REVISITING THE GENTRY-SZYDLO ALGORITHM

H. W. LENSTRA AND A. SILVERBERG

Abstract. We put the Gentry-Szydlo algorithm in a mathematical framework, and show that it is part of a general theory of "lattices with symmetry". For large ranks, there is no good algorithm that decides whether a given lattice has an orthonormal basis. But when the lattice is given with enough symmetry, we can construct a provably deterministic polynomial time algorithm to accomplish this, based on the work of Gentry and Szydlo. The techniques involve algorithmic algebraic number theory, analytic number theory, commutative algebra, and lattice basis reduction. This sheds new light on the Gentry-Szydlo algorithm, and the ideas should be applicable to a range of questions in cryptography.

1. Introduction

In §7 of [6], Gentry and Szydlo introduced some powerful new ideas that combined in a clever way lattice basis reduction and number theory. They used these ideas to cryptanalyze NTRU Signatures. The recent interest in Fully Homomorphic Encryption (FHE) and in the candidate multilinear maps of Garg-Gentry-Halevi [2] bring the Gentry-Szydlo results once again to the fore. Gentry's first FHE scheme [3] used ideal lattices, as have a number of subsequent schemes. Fully Homomorphic Encryption is performed more efficiently with ideal lattices than with general lattices. However, ideal lattices are special, with much structure ("symmetries") that has the potential to be exploited. In his thesis [4], Gentry mentions that the Gentry-Szydlo attack on NTRU signatures can be used to attack principal ideal lattices in the ring $\mathbb{Z}[X]/(X^n - 1)$, if the lattice has an orthonormal basis.

As Gentry pointed out [5], the Gentry-Szydlo algorithm "seems to be a rather crazy, unusual combination of LLL with more 'algebraic' techniques. It seems like it should have more applications—e.g., perhaps to breaking or weakening ideal lattices." Generalizing or improving the Gentry-Szydlo algorithm would potentially affect the security of all cryptography that is built from ideal lattices, or whose security is based on hard problems for ideal lattices. Candidate multilinear maps were recently cryptanalyzed using the Gentry-Szydlo algorithm. As remarked by Garg, Gentry, and Halevi in [2], their "new algebraic/lattice attacks are extensions of an algorithm by Gentry and Szydlo, which combines lattice reduction and Fermat's Little Theorem in a clever way to solve a relative norm equation in a cyclotomic field."

The Gentry-Szydlo algorithm has been viewed by some as magic. In this paper we revisit the algorithm and put it in a mathematical framework, in order to make it easier to understand, generalize, and improve on. That should help make it more widely applicable in cryptographic applications. We embed the algorithm in a wider theory that we refer to as "lattices with symmetry".

The algorithm of Gentry and Szydlo can be viewed as a way to find an orthonormal basis (if one exists) for an ideal lattice. Determining whether a lattice has an orthonormal basis is a difficult

Key words and phrases. lattices, Gentry-Szydlo algorithm, ideal lattices, lattice-based cryptography.

This material is based on research sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750-13-2-0054. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

We thank the participants of the August 2013 Workshop on Lattices with Symmetry, in particular Craig Gentry, René Schoof, and Mike Szydlo.

algorithmic problem that is easier when the lattice has many symmetries. In this paper we solve this problem when the lattice comes with a sufficiently large abelian group of automorphisms, and we show how the Gentry-Szydlo algorithm is a special case of this result.

Our algorithm runs in deterministic polynomial time, whereas [6] relies on a probabilistic algorithm. Also, our setting is more general (our theory applies to arbitrary finite abelian groups, where [6] considers only cyclic groups of odd prime order), thereby covering other cases of potential cryptographic interest.

Briefly, our main result is as follows (see §2 for background information). If G is a finite abelian group and $u \in G$ has order 2, define a G-lattice to be a lattice L with a group homomorphism $G \to \mathrm{Aut}(L)$ that takes u to -1. The "standard" G-lattice is the modified group ring $\mathbb{Z}\langle G\rangle = \mathbb{Z}[G]/(u+1)$. A G-isomorphism is an isomorphism of lattices that respects the G-actions.

Theorem 1.1. *There is a deterministic polynomial time algorithm that, given a finite abelian group G, an element $u \in G$ of order 2, and a G-lattice L, decides whether L and $\mathbb{Z}\langle G\rangle$ are G-isomorphic, and if they are, exhibits a G-isomorphism.*

The ingredients include the technique invented by Gentry and Szydlo in [6], lattice basis reduction, commutative algebra (finite rings and tensor algebras), analytic number theory, and algorithmic algebraic number theory. The graded tensor algebra Λ introduced in §3.4 is in a sense the hero of our story. It replaces Gentry's and Szydlo's polynomial chains. In §7 of [6], taking powers of an ideal in the ring $R = \mathbb{Z}[X]/(X^n - 1)$ required complicated bookkeeping, via polynomial chains and lattice basis reduction to avoid coefficient blow-up. We do away with this, by using the module structure of the ideal, rather than its ideal structure. More precisely, an ideal in a commutative ring R is the same as an R-module M along with an embedding $M \hookrightarrow R$ of R-modules. While Gentry and Szydlo use the embedding, we observe that one can avoid coefficient blow-up by using the module structure of M but not the actual embedding. We replace ideal multiplication with tensor products of lattices.

