TESTING ISOMORPHISM OF LATTICES OVER CM-ORDERS

H. W. LENSTRA, JR. AND A. SILVERBERG

Abstract. A *CM-order* is a reduced order equipped with an involution that mimics complex conjugation. The *Witt-Picard group* of such an order is a certain group of ideal classes that is closely related to the "minus part" of the class group. We present a deterministic polynomial-time algorithm for the following problem, which may be viewed as a special case of the principal ideal testing problem: given a CM-order, decide whether two given elements of its Witt-Picard group are equal. In order to prevent coefficient blow-up, the algorithm operates with lattices rather than with ideals. An important ingredient is a technique introduced by Gentry and Szydlo in a cryptographic context. Our application of it to lattices over CM-orders hinges upon a novel existence theorem for auxiliary ideals, which we deduce from a result of Konyagin and Pomerance in elementary number theory.

1. Introduction

An *order* is a commutative ring of which the additive group is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$. We call n the $\mathbb{Z}$*-rank* of the order. In algorithms, we shall specify an order by a system $(b_{ijk})_{i,j,k=1}^n$ of integers with the property that, for some $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of the order, one has $\alpha_i\alpha_j = \sum_{k=1}^n b_{ijk}\alpha_k$ for all $1 \leq i, j \leq n$.

Definition 1.1. A *CM-order A* is an order such that:

(i) A has no non-zero nilpotent elements (i.e., A is reduced), and
(ii) A is equipped with an automorphism $x \mapsto \bar{x}$ of A such that $\psi(\bar{x}) = \overline{\psi(x)}$ for all $x \in A$ and all ring homomorphisms $\psi : A \to \mathbb{C}$.

One can show that each CM-order has exactly one such automorphism, and it satisfies $\bar{\bar{x}} = x$ for all x (see Lemma 3.4 below). In algorithms one specifies an automorphism of an order by means of its matrix on the same $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ that was used for the b_{ijk}.

Examples 1.2. Examples of CM-orders (see also Definition 2.1 and Examples 3.7) include the following:

(i) rings of integers of CM-fields (in particular, cyclotomic number fields),
(ii) group rings $\mathbb{Z}[G]$ for finite abelian groups G, with $\bar{\sigma} = \sigma^{-1}$ for $\sigma \in G$,
(iii) the rings $\mathbb{Z}\langle G\rangle = \mathbb{Z}[G]/(u+1)$ occurring in [14], where G is a finite abelian group, $u \in G$ has order 2, and $\bar{\sigma} = \sigma^{-1}$ for $\sigma \in G$.

We show that CM-orders are easy to recognize. In Algorithm 3.11 we give a deterministic polynomial-time algorithm that, given an order A, decides whether

2010 *Mathematics Subject Classification.* 11Y16 (primary), 68W30 (secondary).

Key words and phrases. lattices, orders, complex multiplication.

Support for the research was provided by the Alfred P. Sloan Foundation and the National Science Foundation.

it has an automorphism that makes it into a CM-order, and if so computes that automorphism.

Suppose A is an order. We denote the $\mathbb{Q}$-algebra $A \otimes_{\mathbb{Z}} \mathbb{Q}$ by $A_{\mathbb{Q}}$. We write $(A_{\mathbb{Q}}^{+})_{\gg 0}$ for the set of all $w \in A_{\mathbb{Q}}$ with the property that $\psi(w) \in \mathbb{R}_{>0}$ for each ring homomorphism $\psi : A_{\mathbb{Q}} \to \mathbb{C}$; this is a subgroup of the group $A_{\mathbb{Q}}^{*}$ of units of $A_{\mathbb{Q}}$. By a *fractional A-ideal* we mean a finitely generated sub-A-module I of $A_{\mathbb{Q}}$ that spans $A_{\mathbb{Q}}$ as a $\mathbb{Q}$-vector space. An *invertible* fractional A-ideal is a fractional A-ideal I such that there is a fractional A-ideal J with $IJ = A$, where IJ is the fractional A-ideal generated by the products of elements from I and J.

We next state our main result, which says that, in a special case, principal ideal testing can be done in polynomial time.

Theorem 1.3. *There is a deterministic polynomial-time algorithm that given a CM-order A, a fractional A-ideal I, and an element $w \in (A_{\mathbb{Q}}^{+})_{\gg 0}$ satisfying $I\bar{I} = Aw$, decides whether there exists $v \in A_{\mathbb{Q}}$ such that $I = Av$ and $v\bar{v} = w$, and if so computes such an element v.*

More generally, we show:

Theorem 1.4. *There is a deterministic polynomial-time algorithm that given a CM-order A, fractional A-ideals I_1 and I_2, and elements $w_1, w_2 \in (A_{\mathbb{Q}}^{+})_{\gg 0}$ satisfying $I_1\overline{I_1} = Aw_1$ and $I_2\overline{I_2} = Aw_2$, decides whether there exists $v \in A_{\mathbb{Q}}$ such that $I_1 = vI_2$ and $w_1 = v\bar{v}w_2$, and if so computes such an element v.*

See the very end of this paper for proofs of Theorems 1.3 and 1.4.

The set of all pairs (I, w) as in Theorem 1.3 is a multiplicative group (see Section 12), and $\{(Av, v\bar{v}) : v \in A_{\mathbb{Q}}^{*}\}$ is a subgroup. Writing $\mathrm{WPic}(A)$ for the quotient group, Theorem 1.4 provides an efficient equality test in $\mathrm{WPic}(A)$. The set of principal invertible fractional A-ideals $\{Av : v \in A_{\mathbb{Q}}^{*}\}$ is a subgroup of the set of all invertible fractional A-ideals; write $\mathbf{Cl}(A)$ for the quotient group, and write $\mathbf{Cl}^{-}(A)$ for the subgroup of classes $[I] \in \mathbf{Cl}(A)$ for which $I\bar{I}$ is principal. We can show that the group homomorphism $\mathrm{WPic}(A) \to \mathbf{Cl}^{-}(A)$ sending the class of (I, w) to the class of I is almost an isomorphism in the sense that both its kernel and its cokernel are annihilated by 2 (Theorem 12.3 below). Hence we can efficiently do an equality test in a group that is closely related to the "minus part" of the class group of a CM-order.

To obtain these results, we view our fractional A-ideals as lattices with an A-module structure. This allows us to avoid blow-up of the coefficients with respect to a $\mathbb{Z}$-basis, when ideals are repeatedly multiplied together.

By a *lattice*, or *integral lattice*, we mean a finitely generated free abelian group L equipped with a positive definite symmetric $\mathbb{Z}$-bilinear map $\langle \cdot\,, \cdot \rangle : L \times L \to \mathbb{Z}$; this map will be referred to as the *inner product*. A lattice is specified by means of the matrix $(\langle b_i, b_j \rangle)_{i,j=1}^{m}$ for some $\mathbb{Z}$-basis $b_1, \ldots, b_m$ of L.

Let A be a CM-order. By an *A-lattice* we mean a lattice L that is given an A-module structure with the property that for all $a \in A$ and $x, y \in L$ one has $\langle ax, y \rangle = \langle x, \bar{a}y \rangle$. One specifies an A-lattice by specifying it as a lattice and listing the system of nm^2 integer coefficients that express $\alpha_i b_j$ on $b_1, \ldots, b_m$, with the $\mathbb{Z}$-bases $(\alpha_i)_{i=1}^{n}$ for A and $(b_j)_{j=1}^{m}$ for L being as above. An *A-isomorphism* $f : L \to M$ of A-lattices is an isomorphism of A-modules with $\langle f(x), f(y) \rangle = \langle x, y \rangle$ for all $x, y \in L$; such an isomorphism is specified by its matrix on the $\mathbb{Z}$-bases for L and

M that are used. An example of an A-lattice is the A-module A itself, with inner product $(a,b) = \mathrm{Tr}(a\bar{b})$; here $\mathrm{Tr} : A \to \mathbb{Z}$ is the trace function of A as a $\mathbb{Z}$-algebra. This A-lattice is called the *standard* A-lattice.

Deciding whether two lattices are isomorphic is a notorious algorithmic problem. Our results here and in [14] show that the problem admits a polynomial-time solution if the lattices are equipped with sufficient structure.

Theorem 1.5. *There is a deterministic polynomial-time algorithm that, given a CM-order A and an A-lattice L, decides whether or not L is A-isomorphic with the standard A-lattice, and if so, computes such an A-isomorphism.*

The algorithm and the proof are given in Section 18. An imprecise summary is as follows. Finding an A-isomorphism as in Theorem 1.5 is equivalent to finding a "short" vector in L. Using a suitable tensor power L^m, one can force a short vector to lie in a certain coset of L^m modulo $\mathfrak{a}L^m$. Here $\mathfrak{a}$ is an auxiliary ideal of A that is chosen to have large norm, which enables us to recover the short vector itself. If one can do this for m_1 and m_2, then they combine into a short vector in $L^{\gcd(m_1,m_2)}$. Ultimately, one obtains a short vector in L^k, where the final gcd k has relatively small prime factors. Removing these one by one, one finds the desired short vector in L.

As a corollary of Theorem 1.5 we obtain the following result (with *invertible* defined as in Definition 4.3), from which Theorem 1.4 follows.

Theorem 1.6. *There is a deterministic polynomial-time algorithm that given a CM-order A and invertible A-lattices L and M, decides whether or not L and M are isomorphic as A-lattices, and if so, exhibits such an A-isomorphism.*

Theorems 1.5 and 1.6 generalize the main results of [14], which concerned the special case $A = \mathbb{Z}\langle G\rangle$ mentioned in Example 1.2(iii). While the proofs are different from those in [14], since the general strategies are similar we structured this paper so that in broad outline our proofs follow the same logical order as that of [14], which was devoted to the case $A = \mathbb{Z}\langle G\rangle$.

One important difference between the present paper and [14] lies in the manner in which auxiliary ideals of A are constructed. In the case $A = \mathbb{Z}\langle G\rangle$, we could use Linnik's theorem for this purpose (see Section 18 of [14]), but for general A this cannot be done. Here we show that the following result suffices.

Theorem 1.7. *Let A be an order of $\mathbb{Z}$-rank $n \geq 1$, and let ℓ be a prime number with $\ell > n^2$. Then there exists a maximal ideal $\mathfrak{p}$ of A that contains a prime number $p \leq 4(1 + (\log n)^2)$ and that satisfies $\#(A/\mathfrak{p}) \not\equiv 1 \bmod \ell$.*

It is remarkable that the upper bound $4(1+(\log n)^2)$ on p in Theorem 1.7 depends on A only through its $\mathbb{Z}$-rank n, and that it is so small. One may actually conjecture that Theorem 1.7 remains true with $4(1+(\log n)^2)$ replaced by 5; we give a heuristic argument after the proof of Proposition 15.6 below. For the elementary proof of Theorem 1.7, see the proof of Proposition 15.6, which relies on a result of Konyagin and Pomerance [6].

The price that we pay for the very small upper bound on p in Theorem 1.7 is that we have to work with ideals $\mathfrak{a}$ of A that are not necessarily generated by elements of $\mathbb{Z}$. This leads to a number of technical difficulties (see for example Sections 8, 15, 16, and 17) that were not present in [14]. Applying Theorem 1.7 instead of

Linnik's theorem in the case $A = \mathbb{Z}\langle G\rangle$, one may expect to obtain a dramatically lower run time exponent than the one achieved in [14].

Another difference between this paper and [14] is that, in order to preserve integrality, we replaced the "scaled trace map" t (from Definition 6.2 of [14]) by the trace map Tr given before Theorem 1.5. As a consequence, the inner product $(\ ,\ )$ used for the standard A-lattice in this paper is, in the special case $A = \mathbb{Z}\langle G\rangle$, equal to n times the inner product used in [14], where $n = (\#G)/2$. For similar reasons, the definition of an *invertible* A-lattice (see Definition 4.3) requires more care than in [14]. We needed to redefine *short vector* (Definition 6.1), and the short vectors now behave differently. What remains true is that an A-lattice is A-isomorphic to the standard A-lattice if and only if it is invertible and has a short vector. However, the group of roots of unity in A now might be too large to even write down in polynomial time, so the set of short vectors in L and thus the set of all A-isomorphisms from L to A might be too large to enumerate.

Any choices and recommendations that we make, especially those concerning the selection of auxiliary ideals, are intended to optimize the efficiency of our proofs rather than of our algorithm.

Our work on this subject was inspired by an algorithm of Gentry and Szydlo (Section 7 of [4]), and is related to our work on lattices with symmetry [11, 14]. In this paper we give the details for the proofs of the results announced in our 2013 workshop on this subject [19]; see especially [10]. In [5], P. Kirchner gave a version of our Theorem 1.3 that, due to the inapplicability of Linnik's theorem for general CM-orders, either assumes the generalized Riemann hypothesis or allows probabilistic algorithms.

The setting in this paper is applicable to the setting considered by Garg, Gentry, and Halevi in [3] where the CM-order A is a cyclotomic ring $\mathbb{Z}[\zeta_m]$, to the setting considered by Gentry and Szydlo where the order is $\mathbb{Z}[X]/(X^m - 1)$, and to the orders $\mathbb{Z}[X]/(X^m + 1)$ used for fully homomorphic encryption.

1.1. **Overview of algorithm for Theorem 1.5.** The algorithm starts by testing whether the given A-lattice L is invertible. Then it computes the primitive idempotents of A, in order to decompose A as a product of connected rings and reduce the problem to the case where A is connected. We work in a $\mathbb{Z}$-graded extended tensor algebra $\Lambda = \bigoplus_{i\in\mathbb{Z}} L^{\otimes i}$. Let $n = \operatorname{rank}_{\mathbb{Z}}(A)$. We make use of Theorem 1.7 to construct a finite set of "good" ideals $\mathfrak{a}$ of A, and for each $\mathfrak{a}$ a positive integer $k(\mathfrak{a})$ divisible by the exponent of the group $(A/\mathfrak{a})^*$, such that every prime divisor of $k = \gcd\{k(\mathfrak{a})\}$ is at most n^2. Next, for each good ideal $\mathfrak{a}$ one tries to find a short vector $z_{\mathfrak{a}} \in L^{\otimes k(\mathfrak{a})}$ such that for every short vector z of L one has $z^{\otimes k(\mathfrak{a})} = z_{\mathfrak{a}}$; if this fails, one concludes that L is not A-isomorphic to the standard A-lattice (and terminates). We then use the Euclidean algorithm to construct from the $z_{\mathfrak{a}}$ a vector $w \in L^{\otimes k}$ such that if L has a short vector z then $z^{\otimes k} = w$. If $p_1, \ldots, p_m$ are the prime divisors of k with multiplicity, we use our results on graded orders from [16] and our results on roots of unity in orders from [13] to either obtain a short vector z_1 in $L^{\otimes k/p_1}$, then a short vector z_2 in $L^{\otimes k/(p_1p_2)}$, and so on, until one obtains a short vector in L, or else prove that L has no short vector. If the algorithm produces a short vector z in L, then the map $A \to L$, $a \mapsto az$ is an A-isomorphism, and otherwise no A-isomorphism exists.

1.2. **Structure of the paper.** In Sections 2–4 we give background and results about CM-orders and A-lattices. In Section 5 we obtain bounds for LLL-reduced bases of invertible lattices (Proposition 5.5) that allow us to show that the Witt-Picard group is finite and that our algorithms run in polynomial time. In Section 6 we show how to find the unique "short" vector in a suitable lattice coset, when such a vector exists. In Section 7 we characterize short vectors in A-lattices. In Section 8 we give conditions under which we can easily apply the results in Section 6. In Section 9 we relate A-lattices to fractional A-ideals, and in Section 10 we give results on invertible A-lattices. In Section 11 we study short vectors in invertible A-lattices; in particular, we show that an A-lattice is A-isomorphic to the standard one if and only if it is invertible and has a short vector. In Section 12 we study the Witt-Picard group of A. Section 13 deals with multiplying and exponentiating invertible A-lattices. In Section 14 we introduce the extended tensor algebra Λ, which is a single algebraic structure that comprises all rings and lattices occurring in our main algorithm. Sections 15 and 16 are the heart of the paper, and consist of finding the auxiliary ideals. In Section 17 we give algorithms that make use of our choice of auxiliary ideals; we use these algorithms as subroutines for our main algorithm, which is given in Section 18.

1.3. **Notation.** As usual, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote respectively the ring of integers, and fields of rational numbers, real numbers, and complex numbers. Suppose B and C are commutative rings. Let $\mathrm{Rhom}(B, C)$ denote the set of ring homomorphisms from B to C, let $\mathrm{Spec}(B)$ denote the set of prime ideals of B, and let $\mu(B)$ denote the group of roots of unity of B. If $\mathfrak{p} \in \mathrm{Spec}(B)$, let $B_\mathfrak{p}$ denote the localization of B at $\mathfrak{p}$ and let $\mathrm{N}(\mathfrak{p}) = \#(B/\mathfrak{p})$. If A is an order, let $\mathrm{Minspec}(A)$ denote the set of minimal prime ideals of A and let $\mathrm{Maxspec}(A)$ denote the set of maximal ideals of A. If R is a commutative ring and B and C are R-algebras, let $\mathrm{Rhom}_R(B, C)$ denote the set of R-algebra homomorphisms from B to C, and if D is a $\mathbb{Z}$-module let $D_R = D \otimes_\mathbb{Z} R$.

Acknowledgments. We thank all the participants of the 2013 Workshop on Lattices with Symmetry, and especially Daniele Micciancio for his interest in our work. We also thank Abtien Javanpeykar for his help with Theorem 1.7.

2. CM-fields and CM-algebras

By a *classical CM-field* we will mean a totally imaginary quadratic extension of a totally real number field. We define a *CM-field* to be any subfield of a classical CM-field. A number field is a CM-field if and only if it is either a classical CM-field or totally real (by Lemma 18.2(iv) on p. 122 of [18]).

Definition 2.1. A *CM-algebra* is a commutative $\mathbb{Q}$-algebra E such that:

(i) $\dim_\mathbb{Q}(E) < \infty$,
(ii) E has no non-zero nilpotent elements,
(iii) E is equipped with an automorphism $x \mapsto \bar{x}$ such that $\psi(\bar{x}) = \overline{\psi(x)}$ for all $x \in E$ and all $\psi \in \mathrm{Rhom}(E, \mathbb{C})$.

Remark 2.2. It follows from Lemma 18.2(i) on p. 122 of [18] that a finite dimensional commutative $\mathbb{Q}$-algebra E is a CM-algebra if and only if all elements of E are separable and $E/\mathfrak{m}$ is a CM-field for all $\mathfrak{m} \in \mathrm{Spec}(E)$. In other words, a finite dimensional commutative $\mathbb{Q}$-algebra is a CM-algebra if and only if it is a product of finitely many CM-fields. In particular, the CM-algebras that are fields are exactly the CM-fields.

Remark 2.3. If E is a CM-algebra and $x \in E$, then $\mathrm{Tr}_{E/\mathbb{Q}}(x\bar{x}) > 0$ for all $x \in E \smallsetminus \{0\}$.

Lemma 2.4. *Suppose V is a finite-dimensional $\mathbb{Q}$-vector space, $f : V \to \mathbb{Q}$ is a quadratic form, and $f_{\mathbb{R}} : V_{\mathbb{R}} \to \mathbb{R}$ is the $\mathbb{R}$-linear extension of f. Then f is positive definite if and only if $f_{\mathbb{R}}$ is positive definite.*

Proof. Diagonalize f over $\mathbb{Q}$, so $f(x) = \sum_{i=1}^{n} a_i x_i^2$ where the x_i are the coordinates of x on some $\mathbb{Q}$-basis of V and all $a_i \in \mathbb{Q}$. Then f is positive definite if and only if all $a_i > 0$. Using the same basis for $V_{\mathbb{R}}$ over $\mathbb{R}$ now gives the desired result. □

The following result will be used to prove Proposition 14.3. It generalizes Lemma 2 on p. 37 of [18], which dealt with the case where E is a number field.

Proposition 2.5. *Suppose E is a finite dimensional commutative $\mathbb{Q}$-algebra, $\rho \in \mathrm{Aut}(E)$, and $\mathrm{Tr}_{E/\mathbb{Q}}(x\rho(x)) > 0$ for all $x \in E \smallsetminus \{0\}$. Then:*

(i) *$\mathrm{Tr}_{E_{\mathbb{R}}/\mathbb{R}}(x\rho(x)) > 0$ for all $x \in E_{\mathbb{R}} \smallsetminus \{0\}$,*
(ii) *$\rho(\rho(x)) = x$ for all $x \in E$,*
(iii) *and E is a CM-algebra with ρ serving as $^{-}$.*

Proof. By Lemma 2.4 we have (i).

If y is a nilpotent element of E, then $y\rho(y)$ is nilpotent, so $\mathrm{Tr}_{E/\mathbb{Q}}(y\rho(y)) = 0$, so $y = 0$ by our hypothesis. Thus, E is reduced.

