} \mid \mathfrak{b}_1$. Then $\mathfrak{p} \mid \mathfrak{c}_1$ and hence $e_1 \in \mathfrak{p}$, $e_0 \notin \mathfrak{p}$. Moreover,

$$\begin{aligned}v_{\mathfrak{p}}(e_0x_1) &= v_{\mathfrak{p}}(e_0) + v_{\mathfrak{p}}(x_1) = v_{\mathfrak{p}}(e_0) + v_{\mathfrak{p}}(\mathfrak{a}_1) = v_{\mathfrak{p}}(e_0) = 0,\\ v_{\mathfrak{p}}(e_1x_0) &= v_{\mathfrak{p}}(e_1) + v_{\mathfrak{p}}(x_0) \geq v_{\mathfrak{p}}(e_1) > 0.\end{aligned}$$

Hence, $v_{\mathfrak{p}}(x) = \min(v_{\mathfrak{p}}(e_0x_1), v_{\mathfrak{p}}(e_1x_0)) = 0 = v_{\mathfrak{p}}(\mathfrak{a})$. The subcase $\mathfrak{p} \mid \mathfrak{b}_0$ is similar.

Case 2: $\mathfrak{p} \mid \mathfrak{a}$. Assume that $\mathfrak{p} \mid \mathfrak{b}_1$. Then $\mathfrak{p} \notin S$ and hence $\mathfrak{p} \nmid \mathfrak{a}_0$. It follows that $\mathfrak{p} \mid \mathfrak{a}_1$, and hence $e_0 \notin \mathfrak{p}, e_1 \in \mathfrak{p}$. Moreover,

$$\begin{aligned}v_{\mathfrak{p}}(e_0x_1) &= v_{\mathfrak{p}}(e_0) + v_{\mathfrak{p}}(x_1) = v_{\mathfrak{p}}(e_0) + v_{\mathfrak{p}}(\mathfrak{a}_1) = v_{\mathfrak{p}}(e_0) + v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{a}),\\ v_{\mathfrak{p}}(e_1x_0) &= v_{\mathfrak{p}}(e_1) + v_{\mathfrak{p}}(x_0) \geq v_{\mathfrak{p}}(e_1) \geq 2v_{\mathfrak{p}}(\mathfrak{a}_1) > v_{\mathfrak{p}}(\mathfrak{a}_1) = v_{\mathfrak{p}}(\mathfrak{a}).\end{aligned}$$

Hence, $v_{\mathfrak{p}}(x) = \min(v_{\mathfrak{p}}(e_0x_1), v_{\mathfrak{p}}(e_1x_0)) = v_{\mathfrak{p}}(\mathfrak{a})$. The subcase $\mathfrak{p} \mid \mathfrak{b}_0$ is similar. □

Corollary A.2. *There exists a probabilistic polynomial-time algorithm that given nonzero integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$ returns an element $x \in K^\times$ such that $x\mathfrak{a}$ is integral and coprime to $\mathfrak{b}$.*

Proof. We need to find an element $x \in \mathfrak{a}^{-1}$ such that $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(\mathfrak{a}^{-1})$ for all prime ideals $\mathfrak{p}$ dividing $\mathfrak{b}$. Setting $a = \min(\mathfrak{a} \cap \mathbb{Z}_{>0})$ to be the minimum of $\mathfrak{a}$, this is equivalent to $v_{\mathfrak{p}}(ax) = v_{\mathfrak{p}}(a\mathfrak{a}^{-1})$ for all $\mathfrak{p}$ dividing $\mathfrak{b}$. As $a\mathfrak{a}^{-1}$ is integral, the result follows from Proposition A.1 applied to $a\mathfrak{a}^{-1}$ and $\mathfrak{b}$. □

Corollary A.3. *There exists a probabilistic polynomial-time algorithm that, given a generating set of an $\mathcal{O}$-lattice $M \subseteq K^n$ of rank n, determines a Steinitz form of M, that is, elements $w_1, \ldots, w_n \in K^n$ and*

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

a fractional ideal $\mathfrak{a}$ *of* $\mathcal{O}$ *such that*

$$M = \mathcal{O}w_1 \oplus \cdots \oplus \mathcal{O}w_{n-1} \oplus \mathfrak{a}w_n.$$

Proof. A pseudo-Hermite normal form can be determined in probabilistic polynomial time by [BFH17, Theorem 34]. The reduction to the Steinitz form is described in [Coh00, Lemma 1.2.20] and requires the computation of coprime representatives of ideal classes. Thus, the claim follows from Corollary A.2. □

Acknowledgements. The authors wish to thank Nigel Byott, Fabio Ferri, Claus Fieker and Jürgen Klüners for useful conversations and are grateful for numerous helpful comments and corrections from Nigel Byott, Gunter Malle, Stefano Marseglia and an anonymous referee. The second 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).