In §2 we introduce the concept of a G-lattice, and in §2.3 we show that Theorem 1.1 implies the result of Gentry and Szydlo. In §3–§4 we introduce invertible G-lattices, of which the ideal lattices considered by Gentry and Szydlo are examples, and give the concepts and results that we use to state our new algorithm and prove its correctness. We explicitly present the algorithm in §5.

2. G-lattices and the modified group ring

In this section we explain some notation and concepts that we use in our main result.

2.1. **Lattices and G-lattices.** We first give some background on lattices (see also [10]), and introduce G-lattices.

Definition 2.1. A **lattice** or **integral lattice** is a finitely generated abelian group L with a map $\langle \cdot, \cdot \rangle : L \times L \to \mathbb{Z}$ that is

- bilinear: $\langle x, y+z\rangle = \langle x, y\rangle + \langle x, z\rangle$ and $\langle x+y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$ for all $x, y, z \in L$,
- symmetric: $\langle x, y\rangle = \langle y, x\rangle$ for all $x, y \in L$, and
- positive definite: $\langle x, x\rangle > 0$ if $0 \neq x \in L$.

As groups, L is isomorphic to $\mathbb{Z}^n$ for some n, which is called the **rank** of L. In algorithms, a lattice is specified by a Gram matrix $(\langle b_i, b_j\rangle)_{i,j=1}^n$ associated to a $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$.

Definition 2.2. The **standard lattice** of rank n is $L = \mathbb{Z}^n$ with $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$. Its Gram matrix is the $n \times n$ identity matrix I_n.

Definition 2.3. A lattice L is **unimodular** if the map $L \to \mathrm{Hom}(L, \mathbb{Z})$ that takes each $x \in L$ to the map $y \mapsto \langle x, y\rangle$ is bijective. Equivalently, L is unimodular if its Gram matrix has determinant 1.

Definition 2.4. An **isomorphism** $L \xrightarrow{\sim} M$ of lattices is a group isomorphism $\varphi : L \xrightarrow{\sim} M$ that respects the lattice structures, i.e., $\langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$ for all $x, y \in L$. If such a map φ exists, then L and M are **isomorphic** lattices. An **automorphism** of a lattice L is an isomorphism from L onto itself. The set of automorphisms of L is a finite group $\mathrm{Aut}(L)$ whose center contains -1 (represented by $-I_n$).

In algorithms, isomorphisms are specified by their matrices on the given bases of L and M.

Examples 2.5. (i) "Random" lattices have $\mathrm{Aut}(L) = \{\pm 1\}$.

(ii) Letting S_n denote the symmetric group on n letters and $\rtimes$ denote semidirect product, then $\mathrm{Aut}(\mathbb{Z}^n) \cong \{\pm 1\}^n \rtimes S_n$. (The standard basis vectors can be permuted, and negatives taken.)

(iii) If L is the equilateral triangular lattice in the plane, then $\mathrm{Aut}(L)$ is the symmetry group of the regular hexagon, which is a dihedral group of order 12.

From now on, suppose that G is a finite abelian group, and $u \in G$ is a fixed element of order 2.

Definition 2.6. A **G-lattice** is a lattice L together with a group homomorphism $f : G \to \mathrm{Aut}(L)$ such that $f(u) = -1$. For each $\sigma \in G$ and $x \in L$, define $\sigma x \in L$ by $\sigma x = f(\sigma)(x)$.

The abelian group G is specified by a multiplication table. The G-lattice L is specified as a lattice along with, for each $\sigma \in G$, the matrix describing the action of σ on L.

Definition 2.7. If L and M are G-lattices, then a **G-isomorphism** is an isomorphism $\varphi : L \xrightarrow{\sim} M$ of lattices that respects the G-actions, i.e., $\varphi(\sigma x) = \sigma \varphi(x)$ for all $x \in L$ and $\sigma \in G$. If such an isomorphism exists, we say that L and M are G-isomorphic, or isomorphic as G-lattices.

2.2. **The Modified Group Ring $\mathbb{Z}\langle G \rangle$.** We define a modified group ring $A\langle G \rangle$ whenever A is a commutative ring. We will usually take $A = \mathbb{Z}$, but will also take $A = \mathbb{Z}/m\mathbb{Z}$. We consider $A\langle G \rangle$ rather than the standard group ring $A[G]$, since G-lattices become $\mathbb{Z}\langle G \rangle$-modules. Also, it allows us to include the cyclotomic rings $\mathbb{Z}[X]/(X^{2^k} + 1)$ in our theory.

The group ring $A[G]$ is the set of formal sums $\sum_{\sigma \in G} a_\sigma \sigma$ with $a_\sigma \in A$, with addition defined by $\sum_{\sigma \in G} a_\sigma \sigma + \sum_{\sigma \in G} b_\sigma \sigma = \sum_{\sigma \in G} (a_\sigma + b_\sigma)\sigma$ and multiplication defined by $(\sum_{\sigma \in G} a_\sigma \sigma)(\sum_{\tau \in G} b_\tau \tau) = \sum_{\rho \in G} (\sum_{\sigma\tau = \rho} a_\sigma b_\tau)\rho$. For example, if G is a cyclic group of order m and g is a generator, then as rings $\mathbb{Z}[X]/(X^m - 1) \cong \mathbb{Z}[G]$ via the map $\sum_{i=0}^{m-1} a_i X^i \mapsto \sum_{i=0}^{m-1} a_i g^i$.