We have $E \hookrightarrow E_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$ for some $r, s \in \mathbb{Z}_{\geq 0}$, and ρ extends to an automorphism of $E_{\mathbb{R}}$ as an $\mathbb{R}$-algebra. For $1 \leq j \leq r + s$, let $\alpha_j = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{R}^r \times \mathbb{C}^s = E_{\mathbb{R}}$ with 1 in the j-th position. We claim that $\rho(\alpha_j) = \alpha_j$ for all j. If not, then since the α_j's are exactly the primitive idempotents of $E_{\mathbb{R}}$ we have $\rho(\alpha_j) = \alpha_k$ for some $k \neq j$, so $0 < \mathrm{Tr}_{E_{\mathbb{R}}/\mathbb{R}}(\alpha_j\rho(\alpha_j)) = \mathrm{Tr}_{E_{\mathbb{R}}/\mathbb{R}}(\alpha_j\alpha_k) = 0$, a contradiction. Thus ρ acts componentwise, and is the identity on each $\mathbb{R}$ and either the identity or complex conjugation on each $\mathbb{C}$. In particular, $\rho(\rho(x)) = x$ for all $x \in E_{\mathbb{R}}$, and we have (ii).

If ρ is the identity on the j-th $\mathbb{C}$, then letting $x = \sqrt{-1}\alpha_j$ we have

$$\mathrm{Tr}_{E_{\mathbb{R}}/\mathbb{R}}(x\rho(x)) = \mathrm{Tr}_{E_{\mathbb{R}}/\mathbb{R}}(-\alpha_j) = -2 < 0,$$

a contradiction. It follows that $\psi(\rho(x)) = \overline{\psi(x)}$ for all $\psi \in \mathrm{Rhom}(E, \mathbb{C})$ and all $x \in E$, giving (iii). □

The next algorithm will be used in Algorithm 3.11. For the input, a degree n field F is specified (as in [15]) by listing a system of "structure constants" $a_{ijk} \in \mathbb{Q}$, for $i, j, k \in \{1, 2, \ldots, n\}$, that determine the multiplication in the sense that for some $\mathbb{Q}$-basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of F one has $\alpha_i\alpha_j = \sum_{k=1}^{n} a_{ijk}\alpha_k$ for all i, j. Elements of F are then represented by their vector of coordinates on that basis.

Algorithm 2.6. Given a number field F, the algorithm decides whether F is a CM-field, and if so computes $^{-} \in \mathrm{Aut}(F)$.

Steps:

(i) Compute $\mathrm{Aut}(F)$.

(ii) For all $\sigma \in \mathrm{Aut}(F)$ with $\sigma^2 = \mathrm{id}_F$ in succession compute $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha_i \cdot \sigma(\alpha_j))$ for the given $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of F and test whether for all $k \in \{1, 2, \ldots, n\}$ we have $\det((\mathrm{Tr}_{F/\mathbb{Q}}(\alpha_i \cdot \sigma(\alpha_j)))_{i,j=1}^{k}) > 0$. If not, pass to the next σ or if there is no next σ terminate with "no". If yes, terminate with "yes" and $\bar{} = \sigma$.

Proposition 2.7. *Algorithm 2.6 is correct and runs in polynomial time.*

Proof. Let $f_\sigma : F \to \mathbb{Q}$ be the quadratic form $f_\sigma(x) = \mathrm{Tr}_{F/\mathbb{Q}}(x\sigma(x))$. Then f_σ is positive definite if and only if $(f_\sigma)_{\mathbb{R}}$ is positive definite, by Lemma 2.4. Further, $(f_\sigma)_{\mathbb{R}}$ is positive definite if and only if the matrix $A = (\mathrm{Tr}_{F/\mathbb{Q}}(\alpha_i \cdot \sigma(\alpha_j)))_{i,j=1}^{n}$ is positive definite. By Sylvester's criterion, A is positive definite if and only if its leading principal minors $\det((\mathrm{Tr}_{F/\mathbb{Q}}(\alpha_i \cdot \sigma(\alpha_j)))_{i,j=1}^{k})$ are all positive. Correctness of the algorithm now follows from Proposition 2.5 and Lemma 2.3. Computing $\mathrm{Aut}(F)$ can be done in polynomial time, by §2.9 of [8]. □

Remark 2.8. There is a deterministic polynomial-time algorithm that given a finite dimensional commutative $\mathbb{Q}$-algebra E decides whether it is a CM-algebra and if so produces $\bar{}$. Namely, use Algorithms 5.5 and 7.2 of [15] to determine whether all elements of E are separable and if so to compute all $\mathfrak{m} \in \mathrm{Spec}(E)$ and apply Algorithm 2.6 above to check whether each $E/\mathfrak{m}$ is a CM-field and find its automorphism $\bar{}$.

3. CM-orders

If A is a reduced order, then the trace map $\mathrm{Tr} = \mathrm{Tr}_{A/\mathbb{Z}} : A \to \mathbb{Z}$ extends by linearity to trace maps $\mathrm{Tr} : A_{\mathbb{Q}} \to \mathbb{Q}$ and $\mathrm{Tr} : A_{\mathbb{R}} \to \mathbb{R}$, and for all $a \in A$ we have $\mathrm{Tr}(a) = \sum_{\psi \in \mathrm{Rhom}(A,\mathbb{C})} \psi(a)$. (Note that $\#\mathrm{Rhom}(A, \mathbb{C}) = \mathrm{rank}_{\mathbb{Z}}(A)$.)

Recall that the discriminant $\Delta_{A/\mathbb{Z}}$ of an order A is the determinant of the matrix $(\mathrm{Tr}_{\mathcal{O}/\mathbb{Z}}(\alpha_i\alpha_j))_{i,j}$ for any $\mathbb{Z}$-basis $\{\alpha_i\}$ of A.

In Section 1, a CM-order A was specified by $n = \mathrm{rank}_{\mathbb{Z}}(A)$, and a system $(b_{ijk})_{i,j,k=1}^{n}$ of integers such that for some $\mathbb{Z}$-basis $\{\alpha_i\}_{i=1}^{n}$ of A one has $\alpha_i\alpha_j = \sum_{k=1}^{n} b_{ijk}\alpha_k$ for all $1 \le i, j \le n$, and a matrix giving $\bar{}$ on A. We improve the way the data for A are specified, as follows. Note that $\mathrm{Tr}(\alpha_i) = \sum_{j=1}^{n} b_{ijj}$. It is straightforward to use the specified data to compute the Gram matrix $((\alpha_i, \alpha_j))_{1 \le i,j \le n}$ for A relative to the basis $\{\alpha_i\}_{i=1}^{n}$, where $(a, b) = \mathrm{Tr}_{A/\mathbb{Z}}(a\bar{b})$ for all $a, b \in A$, and compute $\det((\alpha_i, \alpha_j)) = |\Delta_{A/\mathbb{Z}}|$, which is the determinant of A as a lattice (Definition 5.3 below). Run the LLL lattice basis reduction algorithm ([7]) to replace $\{\alpha_i\}_{i=1}^{n}$ by an LLL-reduced basis (see Definition 5.1 for the definition), and recompute the constants b_{ijk} and the matrix giving $\bar{}$. We always first run the above algorithm to give an LLL-reduced basis, and convert back to the original basis at the end. We suppress this in the algorithms below, and assume our input A is given with an LLL-reduced basis, and that we have kept track of how the LLL-basis is expressed in terms of the original basis $\{\alpha_i\}$, so that one can give the final answer in terms of the original basis.

Lemma 3.1. *If A is a reduced order, then $\bigcap_{\psi \in \mathrm{Rhom}(A,\mathbb{C})} \ker(\psi) = 0$.*

Proof. Let $n = \mathrm{rank}_{\mathbb{Z}}(A)$. Since A is reduced, we have $A \subset A_{\mathbb{C}} \cong \mathbb{C}^n$, so $\bigcap_{\psi \in \mathrm{Rhom}(A,\mathbb{C})} \ker(\psi) \subset \bigcap_{\psi \in \mathrm{Rhom}_{\mathbb{C}}(\mathbb{C}^n,\mathbb{C})} \ker(\psi) = 0$. □

Definition 3.2. If A is a CM-order, and $a, b \in A$, define $(a, b) = \mathrm{Tr}_{A/\mathbb{Z}}(a\bar{b})$.

Lemma 3.3. *If A is a CM-order, then A is an integral lattice with respect to the inner product $(\ ,\ )$.*

Proof. The map $(a,b) \mapsto \mathrm{Tr}_{A/\mathbb{Z}}(a\bar{b})$ is clearly $\mathbb{Z}$-valued, $\mathbb{Z}$-bilinear, and symmetric. If $a \in A$, then $\psi(a\bar{a}) = \psi(a)\overline{\psi(a)} \in \mathbb{R}_{\geq 0}$ for all $\psi \in \mathrm{Rhom}(A,\mathbb{C})$, so

$$(a,a) = \mathrm{Tr}_{A/\mathbb{Z}}(a\bar{a}) = \sum_{\psi \in \mathrm{Rhom}(A,\mathbb{C})} \psi(a\bar{a}) \in \mathbb{R}_{\geq 0}.$$

Suppose $a \neq 0$. Since $\bigcap_{\psi \in \mathrm{Rhom}(A,\mathbb{C})} \ker \psi = 0$ by Lemma 3.1, there exists $\psi \in \mathrm{Rhom}(A,\mathbb{C})$ such that $\psi(a) \neq 0$. Thus $\psi(\bar{a}) = \overline{\psi(a)} \neq 0$, so $\psi(a\bar{a}) = \psi(a)\psi(\bar{a}) \neq 0$, so $(a,a) > 0$. □

Lemma 3.4. *Suppose A is a CM-order. Then:*

(i) *$a \mapsto \bar{a}$ is an involution on A (i.e., $\bar{\bar{a}} = a$ for all $a \in A$);*
(ii) *A has exactly one involution satisfying Definition 1.1(ii);*
(iii) *the involution $^-$ extends $\mathbb{R}$-linearly to $A_{\mathbb{R}}$, and is the unique involution on $A_{\mathbb{R}}$ such that $\psi(\bar{a}) = \overline{\psi(a)}$ for all $a \in A_{\mathbb{R}}$ and all $\psi \in \mathrm{Rhom}_{\mathbb{R}}(A_{\mathbb{R}},\mathbb{C})$;*
(iv) *$\mathrm{Tr}_{A_{\mathbb{R}}/\mathbb{R}}(a\bar{a}) > 0$ for all non-zero $a \in A_{\mathbb{R}}$.*

Proof. For all $\psi \in \mathrm{Rhom}(A,\mathbb{C})$ and all $a \in A$ we have $\psi(a) = \overline{\psi(\bar{a})} = \psi(\bar{\bar{a}})$, so $a = \bar{\bar{a}}$ by Lemma 3.1.

Suppose ρ_1 and ρ_2 are two involutions satisfying Definition 1.1(ii). Then for all $a \in A$ and all $\psi \in \mathrm{Rhom}(A,\mathbb{C})$ we have $\psi(\rho_1(a)) = \overline{\psi(a)} = \psi(\rho_2(a))$. Thus $\rho_1 = \rho_2$ by Lemma 3.1, giving (ii).

The map $^-$ extends $\mathbb{R}$-linearly to $A_{\mathbb{R}}$, and the proofs of (i) and (ii) extend to $A_{\mathbb{R}}$ to give (iii).

We have $A_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s$ for some $r,s \in \mathbb{Z}_{\geq 0}$, and $\mathrm{Rhom}_{\mathbb{R}}(A_{\mathbb{R}},\mathbb{C}) = \{\psi_j\}_{j=1}^{r+2s}$ with $\psi_j : A_{\mathbb{R}} \to \mathbb{R}$ for $1 \leq j \leq r$ and $\psi_{s+j} = \overline{\psi_j}$ for $r+1 \leq j \leq r+s$. For (iv), suppose $0 \neq a \in A_{\mathbb{R}}$. Then

$$\mathrm{Tr}_{A_{\mathbb{R}}/\mathbb{R}}(a\bar{a}) = \sum_{\psi \in \mathrm{Rhom}_{\mathbb{R}}(A_{\mathbb{R}},\mathbb{C})} \psi(a\bar{a}) = \sum_{i=1}^{r} \psi_i(a)^2 + 2\sum_{i=r+1}^{r+s} \psi_i(a)\overline{\psi_i(a)} > 0.$$

□

Remark 3.5. If A is an order, then A is a CM-order if and only if $A_{\mathbb{Q}}$ is a CM-algebra and $A = \bar{A}$.

Definition 3.6. If A is a CM-order, define

$$\hat{A} = \{a \in A_{\mathbb{Q}} : \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(aA) \subset \mathbb{Z}\} \subset A_{\mathbb{Q}},$$

$$A_{\mathbb{R}}^+ = \{a \in A_{\mathbb{R}} : a = \bar{a}\} = \{a \in A_{\mathbb{R}} : \forall \psi \in \mathrm{Rhom}(A,\mathbb{C}), \psi(a) \in \mathbb{R}\},$$

$$\begin{aligned}(A_{\mathbb{R}}^+)_{>0} &= \{a \in A_{\mathbb{R}} : \forall \psi \in \mathrm{Rhom}_{\mathbb{R}}(A_{\mathbb{R}},\mathbb{C}), \psi(a) \in \mathbb{R}_{\geq 0} \text{ and } \exists \psi : \psi(a) > 0\} \\ &= \{a \in A_{\mathbb{R}} : \forall \psi \in \mathrm{Rhom}_{\mathbb{R}}(A_{\mathbb{R}},\mathbb{C}), \psi(a) \in \mathbb{R}_{\geq 0}\} - \{0\}, \\ (A_{\mathbb{R}}^+)_{\gg 0} &= \{a \in A_{\mathbb{R}} : \forall \psi \in \mathrm{Rhom}_{\mathbb{R}}(A_{\mathbb{R}},\mathbb{C}), \psi(a) \in \mathbb{R}_{>0}\},\end{aligned}$$

and for $B \subset A_{\mathbb{R}}$ define

$$B^+ = B \cap A_{\mathbb{R}}^+, \quad B_{>0}^+ = B \cap (A_{\mathbb{R}}^+)_{>0}, \quad B_{\gg 0}^+ = B \cap (A_{\mathbb{R}}^+)_{\gg 0}.$$

We will apply Definition 3.6 with $B = A$ and with $B = \hat{A}$.

The set $A^{+}_{>0}$ is not necessarily closed under multiplication (since A is not necessarily a domain).

Examples 3.7. (i) If F is a CM-field, then the ring of integers of F is a CM-order, with complex conjugation serving as $\bar{\ }$.

(ii) If B is a subring of a CM-order, then the subring generated by B and $\bar{B}$ is a CM-order.

(iii) If A_1 and A_2 are CM-orders, then so are $A_1 \times A_2$ and $A_1 \otimes_{\mathbb{Z}} A_2$.

(iv) Suppose G is a finite abelian group of order n. If $A = \mathbb{Z}[G]$ then $\hat{A} = \frac{1}{n}\mathbb{Z}[G]$.

Example 3.8. A suborder of a CM-order is not necessarily a CM-order, since the automorphism $\bar{\ }$ might not preserve the suborder. For example, suppose A is a CM-order, and $\mathfrak{m}$ is a maximal ideal of A such that $\mathfrak{m} \neq \bar{\mathfrak{m}}$ and $A/\mathfrak{m}$ is not a prime field. Then $A/\mathfrak{m}$ contains a prime field F, and the inverse image of F under the natural map $A \to A/\mathfrak{m}$ is a proper subring R of A such that $R \neq \bar{R}$, so R is not a CM-order.

Example 3.9. Suppose that q is a prime power and π is a q-Weil number, i.e., π is an algebraic integer in $\mathbb{C}$ such that $|\sigma(\pi)| = \sqrt{q}$ for all $\sigma \in \operatorname{Aut}(\mathbb{C})$. Then $\mathbb{Z}[\pi, \bar{\pi}]$ is a CM-order, but if $[\mathbb{Q}(\pi) : \mathbb{Q}] > 2$ then its suborder $\mathbb{Z}[\pi]$ is not a CM-order. To see the latter, consider the irreducible polynomial $\sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ that π satisfies with $a_n = 1$. Then $\pi \sum_{i=0}^{n-1} a_{i+1}\pi^i = -a_0 = \pm q^{n/2} = \pm q^{n/2-1}\pi\bar{\pi}$. Thus, $\bar{\pi} = \pm q^{1-n/2}(\sum_{i=0}^{n-1} a_{i+1}\pi^i)$. The coefficient of $\bar{\pi}$ at π^{n-1} is $\pm q^{1-n/2} \notin \mathbb{Z}$, so $\bar{\pi} \notin \mathbb{Z}[\pi]$. The order $\mathbb{Z}[\pi]$ passes steps (i)–(iv) of Algorithm 3.11 below, but not step (v).

Proposition 3.10. *Suppose A is a CM-order and $a \in A^{+}_{\gg 0}$. Then the following are equivalent:*

(i) $a = 1$,

(ii) $\operatorname{Tr}(a) = \operatorname{rank}_{\mathbb{Z}}(A)$,

(iii) $\operatorname{Tr}(a) \leq \operatorname{rank}_{\mathbb{Z}}(A)$.

Proof. The implications (i) ⇒ (ii) ⇒ (iii) are clear. Since $a \in A^{+}_{\gg 0}$, we have $\sigma(a) \in \mathbb{R}_{>0}$ for all $\sigma \in \operatorname{Rhom}(A_{\mathbb{Q}}, \mathbb{C})$, and $\prod_{\sigma} \sigma(a) \in \mathbb{Z}_{>0}$. Assuming (iii), then applying the arithmetic-geometric mean inequality we have

$$\operatorname{rank}_{\mathbb{Z}}(A) \geq \operatorname{Tr}(a) = \sum_{\sigma \in \operatorname{Rhom}(A_{\mathbb{Q}},\mathbb{C})} \sigma(a) = \operatorname{rank}_{\mathbb{Z}}(A) \cdot \frac{\sum_{\sigma} \sigma(a)}{\#\operatorname{Rhom}(A_{\mathbb{Q}}, \mathbb{C})}$$

$$\geq \operatorname{rank}_{\mathbb{Z}}(A) \cdot [\prod_{\sigma \in \operatorname{Rhom}(A_{\mathbb{Q}},\mathbb{C})} \sigma(a)]^{1/\#\operatorname{Rhom}(A_{\mathbb{Q}},\mathbb{C})} \geq \operatorname{rank}_{\mathbb{Z}}(A).$$

Thus we have equality everywhere, and all $\sigma(a) = 1$, so $a = 1$, and (iii) ⇒ (i). □

The following algorithm is patterned after the algorithm described in Remark 2.8.

Algorithm 3.11. Given an order A, the algorithm decides whether A is a CM-order, and if so computes the automorphism $\bar{\ }$.

Steps:

(i) Compute the discriminant $\Delta_{A/\mathbb{Z}}$ of A. If it is 0, terminate with "no".

(ii) Use Algorithm 7.2 of [15] to find all $\mathfrak{m} \in \operatorname{Spec}(A_{\mathbb{Q}})$ and to find a $\mathbb{Q}$-basis for each field $A_{\mathbb{Q}}/\mathfrak{m}$.

(iii) For each $\mathfrak{m} \in \operatorname{Spec}(A_{\mathbb{Q}})$, apply Algorithm 2.6 to determine whether the field $A_{\mathbb{Q}}/\mathfrak{m}$ is a CM-field. If one is not, terminate with "no", and if all are, use Algorithm 2.6 to compute $^-$ on each $A_{\mathbb{Q}}/\mathfrak{m}$ and thus on $A_{\mathbb{Q}} \xrightarrow{\sim} \prod_{\mathfrak{m}} A_{\mathbb{Q}}/\mathfrak{m}$.

(iv) Express the given $\mathbb{Z}$-basis for A with respect to the $\mathbb{Q}$-basis for $A_{\mathbb{Q}}$ obtained in Step (ii).

(v) Compute the matrix for $^-$ with respect to the $\mathbb{Z}$-basis for A. If all entries are integers, then output "yes" and this matrix, and otherwise terminate with "no".

Proposition 3.12. *Algorithm 3.11 is correct and runs in polynomial time.*

Proof. The algorithm is correct by Remarks 2.2, 2.8, and 3.5 (since $\Delta_{A/\mathbb{Z}} \neq 0$ if and only if every element of A is separable), and runs in polynomial time since each step does. □

4. A-lattices

Throughout this section A is a CM-order, except for Lemma 4.7. Suppose that L is an A-module. Then there is an A-module $\overline{L}$ with a group isomorphism $^- : L \to \overline{L}$ that is semi-linear, i.e., $\overline{rx} = \bar{r} \cdot \bar{x}$ for all $r \in A$ and $x \in L$. The module $\overline{L}$ is easy to construct. If $L = A$, one can take $\overline{L} = A$, and take $^-$on L to be the same as $^-$on A.

Recall that we define an A-lattice L to be a lattice that is given an A-module structure with the property that for all $a \in A$ and $x, y \in L$ one has $\langle ax, y\rangle = \langle x, \bar{a}y\rangle$. Recall the definition of $\hat{A}$ in Definition 3.6.