Conflicts of Interest. None.

Data availability statement. The source code for Hecke is available at https://github.com/thofma/Hecke.jl.

References

[AO81] H. Appelgate and H. Onishi, 'Continued fractions and the conjugacy problem in $\mathrm{SL}_2(\mathbb{Z})$', *Comm. Algebra* **9**(11) (1981), 1121–1130.

[AO82] H. Appelgate and H. Onishi, 'The similarity problem for 3×3 integer matrices', *Linear Algebra Appl.* **42** (1982), 159–174.

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

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

[BCP97] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbol. Computat.* **24** (1997), 235–265.

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

[Bel04] K. Belabas, 'Topics in computational algebraic number theory', *J. Théor. Nombres Bordeaux* **16**(1) (2004), 19–63.

[BF14] J.-F. Biasse and C. Fieker, 'Subexponential class group and unit group computation in large degree number fields', *LMS J. Comput. Math.* **17**(suppl. A) (2014), 385–403.

[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**(3) (2017), 581–615.

[Bia14] J.-F. Biasse, 'Subexponential time relations in the class group of large degree number fields', *Adv. Math. Commun.* **8**(4) (2014), 407–425.

[BJ08] W. Bley and H. Johnston, 'Computing generators of free modules over orders in group algebras', *J. Algebra* **320**(2) (2008), 836–852.

[BJ11] W. Bley and H. Johnston, 'Computing generators of free modules over orders in group algebras II', *Math. Comp.* **80**(276) (2011), 2411–2434.

[Ble97] W. Bley, 'Computing associated orders and Galois generating elements of unit lattices', *J. Number Theory* **62**(2) (1997), 242–256.

[BS16] J.-F. Biasse and F. Song, 'Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields', in *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, (ACM, New York, 2016), 893–902.

[Buc90] J. Buchmann, 'A subexponential algorithm for the determination of class groups and regulators of algebraic number fields', in *Séminaire de Théorie des Nombres, Paris 1988–1989*, Progr. Math., vol. **91**, (Birkhäuser Boston, Boston, MA, 1990), 27–41.

[BVdM02] A. Behn and A. B. Van der Merwe, 'An algorithmic version of the theorem by Latimer and MacDuffee for 2×2 integral matrices', *Linear Algebra Appl.* **346** (2002), 1–14.

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

[CIK97] A. Chistov, G. Ivanyos and M. Karpinski, 'Polynomial time algorithms for modules over finite dimensional algebras', in *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, (ACM, New York, 1997), 68–74.