Definition 2.8. If A is a commutative ring, then writing 1 for the identity element of the group G, we define the **modified group ring**

$$A\langle G \rangle = A[G]/(u + 1).$$

Every G-lattice is a $\mathbb{Z}\langle G \rangle$-module, where one uses the G-action on L to define ax whenever $x \in L$ and $a \in \mathbb{Z}\langle G \rangle$.

Definition 2.9. Define the **scaled trace function** $t : A\langle G \rangle \to A$ by

$$t\Big(\sum_{\sigma \in G} a_\sigma \sigma\Big) = a_1 - a_u.$$

Then t is the (additive) group homomorphism satisfying $t(1) = 1$, $t(u) = -1$, and $t(\sigma) = 0$ if $\sigma \in G$ and $\sigma \neq 1, u$.

Definition 2.10. For $a = \sum_{\sigma \in G} a_\sigma \sigma \in A\langle G \rangle$, define $\overline{a} = \sum_{\sigma \in G} a_\sigma \sigma^{-1}$.

The map $a \mapsto \overline{a}$ is a ring automorphism of $A\langle G \rangle$. Since $\overline{\overline{a}} = a$, it is an involution. (An involution is a map that is its own inverse.) In practice, this map plays the role of complex conjugation.

Remark 2.11. If L is a G-lattice and $x, y \in L$, then $\langle \sigma x, \sigma y \rangle = \langle x, y \rangle$ for all $\sigma \in G$. It follows that $\langle ax, y \rangle = \langle x, \overline{a}y \rangle$ for all $a \in \mathbb{Z}\langle G \rangle$.

Definition 2.12. For $x, y \in \mathbb{Z}\langle G \rangle$ define $\langle x, y \rangle_{\mathbb{Z}\langle G \rangle} = t(x\overline{y})$.

Let $n = |G|/2 \in \mathbb{Z}$.

Definition 2.13. Let S be a set of coset representatives of $G/\langle u \rangle$ (i.e., $\#S = n$ and $G = S \sqcup uS$), and for simplicity take S so that $1 \in S$.

The following result is straightforward.

Proposition 2.14. (i) *The additive group of the ring $\mathbb{Z}\langle G \rangle$ is a G-lattice of rank n, with lattice structure defined by $\langle x, y \rangle_{\mathbb{Z}\langle G \rangle}$ and G-action defined by $\sigma x = \sigma x$ where the right side is ring multiplication in $\mathbb{Z}\langle G \rangle$.*

(ii) *As lattices, $\mathbb{Z}\langle G \rangle \cong \mathbb{Z}^n$.*

(iii) $\mathbb{Z}\langle G \rangle = \{\sum_{\sigma \in S} a_\sigma \sigma : a_\sigma \in \mathbb{Z}\} = \bigoplus_{\sigma \in S} \mathbb{Z}\sigma$ *and* $t(\sum_{\sigma \in S} a_\sigma \sigma) = a_1$.

Definition 2.15. We call $\mathbb{Z}\langle G \rangle$ the **standard G-lattice**.

Example 2.16. Suppose $G = H \times \langle u \rangle$ with $H \cong \mathbb{Z}/n\mathbb{Z}$. Then $\mathbb{Z}\langle G \rangle \cong \mathbb{Z}[H] \cong \mathbb{Z}[X]/(X^n - 1)$ as rings and as lattices. When n is odd (so G is cyclic), then (by sending X to $-X$) we have $\mathbb{Z}\langle G \rangle \cong \mathbb{Z}[X]/(X^n - 1) \cong \mathbb{Z}[X]/(X^n + 1)$.

Remark 2.17. The ring $\mathbb{Z}\langle G \rangle$ is an integral domain (i.e., no zero divisors) if and only if G is cyclic and n is a power of 2. If G is cyclic of order 2^r, then $\mathbb{Z}\langle G \rangle \cong \mathbb{Z}[\zeta_{2^r}]$.

2.3. **Ideal Lattices.**

Example 2.18. Suppose I is an ideal in the ring $\mathbb{Z}\langle G \rangle$ and $w \in \mathbb{Z}\langle G \rangle$. Suppose that $I\overline{I} = \mathbb{Z}\langle G \rangle \cdot w$ and $\psi(w) \in \mathbb{R}_{>0}$ for all ring homomorphisms $\psi : \mathbb{Z}\langle G \rangle \to \mathbb{C}$. It follows that the ideal I has finite index in $\mathbb{Z}\langle G \rangle$, that $\overline{w} = w$, and that w is not a zero divisor. Define the G-lattice $L_{(I,w)}$ to be I with G-action given by multiplication in $\mathbb{Z}\langle G \rangle$, and with lattice structure defined by

$$\langle x, y \rangle_{I,w} = t\left(\frac{x\overline{y}}{w}\right)$$

with t as in Definition 2.9. (Note that $\frac{x\overline{y}}{w} \in \mathbb{Z}\langle G \rangle$ since w generates the ideal $I\overline{I}$.) In particular, $L_{(\mathbb{Z}\langle G \rangle, 1)} = \mathbb{Z}\langle G \rangle$.