Proposition 4.1. *Suppose L is an A-lattice. Then:*

(i) *if $x, y \in L$, then there exists a unique $z_{x,y} \in \hat{A}$ such that*

$$\operatorname{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(az_{x,y}) = \langle ax, y\rangle$$

for all $a \in A$;

(ii) *there is a unique A-linear homomorphism $\varphi = \varphi_L : L \otimes_A \bar{L} \to \hat{A}$ such that*

$$\operatorname{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(\varphi(x \otimes \bar{y})) = \langle x, y\rangle$$

for all $x, y \in L$; for this map φ we have

(a) *$\varphi(x \otimes \bar{y}) = z_{x,y}$ for all $x, y \in L$,*

(b) *$\varphi(x \otimes \bar{y}) = \overline{\varphi(y \otimes \bar{x})}$ for all $x, y \in L$,*

(c) *$\varphi(x \otimes \bar{x}) \in \hat{A}^{+}_{>0}$ for all $0 \neq x \in L$.*

Proof. Since $g : \hat{A} \xrightarrow{\sim} \operatorname{Hom}_{\mathbb{Z}}(A, \mathbb{Z})$, $b \mapsto (a \mapsto \operatorname{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(ab))$ is an isomorphism, for every $x, y \in L$ there exists a unique $z_{x,y} \in \hat{A}$ such that $g(z_{x,y})$ is the map $a \mapsto \langle ax, y\rangle$. This proves (i).

It is straightforward to check that the map $L \times \bar{L} \to \hat{A}, (x, \bar{y}) \mapsto z_{x,y}$ is A-bilinear. Thus there exists a unique A-linear map $\varphi : L \otimes_A \bar{L} \to \hat{A}, x \otimes \bar{y} \mapsto z_{x,y}$, and by (i) we have $\operatorname{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(a\varphi(x \otimes \bar{y})) = \langle ax, y\rangle$ for all $x, y \in L$ and $a \in A$.

If a map $\varphi : L \otimes_A \bar{L} \to \hat{A}$ is A-linear and satisfies $\operatorname{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(\varphi(x \otimes \bar{y})) = \langle x, y\rangle$ for all $x, y \in L$, then $\operatorname{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(a\varphi(x \otimes \bar{y})) = \langle ax, y\rangle$ for all $x, y \in L$ and $a \in A$, so $\varphi(x \otimes \bar{y}) = z_{x,y}$ by (i), giving the uniqueness in (ii).

Since for all $a \in A$ we have

$$\operatorname{Tr}(az_{x,y}) = \langle ax, y\rangle = \langle x, \bar{a}y\rangle = \langle \bar{a}y, x\rangle = \operatorname{Tr}(\bar{a}z_{y,x}) = \operatorname{Tr}(a\overline{z_{y,x}})$$

it follows that $z_{x,y} = \overline{z_{y,x}}$ and thus $\varphi(x \otimes \bar{y}) = \overline{\varphi(y \otimes \bar{x})}$ for all $x, y \in L$.

Substituting x for y, it follows that $\varphi(x \otimes \bar{x}) \in \hat{A}^+$. If $x \neq 0$ then $\langle x, x\rangle \neq 0$, so $\mathrm{Tr}(\varphi(x \otimes \bar{x})) \neq 0$, so $\varphi(x \otimes \bar{x}) \neq 0$. Extending φ $\mathbb{R}$-linearly, we have

$$\mathrm{Tr}_{A_\mathbb{R}/\mathbb{R}}(a\bar{a}\varphi(x \otimes \bar{x})) = \langle a\bar{a}x, x\rangle = \langle \bar{a}x, \bar{a}x\rangle \geq 0$$

for all $x \in L_\mathbb{R}$ and $a \in A_\mathbb{R}$. The proof of Lemma 7.3(vii) of [14] with $A_\mathbb{R}$ in the role of $\mathbb{R}\langle G\rangle$ and $z = \varphi(x \otimes \bar{x})$ now gives that $\psi(\varphi(x \otimes \bar{x})) \geq 0$ for all $\psi \in \mathrm{Rhom}_\mathbb{R}(A_\mathbb{R}, \mathbb{C})$ and all $x \in L_\mathbb{R}$. It follows now that $\varphi(x \otimes \bar{x}) \in \hat{A}^+_{>0}$ for all $0 \neq x \in L$, and we have (ii). □

Proposition 4.2. *Suppose L is a finitely generated A-module, and $\varphi = \varphi_L : L \otimes_A \bar{L} \to \hat{A}$ is an A-linear homomorphism such that*

(i) $\varphi(x \otimes \bar{y}) = \overline{\varphi(y \otimes \bar{x})}$ *for all $x, y \in L$, and*
(ii) $\varphi(x \otimes \bar{x}) \in \hat{A}^+_{>0}$ *for all $0 \neq x \in L$.*

Then L is an A-lattice with respect to the inner product

$$\langle x, y\rangle = \mathrm{Tr}_{A_\mathbb{Q}/\mathbb{Q}}(\varphi(x \otimes \bar{y})).$$

Proof. Define $\langle\ ,\ \rangle : L \otimes_A \bar{L} \to \mathbb{Z}$ by $\langle x, y\rangle = \mathrm{Tr}_{A_\mathbb{Q}/\mathbb{Q}}(\varphi(x \otimes \bar{y}))$. Note that the image lies in $\mathbb{Z}$ by the definition of $\hat{A}$, and $\mathbb{Z}$-bilinearity is also clear. We have

$$\langle x, y\rangle = \mathrm{Tr}(\varphi(x \otimes \bar{y})) = \mathrm{Tr}(\overline{\varphi(y \otimes \bar{x})}) = \mathrm{Tr}(\varphi(y \otimes \bar{x})) = \langle y, x\rangle.$$

If $x \neq 0$ then

$$\langle x, x\rangle = \mathrm{Tr}_{A_\mathbb{Q}/\mathbb{Q}}(\varphi(x \otimes \bar{x})) = \sum_{\psi \in \mathrm{Rhom}(A_\mathbb{Q}, \mathbb{C})} \psi(\varphi(x \otimes \bar{x})) > 0,$$

the inequality holding since each $\psi(\varphi(x \otimes \bar{x}))$ is real and non-negative, and at least one is positive. By the A-linearity of φ we have

$$\langle ax, y\rangle = a\mathrm{Tr}_{A_\mathbb{Q}/\mathbb{Q}}(\varphi(x \otimes \bar{y})) = \langle x, \bar{a}y\rangle.$$

□

Definition 4.3. An A-lattice L is *invertible* if the values of the map φ_L of Proposition 4.1 all lie in A and the map $\varphi_L : L \otimes_A \bar{L} \to A$ is an isomorphism of A-modules.

Remarks 4.4. (i) For the standard A-lattice $L = A$ we have $\varphi_A(x \otimes \bar{y}) = x\bar{y}$ and $\langle x, y\rangle = \mathrm{Tr}_{A/\mathbb{Z}}(x\bar{y})$. The standard A-lattice is invertible since the map $A \otimes_A \bar{A} \to A$, $x \otimes \bar{y} \mapsto x\bar{y}$ is an isomorphism.
(ii) Invertibility is preserved under A-lattice isomorphisms.

Definition 4.5. An A-module L is *invertible* if there is an A-module M such that $L \otimes_A M$ and A are isomorphic as A-modules.

Remark 4.6. If L is an invertible A-lattice, then L is an invertible A-module.

Lemma 4.7. *If A is a reduced order and L is an invertible A-module, then $L_\mathbb{Q}$ and $A_\mathbb{Q}$ are isomorphic as $A_\mathbb{Q}$-modules, and* $\mathrm{rank}_\mathbb{Z}(L) = \mathrm{rank}_\mathbb{Z}(A)$.

Proof. We use the argument that shows (c) ⇒ (a) of Theorem 11.1 in [14]. Since $A_\mathbb{Q}$ is a product of finitely many fields $A_\mathbb{Q}/\mathfrak{m}$ with $\mathfrak{m} \in \mathrm{Maxspec}(A)$, and $L_\mathbb{Q}$ is an $A_\mathbb{Q}$-module, we have $L_\mathbb{Q} = \prod_\mathfrak{m} V_\mathfrak{m}$ where $V_\mathfrak{m}$ is a vector space over $A_\mathbb{Q}/\mathfrak{m}$. Let $d_\mathfrak{m}(L) = \dim(V_\mathfrak{m})$. Since L is invertible, there is an A-module M such that $L_\mathbb{Q} \otimes_{A_\mathbb{Q}} M_\mathbb{Q} \cong A_\mathbb{Q}$. Thus, $d_\mathfrak{m}(L)d_\mathfrak{m}(M) = d_\mathfrak{m}(A) = 1$, so $d_\mathfrak{m}(L) = 1 = d_\mathfrak{m}(M)$. The desired result now follows. □

Notation 4.8. If $x, y \in L$, when we write $x \cdot \bar{y}$ or $x\bar{y}$ we mean $\varphi(x \otimes \bar{y})$.

Remark 4.9. If L is an A-lattice, $x \in L$, and $x\bar{x} = 1$, then $\langle x, x\rangle = \mathrm{rank}_{\mathbb{Z}}(A)$, by Propositions 3.10 and 4.1.

We call a commutative ring R *connected* if it has exactly two idempotents. The following result allows us to reduce our main algorithm (Theorem 1.5) to the case where A is connected.

Lemma 4.10. *Suppose $\mathcal{I}$ is the set of primitive idempotents of A. Then:*

(i) *$A = \prod_{e\in\mathcal{I}} eA$ and each eA is a CM-order (viewing eA as a ring with identity e),*
(ii) *if L is an A-lattice, then L is the orthogonal sum $\perp_{e\in\mathcal{I}} eL$ and each eL is an eA-lattice,*
(iii) *if L is an invertible A-lattice, then each eL is an invertible eA-lattice.*

Proof. Since $\mathcal{I}$ is the set of primitive idempotents of A we have $1 = \sum_{e\in\mathcal{I}} e$, so $A = \prod_{e\in\mathcal{I}} eA$ and $L = \bigoplus_{e\in\mathcal{I}} eL$. Suppose $e \in \mathcal{I}$. Then $\psi(e) \in \{0, 1\}$ for all $\psi \in \mathrm{Rhom}(A, \mathbb{C})$, so $\psi(e) = \overline{\psi(e)} = \psi(\bar{e})$ for all ψ. Thus, $e = \bar{e}$, so $\overline{eA} = \bar{e}\bar{A} = eA$. Parts (i) and (ii) now follow easily from Definition 1.1 and the definition of an A-lattice. Part (iii) follows from the definition of invertibility since $1\otimes 1 = \sum_{e\in\mathcal{I}}(e\otimes\bar{e})$ and $(e \otimes \bar{e})(L \otimes_A \bar{L}) = eL \otimes_{eA} \overline{eL}$. □

5. Reduced bases

The main result of this section is Proposition 5.5. It shows that there exists $B \in \mathbb{R}$ depending only on the CM-order A, and polynomially bounded in the length of the data specifying A, such that for each invertible A-lattice L, the length of the data specifying L is bounded by B. It is an analogue of Proposition 3.4 of [14] (see also Lemma 3.12 of [11]), which was for integral unimodular lattices. It allows us to show that the Witt-Picard group of A is finite (Theorem 12.2 below), and helps to show, as in [14], that the algorithms associated with Theorem 13.1 run in polynomial time.

Definition 5.1. If $\{b_1, \ldots, b_m\}$ is a basis for a lattice L, and $\{b_1^*, \ldots, b_m^*\}$ is its Gram-Schmidt orthogonalization, and $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*$ with $\mu_{ij} \in \mathbb{R}$, then $\{b_1, \ldots, b_m\}$ is **LLL-reduced** if

(i) $|\mu_{ij}| \le \frac{1}{2}$ for all $j < i \le m$, and
(ii) $|b_i^*|^2 \le 2|b_{i+1}^*|^2$ for all $i < m$.

The LLL basis reduction algorithm [7] takes as input a lattice, and produces an LLL-reduced basis of the lattice, in polynomial time.

Recall the definition of the inner product $(\ ,\ )$ in Definition 3.2.

Lemma 5.2. *If A is a CM-order, L is an A-lattice, $a \in A$, and $x \in L$, then $\langle ax, ax\rangle \le (a, a)\langle x, x\rangle$.*

Proof. If $\sigma \in \mathrm{Rhom}(A_{\mathbb{Q}}, \mathbb{C})$, then $\sigma(a\bar{a}) = \sigma(a)\overline{\sigma(a)} \in \mathbb{R}_{\geq 0}$, and $\sigma(\varphi(x \otimes \bar{x})) \in \mathbb{R}_{\geq 0}$ by Proposition 4.1(ii)(c). Then by Proposition 4.1(ii) we have

$$\begin{aligned}\langle ax, ax\rangle &= \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(\varphi(ax \otimes \overline{ax})) = \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(a\bar{a}\varphi(x \otimes \overline{x})) \\ &= \sum_{\sigma \in \mathrm{Rhom}(A_{\mathbb{Q}}, \mathbb{C})} \sigma(a\bar{a})\sigma(\varphi(x \otimes \bar{x})) \leq \left(\sum_{\sigma} \sigma(a\bar{a})\right)\left(\sum_{\sigma} \sigma(\varphi(x \otimes \bar{x}))\right) \\ &\qquad\qquad = (a, a)\mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(\varphi(x \otimes \overline{x})) = (a, a)\langle x, x\rangle.\end{aligned}$$

□

Definition 5.3. We define the determinant $\det(L)$ of a lattice L to be the determinant of its Gram matrix, or equivalently, the order of the cokernel of the map $L \to \mathrm{Hom}(L, \mathbb{Z})$, $x \mapsto (y \mapsto \langle x, y\rangle)$.

Lemma 5.4. *If L is an invertible A-lattice, then* $\det(L) = \det(A) = |\Delta_{A/\mathbb{Z}}|$.

Proof. Consider the maps:

$$L \to \mathrm{Hom}_A(\overline{L}, A) \to \mathrm{Hom}(\overline{L}, \mathbb{Z}) \to \mathrm{Hom}(L, \mathbb{Z})$$

where the left-hand map is the A-module isomorphism $x \mapsto (\bar{y} \mapsto \varphi(x \otimes \overline{y}))$ with inverse $f \mapsto (\mathrm{id}_L \otimes f) \circ \varphi^{-1}(1)$, the middle map is $f \mapsto \mathrm{Tr}_{A/\mathbb{Z}} \circ f$, and the right-hand map is the group isomorphism $g \mapsto (y \mapsto g(\overline{y}))$. By Proposition 4.1, the composition is the map $x \mapsto (y \mapsto \langle x, y\rangle)$ of Definition 5.3. We will show that the cokernel of the middle map has order $|\Delta_{A/\mathbb{Z}}|$. By the definition of $\Delta_{A/\mathbb{Z}}$, this holds with A in place of $\overline{L}$, and we next reduce to that case. Since L is invertible, we may identify $\overline{L}_{\mathbb{Q}}$ with $A_{\mathbb{Q}}$ by Lemma 4.7. Multiplying $\overline{L}$ by a sufficiently large positive integer, we may assume that $\overline{L} \subset A$. Let

$$L' = \{a \in A_{\mathbb{Q}} : a\overline{L} \subset A\}.$$

Consider the commutative diagram

$$\begin{tikzcd} L' = \mathrm{Hom}_A(\overline{L}, A) \arrow[r] & \mathrm{Hom}(\overline{L}, \mathbb{Z}) \\ A = \mathrm{Hom}_A(A, A) \arrow[r] \arrow[u] & \mathrm{Hom}(A, \mathbb{Z}) \arrow[u] \end{tikzcd}$$

where the vertical maps are the restriction maps. The orders of the cokernels of the left and right maps are, respectively, $(L' : A)$ and $(A : \overline{L})$. It suffices to show that these two numbers are equal.

We have $A \to L \otimes_A \overline{L} \twoheadrightarrow L \cdot \overline{L}$ where the first map is the inverse of the isomorphism φ_L, so $L \cdot \overline{L}$ is a principal ideal of A. Hence $I = \overline{L}$ is an invertible A-ideal of finite index, and $I^{-1} = \{a \in A_{\mathbb{Q}} : aI \subset A\} = L'$. It remains to show that $(I^{-1} : A) = (A : I)$. The map $J \mapsto J \cdot I$ from the set of intermediate A-modules of $I^{-1} \supset A$ to the set of intermediate A-modules of $A \supset I$ is a bijection with inverse $K \mapsto K \cdot I^{-1}$. So a composition chain of I^{-1}/A gives a composition chain of A/I. Thus it suffices to prove that if J/J' is simple then $J/J' \cong J \cdot I/J' \cdot I$. If $J/J' \cong A/\mathfrak{m}$ with $\mathfrak{m} \in \mathrm{Maxspec}(A)$, then $J \cdot I/J' \cdot I$ is also simple and annihilated by $\mathfrak{m}$, so is also isomorphic to $A/\mathfrak{m}$. This gives the desired result. □

We specify an A-lattice L by giving A as before, $m = \mathrm{rank}_{\mathbb{Z}}(L)$, the Gram matrix $(\langle b_i, b_j\rangle)_{i,j=1}^{m}$ with respect to a $\mathbb{Z}$-basis $\{b_1, \ldots, b_m\}$ for L, and $d_{ijk} \in \mathbb{Z}$

for $i \in \{1,\dots,n\}$ and $j,k \in \{1,\dots,m\}$ such that $\alpha_i b_j = \sum_{k=1}^m d_{ijk} b_k$ for all i and j, with respect to the same $\mathbb{Z}$-basis $\{\alpha_i\}_{i=1}^n$ that was used for the system of integers $\{b_{ijk}\}_{i,j,k=1}^n$ used to specify A. We always work with LLL-reduced bases for A-lattices, as we explained for A at the beginning of Section 3.

If $x \in L_{\mathbb{R}}$ let $|x| = \langle x,x\rangle^{1/2}$, and if $a \in A_{\mathbb{R}}$ let $|a| = (a,a)^{1/2}$.

Proposition 5.5. *If A is a CM-order, n is its rank, L is an invertible A-lattice, $\{b_1,\dots,b_m\}$ is an LLL-reduced basis for L, and $\{b_1^*,\dots,b_m^*\}$ is its Gram-Schmidt orthogonalization, then $m = n$ and:*

(i) $2^{1-i} \le |b_i^*|^2 \le 2^{n-i}|\Delta_{A/\mathbb{Z}}|$ *for all i,*
(ii) $|b_i|^2 \le 2^{n-1}|\Delta_{A/\mathbb{Z}}|$ *for all i,*
(iii) $|\langle b_i,b_j\rangle| \le 2^{n-1}|\Delta_{A/\mathbb{Z}}|$ *for all i and j,*
(iv) $|d_{ijk}|, |b_{ijk}| \le (3\sqrt{2})^{n-1}|\Delta_{A/\mathbb{Z}}|$ *for all i, j, and k.*

Proof. The proof generalizes our proof of Proposition 3.4 of [14] (and corrects some typographical errors therein). Since L is an invertible A-lattice, we have $m = n$ and $\det(L) = |\Delta_{A/\mathbb{Z}}|$, by Lemma 5.4. It follows from Definition 5.1(ii) that for all $1 \le i \le j \le n$ we have $|b_i^*|^2 \le 2^{j-i}|b_j^*|^2$, so for all i we have $2^{1-i}|b_1^*|^2 \le |b_i^*|^2 \le 2^{n-i}|b_n^*|^2$. Since L is integral we have $|b_1^*|^2 = |b_1|^2 = \langle b_1,b_1\rangle \ge 1$, so $|b_i^*|^2 \ge 2^{1-i}$. Letting $L_i = \sum_{j=1}^i \mathbb{Z}b_j$, we have $|b_i^*|^2 = \det(L_i)/\det(L_{i-1})$. Since L is integral we have $|b_n^*|^2 = \det(L_n)/\det(L_{n-1}) \le |\Delta_{A/\mathbb{Z}}|$, so $|b_i^*|^2 \le 2^{n-i}|\Delta_{A/\mathbb{Z}}|$, giving (i).

Following the proof of Proposition 3.4(ii,iii) of [14] now gives (ii) and (iii).

Define $\{c_1,\dots,c_n\}$ to be the $\mathbb{Q}$-basis of $L_{\mathbb{Q}}$ that is dual to $\{b_1,\dots,b_n\}$, i.e., $\langle c_i,b_j\rangle = \delta_{ij}$ for all i and j, where δ_{ij} is the Kronecker delta symbol. Then $d_{ijk} = \langle c_j, \alpha_i b_j\rangle$, so

$$|d_{ijk}| \le |c_j||\alpha_i b_j| \le |c_j||\alpha_i||b_j| \le 2^{n-1}|\Delta_{A/\mathbb{Z}}||c_j|$$

by the Cauchy-Schwarz inequality, Lemma 5.2, and (ii) applied to the A-lattices L and A. The proof of Proposition 3.4(iv) of [14] shows that $|c_j|^2 \le (9/2)^{n-1}$, and this gives the desired bound on $|d_{ijk}|$ in (iv). Applying this to the standard A-lattice A (recall that $\{\alpha_i\}_{i=1}^n$ is LLL-reduced) gives the desired bound on $|b_{ijk}|$. □

6. Short vectors in lattice cosets

We show how to find the unique "short" vector in a suitable lattice coset, when such a vector exists.