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

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

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

[CR81] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, vol. **I** (John Wiley & Sons, Inc., New York, 1981).
[CR87] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, vol. **II** (John Wiley & Sons, Inc., New York, 1987).
[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), 371–386.
[EHKS14] K. Eisenträger, S. Hallgren, A. Kitaev and F. Song, 'A quantum algorithm for computing the unit group of an arbitrary degree number field', in *STOC'14—Proceedings of the 2014 ACM Symposium on Theory of Computing* (ACM, New York, 2014), 293–302.
[EHO19] B. Eick, T. Hofmann, and E. A. O'Brien, 'The conjugacy problem in $\mathrm{GL}(n, \mathbb{Z})$', *J. Lond. Math. Soc. (2)* **100**(3) (2019), 731–756.
[Fad66] D. K. Faddeev, 'On the equivalence of systems of integral matrices', *Izv. Akad. Nauk SSSR Ser. Mat.* **30** (1966), 449–454.
[FHHJ17] C. Fieker, W. Hart, T. Hofmann and F. Johansson, 'Nemo/Hecke: computer algebra and number theory packages for the Julia programming language', in *ISSAC'17—Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation* (ACM, New York, 2017), 157–164.
[FHS19] C. Fieker, T. Hofmann and C. Sircana, 'On the construction of class fields', in *ANTS XIII—Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, Open Book Ser., vol. **2** (Math. Sci. Publ., Berkeley, CA, 2019), 239–255.
[FR85] K. Friedl and L. Ronyai, 'Polynomial time solutions of some problems in computational algebra', in *STOC '85: Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing* (ACM, New York, 1985), 153–162.
[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, DC, 1967), 1–41.
[Gru80] F. J. Grunewald, *Solution of the Conjugacy Problem in Certain Arithmetic Groups*, *Word Problems, II (Conf. on Decision Problems in Algebra, Oxford, 1976),* Stud. Logic Foundations Math., vol. **95** (North-Holland, Amsterdam-New York, 1980), 101–139.
[Gur80] R. M. Guralnick, 'A note on the local-global principle for similarity of matrices', *Linear Algebra Appl.* **30** (1980), 241–245.
[HJ20] T. Hofmann and H. Johnston, 'Computing isomorphisms between lattices', *Math. Comp.* **89**(326) (2020), 2931–2963.
[Hus17] D. Husert, Similarity of integer matrices, Ph.D. thesis, University of Paderborn, 2017.
[IR93] G. Ivanyos and L. Rónyai, 'Finding maximal orders in semisimple algebras over Q', *Comput. Complexity* **3**(3) (1993), 245–261.
[IRS12] G. Ivanyos, L. Rónyai and J. Schicho, 'Splitting full matrix algebras over algebraic number fields', *J. Algebra* **354** (2012), 211–223.
[KV10] M. Kirschmer and J. Voight, 'Algorithmic enumeration of ideal classes for quaternion orders', *SIAM J. Comput.* **39**(5) (2010), 1714–1747.
[Len83] A. K. Lenstra, *Factoring Polynomials over Algebraic Number Fields*, *Computer Algebra (London, 1983)*, Lecture Notes in Comput. Sci., vol. **162** (Springer, Berlin, 1983), 245–254.
[Len92] H. W. Lenstra, Jr., 'Algorithms in algebraic number theory', *Bull. Amer. Math. Soc. (N.S.)* **26**(2) (1992), 211–244.
[LM33] C. G. Latimer and C. C. MacDuffee, 'A correspondence between classes of ideals and classes of matrices', *Ann. of Math. (2)* **34**(2) (1933), 313–316.
[LP92] H. W. Lenstra, Jr. and Carl Pomerance, 'A rigorous time bound for factoring integers', *J. Amer. Math. Soc.* **5**(3) (1992), 483–516.
[Mar20] S. Marseglia, 'Computing the ideal class monoid of an order', *J. Lond. Math. Soc. (2)* **101**(3) (2020), 984–1007.
[NS09] G. Nebe and A. Steel, 'Recognition of division algebras', *J. Algebra* **322**(3) (2009), 903–909.
[Odl00] A. Odlyzko, 'Discrete logarithms: the past and the future', *Des. Codes Cryptogr.* **19**(2–3) (2000), 129–145.
[OPS98] J. Opgenorth, W. Plesken and T. Schulz, 'Crystallographic algorithms and tables', *Acta Cryst. Sect. A* **54**(5) (1998), 517–531.
[OSC22] Oscar – Open Source Computer Algebra Research System, version 0.10.0, 2022.
[Pag14] A. Page, 'An algorithm for the principal ideal problem in indefinite quaternion algebras', *LMS J. Comput. Math.* **17**(suppl. A) (2014), 366–384.
[Rei03] I. Reiner, *Maximal Orders, London Mathematical Society Monographs*, vol. **28** (The Clarendon Press Oxford University Press, Oxford, 2003).
[Ron87] L. Ronyai, 'Simple algebras are difficult', in *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1987) 398–408.
[Ros94] J. Rosenberg, *Algebraic K-Theory and Its Applications*, Graduate Texts in Mathematics, vol. **147** (Springer-Verlag, New York, 1994).
[Sar79] R. A. Sarkisyan, 'Conjugacy problem for sets of integral matrices', *Math. Notes* **25** (1979), 419–432.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press

[Sho97] P. W. Shor, 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', *SIAM J. Comput.* **26**(5) (1997), 1484–1509.
[Tay87] D. E. Taylor, 'Pairs of generators for matrix groups I', *The Cayley Bulletin* (3) (1987), 76–85.
[Vil93] G. Villard, 'Computation of the Smith normal form of polynomial matrices', in *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation* (ACM, New York, 1993) 209–217.

https://doi.org/10.1017/fms.2022.74 Published online by Cambridge University Press