The lattice $L_{(I,w)}$ is G-isomorphic to $\mathbb{Z}\langle G \rangle$ if and only if there exists $v \in \mathbb{Z}\langle G \rangle$ such that $I = (v)$ and $w = v\overline{v}$. Further, *knowing* such a G-isomorphism is equivalent to *knowing* v. More precisely, v is the image of 1 under a G-isomorphism $\mathbb{Z}\langle G \rangle \xrightarrow{\sim} L_{(I,w)}$, and $w = v\overline{v}$ if and only if $\langle av, bv \rangle_{I,w} = t(a\overline{b}) = \langle a, b \rangle_{\mathbb{Z}\langle G \rangle}$ for all $a, b \in \mathbb{Z}\langle G \rangle$. Thus, finding v from I and $v\overline{v}$ in polynomial time is equivalent to finding a G-isomorphism $\mathbb{Z}\langle G \rangle \xrightarrow{\sim} L_{(I,w)}$ in polynomial time.

The point of dividing by w in the definition of $\langle x, y \rangle_{I,w}$ is to make the lattice L unimodular. It follows that when we take tensor powers of L over $\mathbb{Z}\langle G \rangle$, as we will do in §3 below, there will be no coefficient blow-up.

We next show how to recover the Gentry-Szydlo result from Theorem 1.1. The Gentry-Szydlo algorithm finds a generator v of an ideal I of finite index in the ring $R = \mathbb{Z}[X]/(X^n - 1)$, given $v\overline{v}$, a $\mathbb{Z}$-basis for I, and a "promise" that v exists. Here, n is an odd prime, and for $v = v(X) = \sum_{i=0}^{n-1} a_i X^i \in R$, its "reversal" is $\overline{v} = v(X^{-1}) = a_0 + \sum_{i=1}^{n-1} a_{n-i} X^i \in R$. We take G to be a cyclic group of order $2n$. Then $R \cong \mathbb{Z}\langle G \rangle$ as in Example 2.16, and we identify R with $\mathbb{Z}\langle G \rangle$. Let $w = v\overline{v} \in \mathbb{Z}\langle G \rangle$ and let $L = L_{(I,w)}$ as above. Then L is the "implicit orthogonal lattice" in §7.2 of [6]. Once you know a $\mathbb{Z}$-basis for I and w, you know L. Theorem 1.1 produces a G-isomorphism $\mathbb{Z}\langle G \rangle \xrightarrow{\sim} L$ in polynomial time, and thus gives a generator v in polynomial time.

3. Invertible G-lattices, short vectors, and the tensor algebra Λ

In this section we give some concepts that we will use to prove Theorem 1.1.

3.1. **Invertible G-lattices.**

Definition 3.1. If L is a G-lattice, then the G-lattice $\overline{L}$ is a lattice equipped with a lattice isomorphism $L \xrightarrow{\sim} \overline{L}$, $x \mapsto \overline{x}$ and a group homomorphism $G \to \mathrm{Aut}(\overline{L})$ defined by $\sigma\overline{x} = \overline{\sigma^{-1}x} = \overline{\sigma}\overline{x}$ for all $\sigma \in G$ and $x \in L$, i.e., $\overline{\sigma x} = \overline{\sigma}\,\overline{x}$.

Definition 3.2. If L is a G-lattice, define the lifted inner product

$$\cdot : L \times \overline{L} \to \mathbb{Z}\langle G\rangle \quad \text{by} \quad x \cdot \overline{y} = \sum_{\sigma \in S} \langle x, \sigma y\rangle \sigma \in \mathbb{Z}\langle G\rangle.$$

Then

$$\langle x, y\rangle = t(x \cdot \overline{y}) \tag{1}$$

and $x \cdot \overline{y} = \overline{y \cdot \overline{x}}$. This lifted inner product is $\mathbb{Z}\langle G\rangle$-bilinear, i.e., $(ax) \cdot \overline{y} = x \cdot (a\overline{y}) = a(x \cdot \overline{y})$ for all $a \in \mathbb{Z}\langle G\rangle$ and all $x, y \in L$.

Example 3.3. If $L = \mathbb{Z}\langle G\rangle$, then $\overline{L} = \mathbb{Z}\langle G\rangle$ with $^-$ having the same meaning as in Definition 2.10 for $A = \mathbb{Z}$, and with $\cdot$ being multiplication in $\mathbb{Z}\langle G\rangle$.

Definition 3.4. A G-lattice L is **invertible** if the following three conditions all hold:

(i) $\mathrm{rank}(L) = n = |G|/2$;
(ii) L is unimodular (see Definition 2.3);
(iii) for each $m \in \mathbb{Z}_{>0}$ there exists $e_m \in L$ such that $\{\sigma e_m + mL : \sigma \in G\}$ generates the abelian group L/mL.

Example 3.5. If a G-lattice L is G-isomorphic to the standard G-lattice then L is invertible. For (iii), observe that the group $\mathbb{Z}\langle G\rangle$ is generated by $\{\sigma 1 : \sigma \in G\}$, so the group L is generated by $\{\sigma e : \sigma \in G\}$ where e is the image of 1 under the isomorphism. Now let $e_m = e$ for all m.