Definition 6.1. Suppose A is a CM-order and L is an A-lattice. We say $x \in L$ is *short* if $\varphi(x \otimes \bar{x}) = 1$, where φ is the map from Proposition 4.1.

Shortness is preserved by A-lattice isomorphisms. Recalling Notation 4.8, the element x is short if and only if $x\bar{x} = 1$. Hence $\langle x,x\rangle = \mathrm{rank}_{\mathbb{Z}}(A)$ when x is short.

The following algorithm is an analogue of Algorithm 4.2 of [14]. We will use it in Algorithms 17.5 and 14.5 below.

Algorithm 6.2. Given a CM-order A, an A-lattice L of $\mathbb{Z}$-rank n, an A-ideal $\mathfrak{a}$ of finite index in A such that

$$\langle \beta,\beta\rangle \ge (2^{n/2}+1)^2 \mathrm{rank}_{\mathbb{Z}}(A) \text{ for all } \beta \in \mathfrak{a}L \smallsetminus \{0\}, \tag{6.2.1}$$

and $C \in L/\mathfrak{a}L$, the algorithm computes all $y \in C$ with $\langle y,y\rangle = \mathrm{rank}_{\mathbb{Z}}(A)$.

Steps:

(i) Compute an LLL-reduced basis for $\mathfrak{a}L$ and use it as in §10 of [9] to compute $y \in C$ such that $\langle y, y\rangle \leq (2^n - 1)\langle x, x\rangle$ for all $x \in C$, i.e., find an approximate solution to the shortest vector problem.
(ii) Compute $\langle y, y\rangle$.
(iii) If $\langle y, y\rangle = \mathrm{rank}_{\mathbb{Z}}(A)$, output y.
(iv) If $\langle y, y\rangle \neq \mathrm{rank}_{\mathbb{Z}}(A)$, output "there is no $y \in C$ with $\langle y, y\rangle = \mathrm{rank}_{\mathbb{Z}}(A)$".

The following result is used to prove Proposition 17.6.

Proposition 6.3. *Algorithm 6.2 is correct and runs in polynomial time. Further, the number of y output by the algorithm is* 0 *or* 1, *and if such a y exists then it is the unique shortest element of C.*

Proof. Let $y \in C$ be as computed in Step (i). Then $\langle y, y\rangle \leq (2^n - 1)\langle x, x\rangle$ for all $x \in C$. Suppose $z \in C$ is such that $\langle z, z\rangle \leq \mathrm{rank}_{\mathbb{Z}}(A)$, and let $\beta = z - y \in \mathfrak{a}L$. Then

$$\langle \beta, \beta\rangle \leq \left(\langle z, z\rangle^{1/2} + \sqrt{2^n - 1}\langle z, z\rangle^{1/2}\right)^2 < (2^{n/2} + 1)^2 \mathrm{rank}_{\mathbb{Z}}(A),$$

so $\beta = 0$ by (6.2.1) and $z = y$. It follows that the algorithm finds all $y \in C$ with $\langle y, y\rangle = \mathrm{rank}_{\mathbb{Z}}(A)$, there is at most one such, and if one exists then it is the unique shortest element of C. □

Remark 6.4. Note that $2^{2(n+1)} \geq (2^{n/2} + 1)^2 n$. Thus if L is an A-lattice, $n = \mathrm{rank}_{\mathbb{Z}}(A) = \mathrm{rank}_{\mathbb{Z}}(L)$, and $\mathfrak{a} = 2^{n+1}A$, then (6.2.1) holds. We will make special use of the ideal $2^{n+1}A$ in Algorithms 14.5 and 17.5.

7. Short vectors and regular elements

Definition 7.1. Suppose A is a commutative ring and L is an A-module. An element $x \in L$ is *regular* (or regular in L) if the map $A \to L$ defined by $a \mapsto ax$ is injective.

Recall (Notation 4.8) that $x\bar{y}$ is shorthand for $\varphi(x \otimes \bar{y})$.

Proposition 7.2. *Suppose A is a CM-order, L is an A-lattice, and $x \in L$. Then the following are equivalent:*
(i) *x is regular,*
(ii) *$x\bar{x} \in \hat{A}^+_{\gg 0}$,*
(iii) *$x\bar{x}$ is regular (in $A_{\mathbb{Q}}$).*

Proof. Let $(y_{\mathbf{r}})_{\mathbf{r} \in \mathrm{Minspec}(A)}$ denote the image of $y \in A_{\mathbb{Q}}$ under the natural isomorphism $A_{\mathbb{Q}} \xrightarrow{\sim} \prod_{\mathbf{r} \in \mathrm{Minspec}(A)} A_{\mathbf{r}}$, where each $A_{\mathbf{r}}$ is a field (cf. Remark 2.2). Then $y \in A_{\mathbb{Q}}$ is regular in $A_{\mathbb{Q}}$ if and only if $y_{\mathbf{r}} \neq 0$ for all $\mathbf{r}$. This implies that (ii) and (iii) are equivalent, by Proposition 4.1(ii)(c).

Suppose x is regular. If $0 \neq a \in A$, then $ax \neq 0$, so

$$0 \neq \langle ax, ax\rangle = \mathrm{Tr}(a\bar{a}(x\bar{x})). \tag{7.2.1}$$

If $\mathbf{r} \in \mathrm{Minspec}(A)$ and $(x\bar{x})_{\mathbf{r}} = 0$ in $A_{\mathbf{r}}$, then there exists $b \in A_{\mathbb{Q}} \smallsetminus \{0\}$ such that $b(x\bar{x}) = 0$, so there exists $a \in A \smallsetminus \{0\}$ such that $a(x\bar{x}) = 0$. Thus, $a\bar{a}(x\bar{x}) = 0$, so $\mathrm{Tr}(a\bar{a}(x\bar{x})) = 0$, contradicting (7.2.1). It follows that (i) implies (ii).

Next we show that (ii) implies (i). Suppose $a \in A$ and $ax = 0$. Then $a(x\bar{x}) = (ax)\bar{x} = 0$. By (ii) we have $x\bar{x} \in \hat{A}^+_{\gg 0} \subset A^*_{\mathbb{Q}}$. Thus $a = 0$, giving (i). □

Recall the definition of *short* in Definition 6.1.

Proposition 7.3. *Suppose A is a CM-order, L is an A-lattice, $\varphi(L \otimes \bar{L}) \subset A$, and $x \in L$. Then the following are equivalent:*

(i) *x is short,*
(ii) *x is regular and $\langle x, x\rangle = \mathrm{rank}_{\mathbb{Z}}(A)$.*

Proof. That (i) implies (ii) follows from Proposition 7.2 and $\mathrm{Tr}(1) = \mathrm{rank}_{\mathbb{Z}}(A)$.

Conversely, assume (ii) and let $a = x\bar{x}$. Then $a \in A^+_{\gg 0}$ by Proposition 7.2, and $\mathrm{Tr}(a) = \langle x, x\rangle = \mathrm{rank}_{\mathbb{Z}}(A)$, so by Proposition 3.10 we have $a = 1$. □

The next result may be viewed as a variation on Kronecker's theorem that every algebraic integer all of whose conjugates lie on the unit circle must be a root of unity. We will use it to prove Theorem 11.1(iv).

Proposition 7.4. *Suppose A is a CM-order and $a \in A$. Then the following are equivalent:*

(i) *$a \in \mu(A)$,*
(ii) *a is regular and $\mathrm{Tr}(a\bar{a}) = (a, a) = \mathrm{rank}_{\mathbb{Z}}(A)$,*
(iii) *a is regular and $\mathrm{Tr}(a\bar{a}) = (a, a) \leq \mathrm{rank}_{\mathbb{Z}}(A)$,*
(iv) *$a\bar{a} = 1$.*

Proof. That (i) ⇒ (ii) follows by applying Proposition 7.3 to the standard A-lattice $L = A$. The implication (ii) ⇒ (iii) is clear. For (iii) ⇒ (iv), suppose we have (iii). Then $\bar{a}$ is regular, so $a\bar{a}$ is regular. By Proposition 7.2, $a\bar{a} \in A^+_{\gg 0}$. Since $\mathrm{Tr}(a\bar{a}) \leq \mathrm{rank}_{\mathbb{Z}}(A)$, by Proposition 3.10 we have $a\bar{a} = 1$ as desired.

To show (iv) ⇒ (i), suppose $a\bar{a} = 1$. We have $A_{\mathbb{Q}} \cong \prod_{\mathbf{r} \in \mathrm{Minspec}(A)} A_{\mathbf{r}}$ with each localization $A_{\mathbf{r}}$ being a number field, and the components $a_{\mathbf{r}}$ of a are algebraic integers all of whose conjugates lie on the unit circle, so each $a_{\mathbf{r}}$ is a root of unity. Thus, $a \in \mu(A)$. □

Example 7.5. For an example of a CM-order with a vector shorter than a "short" one, suppose that A_1 and A_2 are non-zero CM-orders and let $A = A_1 \times A_2$, a disconnected order. Then the unit element $1 \in A$ satisfies $\langle 1, 1\rangle = \mathrm{Tr}(1 \cdot \bar{1}) = \mathrm{Tr}(1) = \mathrm{rank}_{\mathbb{Z}}(A)$, so by Proposition 7.3 with $L = A$ the vector 1 is "short". For $(1, 0) \in A_1 \times A_2 = A$ we have

$$\langle (1, 0), (1, 0)\rangle = \mathrm{Tr}((1, 0) \cdot \overline{(1, 0)}) = \mathrm{rank}_{\mathbb{Z}}(A_1) < \mathrm{rank}_{\mathbb{Z}}(A)$$

and similarly

$$\langle (0, 1), (0, 1)\rangle = \mathrm{rank}_{\mathbb{Z}}(A_2) < \mathrm{rank}_{\mathbb{Z}}(A),$$

giving shorter vectors than our "short" vector $1 = (1, 1) \in A$.

Example 7.6. For an example of a *connected* order with a non-zero vector shorter than a "short" one, let

$$A = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{Z}^5 : \text{ all } x_i \text{ have the same parity}\}$$

with coordinate-wise multiplication. Then A is a subring of $\mathbb{Z}^5$ of index 16, and A is a connected order. The element $x = (2, 0, 0, 0, 0) \in A$ has $\langle x, x\rangle = 4$, while $\mathrm{rank}_{\mathbb{Z}}(A) = \langle 1, 1\rangle = 5 > 4$.

Example 7.7. Let

$$A = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : \text{ all } x_i \text{ have the same parity}\}$$

with coordinate-wise multiplication. The element $x = (2, 0, 0, 0) \in A$ has $\langle x, x\rangle = 4 = \langle 1, 1\rangle$. While 1 is regular, x is not (since in A, an element is regular if and only if no coordinate is 0).

8. Vigilant sets and lower bounds

Suppose A is a CM-order. The main result of this section is Proposition 8.5, which for any A-ideal $\mathfrak{a}$ that can be written as a product of finitely many maximal ideals, finds a lower bound for $\min\{\langle \beta, \beta\rangle : \beta \in \mathfrak{a}L \smallsetminus \{0\}\}$ in terms of $\mathfrak{a}$, valid for all A-lattices L for which the image of φ is contained in A. We will use it to prove Proposition 17.4. We start with some lemmas.

See Corollary 2.5 of [1] for the following version of Nakayama's Lemma.

Proposition 8.1 (Nakayama's Lemma)**.** *Suppose A is a commutative ring, L is a finitely generated A-module, and $\mathfrak{a}$ is an ideal of A such that $\mathfrak{a}L = L$. Then there exists $x \in 1 + \mathfrak{a} \subset A$ such that $xL = 0$.*

Lemma 8.2. *Suppose A is an order, $I \subset A_{\mathbb{Q}}$ is a fractional A-ideal, and $\mathfrak{a} \subsetneq A$ is an ideal. Then $\mathfrak{a}I \subsetneq I$.*

Proof. If not, then $\mathfrak{a}I = I$, so Nakayama's Lemma (Proposition 8.1) gives $x \in 1 + \mathfrak{a} \subset A$ such that $xI = 0$. Then $xI_{\mathbb{Q}} = 0$. But $I_{\mathbb{Q}} = A_{\mathbb{Q}}$. So $x = x \cdot 1 \in x \cdot A_{\mathbb{Q}} = xI_{\mathbb{Q}} = \{0\}$. Thus, $1 \in \mathfrak{a}$, so $\mathfrak{a} = A$, a contradiction. □

Recall that if $\mathfrak{p} \in \mathrm{Spec}(A)$, then $\mathrm{N}(\mathfrak{p}) = \#(A/\mathfrak{p})$.

Lemma 8.3. *Suppose A is an order, $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \in \mathrm{Maxspec}(A)$, and I is a fractional A-ideal. Then*

$$\#(I/\mathfrak{p}_1 \cdots \mathfrak{p}_m I) \geq \prod_{i=1}^{m} \mathrm{N}(\mathfrak{p}_i).$$

Proof. We proceed by induction on m. The case $m = 0$ is clear. For $m > 0$, letting J denote the fractional A-ideal $\mathfrak{p}_1 \cdots \mathfrak{p}_{m-1} I$ we have

$$\#(I/\mathfrak{p}_1 \cdots \mathfrak{p}_m I) = \#(I/J)\#(J/\mathfrak{p}_m J).$$

By Lemma 8.2 we have $J \neq \mathfrak{p}_m J$. Thus, $\dim_{A/\mathfrak{p}_m}(J/\mathfrak{p}_m J) \geq 1$, so $\#(J/\mathfrak{p}_m J) \geq \mathrm{N}(\mathfrak{p}_m)$. □

Definition 8.4. Suppose A is a reduced order. We will say that a set S of maximal ideals of A is a *vigilant* set for A if for all $\mathbf{r} \in \mathrm{Minspec}(A)$ there exists $\mathfrak{p} \in S$ such that $\mathbf{r} \subset \mathfrak{p}$.

Being a vigilant set for A is equivalent to the natural map $A \to \prod_{\mathfrak{p}\in S} A_{\mathfrak{p}}$ being injective. If $S \subset \mathrm{Maxspec}(A)$ and $\mathbf{r} \in \mathrm{Minspec}(A)$, let

$$S(\mathbf{r}) = \{\mathfrak{p} \in S : \mathbf{r} \subset \mathfrak{p}\}.$$

Then $S = \bigcup_{\mathbf{r}\in\mathrm{Minspec}(A)} S(\mathbf{r})$, and S is a vigilant set for A if and only if each $S(\mathbf{r})$ is non-empty. If S is vigilant, we think of S as "seeing" all the irreducible components of $\mathrm{Spec}(A)$.

Proposition 8.5. *Suppose that A is a CM-order, n is its rank, L is an A-lattice such that the map φ of Proposition 4.1 takes values in A, and S is a finite subset of* $\mathrm{Maxspec}(A)$. *Suppose $t : S \to \mathbb{Z}_{\geq 0}$ is a function, and $\mathfrak{a} = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{t(\mathfrak{p})}$. For $\mathbf{r} \in \mathrm{Minspec}(A)$, let $d_{\mathbf{r}} = \mathrm{rank}_{\mathbb{Z}}(A/\mathbf{r})$. Then:*

(i) *for all non-zero $\beta \in \mathfrak{a}L$ we have*

$$\langle \beta, \beta \rangle \geq \min_{\mathbf{r}\in\mathrm{Minspec}(A)} d_{\mathbf{r}} \prod_{\mathfrak{p}\in S(\mathbf{r})} \mathrm{N}(\mathfrak{p})^{\frac{2t(\mathfrak{p})}{d_{\mathbf{r}}}};$$

(ii) *if S is vigilant and $t(\mathfrak{p}) \geq n(n+1)$ for all $\mathfrak{p} \in S$, then $\langle \beta, \beta \rangle \geq (2^{n/2}+1)^2 n$ for all $\beta \in \mathfrak{a}L \smallsetminus \{0\}$.*

Proof. Suppose $\mathbf{r} \in \mathrm{Minspec}(A)$. Then $\mathbf{r} = \ker(A \to A_{\mathbf{r}}, \alpha \mapsto \alpha_{\mathbf{r}})$, and $A_{\mathbf{r}}$ is a zero-dimensional local ring with no nilpotent elements, so it is a field, namely the field of fractions of $A/\mathbf{r}$. (Note that $A/\mathbf{r}$ is a domain but not a field.) For $C \subset A$, let $C(\mathbf{r})$ denote the image of C in $A_{\mathbf{r}}$. We have $\mathfrak{a}(\mathbf{r}) = \prod_{\mathfrak{p}\in S(\mathbf{r})} \mathfrak{p}(\mathbf{r})^{t(\mathfrak{p})}$ and $\bar{\mathfrak{a}}(\mathbf{r}) = \prod_{\mathfrak{p}\in S(\mathbf{r})} \overline{\mathfrak{p}(\mathbf{r})}^{t(\mathfrak{p})}$. If $\mathfrak{p} \in S(\mathbf{r})$, then

$$A(\mathbf{r})/\mathfrak{p}(\mathbf{r}) \cong (A/\mathbf{r})/(\mathfrak{p}/\mathbf{r}) \cong A/\mathfrak{p},$$

so

$$\#(A(\mathbf{r})/\mathfrak{p}(\mathbf{r})) = \mathrm{N}(\mathfrak{p}). \tag{8.5.1}$$

For (i), put $w = \beta\bar{\beta} \in \mathfrak{a}\bar{\mathfrak{a}}A$. Then $0 \neq w \in A^{+}_{>0}$. Choose $\mathbf{f} \in \mathrm{Minspec}(A)$ such that $w \notin \mathbf{f}$ (which we can do since $\bigcap_{\mathbf{r}\in\mathrm{Minspec}(A)} \mathbf{r} = (0)$). Then $A/\mathbf{f} \cong A(\mathbf{f}) \subset A_{\mathbf{f}}$, and $0 \neq w(\mathbf{f}) \in \mathfrak{a}\bar{\mathfrak{a}}A(\mathbf{f})$. Then

$$\begin{aligned}
\langle \beta, \beta \rangle &= \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(w) \geq \mathrm{Tr}_{A_{\mathbf{f}}/\mathbb{Q}}(w(\mathbf{f})) = \sum_{\sigma\in\mathrm{Rhom}(A_{\mathbf{f}},\mathbb{C})} \sigma(w(\mathbf{f})) \\
&= d_{\mathbf{f}} \cdot \frac{1}{d_{\mathbf{f}}} \sum_{\sigma} \sigma(w(\mathbf{f})) \\
&\geq d_{\mathbf{f}} \left(\prod_{\sigma} \sigma(w(\mathbf{f})) \right)^{1/d_{\mathbf{f}}} \qquad \text{by the arithmetic-geometric mean inequality} \\
&= d_{\mathbf{f}} |\mathrm{N}_{A(\mathbf{f})/\mathbb{Z}}(w(\mathbf{f}))|^{1/d_{\mathbf{f}}} \quad = \quad d_{\mathbf{f}}[\#(A(\mathbf{f})/w(\mathbf{f})A(\mathbf{f}))]^{1/d_{\mathbf{f}}} \\
&\geq d_{\mathbf{f}}[\#(A(\mathbf{f})/\mathfrak{a}\bar{\mathfrak{a}}A(\mathbf{f}))]^{1/d_{\mathbf{f}}} \\
&\geq d_{\mathbf{f}} \prod_{\mathfrak{p}\in S(\mathbf{f})} \mathrm{N}(\mathfrak{p})^{2t(\mathfrak{p})/d_{\mathbf{f}}} \quad \text{by (8.5.1), Lemma 8.3, and } \mathrm{N}(\overline{\mathfrak{p}}) = \mathrm{N}(\mathfrak{p}) \\
&\geq \min_{\mathbf{r}\in\mathrm{Minspec}(A)} d_{\mathbf{r}} \prod_{\mathfrak{p}\in S(\mathbf{r})} \mathrm{N}(\mathfrak{p})^{2t(\mathfrak{p})/d_{\mathbf{r}}},
\end{aligned}$$

giving (i).

For (ii), since S is vigilant each $S(\mathbf{r})$ is non-empty. Since $1 \leq d_{\mathbf{r}} \leq n$, by (i) we have

$$\langle \beta, \beta \rangle \geq \min_{\mathbf{r}\in\mathrm{Minspec}(A)} d_{\mathbf{r}} \prod_{\mathfrak{p}\in S(\mathbf{r})} \mathrm{N}(\mathfrak{p})^{\frac{2n(n+1)}{d_{\mathbf{r}}}} \geq 2^{2n+2} \geq (2^{n/2}+1)^2 n.$$

□

Example 8.6. Let $A = \mathbb{Z} \times_{\mathbb{F}_3} \mathbb{Z}$. Then $\operatorname{Spec}(A)$ is connected, and is the union of 2 copies of $\operatorname{Spec}(\mathbb{Z})$ that are identified at the prime 3. The minimal prime ideals of A are $\mathbf{r}_1 = \{0\} \times 3\mathbb{Z}$ and $\mathbf{r}_2 = 3\mathbb{Z} \times \{0\}$. Let $\mathfrak{p} = (2\mathbb{Z} \times \mathbb{Z}) \cap A$ and $S = \{\mathfrak{p}\}$. Then $S(\mathbf{r}_1) = S$, but $S(\mathbf{r}_2)$ is empty so S is not vigilant. Let $L = A$ be the standard A-lattice. For every $t \in \mathbb{Z}_{>0}$, one has $\mathfrak{p}^t = (2^t\mathbb{Z} \times \mathbb{Z}) \cap A$. Hence, independently of t, one has $\beta = (0,3) \in \mathfrak{p}^t = \mathfrak{p}^t L$, and $\langle \beta, \beta \rangle = \operatorname{Tr}((0,3)) = 9$. Thus, the hypothesis that S is vigilant cannot be removed in Proposition 8.5(ii).

9. Ideal lattices

The proof of Theorem 8.2 of [14] carries over essentially verbatim, with $\mathbb{Z}\langle G\rangle$ replaced by A and $\mathbb{Q}\langle G\rangle$ replaced by $A_\mathbb{Q}$, to show:

Theorem 9.1. *Suppose A is a CM-order, $I \subset A_\mathbb{Q}$ is a fractional A-ideal, and $w \in (A^+_\mathbb{Q})_{\gg 0}$. Suppose that $I\bar{I} \subset \hat{A}w$. Then:*

(i) *$\overline{w} = w$;*
(ii) *$w \in A^*_\mathbb{Q}$;*
(iii) *I is an A-lattice, with $\varphi(x \otimes \bar{y}) = \frac{x\bar{y}}{w}$ and $\langle x, y\rangle = \operatorname{Tr}_{A_\mathbb{Q}/\mathbb{Q}}\left(\frac{x\bar{y}}{w}\right)$.*

Notation 9.2. With I and w as in Theorem 9.1, define $L_{(I,w)}$ to be the A-lattice I with $\langle x, y\rangle = \operatorname{Tr}_{A_\mathbb{Q}/\mathbb{Q}}(x\bar{y}/w)$.

The proof of Theorem 8.5 of [14] carries over (with Tr playing the role of the scaled trace function t of [14]) to give the following result, which allows us to deduce Theorem 1.3 from Theorem 1.5.

Theorem 9.3. *Suppose A is a CM-order, I_1 and I_2 are fractional A-ideals, and $w_1, w_2 \in (A^+_\mathbb{Q})_{\gg 0}$ satisfy $I_1\overline{I_1} \subset \hat{A}w_1$ and $I_2\overline{I_2} \subset \hat{A}w_2$. Let $L_j = L_{(I_j,w_j)}$ for $j = 1, 2$. Then sending v to multiplication by v gives a bijection from*

$$\{v \in A_\mathbb{Q} : I_1 = vI_2, w_1 = v\bar{v}w_2\} \quad \text{to} \quad \{A\text{-isomorphisms } L_2 \xrightarrow{\sim} L_1\}$$

and gives a bijection from

$$\{v \in A_\mathbb{Q} : I_1 = vA, w_1 = v\bar{v}\} \quad \text{to} \quad \{A\text{-isomorphisms } A \xrightarrow{\sim} L_1\}.$$

In particular, L_1 is A-isomorphic to A if and only if there exists $v \in A_\mathbb{Q}$ such that $I_1 = (v)$ and $w_1 = v\bar{v}$.

Remark 9.4. If I, w, and $L_{(I,w)}$ are as in Theorem 9.1 and Notation 9.2, then $\overline{L_{(I,w)}} = L_{(\bar{I},w)}$.

10. Invertible A-lattices

Recall the definition of invertible A-lattice from Definition 4.3. Theorem 11.1 of [14] gave equivalent statements for invertibility of a G-lattice. The following example shows that the result does not fully extend to the case of A-lattices, while Theorem 10.3 gives a part that does carry over.

Example 10.1. We give an example of an A-lattice L that is invertible as an A-module and satisfies $\det(L) = |\Delta_{A/\mathbb{Z}}|$, but is not invertible as an A-lattice. The CM-order $A = \mathbb{Z}\left[\frac{1+\sqrt{17}}{2}, \sqrt{-1}\right]$ has

$$A^+ = \mathbb{Z}\left[\frac{1+\sqrt{17}}{2}\right], \quad \hat{A} = \frac{1}{2\sqrt{17}}A, \quad \Delta_{A/\mathbb{Z}} = 2^4 \cdot 17^2.$$

We can view A as a rank four A-lattice with $\langle x, y\rangle = \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(x\bar{y}z)$, where

$$z = \frac{5+\sqrt{17}}{5-\sqrt{17}} \in \frac{1}{2}A^{+}_{\gg 0} \subset \frac{1}{2}A \subset \hat{A}.$$

This A-lattice has determinant $2^4 \cdot 17^2$ and is invertible as an A-module. However, it is not invertible as an A-lattice, since $\varphi(1 \otimes \bar{1}) = z \notin A$.

The following lemma, which is used to prove Theorem 10.3, is an analogue of Lemma 11.4 of [14].

Lemma 10.2. *If A is a CM-order and I is an invertible fractional A-ideal, then:*

(i) *if $m \in \mathbb{Z}_{>0}$, then I/mI is isomorphic to A/mA as A-modules;*

(ii) *if $\mathfrak{a} \subset A$ is an ideal of finite index, then $I/\mathfrak{a}I$ is isomorphic to $A/\mathfrak{a}$ both as A-modules and as $A/\mathfrak{a}$-modules;*

(iii) *if I' is a fractional A-ideal, then the natural surjective map*

$$I \otimes_A I' \to II'$$

is an isomorphism.

Proof. The proof of (i) is the same as the proof of Lemma 11.4(i) of [14]. Now (ii) follows by letting $m = \#(A/\mathfrak{a})$, so that $mA \subset \mathfrak{a}$, and applying (i) to show $I/mI \cong A/mA$ as A-modules. Tensoring with $A/\mathfrak{a}$ we have

$$I/\mathfrak{a}I \cong (I/mI) \otimes_{A/mA} (A/\mathfrak{a}) \cong (A/mA) \otimes_{A/mA} (A/\mathfrak{a}) \cong A/\mathfrak{a}$$

as A-modules and as $A/\mathfrak{a}$-modules, giving (ii). The proof of (iii) is the same as the proof of Lemma 11.4(iii) of [14]. □

Theorem 10.3. *Suppose A is a CM-order and L is an A-lattice. Then L is invertible as an A-lattice if and only if there exist a fractional A-ideal $I \subset A_{\mathbb{Q}}$ and an element $w \in (A^{+}_{\mathbb{Q}})_{\gg 0}$ such that*

(i) *$I\bar{I} = Aw$ and*

(ii) *L and $L_{(I,w)}$ are isomorphic as A-lattices.*

Proof. Suppose there exist a fractional A-ideal $I \subset A_{\mathbb{Q}}$ and an element $w \in (A^{+}_{\mathbb{Q}})_{\gg 0}$ satisfying (i) and (ii). By Lemma 10.2(iii) we have

$$I \otimes_A \bar{I} \xrightarrow{\sim} I\bar{I} \xrightarrow{\sim} A, \quad x \otimes \bar{y} \mapsto x\bar{y} \mapsto \frac{x\bar{y}}{w}.$$

Thus the composition $\varphi : L \otimes_A \bar{L} = I \otimes_A \bar{I} \xrightarrow{\sim} A$ is an isomorphism, and

$$\mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(\varphi(x \otimes \bar{y})) = \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}\left(\frac{x\bar{y}}{w}\right) = \langle x, y\rangle_{L_{(I,w)}} = \langle x, y\rangle_L,$$

so $\varphi = \varphi_L$.

Conversely, suppose that L is an invertible A-lattice. Extending $\mathbb{Q}$-linearly the map φ from Proposition 4.1 we have an isomorphism $\varphi : L_{\mathbb{Q}} \otimes_{A_{\mathbb{Q}}} \bar{L}_{\mathbb{Q}} \xrightarrow{\sim} A_{\mathbb{Q}}$ as $A_{\mathbb{Q}}$-modules. Lemma 4.7 gives that $L_{\mathbb{Q}}$ and $A_{\mathbb{Q}}$ are isomorphic as $A_{\mathbb{Q}}$-modules, so we may assume $L_{\mathbb{Q}} = A_{\mathbb{Q}}$. Then L is a finitely generated A-submodule of $A_{\mathbb{Q}}$ spanning $A_{\mathbb{Q}}$ over $\mathbb{Q}$, so $L = I$ for some fractional ideal I. We may then take $\bar{L} = \bar{I}$. The inclusion $I \subset A_{\mathbb{Q}}$ induces an isomorphism $I_{\mathbb{Q}} \xrightarrow{\sim} A_{\mathbb{Q}}$, which induces an $A_{\mathbb{Q}}$-module isomorphism $f : I_{\mathbb{Q}} \otimes_{A_{\mathbb{Q}}} \bar{I}_{\mathbb{Q}} \xrightarrow{\sim} A_{\mathbb{Q}} \otimes_{A_{\mathbb{Q}}} A_{\mathbb{Q}}$. Letting i be the isomorphism $i : A_{\mathbb{Q}} \otimes_{A_{\mathbb{Q}}} A_{\mathbb{Q}} \xrightarrow{\sim} A_{\mathbb{Q}}$, $x \otimes y \mapsto xy$, then the composition $i \circ f \circ \varphi^{-1} : A_{\mathbb{Q}} \xrightarrow{\sim} A_{\mathbb{Q}}$ is an $A_{\mathbb{Q}}$-module isomorphism and thus is multiplication by a unit $w \in A^{*}_{\mathbb{Q}}$. So the isomorphism $\varphi : I \otimes_A \bar{I} = L \otimes_A \overline{L} \xrightarrow{\sim} A$ takes $x \otimes y \in I \otimes_A \bar{I}$ to $x\bar{y}/w \in A$, so $I\bar{I}/w = A$.

Suppose $x \in I \cap \mathbb{Q}_{>0}$. Then

$$x^2/w = \varphi(x \otimes \bar{x}) = \overline{\varphi(x \otimes \bar{x})} = \overline{x^2/w} = x^2/\bar{w},$$

so $w = \bar{w}$. Further, $x^2/w \in A^+_{>0}$, so for all $\psi \in \mathrm{Rhom}(A_\mathbb{Q}, \mathbb{C})$ we have $\psi(x^2/w) \in \mathbb{R}_{\geq 0}$, so $\psi(w) \geq 0$. Since $w \in A^*_\mathbb{Q}$, for all $\psi \in \mathrm{Rhom}(A_\mathbb{Q}, \mathbb{C})$ we have $\psi(w) \neq 0$. Thus $w \in (A^+_\mathbb{Q})_{\gg 0}$, and L and $L_{(I,w)}$ are A-isomorphic. □

The following result will be used to prove Propositions 10.11 and 17.6.

Corollary 10.4. *If A is a CM-order, L is an invertible A-lattice, and $\mathfrak{a} \subset A$ is an ideal of finite index, then there exists $e_\mathfrak{a} \in L$ such that $(A/\mathfrak{a})e_\mathfrak{a} = L/\mathfrak{a}L$.*

Proof. This follows directly from Theorem 10.3 and Lemma 10.2(ii). □

In Algorithm 1.1 of [12] we obtained a deterministic polynomial-time algorithm that on input a finite commutative ring R and a finite R-module M, decides whether there exists $y \in M$ such that $M = Ry$, and if there is, finds such a y. Applying this with $R = A/\mathfrak{a}$ and $M = L/\mathfrak{a}L$, gives the algorithm in the following result, which is an analogue of Proposition 10.1 of [14].

Proposition 10.5. *There is a deterministic polynomial-time algorithm that, given a CM-order A, an A-lattice L, and an ideal $\mathfrak{a} \subset A$ of finite index, decides whether there exists $e_\mathfrak{a} \in L$ such that $(A/\mathfrak{a})e_\mathfrak{a} = L/\mathfrak{a}L$, and if there is, finds one.*

If L is an *invertible* A-lattice then $e_\mathfrak{a}$ exists by Corollary 10.4.

Recall the definition of vigilant in Definition 8.4.

Definition 10.6. Suppose A is a reduced order and $\mathfrak{a}$ is an ideal of A. Let

$$V(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Maxspec}(A) : \mathfrak{p} \supset \mathfrak{a}\}.$$

We say $\mathfrak{a}$ is *good* if $\#(A/\mathfrak{a}) < \infty$ and $V(\mathfrak{a})$ is vigilant.

In other words, $\mathfrak{a}$ is good if $\#(A/\mathfrak{a}) < \infty$ and for all $\mathbf{r} \in \mathrm{Minspec}(A)$ we have $\mathbf{r} + \mathfrak{a} \neq A$.

Lemma 10.7. *If A is a reduced order and $m \in \mathbb{Z}_{>1}$, then $V(mA)$ is vigilant and mA is good.*

Proof. Suppose $\mathbf{r} \in \mathrm{Minspec}(A)$. Then $A/\mathbf{r}$ is an order. Since $m > 1$ we have $m(A/\mathbf{r}) \neq A/\mathbf{r}$, so $\mathbf{r} + mA \neq A$. The desired result now follows. □

The following result is an analogue of Lemma 10.2 of [14].

Lemma 10.8. *Suppose A is a CM-order, L is an A-lattice, and $e \in L$.*

(i) *Suppose $m \in \mathbb{Z}_{>1}$. Then $(A/mA)e = L/mL$ if and only if $L/(Ae)$ is finite of order coprime to m.*

(ii) *Suppose* $\mathrm{rank}_\mathbb{Z}(L) = \mathrm{rank}_\mathbb{Z}(A)$ *and $L/(Ae)$ is finite. Then the map $A \to Ae$, $a \mapsto ae$ is an isomorphism of A-modules, i.e., e is regular.*

(iii) *Suppose $\mathfrak{a}$ is a good ideal of A and $(A/\mathfrak{a})e = L/\mathfrak{a}L$. Then $L/(Ae)$ is finite and $L_\mathbb{Q} = A_\mathbb{Q} \cdot e$.*

Proof. The proof of Lemma 10.2 of [14] with $\mathbb{Z}\langle G\rangle$ replaced by A shows (i) and (ii).

For (iii), we have $Ae + \mathfrak{a}L = L$, so $\mathfrak{a}(L/Ae) = L/Ae$. By Proposition 8.1 (Nakayama's Lemma) there exists $x \in 1 + \mathfrak{a} \subset A$ such that $x(L/Ae) = 0$. Since $\mathfrak{a}$ is good, for all $\mathbf{r} \in \mathrm{Minspec}(A)$ we have $\mathfrak{a} + \mathbf{r} \neq A$; thus $1 \notin \mathfrak{a} + \mathbf{r}$. Since $x \in 1 + \mathfrak{a}$, it follows that $x \notin \mathbf{r}$ for all $\mathbf{r} \in \mathrm{Minspec}(A)$, so $x \in A_{\mathbb{Q}}^*$. Since $x(L/Ae)_{\mathbb{Q}} = 0$ we have $(L/Ae)_{\mathbb{Q}} = 0$, so L/Ae is finite and $L_{\mathbb{Q}} = A_{\mathbb{Q}} \cdot e$. □

The following lemma will be used to prove Proposition 10.11. It serves as an analogue of Lemma 11.5 of [14].

Lemma 10.9. *Suppose A is a CM-order, L is an A-lattice, and $\mathrm{rank}_{\mathbb{Z}}(L) = \mathrm{rank}_{\mathbb{Z}}(A)$. Suppose $e_2 \in L$ satisfies $(A/2A)e_2 = L/2L$, and let $z = e_2\overline{e_2} \in A_{\mathbb{Q}}$ and $I = \{a \in A_{\mathbb{Q}} : ae_2 \in L\}$. Then:*

(i) *$L/(Ae_2)$ is finite, e_2 is regular, $L_{\mathbb{Q}} = A_{\mathbb{Q}}e_2$, and $L = Ie_2$;*

(ii) *$z \in A_{\mathbb{Q}}^* \cap (A_{\mathbb{Q}}^+)_{\gg 0}$;*

(iii) *if L is invertible as an A-lattice and $w = z^{-1}$, then $I\bar{I} = Aw$, the map $I \to L$, $a \mapsto ae_2$ induces an A-isomorphism from $L_{(I,w)}$ to L, and*

$$\varphi_L(x \otimes \bar{y}) = \sigma^{-1}(x)\overline{\sigma^{-1}(y)}z$$

for all $x, y \in L$, where $\sigma : I \xrightarrow{\sim} L$, $a \mapsto ae_2$.

Proof. In the notation of Proposition 4.1 we have $z = e_2\overline{e_2} = z_{e_2,e_2} = \varphi(e_2 \otimes \overline{e_2})$, and $\langle ae_2, ae_2\rangle = \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(a\bar{a}z)$ for all $a \in A$. By Proposition 4.1(ii)(c) we have $z \in (A_{\mathbb{Q}}^+)_{>0}$.

By Lemma 10.8 we have that $L/(Ae)$ is finite, e_2 is regular, the map $A_{\mathbb{Q}} \to L_{\mathbb{Q}}$, $a \mapsto ae_2$ is an isomorphism, and $L_{\mathbb{Q}} = A_{\mathbb{Q}}e_2$. By the definition of I, we now have $L = Ie_2$. This gives (i).

If $a \in A$ and $az = 0$, then $\langle ae_2, ae_2\rangle = \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(a\bar{a}z) = 0$, so $ae_2 = 0$, so $a = 0$. Thus multiplication by z is injective, and therefore surjective, on $A_{\mathbb{Q}}$. Thus $z \in A_{\mathbb{Q}}^*$. Since $z \in (A_{\mathbb{Q}}^+)_{>0}$ we now have $z \in (A_{\mathbb{Q}}^+)_{\gg 0}$, giving (ii).

Suppose L is invertible. Then $A = \varphi_L(L \otimes_A \overline{L}) = \varphi_L(Ie_2 \otimes_A \overline{Ie_2}) = I\bar{I}z$, and $\langle a, b\rangle_{L_{(I,w)}} = \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(a\bar{b}/w) = \mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(a\bar{b}z) = \langle ae_2, be_2\rangle_L$ for all $a, b \in A$.

If $x = ae_2$ and $y = be_2$ with $a, b \in I$, then $\varphi_L(x \otimes \bar{y}) = x\bar{y} = (ae_2)(\overline{be_2}) = a\bar{b}z$ as desired, giving (iii). □

Algorithm 10.10 and Proposition 10.11 below extend Algorithm 10.3 and Proposition 10.4 of [14].

Algorithm 10.10. Given a CM-order A and an A-lattice L, the algorithm decides whether L is invertible, and if so, outputs the map $\varphi : L \otimes_A \bar{L} \xrightarrow{\sim} A$ from Proposition 4.1.

Steps:

(i) Check whether $\mathrm{rank}_{\mathbb{Z}}(L) = \mathrm{rank}_{\mathbb{Z}}(A)$. If it does not, output "no" and stop.

(ii) Run the algorithm associated with Proposition 10.5 to decide if there exists $e_2 \in L$ such that $(A/2A)e_2 = L/2L$, and if so, to compute such an e_2. If not, output "no" and stop.

(iii) Use linear algebra over $\mathbb{Z}$ to compute a $\mathbb{Z}$-basis for $I = \{a \in A_{\mathbb{Q}} : ae_2 \in L\}$.

(iv) Solve for $z \in A_{\mathbb{Q}}$ in the system of linear equations

$$\mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(\alpha_i z) = \langle \alpha_i e_2, e_2\rangle$$

where $\{\alpha_i\}_{i=1}^n$ is the $\mathbb{Z}$-basis used for A.

(v) Output "no" and stop if $I\bar{I}z \neq A$, and otherwise output "yes" and the map

$$\varphi : L \otimes_A \bar{L} \to A, \quad x \otimes \bar{y} \mapsto \sigma^{-1}(x)\overline{\sigma^{-1}(y)}z$$

where $\sigma : I \xrightarrow{\sim} L$, $a \mapsto ae_2$.

Proposition 10.11. *Algorithm 10.10 is correct and runs in polynomial time.*

Proof. If L is invertible, then $\mathrm{rank}_{\mathbb{Z}}(L) = \mathrm{rank}_{\mathbb{Z}}(A)$ by Lemma 4.7, and there exists e_2 as in Step (ii) by Corollary 10.4.