Remark 3.6. One can show that a G-lattice L is invertible if and only if there is a $\mathbb{Z}\langle G\rangle$-module M such that $L \otimes_{\mathbb{Z}\langle G\rangle} M$ and $\mathbb{Z}\langle G\rangle$ are isomorphic as $\mathbb{Z}\langle G\rangle$-modules and L is unimodular. (See Chapter XVI of [8] for tensor products.) This is equivalent to the map $\varphi : L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} \to \mathbb{Z}\langle G\rangle$ defined by $\varphi(x \otimes \overline{y}) = x \cdot \overline{y}$ being an isomorphism of $\mathbb{Z}\langle G\rangle$-modules. One can also show that L is invertible if and only if L is G-isomorphic to $L_{(I,w)}$ for some I and w as in Example 2.18.

Definition 3.4(iii) states that L/mL is a free $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$-module of rank one for all $m > 0$. Given an ideal, it is a hard problem to decide if it is principal. But checking (iii) of Definition 3.4 is easy algorithmically; see Proposition 4.3(ii) below.

3.2. **Short vectors.**

Definition 3.7. We will say that a vector e in an integral lattice L is **short** if $\langle e, e\rangle = 1$.

Example 3.8. The short vectors in the standard lattice of rank n are the $2n$ signed standard basis vectors $\{(0, \ldots, 0, \pm 1, 0, \ldots, 0)\}$. Thus, the set of short vectors in $\mathbb{Z}\langle G\rangle$ is G.

Proposition 3.9. *Suppose L is an invertible G-lattice. Then:*

(i) *if e is short, then $\{\sigma \in G : \sigma e = e\} = \{1\}$;*
(ii) *if e is short, then $\langle e, \sigma e\rangle$ is 1 if $\sigma = 1$, is -1 if $\sigma = u$, and is 0 for all other $\sigma \in G$;*
(iii) *$e \in L$ is short if and only if $e \cdot \overline{e} = 1$, with inner product $\cdot$ defined in Definition 3.2.*

Proof. Suppose $e \in L$ is short. Let $H = \{\sigma \in G : \sigma e = e\}$. For all $\sigma \in G$, by the Cauchy-Schwarz inequality we have $|\langle e, \sigma e\rangle| \leq (\langle e, e\rangle\langle \sigma e, \sigma e\rangle)^{1/2} = \langle e, e\rangle = 1$, and $|\langle e, \sigma e\rangle| = 1$ if and only if e and σe lie on the same line through 0. Thus $\langle e, \sigma e\rangle \in \{1, 0, -1\}$. Then $\langle e, \sigma e\rangle = 1$ if and only if $\sigma \in H$. Also, $\langle e, \sigma e\rangle = -1$ if and only if $\sigma e = -e$ if and only if $\sigma \in Hu$. Otherwise, $\langle e, \sigma e\rangle = 0$. Thus for (i,ii), it suffices to prove $H = \{1\}$.

Let T be a set of coset representatives for G mod $H\langle u\rangle$ and let $S = T \cdot H$, a set of coset representatives for G mod $\langle u\rangle$. If $a = \sum_{\sigma\in S} a_\sigma \sigma \in (\mathbb{Z}/m\mathbb{Z})\langle G\rangle$ is fixed by H, then $a_{\tau\sigma} = a_\sigma$ for all $\sigma \in S$ and $\tau \in H$, so $a \in (\sum_{\tau\in H} \tau)(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$.

Let $m = |H|$. By Definition 3.4(iii), there is a $\mathbb{Z}[H]$-module isomorphism $L/mL \cong (\mathbb{Z}/m\mathbb{Z})\langle G\rangle$. The latter is a free module over $(\mathbb{Z}/m\mathbb{Z})[H]$ with basis T. Since $e + mL \in (L/mL)^H$ we have $e = m\varepsilon_1 + (\sum_{\tau\in H} \tau)\varepsilon_2$ with $\varepsilon_1, \varepsilon_2 \in L$. Since $\langle e, \tau\varepsilon_2\rangle = \langle \tau e, \tau\varepsilon_2\rangle = \langle e, \varepsilon_2\rangle$ for all $\tau \in H$, we have

$$1 = \langle e, e\rangle = m\langle e, \varepsilon_1\rangle + \sum_{\tau\in H} \langle e, \tau\varepsilon_2\rangle = m\langle e, \varepsilon_1 + \varepsilon_2\rangle \equiv 0 \mod m.$$

Thus, $m = 1$ as desired. Part (iii) follows directly from (ii) and Definition 3.2. □

This enables us to prove the following result.