The set I in Step (iii) is clearly a fractional A-ideal. Step (iv) computes $z \in A_{\mathbb{Q}}$ such that $\mathrm{Tr}_{A_{\mathbb{Q}}/\mathbb{Q}}(x\bar{y}z) = \langle xe_2, ye_2\rangle$ for all $x, y \in I$. It follows from Proposition 4.1(i) that there is a unique such z in $A_{\mathbb{Q}}$, and $z = z_{e_2,e_2} = \varphi(e_2 \otimes \overline{e_2}) = e_2\overline{e_2}$. By Step (i) and Lemma 10.9, the element e_2 is regular, the map $A_{\mathbb{Q}} \to L_{\mathbb{Q}}$, $a \mapsto ae_2$ is an isomorphism that takes I to L, and $z \in A_{\mathbb{Q}}^* \cap (A_{\mathbb{Q}}^+)_{\gg 0}$.

By Lemma 10.9, if L is invertible, then $I\bar{I}z = A$ and Step (v) produces the desired map φ. Conversely, if Step (v) determines that $I\bar{I}z = A$, then the A-lattice L is invertible by Theorem 10.3. □

Remark 10.12. To obtain an algorithm that, given a CM-order A and an *invertible* A-lattice L, outputs φ, one can simply run Steps (ii)–(v) of Algorithm 10.10 to compute the map φ, without performing the checks for invertibility. In the algorithms in this paper, for invertible A-lattices we generally assume (and suppress mention) that this has been done, if one needs to perform computations using φ.

11. Short vectors in invertible lattices

The following theorem generalizes Theorem 12.4 of [14].

Theorem 11.1. *Suppose A is a CM-order and L is an A-lattice. Then:*

(i) *if L is invertible, then the map*

$$F : \{A\text{-isomorphisms } A \xrightarrow{\sim} L\} \to \{\text{short vectors of } L\}, \quad f \mapsto f(1)$$

is bijective;

(ii) *if L is invertible and $e \in L$ is short, then e generates L as an A-module;*

(iii) *L is A-isomorphic to the standard A-lattice if and only if L is invertible and has a short vector;*

(iv) *if L is invertible and $e \in L$ is short, then the map*

$$\mu(A) \to \{\text{short vectors of } L\}, \qquad \zeta \mapsto \zeta e$$

is bijective.

Proof. Suppose L is invertible. First suppose $f : A \xrightarrow{\sim} L$ is an A-isomorphism. Since $1 \in A$ is short, it follows that $f(1) \in L$ is short. Thus, F is well-defined. Since $f(a) = f(a \cdot 1) = af(1)$, the map f is determined by $f(1)$. Thus, F is injective.

For surjectivity of F, let $x \in L$ be short and define $f : A \to L$ by $f(a) = ax$. Then f is A-linear, $f(1) = x$, and f is injective (since x is regular by Proposition 7.3). The map f preserves the lattice structure since for all $a, b \in A$ we have

$$\varphi_L(f(a) \otimes \overline{f(b)}) = \varphi_L(ax \otimes \bar{b}\bar{x}) = a\bar{b}\varphi_L(x \otimes \bar{x}) = a \cdot \bar{b} = \varphi_A(a \otimes \bar{b}).$$

To see that f is surjective, consider the exact sequences

$$A \otimes_A \bar{A} \xrightarrow{f \otimes \mathrm{id}} L \otimes_A \bar{A} \to (\operatorname{coker}(f)) \otimes_A \bar{A} \to 0$$

and

$$L \otimes_A \bar{A} \xrightarrow{\mathrm{id} \otimes \bar{f}} L \otimes_A \bar{L} \to L \otimes_A \overline{(\operatorname{coker}(f))} \to 0.$$

Since L is invertible,

$$(\mathrm{id} \otimes \bar{f}) \circ (f \otimes \mathrm{id}) = f \otimes \bar{f} = (\varphi_L)^{-1} \circ \varphi_A : A \otimes_A \bar{A} \to L \otimes_A \bar{L}$$

is an isomorphism, so $\mathrm{id} \otimes \bar{f}$ is onto. Thus $L \otimes_A \overline{(\operatorname{coker}(f))} = 0$, so

$$A \otimes_A \operatorname{coker}(f) = L \otimes_A \bar{L} \otimes_A \operatorname{coker}(f) = 0,$$

so $\operatorname{coker}(f) = 0$. This proves (i).

If L is invertible and $e \in L$ is short, then $L = Ae$ by (i), and this gives (ii).

For (iii), it suffices to assume that L is invertible, and in that case (iii) follows from (i).

For (iv), by (iii) we can (and do) reduce to the case where L is the standard A-lattice. By Proposition 7.4, the short vectors are exactly the roots of unity in A. Now (iv) follows easily. □

By Theorem 11.1(iii) and (iv), if L is an invertible A-lattice and X is the set of short vectors in L, then $X = \mu(A)e$ if L is A-isomorphic to the standard A-lattice and $e \in X$, and X is empty otherwise. Thus, X might be too large to even write down in polynomial time.

12. The Witt-Picard group

As in the introduction, we define $\mathrm{WPic}(A)$ to be the quotient of

$$\{(I, w) : I \text{ is an invertible fractional } A\text{-ideal}, \ w \in (A^+_{\mathbb{Q}})_{\gg 0}, \text{ and } I \cdot \bar{I} = Aw\}$$

by $\{(Av, v\bar{v}) : v \in A^*_{\mathbb{Q}}\}$. Just as for the class groups in algebraic number theory, $\mathrm{WPic}(A)$ is a finite abelian group (Theorem 12.2 below).

The following result is an analogue of Theorem 13.3, Proposition 13.4, and Corollary 14.3 of [14], and can be proved in a similar manner, but now also making use of Propositions 4.1 and 4.2.

Proposition 12.1. *Suppose A is a CM-order and L, M, and N are invertible A-lattices. Then:*

(i) *$L \otimes_A M$ is an invertible A-lattice with the map*

$$\varphi_{L \otimes_A M} : (L \otimes_A M) \otimes_A \overline{(L \otimes_A M)} \to A$$

of Proposition 4.1 given by

$$\varphi_{L \otimes_A M}((x_1 \otimes y_1) \otimes \overline{(x_2 \otimes y_2)}) = \varphi_L(x_1 \otimes \overline{x_2}) \cdot \varphi_M(y_1 \otimes \overline{y_2});$$

(ii) *$\overline{L}$ is an invertible A-lattice with the map $\varphi_{\overline{L}} : \overline{L} \otimes_A L \to A$ defined by*

$$\varphi_{\overline{L}}(\bar{x} \otimes y) = \varphi_L(y \otimes \bar{x}) = \overline{\varphi_L(x \otimes \bar{y})};$$

(iii) *we have the following canonical A-isomorphisms:*

$$L \otimes_A M \cong M \otimes_A L, \quad (L \otimes_A M) \otimes_A N \cong L \otimes_A (M \otimes_A N), \quad L \otimes_A A \cong L, \quad L \otimes_A \overline{L} \cong A;$$

(iv) *L and M are A-isomorphic if and only if $L \otimes_A \overline{M}$ and A are A-isomorphic.*

Note that $\overline{L \otimes_A M} = \overline{L} \otimes_A \overline{M}$ and (canonically)

$$L \otimes_A M \otimes_A \overline{L} \otimes_A \overline{M} \cong (L \otimes_A \overline{L}) \otimes_A (M \otimes_A \overline{M}) \cong A.$$

The following result is an analogue of Proposition 14.4 and Theorem 14.5 of [14].

Theorem 12.2. *The set of invertible A-lattices up to A-isomorphism is a finite abelian group and is isomorphic to* $\mathrm{WPic}(A)$. *Here, the group operation on (isomorphism classes of) invertible A-lattices is given by tensoring over A, the unit element is (A, φ_0) with $\varphi_0(x \otimes \bar{y}) = x\bar{y}$, and the inverse of (L, φ_L) is $(\overline{L}, \varphi_{\overline{L}})$.*

Proof. The proof is a direct generalization of the proofs of Proposition 14.4 and Theorem 14.5 of [14], with Proposition 5.5 serving in the role of Proposition 3.4 of [14]. □

Recall the group $\mathbf{Cl}^-(A)$ from the introduction.

Theorem 12.3. *Let $h : \mathrm{WPic}(A) \to \mathbf{Cl}^-(A)$ be the group homomorphism sending the class of (I, w) to the class of I. Then 2 annihilates the kernel and cokernel of h.*

Proof. If $[I] \in \mathbf{Cl}^-(A)$, then there exists $v \in A_{\mathbb{Q}}^*$ such that $I\bar{I} = Av$. Then $I\bar{I} = A\bar{v}$, so $I^2\bar{I}^2 = Av\bar{v}$. Since $v\bar{v} \in (A_{\mathbb{Q}}^+)_{\gg 0}$ we have $[(I^2, v\bar{v})] \in \mathrm{WPic}(A)$, and $h([(I^2, v\bar{v})]) = [I]^2$.

If $[(I, w)]$ is in the kernel of h, then there exists $v \in A_{\mathbb{Q}}^*$ such that $I = Av$. Since $I\bar{I} = Aw$, it follows that $\bar{I} = Aw/v$. Since $\bar{w} = w$ we have $I = Aw/\bar{v}$. Thus, $I^2 = Au$ where $u = wv/\bar{v} \in A_{\mathbb{Q}}^*$. We now have $(I^2, w^2) = (Au, u\bar{u})$. □

The following proposition summarizes the algorithmic results for $\mathrm{WPic}(A)$ that are proved in the present paper.

Proposition 12.4. *There are deterministic polynomial-time algorithms for finding the unit element, inverting, multiplying, exponentiation, and equality testing in* $\mathrm{WPic}(A)$.

Algorithms for the unit element and inverting follow easily from Theorem 12.2. Multiplication and exponentiation are dealt with in the next section. See Theorem 1.6 for equality testing.

13. Multiplying and exponentiating invertible A-lattices

This section generalizes Section 15 of [14]. All A-lattices in the inputs and outputs of the algorithms are specified via an LLL-reduced basis. Direct generalizations of Algorithms 15.1, 15.2, and 15.3 of [14] give the following (relying on Lemma 10.9 above wherever [14] relied on Lemma 11.5 of [14]).

Theorem 13.1.
(i) *There is a deterministic polynomial-time algorithm that, given a CM-order A of rank n and invertible A-lattices L and M, outputs $L \otimes_A M$ and an $n \times n \times n$ array of integers to describe the multiplication map $L \times M \to L \otimes_A M$.*
(ii) *There is a deterministic polynomial-time algorithm that, given a CM-order A, an ideal $\mathfrak{a}$ of A of finite index, invertible A-lattices L and M, and elements $d \in L/\mathfrak{a}L$ and $f \in M/\mathfrak{a}M$, computes $L \otimes_A M$ and the element $d \otimes f \in (L \otimes M)/\mathfrak{a}(L \otimes M)$.*

(iii) *There is a deterministic polynomial-time algorithm that, given a CM-order A, a positive integer r, an invertible A-lattice L, an ideal $\mathfrak{a}$ of A of finite index, and $d \in L/\mathfrak{a}L$, outputs $L^{\otimes r}$ and $d^{\otimes r} \in L^{\otimes r}/\mathfrak{a}L^{\otimes r}$.*

14. The extended tensor algebra Λ

We next define the extended tensor algebra Λ, which is a single algebraic structure that comprises all rings and lattices that our main algorithm needs. Suppose A is a CM-order and L is an invertible A-lattice. Let $L^{\otimes 0} = A$, and for all $m \in \mathbb{Z}_{>0}$ let

$$L^{\otimes m} = L \otimes_A \cdots \otimes_A L \quad (\text{with } m\ L\text{'s}),$$

and

$$L^{\otimes(-m)} = \overline{L}^{\otimes m} = \overline{L} \otimes_A \cdots \otimes_A \overline{L}.$$

For simplicity, we denote $L^{\otimes m}$ by L^m. If $m \in \mathbb{Z}$, then L^m is an invertible A-lattice by Proposition 12.1, and $\overline{L^m} = \overline{L}^m = L^{-m}$.

Let

$$\Lambda = T_A(L) = \bigoplus_{i\in\mathbb{Z}} L^i,$$

an A-algebra with involution $^-$. The following result is analogous to Proposition 16.1 of [14], and its proof is straightforward.

Proposition 14.1. *Suppose A is a CM-order and L is an invertible A-lattice. Then:*

(i) *the extended tensor algebra Λ is a commutative ring containing A as a subring;*
(ii) *for all $j \in \mathbb{Z}$, the action of A on L^j becomes multiplication in Λ;*
(iii) *Λ has an involution $x \mapsto \overline{x}$ extending both the involution of A and the map $L \xrightarrow{\sim} \overline{L}$;*
(iv) *if $j \in \mathbb{Z}$, then the map $L^j \times \overline{L^j} \to L^j \otimes_A \overline{L^j} \xrightarrow{\sim} A$ induced by the isomorphism φ_{L^j} becomes multiplication in Λ, with $\overline{L^j} = L^{-j}$;*
(v) *if $j \in \mathbb{Z}$ and $e \in L^j$ is short, then $\overline{e} = e^{-1}$ in L^{-j};*
(vi) *if $e \in L$ is short, then $\Lambda = A[e, e^{-1}]$, where the right side is the subring of Λ generated by A, e, and e^{-1}, which is a Laurent polynomial ring.*

In [16] we show the following result, which we will use in Proposition 14.3 below. (In [16], the group Γ was written multiplicatively.)

Proposition 14.2 ([16], Theorem 1.5(ii,iii))**.** *Suppose $B = \bigoplus_{\gamma\in\Gamma} B_\gamma$ is an order that is graded by an additively written finite abelian group Γ (i.e., the additive subgroups B_γ of B satisfy $B_\gamma \cdot B_{\gamma'} \subset B_{\gamma+\gamma'}$ for all $\gamma, \gamma' \in \Gamma$, and the additive group homomorphism $\bigoplus_{\gamma\in\Gamma} B_\gamma \to B$ sending $(x_\gamma)_{\gamma\in\Gamma}$ to $\sum_{\gamma\in\Gamma} x_\gamma$ is bijective). Suppose B_0 is connected. Then B is connected and $\mu(B) \subset \bigcup_{\gamma\in\Gamma} B_\gamma$.*

The following result is analogous to Proposition 16.2 of [14], and will be used in Proposition 14.6.

Proposition 14.3. *Suppose A is a CM-order, L is an invertible A-lattice, $r \in \mathbb{Z}_{>0}$, $y \in L^r$, and $y\overline{y} = 1$. Let $\Lambda = T_A(L)$ and $B = \Lambda/(y-1)\Lambda$. Then:*

(i) *the map $\bigoplus_{i=0}^{r-1} L^i \to B$ induced by the natural map $\bigoplus_{i=0}^{r-1} L^i \subset \Lambda \to B$ is an A-module isomorphism that exhibits the commutative ring B as a $\mathbb{Z}/r\mathbb{Z}$-graded order;*

(ii) *B is a CM-order, with involution $^-$ on B induced by the involution $^-$ on Λ;*

(iii) *$\mu(B) = \{\beta \in B : \beta\bar{\beta} = 1\}$;*

(iv) *if A is connected, then B is connected and $\mu(B) \subset \bigcup_{i=0}^{r-1} L^i$ (identifying B with $\bigoplus_{i=0}^{r-1} L^i$ as in* (i)*).*

Proof. Part (i) is a straightforward exercise.

Each L^i has an A-lattice structure $\langle x, y\rangle = \mathrm{Tr}_{A/\mathbb{Z}}(x\overline{y})$, where $x\overline{y} = \varphi_{L^i}(x \otimes \bar{y})$. If $\beta = (\beta_0, \ldots, \beta_{r-1}) \in \bigoplus_{i=0}^{r-1} L^i = B$, then $\overline{\beta_i} \in L^{-i}$ and $y\overline{\beta_i} \in L^{r-i}$, but $\overline{\beta_i} = y\overline{\beta_i}$ in B, so

$$\bar{\beta} = (\overline{\beta_0}, \overline{\beta_{r-1}}, \ldots, \overline{\beta_1}) = (\overline{\beta_0}, y\overline{\beta_{r-1}}, \ldots, y\overline{\beta_1}) \in \bigoplus_{i=0}^{r-1} L^i = B.$$

By Proposition 2.5 applied to $E = B_{\mathbb{Q}}$ and Remark 3.5, to prove (ii) it suffices to prove that for all β we have $\mathrm{Tr}_{B/\mathbb{Z}}(\beta\bar{\beta}) = r \cdot \sum_{i=0}^{r-1}\langle \beta_i, \beta_i\rangle$. If $a \in A = L^0$, then

$$\mathrm{Tr}_{B/\mathbb{Z}}(a) = \sum_{i=0}^{r-1} \text{trace(action of } a \text{ on } L^i) = r \cdot \mathrm{Tr}_{A/\mathbb{Z}}(a).$$

If $c \in L^i$ with $0 < i < r$, then $\mathrm{Tr}_{B/\mathbb{Z}}(c) = 0$. Thus, $\mathrm{Tr}_{B/\mathbb{Z}}(\beta) = r \cdot \mathrm{Tr}_{A/\mathbb{Z}}(\beta_0)$. If $\beta\bar{\beta} = (\alpha_i)_{i=0}^{r-1}$, then $\alpha_0 = \sum_{i=0}^{r-1} \beta_i\overline{\beta_i}$. Thus,

$$\mathrm{Tr}_{B/\mathbb{Z}}(\beta\bar{\beta}) = r\cdot\mathrm{Tr}_{A/\mathbb{Z}}(\alpha_0) = r\cdot\mathrm{Tr}_{A/\mathbb{Z}}(\sum_{i=0}^{r-1}\beta_i\overline{\beta_i}) = r\cdot\sum_{i=0}^{r-1}\mathrm{Tr}_{A/\mathbb{Z}}(\beta_i\overline{\beta_i}) = r\cdot\sum_{i=0}^{r-1}\langle\beta_i, \beta_i\rangle.$$

This proves (ii). Part (iii) follows from Proposition 7.4 and (ii). Part (iv) follows from Proposition 14.2 with $\Gamma = \mathbb{Z}/r\mathbb{Z}$, where $B_0 = L^0 = A$. □

The algorithm associated to the following result is Algorithm 13.2 of [13].

Proposition 14.4 ([13], Theorem 1.2)**.** *There is a deterministic polynomial-time algorithm that, given an order B, produces a set S of generators for the group $\mu(B)$ of roots of unity in B^*, as well as a set of defining relations for S.*

The following algorithm will be applied repeatedly in Algorithm 18.1. It generalizes Algorithms 17.4 and 19.1(vii)–(ix) of [14].

Algorithm 14.5. Given a connected CM-order A of rank n, an invertible A-lattice L, a positive integer r, an element $\epsilon \in L/2^{n+1}L$ such that $(A/2^{n+1}A)\epsilon = L/2^{n+1}L$, and an element $s \in A/2^{n+1}A$ such that the coset $s\epsilon^r \in L^r/2^{n+1}L^r$ contains a (unique) short vector, the algorithm decides whether L has a short vector, and if so, determines an element $t \in A/2^{n+1}A$ such that the coset $t\epsilon$ contains a (unique) short vector.

Steps:

(i) Pick an element e in the coset ϵ and let $q = (L : Ae)$. Apply the algorithm associated to Proposition 10.5 to find $e_q \in L$ such that $Ae_q + qL = L$. Let $I = \{a \in A_{\mathbb{Q}} : ae \in L\}$ and $w = (e\bar{e})^{-1} \in A_{\mathbb{Q}}^*$, compute w^r, compute $\beta = e_q/e \in A_{\mathbb{Q}} \subset \Lambda_{\mathbb{Q}}$, and for $0 \le i \le r$ compute $I^i = A + A\beta^i$.

(ii) Apply Algorithm 6.2 with $\mathfrak{a} = 2^{n+1}A$ and $L = L_{(I^r,w^r)}$ and $C = s + 2^{n+1}L_{(I^r,w^r)}$ to compute the unique short vector $\nu \in C$.

(iii) Construct the order $B = \bigoplus_{i=0}^{r-1} I^i$ with multiplication

$$I^i \times I^j \to I^{i+j}, \quad (x, y) \mapsto xy \quad \text{if } i + j < r$$

and

$$I^i \times I^j \to I^{i+j-r}, \quad (x, y) \mapsto xy/\nu \quad \text{if } i + j \geq r.$$

(iv) Apply the algorithm from Proposition 14.4 to compute a set of generators $\{\zeta_1, \ldots, \zeta_m\}$ for $\mu(B)$.

(v) Applying the degree map $\deg : \mu(B) \to \mathbb{Z}/r\mathbb{Z}$ that takes $\zeta \in \mu(B)$ to $j \in \mathbb{Z}$ such that $\zeta \in I^j$, either find integers s_i such that $\sum_{i=1}^{m} s_i \deg(\zeta_i) = 1$, or if no such integers exist output "no" and stop. Letting $\alpha = \prod_{i=1}^{m} \zeta_i^{s_i} \in \mu(B)$, use linear algebra over $\mathbb{Z}$ to compute $t \in A/2^{n+1}A$ that maps to α mod $2^{n+1}I$ under the isomorphism $A/2^{n+1}A \xrightarrow{\sim} I/2^{n+1}I$ induced by $a \mapsto a$, and output "yes" and t.