Proposition 3.10. *Suppose L is a G-lattice. Then:*

(i) *if L is invertible, then the map $\{G$-isomorphisms $\mathbb{Z}\langle G\rangle \to L\} \to \{$short vectors of $L\}$ that sends f to $f(1)$ is bijective;*
(ii) *if $e \in L$ is short and L is invertible, then $\{\sigma e : \sigma \in G\}$ generates the abelian group L;*
(iii) *L is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if L is invertible and has a short vector;*
(iv) *if $e \in L$ is short and L is invertible, then the map $G \to \{$short vectors of $L\}$ defined by $\sigma \mapsto \sigma e$ is bijective.*

Proof. For (i), that $f(1)$ is short is clear. Injectivity of the map $f \mapsto f(1)$ follows from $\mathbb{Z}\langle G\rangle$-linearity of G-isomorphisms. For surjectivity, suppose $e \in L$ is short. Proposition 3.9(ii) says that $\{\sigma e\}_{\sigma\in S}$ is an orthonormal basis for L. Parts (ii) and (i) now follow, where the G-isomorphism f is defined by $x \mapsto xe$ for all $x \in \mathbb{Z}\langle G\rangle$. Part (iii) follows from (i) and Example 3.5. For (iv), injectivity follows from Proposition 3.9(i). For surjectivity, suppose $e' \in L$ is short. Take G-isomorphisms f and f' with $f(1) = e$ and $f'(1) = e'$ as in (i), and let $\sigma = f^{-1} \circ f'(1)$. Then σ is a short vector in $\mathbb{Z}\langle G\rangle$ such that $\sigma e = e'$. By Example 3.8 we have $\sigma \in G$. □

3.3. **The Witt-Picard group.** If L and M are invertible G-lattices, then the $\mathbb{Z}\langle G\rangle$-module $L \otimes_{\mathbb{Z}\langle G\rangle} M$ is a G-lattice with lifted inner product $(x \otimes v) \cdot (\overline{y} \otimes \overline{w}) = (x \cdot \overline{y})(v \cdot \overline{w})$, for all $x, y \in L$ and $v, w \in M$, and with lattice structure $\langle a, b\rangle = t(a \cdot \overline{b})$ for all $a, b \in L \otimes_{\mathbb{Z}\langle G\rangle} M$. In the notation of Example 2.18 we have $L_{(I_1,w_1)} \otimes_{\mathbb{Z}\langle G\rangle} L_{(I_2,w_2)} = L_{(I_1I_2,w_1w_2)}$, where I_1I_2 is the product of ideals.

Definition 3.11. If L is an invertible G-lattice, let $[L]$ denote its G-isomorphism class, i.e., the class of all G-lattices that are G-isomorphic to L. We define the **Witt-Picard group of** $\mathbb{Z}\langle G\rangle$ to be the set of all G-isomorphism classes of invertible G-lattices, with group operation defined by $[L] \cdot [M] = [L \otimes_{\mathbb{Z}\langle G\rangle} M]$, with identity element $[\mathbb{Z}\langle G\rangle]$, and with $[L]^{-1} = [\overline{L}]$.

The Witt-Picard group is a finite abelian group. When computing in the Witt-Picard group, one can apply a lattice basis reduction algorithm whenever the numbers get too large. More precisely, algorithmically we represent an invertible G-lattice M by letting $M = \mathbb{Z}^n$ as an abelian group, specifying a group homomorphism $G \to \mathrm{GL}(n, \mathbb{Z})$ giving the action of G on M, and giving data describing the map $\cdot : M \times \overline{M} \to \mathbb{Z}\langle G\rangle$; the lattice structure is then given by $\langle a, b\rangle = t(a \cdot \overline{b})$ for all $a, b \in M$. If M_1 and M_2 are invertible G-lattices, $m_1, m_2 \in \mathbb{Z}_{>0}$, and $d_i \in M_i/m_iM_i$ for $i = 1, 2$, one can compute $(M_1 \otimes_{\mathbb{Z}\langle G\rangle} M_2, d_1 \otimes d_2)$ in polynomial time. Also, there is a deterministic polynomial time algorithm that, given M and given $d \in M/mM$, produces a pair (M', d') and a G-isomorphism $(M, d) \to (M', d')$ such that the standard basis of $M' = \mathbb{Z}^n$ is LLL-reduced (and thus each entry of

the Gram matrix is at most 2^{n-1} in absolute value, by Lemma 3.12 below). This in fact proves the finiteness of the Witt-Picard group.

If $L = L_{(I,w)}$ for some I and w as in Example 2.18, and $j \in \mathbb{Z}_{>0}$, then $[L]^j$ is the G-isomorphism class of $L_{(I^j,w^j)}$. One can compute $[L]^j$ in deterministic polynomial time using an addition chain for j, and LLL-reducing intermediate powers to prevent coefficient blow-up. This takes the place of the polynomial chains in §7.4 of [6].

Lemma 3.12. *If $\{b_1,\dots,b_n\}$ is an LLL-reduced basis for an integral unimodular lattice L and $\{b_1^*,\dots,b_n^*\}$ is its Gram-Schmidt orthogonalization, then $2^{1-i} \le |b_i^*|^2 \le 2^{n-i}$ and $|b_i|^2 \le 2^{n-1}$ for all $i \in \{1,\dots,n\}$.*