Proposition 14.6. *Algorithm 14.5 is correct and runs in time at most polynomial in r plus the length of the input.*

Proof. By Lemma 10.8(i) with $m = 2^{n+1}$ we have that $q < \infty$. Then e_q exists by Corollary 10.4. By Lemma 10.9 we have that $w \in A^*_{\mathbb{Q}}$ and that the map $I \to L$, $a \mapsto ae$ induces an A-isomorphism from $L_{(I,w)}$ to L. That $I^i = A + A\beta^i$ follows exactly as in the proof of Proposition 19.2 of [14], with A in place of $\mathbb{Z}\langle G\rangle$ and making use of Lemma 10.8(i).

The short vector ν in Step (ii) is unique by Proposition 6.3, and $\nu e^r \in L^r$ is the unique short vector in the coset $s\epsilon^r$.

By Proposition 14.3(iv), the degree map in Step (v) makes sense. Since $\deg(\alpha) = 1$ we have $\alpha \in I$. Since $Ae + 2^{n+1}L = L$, we have $A + 2^{n+1}I = I$, and it follows that the map $A/2^{n+1}A \to I/2^{n+1}I$ induced by $a \mapsto a$ is an isomorphism. By Proposition 14.3(iii), the vector $z = \alpha e \in L$ satisfies $z\bar{z} = 1$, and is the unique short vector in the coset $t\epsilon$ by Proposition 6.3.

Computing w^r and β^i in Step (i), and all computations involving B, entail the r entering the runtime. □

15. Some elementary number theory

Definition 15.1. Let $c(n) = n^2$ for $n \geq 2$, let $b(n) = 4(\log n)^2$ for $n \geq 3$, and let $c(1) = b(1) = 2$ and $b(2) = 3$.

Note that $b(n) \leq c(n)$, and c and b are each monotonically increasing. Let

$$\psi(x, y) = \#\{m \in \mathbb{Z} : 0 < m \leq x, \text{ each prime } p|m \text{ satisfies } p \leq y\}.$$

Theorem 15.2 (Konyagin-Pomerance, Theorem 2.1 of [6])**.** *If $x \geq 4$ and $2 \leq y \leq x$, then $\psi(x, y) > x^{1-\mathrm{loglog}x/\mathrm{log}y}$.*

Corollary 15.3. *For all $n \in \mathbb{Z}_{>0}$ we have*

$$\psi(c(n), b(n)) > n.$$

Proof. For $n > 2$ this follows by setting $x = n^2$ and $y = 4(\log n)^2$ in Theorem 15.2. For $n = 1$ and 2 this can be checked by hand. □

Proposition 15.4. *For each $n \in \mathbb{Z}_{>0}$, each prime divisor of*

$$\gcd\{h^n - 1 : h \in \mathbb{Z}_{>0}, \quad h \leq b(n)\}$$

is less than $c(n)$.

Proof. Suppose ℓ is a prime divisor of $\gcd\{h^n - 1 : h \in \mathbb{Z}, h \leq b(n)\}$. Then $h^n \equiv 1 \bmod \ell$ for all integers $h \leq b(n)$. Let S denote the set of $m \in \mathbb{Z}_{>0}$ with $m \leq c(n)$ such that all prime divisors p of m satisfy $p \leq b(n)$. Then $\#S = \psi(c(n), b(n)) > n$ by Corollary 15.3, and for all $a \in S$ we have $a^n \equiv 1 \bmod \ell$. So if all elements of S are pairwise incongruent mod ℓ, then $\#\{x \in \mathbb{F}_\ell : x^n = 1\} \geq \#S > n$, which cannot be. So there exist $s, t \in S$ with $s \neq t$ and $s \equiv t \bmod \ell$. Thus, ℓ divides $|s - t|$, and $|s - t| \leq c(n) - 1$. □

Corollary 15.5. *Suppose $n \in \mathbb{Z}_{>0}$ and ℓ is a prime number such that $\ell > c(n)$. Then there exists a prime number $p \leq b(n)$ such that $p^n \not\equiv 1 \bmod \ell$.*

Proof. By Proposition 15.4, there exists a positive integer $h \leq b(n)$ such that $h^n \not\equiv 1 \bmod \ell$. Then h has a prime divisor $p \leq b(n)$ such that $p^n \not\equiv 1 \bmod \ell$. □

The next result replaces our use of Linnik's theorem in [11, 14], and allows us to prove upper bounds for the runtime that are much better than those proved in [4, 11, 14, 5]. We use it to prove Proposition 16.4.

Proposition 15.6. *Suppose A is an order and $n = \mathrm{rank}_{\mathbb{Z}}(A) \in \mathbb{Z}_{>0}$. Then for each prime number $\ell > c(n)$ there is a maximal ideal $\mathfrak{p}$ of A such that $\mathrm{N}(\mathfrak{p}) \not\equiv 1 \bmod \ell$ and $\mathrm{char}(A/\mathfrak{p}) \leq b(n)$.*

Proof. By Corollary 15.5, there exists a prime number $p \leq b(n)$ such that $p^n \not\equiv 1 \bmod \ell$. Take a sequence of ideals

$$\mathfrak{a}_0 = A \supsetneq \mathfrak{a}_1 \supsetneq \mathfrak{a}_2 \cdots \supsetneq \mathfrak{a}_m = pA$$

such that each $\mathfrak{a}_{i-1}/\mathfrak{a}_i$ is a simple A-module. Then $\mathfrak{a}_{i-1}/\mathfrak{a}_i \cong A/\mathfrak{p}_i$ as A-modules, for some maximal ideal $\mathfrak{p}_i$ of A with $\mathrm{char}(A/\mathfrak{p}_i) = p$. Now,

$$\prod_{i=1}^{m} \mathrm{N}(\mathfrak{p}_i) = \prod_{i=1}^{m} \#(A/\mathfrak{p}_i) = \prod_{i=1}^{m} \#(\mathfrak{a}_{i-1}/\mathfrak{a}_i) = \#(A/pA) = p^n \not\equiv 1 \bmod \ell.$$

Thus $\mathrm{N}(\mathfrak{p}_i) \not\equiv 1 \bmod \ell$ for some i. □

We now give a heuristic argument that $b(n)$ can be replaced with 5 in Corollary 15.5. If ℓ is a prime let $G_\ell = \langle 2, 3, 5 \bmod \ell \rangle \subset (\mathbb{Z}/\ell\mathbb{Z})^\times$, and if $m \in \mathbb{Z}_{>0}$ let

$$T_m = \{\text{primes } \ell : \ell > m^2, \ \ell > 5, \text{ and } m = \#G_\ell\}.$$

If $b(n)$ cannot be replaced with 5 in Corollary 15.5, then there exists $n \in \mathbb{Z}_{>0}$ and a prime number $\ell > c(n) \geq n^2$ such that $p^n \equiv 1 \bmod \ell$ for all $p \in \{2, 3, 5\}$; if g is a generator of the cyclic group G_ℓ, then $g^n \equiv 1 \bmod \ell$, so if $m = \#G_\ell$ then m divides n and it follows that $\ell \in T_m$. Thus it would suffice to show that T_m is empty for all $m \in \mathbb{Z}_{>0}$. Let $T_{m,x} = \{\ell \in T_m : \ell > x\}$. If $\ell \in T_{m,x}$ then we can write $\ell = km + 1$ with $k \in \mathbb{Z}$ and $k \geq m$ (since $\ell > m^2$) and $k \geq x/m$ (since $\ell > x$). Heuristically, a given pair (k, m) gives an $\ell \in T_m$ with "probability" at most c/k^3 with an absolute positive constant c, since the probability that ℓ is prime is at most 1 and the probability that $2^m \equiv 3^m \equiv 5^m \equiv 1 \bmod \ell$ once ℓ is prime might naively be estimated as $1/k^3$, with the constant c accounting for effects coming from quadratic reciprocity. So one "expects" the set $\bigcup_{m \geq 1} T_{m,x}$ to have size at most

$$c\sum_{m\geq 1}\left(\sum_{k\geq \max\{m,x/m\}}\frac{1}{k^3}\right)\leq c'\sum_{m\geq 1}\frac{1}{\max\{m,x/m\}^2}=$$
$$c'\left(\sum_{m\leq\sqrt{x}}\frac{m^2}{x^2}+\sum_{m>\sqrt{x}}\frac{1}{m^2}\right)\leq c''\left(\frac{\sqrt{x}^3}{x^2}+\frac{1}{\sqrt{x}}\right)=\frac{2c''}{\sqrt{x}},$$

which is less than 1 for all sufficiently large x. For all primes ℓ from 7 to 100 million, we easily check that $\ell < m^2 = (\#G_\ell)^2$ (in fact, $\ell < (\#\langle 2, 3 \bmod \ell\rangle)^{1.85}$), so $\ell \notin T_m$. Similarly, $b(n)$ can be replaced with 5, heuristically, in Proposition 15.6 and Theorem 1.7. However, if one deletes the 5 in the definition of G_ℓ, then conjecturally infinitely many T_m are non-empty, by essentially the above argument, but not a single such m is known.

16. Finding auxiliary ideals

Corollary 2.8 of [17] gives a polynomial-time algorithm that on input a prime p and a finite dimensional commutative $\mathbb{F}_p$-algebra (specified by structure constants), computes its nilradical. Corollary 3.2 of [17] gives an algorithm that on input a prime p and a finite dimensional semisimple commutative $\mathbb{F}_p$-algebra R, computes its minimal ideals in time at most polynomial in p plus $\dim_{\mathbb{F}_p}(R)$. Combining these gives the following result.

Theorem 16.1 ([17]). *There is an algorithm that on input a prime p and a finite dimensional commutative $\mathbb{F}_p$-algebra R, computes the prime ideals of R in time at most polynomial in p plus the length of the input.*

Recall the definition of vigilant from Definition 8.4 and the functions b and c from Definition 15.1.

Definition 16.2. Suppose A is a reduced order of rank $n > 0$. We will call a set $\mathfrak{S}$ *usable* for A if $\mathfrak{S}$ consists of vigilant sets S for A such that:

(i) $\mathrm{char}(A/\mathfrak{p}) \leq b(n)$ for all $S \in \mathfrak{S}$ and all $\mathfrak{p} \in S$,
(ii) for each prime number $\ell > c(n)$ there exists $S \in \mathfrak{S}$ such that for all $\mathfrak{p} \in S$ we have $\mathrm{N}(\mathfrak{p}) \not\equiv 1 \bmod \ell$, and
(iii) the set
$$S_0 = \{\mathfrak{p} \in \mathrm{Maxspec}(A) : 2 \in \mathfrak{p}\}$$
belongs to $\mathfrak{S}$.

If $\mathbf{r} \in \mathrm{Minspec}(A)$, let $d_{\mathbf{r}} = \mathrm{rank}_{\mathbb{Z}}(A/\mathbf{r})$.

The next algorithm will be used in Algorithm 17.3.

Algorithm 16.3. Given a reduced order A of rank $n > 0$, the algorithm outputs a finite set $\mathfrak{S}$ that is usable for A.

Steps:

(i) Apply Algorithm 7.2 of [15] to find $\mathrm{Minspec}(A) = \mathrm{Spec}(A_{\mathbb{Q}})$.
(ii) Find $\beta \in \mathbb{Z}$ such that $|\beta - \max_{\mathbf{r}\in\mathrm{Minspec}(A)} b(d_{\mathbf{r}})| < 1$.
(iii) For each prime number $p \leq \beta$ apply the algorithm associated with Theorem 16.1 to find all prime ideals of the finite commutative $\mathbb{F}_p$-algebra A/pA, i.e., find the set $\mathfrak{M}$ of all $\mathfrak{p} \in \mathrm{Maxspec}(A)$ such that $\mathrm{char}(A/\mathfrak{p}) \leq \beta$. For each $\mathfrak{p} \in \mathfrak{M}$, mark which $\mathbf{r} \in \mathrm{Minspec}(A)$ satisfy $\mathbf{r} \subset \mathfrak{p}$.

(iv) With input the finite set

$$\tilde{S} = \{\text{primes } \ell \le c(n)\} \cup \{\mathrm{N}(\mathfrak{p}) - 1 : \mathfrak{p} \in \mathfrak{M}\} \subset \mathbb{Z}_{>0},$$

apply the Coprime Base Algorithm from [2] to obtain a finite set $T \subset \mathbb{Z}_{>1}$ and a map $e : \tilde{S} \times T \to \mathbb{Z}_{\ge 0}$ such that

(a) for all $t, t' \in T$ with $t \neq t'$ we have $\gcd(t, t') = 1$, and

(b) for all $s \in \tilde{S}$ we have $s = \prod_{t \in T} t^{e(s,t)}$.

(v) Define a set T' of integers coprime to all primes $\ell \le c(n)$ by

$$T = T' \amalg \{\text{primes } \ell \le c(n)\}.$$

For all $\mathfrak{p} \in \mathfrak{M}$ and $t \in T$, define $h_{\mathfrak{p}}(t) = e(\mathrm{N}(\mathfrak{p}) - 1, t) \in \mathbb{Z}_{\ge 0}$, i.e.,

$$\mathrm{N}(\mathfrak{p}) - 1 = \prod_{t \in T} t^{h_{\mathfrak{p}}(t)}.$$

With S_0 as in Definition 16.2(iii), define

$$T'' = \{t \in T' : \max\{h_{\mathfrak{p}}(t) : \mathfrak{p} \in S_0\} > 0\}.$$

If T'' is empty, output $\mathfrak{S} = \{S_0\}$ and stop. Otherwise, proceed as follows.

(vi) For each $t \in T''$ and each $\mathbf{r} \in \mathrm{Minspec}(A)$, find $\mathfrak{p}_{t,\mathbf{r}} \in \mathfrak{M}$ from Step (i) such that $h_{\mathfrak{p}_{t,\mathbf{r}}}(t) = 0$ and $\mathbf{r} \subset \mathfrak{p}_{t,\mathbf{r}}$. Let

$$S_t = \{\mathfrak{p}_{t,\mathbf{r}} : \mathbf{r} \in \mathrm{Minspec}(A)\} \subset \mathfrak{M}$$

and output

$$\mathfrak{S} = \{S_0\} \cup \{S_t : t \in T''\}.$$

Proposition 16.4. *Algorithm 16.3 is correct and runs in polynomial time.*

Proof. That Step (vi) can find, for each $t \in T''$ and each $\mathbf{r} \in \mathrm{Minspec}(A)$, a maximal ideal $\mathfrak{p}_{t,\mathbf{r}}$ in A such that $h_{\mathfrak{p}_{t,\mathbf{r}}}(t) = 0$ and $\mathbf{r} \subset \mathfrak{p}_{t,\mathbf{r}}$ can be seen as follows. Since $t \in T'' \subset T$ we have $t > 1$. Suppose ℓ is a prime divisor of t. Since $t \in T'$, we have $\ell > c(n) \ge c(d_{\mathbf{r}})$ so by Proposition 15.6 applied with $A/\mathbf{r}$ in place of A there is a maximal ideal $\mathfrak{p}_{t,\mathbf{r}}$ of A that contains $\mathbf{r}$ such that $\mathrm{char}(A/\mathfrak{p}_{t,\mathbf{r}}) \le b(d_{\mathbf{r}})$ and $\mathrm{N}(\mathfrak{p}_{t,\mathbf{r}}) \not\equiv 1 \bmod \ell$. Thus $\mathrm{N}(\mathfrak{p}_{t,\mathbf{r}}) \not\equiv 1 \bmod t$, so $h_{\mathfrak{p}_{t,\mathbf{r}}}(t) = 0$.

The sets S_t for $t \in T''$ were constructed to be vigilant. The set S_0 is vigilant by Lemma 10.7 with $m = 2$.

To see that $\mathfrak{S}$ is usable, first note that if $S \in \mathfrak{S}$ and $\mathfrak{p} \in S$ then $\mathrm{char}(A/\mathfrak{p}) \le \beta \le b(n)$. Let ℓ be a prime number $> c(n)$. We will show that there exists $S \in \mathfrak{S}$ such that for all $\mathfrak{p} \in S$ we have $\mathrm{N}(\mathfrak{p}) \not\equiv 1 \bmod \ell$. If ℓ divides some $t \in T''$, then take $S = S_t$. If ℓ does not divide any element of T'', take $S = S_0$.

Step (i) runs in polynomial time by Theorem 1.10 of [15].

The primes p in Step (iii) are so small in size and number that the appeals to Theorem 16.1 run in time at most polynomial in the length of the input specifying A.

Step (iv) runs in polynomial time since the Coprime Base Algorithm in [2] does. Steps (v) and (vi) run in polynomial time since T'' is a subset of T, which was computed via a polynomial-time algorithm. □

17. Using the auxiliary ideals

Recall the definition of S_0 in Definition 16.2(iii).

Definition 17.1. Suppose A is an order of rank $n > 0$. If $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathrm{Maxspec}(A)} \mathfrak{p}^{t_\mathfrak{a}(\mathfrak{p})}$ is an ideal in A with $t_\mathfrak{a}(\mathfrak{p}) \in \mathbb{Z}_{\geq 0}$, and $\mathfrak{a} \neq 2^{n+1}A$, let

$$k(\mathfrak{a}) = \mathrm{lcm}_\mathfrak{p}\{(\mathrm{N}(\mathfrak{p}) - 1)p_\mathfrak{p}^{t_\mathfrak{a}(\mathfrak{p})-1}\}$$

where $p_\mathfrak{p} = \mathrm{char}(A/\mathfrak{p})$ denotes the prime number in $\mathfrak{p}$, and $\mathrm{N}(\mathfrak{p}) = \#(A/\mathfrak{p})$, and the lcm is over the maximal ideals $\mathfrak{p}$ with $t_\mathfrak{a}(\mathfrak{p}) \in \mathbb{Z}_{>0}$. Let

$$k(2^{n+1}A) = \frac{2^{2n}\mathrm{lcm}_{\mathfrak{p} \in S_0}\{\mathrm{N}(\mathfrak{p}) - 1\}}{\prod_{\mathfrak{p} \in S_0} \mathrm{N}(\mathfrak{p})}.$$

The number $k(\mathfrak{a})$ is the analogue of the number $k(m)$ that was defined in Notation 18.1 of [14] for positive integers m.

Lemma 17.2. *Let A be an order of rank $n > 0$. The exponent of $(A/2^{n+1}A)^*$ divides $k(2^{n+1}A)$ and is less than 2^{2n}. If $\mathfrak{a} = \prod_{\mathfrak{p} \in \mathrm{Maxspec}(A)} \mathfrak{p}^{t_\mathfrak{a}(\mathfrak{p})}$ is an ideal in A with $t_\mathfrak{a}(\mathfrak{p}) \in \mathbb{Z}_{\geq 0}$, then the exponent of the group $(A/\mathfrak{a})^*$ divides $k(\mathfrak{a})$.*

Proof. Let $G = (A/2^{n+1}A)^*$, let $\mathfrak{c} = \bigcap_{\mathfrak{p} \in S_0} \mathfrak{p}$, let U_0 be the kernel of the natural map $G \to (A/\mathfrak{c})^*$, and for $i \in \{1, \ldots, n+1\}$ let U_i be the kernel of the natural map $G \to (A/2^iA)^*$. We have $G \supset U_0 \supset U_1 \supset \cdots \supset U_{n+1} = 1$. Further,

$$G/U_0 \cong (A/\mathfrak{c})^* \cong \prod_{\mathfrak{p} \in S_0} (A/\mathfrak{p})^*,$$

which has exponent $\mathrm{lcm}_{\mathfrak{p} \in S_0}\{\mathrm{N}(\mathfrak{p}) - 1\}$. Since $U_0/U_1 \cong 1 + \mathfrak{c}/2A$, we have

$$\#(U_0/U_1) = \#(\mathfrak{c}/2A) = \frac{2^n}{\prod_{\mathfrak{p} \in S_0} \mathrm{N}(\mathfrak{p})}.$$

For $1 \leq i \leq n$, the group U_i/U_{i+1} has exponent 2. Thus the exponent of G divides $k(2^{n+1}A)$. Since $G/U_1 \cong (A/2A)^*$, the exponent of G is less than $2^n\#(A/2A) = 2^{2n}$.

For the final result, suppose $\mathfrak{p} \in \mathrm{Maxspec}(A)$ and $t = t_\mathfrak{a}(\mathfrak{p}) > 0$. Now let $U_0 = (A/\mathfrak{p}^t)^*$ and for $i \in \{1, \ldots, t\}$ let U_i be the kernel of the natural map $(A/\mathfrak{p}^t)^* \to (A/\mathfrak{p}^i)^*$. Then $U_0 \supset U_1 \supset \cdots \supset U_t = 1$, so the exponent of U_0 divides the product of the exponents of the groups U_{i-1}/U_i for $i = 1, \ldots, t$. The exponent of U_0/U_1 is $\#((A/\mathfrak{p})^*) = \mathrm{N}(\mathfrak{p}) - 1$. For $i > 1$ the exponent of U_{i-1}/U_i is $p_\mathfrak{p}$. Thus the exponent of $(A/\mathfrak{p}^t)^*$ divides $(\mathrm{N}(\mathfrak{p}) - 1)p_\mathfrak{p}^{t-1}$.

Applying the Chinese Remainder Theorem to the coprime ideals $\mathfrak{p}^{t_\mathfrak{a}(\mathfrak{p})}$ for which $t_\mathfrak{a}(\mathfrak{p}) > 0$, we have a ring isomorphism $A/\mathfrak{a} \xrightarrow{\sim} \prod_{\mathfrak{p}|\mathfrak{a}} A/\mathfrak{p}^{t_\mathfrak{a}(\mathfrak{p})}$. It follows that the exponent of $(A/\mathfrak{a})^*$ divides the lcm of the exponents of the groups $(A/\mathfrak{p}^{t_\mathfrak{a}(\mathfrak{p})})^*$, which combined with the previous paragraph proves the last result. □

Recall the definitions of "good" from Definition 10.6 and of $c(n)$ from Definition 15.1. The next algorithm will be invoked in Algorithm 17.5.

Algorithm 17.3. Given a connected CM-order A of rank n, the algorithm outputs:

- a finite set U of good ideals $\mathfrak{a}$ of A such that $2^{n+1}A \in U$,
- $k(\mathfrak{a})$ for each $\mathfrak{a} \in U$,
- $k = \mathrm{gcd}_{\mathfrak{a} \in U}\{k(\mathfrak{a})\}$,

- an integer $f(\mathfrak{a})$ for each $\mathfrak{a} \in U$

such that:

(a) for all $\mathfrak{a} \in U$, all invertible A-lattices L and all $\beta \in (\mathfrak{a}L) \smallsetminus \{0\}$ we have $\langle \beta, \beta \rangle \geq (2^{n/2}+1)^2 \cdot n$,
(b) $k = \sum_{\mathfrak{a} \in U} f(\mathfrak{a}) k(\mathfrak{a})$,
(c) every prime divisor ℓ of k satisfies $\ell \leq c(n)$,
(d) $\log_2(k) \leq 2n$.

Steps:

(i) Run Algorithm 16.3 to obtain a finite set $\mathfrak{S}$ that is usable for A.
(ii) For each $S \in \mathfrak{S} \smallsetminus \{S_0\}$, let $\mathfrak{a}_S = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n(n+1)}$, and put $\mathfrak{a}_{S_0} = 2^{n+1}A$. Output $U = \{\mathfrak{a}_S : S \in \mathfrak{S}\}$ and the integers $k(\mathfrak{a})$ for each $\mathfrak{a} \in U$.
(iii) Use the extended Euclidean algorithm to compute k and to find integers $f(\mathfrak{a})$ that satisfy (b).

Proposition 17.4. *Algorithm 17.3 is correct and runs in polynomial time.*

Proof. Since $\mathfrak{S}$ is usable, each $S \in \mathfrak{S}$ is vigilant. It follows that each ideal $\mathfrak{a}_S \in U$ is good. By Proposition 8.5(ii) we have (a).

Suppose ℓ is a prime number and $\ell > c(n)$. Since $\mathfrak{S}$ is usable, there exists $S \in \mathfrak{S}$ such that $\mathrm{N}(\mathfrak{p}) \not\equiv 1 \bmod \ell$ and $\mathrm{char}(A/\mathfrak{p}) \leq b(n)$ for all $\mathfrak{p} \in S$. By Definition 17.1, the positive integer $k(\mathfrak{a}_S)$ is not divisible by ℓ. Thus k is not divisible by ℓ, giving (c).

We have $k \leq k(2^{n+1}A) \leq 2^{2n}$, giving (d). □

The following algorithm will be used in Algorithm 18.1. In the algorithm, the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are the analogues of the prime numbers m and ℓ of Algorithm 18.7 of [14], while $k(\mathfrak{a})$ is the analogue of $k(m)$.

Algorithm 17.5. Given a connected CM-order A of rank n and an invertible A-lattice L, the algorithm either outputs "L has no short vector" or finds:

- a positive integer k each of whose prime factors is at most $c(n)$ and such that $\log_2(k) \leq 2n$,
- an element $e_2 \in L$ such that $Ae_2 + 2L = L$, and
- an element $s \in A/2^{n+1}A$ such that the coset $s \cdot (e_2^k + 2^{n+1}L^k) \in L^k/2^{n+1}L^k$ contains a short vector in L^k.

Steps:

(i) Apply Algorithm 17.3 to obtain a finite set U of good ideals $\mathfrak{a}$ of A, and $k(\mathfrak{a})$ and $f(\mathfrak{a})$ for each $\mathfrak{a} \in U$, and $k = \gcd_{\mathfrak{a} \in U}\{k(\mathfrak{a})\}$ satisfying (a-d) of Algorithm 17.3.
(ii) Apply the algorithm associated to Proposition 10.5 to find $e_2 \in L$ such that $Ae_2 + 2L = L$. Let $\mathfrak{b} = 2^{n+1}A$ and let $e_{\mathfrak{b}} = e_2 + \mathfrak{b}L \in L/\mathfrak{b}L$.
(iii) For each $\mathfrak{a} \in U \smallsetminus \{\mathfrak{b}\}$, do the following. Apply the algorithm associated to Proposition 10.5 to find $e_{\mathfrak{a}} \in L/\mathfrak{a}L$ such that $(A/\mathfrak{a}) \cdot e_{\mathfrak{a}} = L/\mathfrak{a}L$. Compute the A-lattice $L^{k(\mathfrak{a})}$ and the cosets $e_{\mathfrak{a}}^{k(\mathfrak{a})} \in L^{k(\mathfrak{a})}/\mathfrak{a}L^{k(\mathfrak{a})}$ and $e_{\mathfrak{b}}^{k(\mathfrak{a})} \in L^{k(\mathfrak{a})}/\mathfrak{b}L^{k(\mathfrak{a})}$. Run Algorithm 6.2 to decide whether the coset $e_{\mathfrak{a}}^{k(\mathfrak{a})}$ contains a vector $\nu_{\mathfrak{a}}$ satisfying $\langle \nu_{\mathfrak{a}}, \nu_{\mathfrak{a}} \rangle = n$. If no such $\nu_{\mathfrak{a}}$ exists, terminate with "no". Otherwise, find $s_{\mathfrak{a}} \in (A/\mathfrak{b})^*$ such that

$$\nu_{\mathfrak{a}} + \mathfrak{b}L^{k(\mathfrak{a})} = s_{\mathfrak{a}} \cdot e_{\mathfrak{b}}^{k(\mathfrak{a})}$$

and find a positive integer $g(\mathfrak{a}) \in f(\mathfrak{a}) + \mathbb{Z} \cdot k(\mathfrak{b})$.

(iv) Compute

$$s = \prod_{\substack{\mathfrak{a} \in U \\ \mathfrak{a} \neq \mathfrak{b}}} s_{\mathfrak{a}}^{g(\mathfrak{a})} \in (A/\mathfrak{b})^*.$$

(v) Use the algorithm associated with Theorem 13.1(iii) to compute the A-lattice L^k and the coset $e_{\mathfrak{b}}^k \in L^k/\mathfrak{b}L^k$.

(vi) Compute $s \cdot e_{\mathfrak{b}}^k = s(e_2^k + 2^{n+1}L^k) \in L^k/\mathfrak{b}L^k$. Apply Algorithm 6.2 to compute all $w \in s \cdot e_{\mathfrak{b}}^k \subset L^k$ satisfying $w\bar{w} = 1$. If there are none, output "no". Otherwise, output k, e_2, and s.

Proposition 17.6. *Algorithm 17.5 is correct and runs in polynomial time.*

Proof. Each prime divisor of the positive integer k output by Algorithm 17.3 is at most $c(n)$, and $\log_2(k) \leq 2n$.

Since L is invertible, by Corollary 10.4 the algorithm associated to Proposition 10.5 will find e_2 and $e_{\mathfrak{a}}$ in Steps (ii) and (iii). Since $L = Ae_2 + 2L$, it follows from Nakayama's Lemma that $(A/\mathfrak{b}) \cdot e_{\mathfrak{b}} = L/\mathfrak{b}L$, with $e_{\mathfrak{b}}$ defined as in Step (ii).

Take $z \in L$ with $z\bar{z} = 1$. Then $Az = L$ by Theorem 11.1(ii).

Suppose $\mathfrak{a} \in U$. Since $(A/\mathfrak{a}) \cdot (z + \mathfrak{a}L) = L/\mathfrak{a}L = (A/\mathfrak{a}) \cdot e_{\mathfrak{a}}$, it follows that $z + \mathfrak{a}L \in (A/\mathfrak{a})^* \cdot e_{\mathfrak{a}}$. By Lemma 17.2 we have

$$z^{k(\mathfrak{a})} \in e_{\mathfrak{a}}^{k(\mathfrak{a})}. \tag{17.6.1}$$

Since $z^{k(\mathfrak{a})}\overline{z^{k(\mathfrak{a})}} = 1$, by Proposition 7.3 we have $\langle z^{k(\mathfrak{a})}, z^{k(\mathfrak{a})} \rangle = n$. Thus, Step (iii) will find a vector $\nu_{\mathfrak{a}}$ for each $\mathfrak{a} \neq \mathfrak{b}$, as long as L has a short vector z. The vector $\nu_{\mathfrak{a}}$ is regular by Lemma 10.8 applied to $L^{k(\mathfrak{a})}$ in place of L, and $\nu_{\mathfrak{a}}$ is short by Proposition 7.3. We have $\nu_{\mathfrak{a}} = z^{k(\mathfrak{a})}$ by the uniqueness property in Proposition 6.3 (using property (a) of Algorithm 17.3), and

$$z^{k(\mathfrak{a})} \bmod \mathfrak{b} = \nu_{\mathfrak{a}} \bmod \mathfrak{b} = s_{\mathfrak{a}} \cdot e_{\mathfrak{b}}^{k(\mathfrak{a})}.$$

Since $g(\mathfrak{a}) \in f(\mathfrak{a}) + \mathbb{Z} \cdot k(\mathfrak{b})$, by Lemma 17.2 we have

$$s = \prod_{\mathfrak{b} \neq \mathfrak{a} \in U} s_{\mathfrak{a}}^{g(\mathfrak{a})} = \prod_{\mathfrak{b} \neq \mathfrak{a} \in U} s_{\mathfrak{a}}^{f(\mathfrak{a})} \in (A/\mathfrak{b})^*.$$

Applying (17.6.1) with $\mathfrak{a} = \mathfrak{b}$ gives $z^{k(\mathfrak{b})} \bmod \mathfrak{b} = 1 \cdot e_{\mathfrak{b}}^{k(\mathfrak{b})} \in \Lambda/\mathfrak{b}\Lambda$. Letting $s_{\mathfrak{b}} = 1$, then

$$\begin{aligned} z^k \bmod \mathfrak{b} = \prod_{\mathfrak{a} \in U} (z^{k(\mathfrak{a})} \bmod \mathfrak{b})^{f(\mathfrak{a})} &= \prod_{\mathfrak{a} \in U} \left(s_{\mathfrak{a}} \cdot e_{\mathfrak{b}}^{k(\mathfrak{a})}\right)^{f(\mathfrak{a})} \\ &= \left(\prod_{\mathfrak{b} \neq \mathfrak{a} \in U} s_{\mathfrak{a}}^{f(\mathfrak{a})}\right) e_{\mathfrak{b}}^k = s \cdot e_{\mathfrak{b}}^k \in \Lambda/\mathfrak{b}\Lambda, \end{aligned}$$

so z^k is a short vector in the coset $s \cdot e_{\mathfrak{b}}^k = s \cdot (e_2^k + 2^{n+1}L^k)$. Thus if L has a short vector z, then Step (vi) outputs an element $s \in A/2^{n+1}A$ such that the coset $s \cdot (e_2^k + 2^{n+1}L^k)$ contains a short vector in L^k.

The algorithm runs in polynomial time since each step does. □

18. Main algorithm

Our main algorithm is Algorithm 18.6, which first makes a reduction to the case of connected orders and then calls on Algorithm 18.1.

Algorithm 18.1. Given a *connected* CM-order A and an invertible A-lattice L, the algorithm decides whether or not L is A-isomorphic to the standard A-lattice, and if so, outputs a short vector $z \in L$ and an A-isomorphism $A \to L$ given by $a \mapsto az$.

Steps:

(i) Apply Algorithm 17.5. If it outputs "L has no short vector", terminate with "no". Otherwise, Algorithm 17.5 outputs k, e_2, and s. Let $t_0 = s$.

(ii) Factor k. Let $p_1, \ldots, p_m$ be the prime divisors of k with multiplicity, and let $q_0 = k$. For $i = 1, \ldots, m$ in succession, compute $q_i = q_{i-1}/p_i$, the lattice L^{q_i}, and the coset $e_2^{q_i} + 2^{n+1}L^{q_i} \in L^{q_i}/2^{n+1}L^{q_i}$, and apply Algorithm 14.5 where in place of inputs L, r, ϵ, and s one takes L^{q_i}, p_i, $e_2^{q_i} + 2^{n+1}L^{q_i}$, and t_{i-1}, respectively, and where the output t is called t_i. If Algorithm 14.5 ever outputs "no", terminate with "no".

(iii) Otherwise output "yes", the short vector z in the coset $t_m \cdot (e_2 + 2^{n+1}L)$ where $t_m \in A/2^{n+1}A$ is the output of the last run of Algorithm 14.5, and the map $A \to L$, $a \mapsto az$.

Remark 18.2. When we iterate Algorithm 14.5 in Algorithm 18.1, it often happens that we compute the same short vector in the same lattice twice, namely in Step (v) of Algorithm 14.5 to compute α and then in Step (ii) of the next iteration of Algorithm 14.5 to compute ν. However, that happens for two *different* representations of the same lattice, say L^h and $(L^{h/p})^{\otimes p}$, that are not easy to identify with each other (but with the *same* $s \in A/2^{n+1}A$).

Remark 18.3. The vector z in Step (iii) of Algorithm 18.1 could be computed either using Algorithm 6.2, or by taking $z = \alpha_m \in L$ where α_m is the element α computed in Step (iv) of the last run of Algorithm 14.5.

Proposition 18.4. *Algorithm 18.1 is correct and runs in polynomial time.*

Proof. The i-th iteration of Step (ii) has as input the invertible A-lattice $L^{q_i} = L^{k/(p_1 \cdots p_i)}$, and finds a coset containing a short vector in $L^{q_{i-1}} = L^{k/(p_1 \cdots p_{i-1})}$, as long as L contains a short vector. The output z, after m iterations, is a short vector in the coset $t_m(e_2 + 2^{n+1}L)$.

Recall that the size of the input describing A is at least n^3. Since each prime divisor of k is at most $c(n)$ (as defined in Definition 15.1), and $\log_2(k) \le 2n$, one can factor k in polynomial time. By Proposition 14.6, Algorithm 14.5 runs in time at most polynomial in r plus the length of the input. In Step (ii), in the i-th run of Algorithm 14.5 we have $r = p_i \le c(n)$. It follows that Step (ii) runs in polynomial time. □

The following result is Theorem 1.1 of [13]; its associated algorithm is Algorithm 6.1 of [13].

Proposition 18.5 ([13]). *There is a deterministic polynomial-time algorithm that, given an order A, lists all primitive idempotents of A.*

Algorithm 18.6. Given a CM-order A and an A-lattice L, the algorithm decides whether or not L is A-isomorphic to the standard A-lattice, and if so, outputs a short vector $z \in L$ and an A-isomorphism $A \to L$ given by $a \mapsto az$.

Steps:

(i) Apply Algorithm 10.10 to test L for invertibility. If L is not invertible, terminate with "no".

(ii) Apply the algorithm from Proposition 18.5 to compute the primitive idempotents of A, and apply Lemma 4.10 to decompose A as a product of finitely many connected rings $A = \prod_i A_i$ and decompose L as an orthogonal sum $L = \perp_i L_i$ where L_i is an invertible A_i-lattice.

(iii) Apply Algorithm 18.1 to each L_i. If it ever terminates with "no", terminate with "no A-isomorphism exists". Otherwise, it outputs maps $A_i \to L_i$, $a \mapsto az_i$ for each i. Output "yes", $z = (z_i)_i \in A = \prod_i A_i$, and the map $A = \prod_i A_i \to L = \perp_i L_i$, $(a_i)_i \mapsto (a_i z_i)_i$.

Proposition 12.1(iii) now enables us to convert Algorithm 18.6 into an algorithm to test whether two A-lattices are A-isomorphic (and produce an isomorphism). This is our analogue of Algorithm 19.4 of [14].

Algorithm 18.7. Given a CM-order A and invertible A-lattices L and M, the algorithm decides whether or not L and M are isomorphic as A-lattices, and if so, gives such an A-isomorphism.

(i) Compute $L \otimes_A \overline{M}$.

(ii) Apply Algorithm 18.6 to find an A-isomorphism $A \xrightarrow{\sim} L \otimes_A \overline{M}$, or a proof that none exists. In the latter case, terminate with "no".

(iii) Using this map and the map $\overline{M} \otimes_A M \to A$, $\overline{y} \otimes x \mapsto \overline{y} \cdot x$, output the composition of the (natural) maps

$$M \xrightarrow{\sim} A \otimes_A M \xrightarrow{\sim} L \otimes_A \overline{M} \otimes_A M \xrightarrow{\sim} L \otimes_A A \xrightarrow{\sim} L.$$

It is clear that Algorithms 18.6 and 18.7 are correct and run in polynomial time. Theorems 1.3 and 1.4 now follow from Algorithms 18.6 and 18.7 and Theorem 9.3.

References

[1] M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, MA, 1969.

[2] D. J. Bernstein, *Factoring into coprimes in essentially linear time*, Journal of Algorithms **54** (2005), 1–30.

[3] S. Garg, C. Gentry, and S. Halevi, *Candidate multilinear maps from ideal lattices*, in Advances in Cryptology—EUROCRYPT 2013, Lect. Notes in Comp. Sci. **7881**, Springer, 2013, 1–17.

[4] C. Gentry and M. Szydlo, *Cryptanalysis of the revised NTRU signature scheme*, in Advances in Cryptology—EUROCRYPT 2002, Lect. Notes in Comp. Sci. **2332** (2002), Springer, 299–320; full version at `http://www.szydlo.com/ntru-revised-full02.pdf`.

[5] P. Kirchner, *Algorithms on ideal over complex multiplication order*, `https://eprint.iacr.org/2016/220`, February 29, 2016, revised April 6, 2016.

[6] S. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time*, in The mathematics of Paul Erdős, I, 176–198, Algorithms Combin. **13**, Springer, Berlin, 1997.

[7] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[8] H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** (1992), 211–244, `https://doi.org/10.1090/S0273-0979-1992-00284-7`.

[9] H. W. Lenstra, Jr., *Lattices*, in Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press, Cambridge, 2008, 127–181.

[10] H. W. Lenstra, Jr., *Lattices over CM-orders*, lecture at Workshop on Lattices with Symmetry, `https://www.youtube.com/watch?v=3Ic4yES5Uxk&feature=youtu.be`, August 16, 2013.

[11] H. W. Lenstra, Jr. and A. Silverberg, *Revisiting the Gentry-Szydlo Algorithm*, in Advances in Cryptology—CRYPTO 2014, Lect. Notes in Comp. Sci. **8616**, Springer, Berlin, 2014, 280–296.

[12] H. W. Lenstra, Jr. and A. Silverberg, *Determining cyclicity of finite modules*, Journal of Symbolic Computation **73** (2016), 153–156, `http://doi.org/10.1016/j.jsc.2015.06.002`.

[13] H. W. Lenstra, Jr. and A. Silverberg, *Roots of unity in orders*, Foundations of Computational Mathematics **17** (2017), 851–877, `http://doi.org/10.1007/s10208-016-9304-1`.

[14] H. W. Lenstra, Jr. and A. Silverberg, *Lattices with symmetry*, Journal of Cryptology **30** (2017), 760–804, `http://doi.org/10.1007/s00145-016-9235-7`.

[15] H. W. Lenstra, Jr. and A. Silverberg, *Algorithms for commutative algebras over the rational numbers*, Foundations of Computational Mathematics **18** (2018), 159–180, `http://doi.org/10.1007/s10208-016-9336-6`.

[16] H. W. Lenstra, Jr. and A. Silverberg, *Universal gradings of orders*, Archiv der Mathematik, **111**, (2018), 579–597, `https://doi.org/10.1007/s00013-018-1228-3`.

[17] L. Rónyai, *Computing the structure of finite algebras*, J. Symbolic Comput. **9** (1990), no. 3, 355–373.

[18] G. Shimura, Abelian varieties with complex multiplication and modular functions, Princeton Mathematical Series **46**, Princeton University Press, Princeton, NJ, 1998.

[19] Workshop on Lattices with Symmetry, August 12–16, 2013, UC Irvine, `http://www.math.uci.edu/~asilverb/Lattices`.

Mathematisch Instituut, Universiteit Leiden, The Netherlands
Email address: `hwl@math.leidenuniv.nl`

Department of Mathematics, University of California, Irvine, CA 92697
Email address: `asilverb@uci.edu`