Proof. Being LLL-reduced means that $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*$ with $|\mu_{ij}| \le \frac{1}{2}$ for all $j < i \le n$, and $|b_i^*|^2 \le 2|b_{i+1}^*|^2$ for all $i < n$. Thus for $1 \le j \le i \le n$ 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 $L_i = \sum_{j=1}^{i} \mathbb{Z} b_j$, then $|b_i^*| = \det(L_i)/\det(L_{i-1})$. Since L is integral and unimodular, $|b_n^*| = \det(L_n)/\det(L_{n-1}) = 1/\det(L_{n-1}) \le 1$, so $|b_i^*| \le 2^{n-i}$. Since $\{b_i^*\}$ is orthogonal we have

$$|b_i|^2 = |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2 \le 2^{n-i} + \frac{1}{4}\sum_{j=1}^{i-1} 2^{n-j} = 2^{n-i} + (2^{n-2} - 2^{n-i-1}) = 2^{n-2} + 2^{n-i-1} \le 2^{n-1}.$$

□

3.4. **The extended tensor algebra Λ.** Suppose L is an invertible G-lattice. Letting $L^{\otimes 0} = \mathbb{Z}\langle G\rangle$ and letting $L^{\otimes m} = L \otimes_{\mathbb{Z}\langle G\rangle} \cdots \otimes_{\mathbb{Z}\langle G\rangle} L$ (m times) and $L^{\otimes(-m)} = \overline{L}^{\otimes m} = \overline{L} \otimes_{\mathbb{Z}\langle G\rangle} \cdots \otimes_{\mathbb{Z}\langle G\rangle} \overline{L}$ for all $m \in \mathbb{Z}_{>0}$, define the extended tensor algebra

$$\Lambda \;=\; \bigoplus_{i\in\mathbb{Z}} L^{\otimes i} \;=\; \dots \oplus \overline{L}^{\otimes 3} \oplus \overline{L}^{\otimes 2} \oplus \overline{L} \oplus \mathbb{Z}\langle G\rangle \oplus L \oplus L^{\otimes 2} \oplus L^{\otimes 3} \oplus \dots$$

("extended" because we extend the usual notion to include negative exponents $L^{\otimes(-m)}$). Each $L^{\otimes i}$ is an invertible G-lattice, and represents $[L]^i$. For simplicity, we denote $L^{\otimes i}$ by L^i. The ring structure on Λ is defined as the ring structure on the tensor algebra, supplemented with the lifted inner product $\cdot$. The following result is straightforward.

Proposition 3.13. (i) *Λ is a commutative ring containing $\mathbb{Z}\langle G\rangle$ as a subring;*

(ii) *the action of G on L becomes multiplication in Λ, and likewise for the action of G on $\overline{L}$;*

(iii) *Λ has an involution $x \mapsto \overline{x}$ extending both the involution of $\mathbb{Z}\langle G\rangle$ and the map $L \xrightarrow{\sim} \overline{L}$;*

(iv) *the lifted inner product $\cdot : L \times \overline{L} \to \mathbb{Z}\langle G\rangle$ becomes multiplication in Λ;*

(v) *if $e \in L$ is short, then $\overline{e} = e^{-1}$ in Λ and $\Lambda = \mathbb{Z}\langle G\rangle[e, e^{-1}]$.*

All computations in Λ and in $\Lambda/m\Lambda$ will be done with homogeneous elements only, where the set of homogeneous elements of Λ is $\bigcup_{i\in\mathbb{Z}} L^i$.

4. The main ingredients

We give the main results that we will use to prove Theorem 1.1. Fix as before a finite abelian group G of order $2n$ and $u \in G$ of order 2. Let k denote the exponent of G. (The exponent of a group H is the least positive integer k such that $\sigma^k = 1$ for all $\sigma \in H$. The exponent of H divides $|H|$ and has the same prime factors as $|H|$.) For all $m \in \mathbb{Z}_{>1}$, denote by $k(m)$ the exponent of the unit group $(\mathbb{Z}\langle G\rangle/(m))^*$.

Remark 4.1. By Proposition 3.10, the G-isomorphisms $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ are in one-to-one correspondence with the short vectors, and if a short $e \in L$ exists, then the short vectors of L are exactly the $2n$ vectors $\{\sigma e : \sigma \in G\}$. If k is the exponent of G, then $(\sigma e)^k = \sigma^k e^k = e^k$ in Λ. Hence for invertible L, all short vectors in L have the same k-th power $e^k \in \Lambda$. At least philosophically, it is easier to find things that are uniquely determined. We look for e^k first, and then recover e from it.

Proposition 4.2. *There is a deterministic polynomial time algorithm that, given a finite commutative ring R and an R-module M, decides whether M is a free R-module of rank one, and if it is, finds a generator.*

Proof. See the appendix. □

Proposition 4.3. (i) *There is a deterministic polynomial time algorithm that, given G, a G-lattice L, and $m \in \mathbb{Z}_{>0}$, decides whether there exists $e_m \in L$ such that $\{\sigma e_m + mL : \sigma \in G\}$ generates L/mL as an abelian group, and if so, finds one.*

(ii) *There is a deterministic polynomial time algorithm that, given G, u, and a G-lattice L, decides whether L is invertible.*

Proof. For (i), apply Proposition 4.2 with $R = \mathbb{Z}\langle G\rangle/(m)$ and $M = L/mL$.

For (ii), it is easy to check whether $\operatorname{rank}(L) = n$ and whether L is unimodular (check whether the Gram matrix has determinant 1). We need to check Definition 3.4(iii) for all m's in polynomial time. We show that it suffices to check two particular values of m. First take $m = 2$, and use (i) to determine if e_2 exists. If not, output "no". If there is one, use (i) to compute $e_2 \in L$. Then $\mathbb{Z}\langle G\rangle e_2 + 2L = L$, so multiplication by 2 is onto as a map from $L/(\mathbb{Z}\langle G\rangle \cdot e_2)$ to itself. Since $L/(\mathbb{Z}\langle G\rangle \cdot e_2)$ is a finitely generated abelian group, it follows that $L/(\mathbb{Z}\langle G\rangle \cdot e_2)$ is finite of odd order. Let q denote its order. Take an LLL-reduced basis $\{b_i\}_{i=1}^n$ for L. Reducing the coefficients mod 2, we may choose e_2 so that $e_2 = \sum_{i\in T} b_i$ for some $T \subseteq \{1, 2, \ldots, n\}$. By Lemma 3.12 we have $|b_i|^2 \le 2^{n-1}$. Using Hadamard's inequality, we have

$$q = [L : \sum_{\sigma\in S} \mathbb{Z}\cdot\sigma e_2] = \det\big(\sum_{\sigma\in S} \mathbb{Z}\cdot\sigma e_2\big)/\det(L) \le \prod_{\sigma\in S} |\sigma e_2| \le |e_2|^n = |\sum_{i\in T} b_i|^n \le (n\cdot 2^{(n-1)/2})^n < 2^{n^2}$$

so we can compute q in polynomial time. Now apply (i) with $m = q$. If no e_q exists, output "no". If e_q exists, then for *all* $m \in \mathbb{Z}_{>0}$ there exists $e_m \in L$ that generates L/mL as a $\mathbb{Z}\langle G\rangle/(m)$-module, as follows. We can reduce to m being a prime power p^t, since if $\gcd(m, m') = 1$ then $L/mm'L$ is free of rank one over $\mathbb{Z}\langle G\rangle/(mm')$ if and only if L/mL is free of rank one over $\mathbb{Z}\langle G\rangle/(m)$ and $L/m'L$ is free of rank one over $\mathbb{Z}\langle G\rangle/(m')$. We can then use Nakayama's Lemma to reduce to the case $m = p$. If $p \nmid q$, we can take $e_p = e_2$. If $p \mid q$, we can take $e_p = e_q$. □

Proposition 4.4. *There is a deterministic polynomial time algorithm that, given a finite abelian group G of order $2n$ and $u \in G$ of order 2, determines prime powers ℓ and m such that $\ell, m \ge 2^{n/2}+1$ and $\gcd(k(\ell), k(m)) = k$.*

Proof. One can prove that if p is prime and $p \equiv 1 \bmod k$, then $k(p^j) = (p-1)p^{j-1}$, using induction on j and the facts that $(\mathbb{Z}\langle G\rangle/(p^j))^* \supset (\mathbb{Z}/p^j\mathbb{Z})^*$ and the latter group has exponent $(p-1)p^{j-1}$.

We next give an algorithm that, given $n, k \in \mathbb{Z}_{>0}$ with k even, computes $r, s \in \mathbb{Z}_{>0}$ and primes p and q such that $p \equiv q \equiv 1 \bmod k$, and $\gcd((p-1)p^{r-1}, (q-1)q^{s-1}) = k$, and $p^r \ge 2^{n/2}+1$, and $q^s \ge 2^{n/2}+1$. (We can then take $\ell = p^r$ and $m = q^s$.) Try $p = k+1, 2k+1, 3k+1, \ldots$ until the smallest prime $p \equiv 1 \bmod k$ is found. Find the least r such that $p^r \ge 2^{n/2}+1$. Try $q = p+k, p+2k, \ldots$ until the least prime $q \equiv 1 \bmod k$ such that $\gcd((p-1)p, q-1) = k$ is found. Find the smallest s such that $q^s \ge 2^{n/2}+1$.

This algorithm terminates, with correct output, in time $(n+k)^{O(1)}$. The key ingredient for proving this is Heath-Brown's version of Linnik's theorem [7], which implies that the prime p found by the algorithm satisfies $p \le ck^{5.5}$ with an effective constant c. If $p - 1 = k_1k_2$ with every prime divisor of

k_1 also dividing k and with $\gcd(k_2, k) = 1$, then to have $\gcd((p-1)p, q-1) = k$ it suffices to have $q \equiv 2 \bmod p$ and $q \equiv 1 + k \bmod k_1$ and $q \equiv 2 \bmod k_2$. This gives a congruence $q \equiv a \bmod p(p-1)$ for some a. Heath-Brown's version of Linnik's theorem implies that $q \leq c(p^2)^{5.5} \leq c^{12}k^{60.5}$. □

Our prime powers ℓ and m play the roles that in the Gentry-Szydlo paper [6] were played by auxiliary prime numbers $P, P' > 2^{(n+1)/2}$ such that $\gcd(P-1, P'-1) = 2n$. Our $k(\ell)$ and $k(m)$ replace their $P-1$ and $P'-1$, respectively. While the Gentry-Szydlo primes P and P' are found with at best a probabilistic algorithm, we can find ℓ and m in deterministic polynomial time. (Further, the ring elements they work with were required to not be zero divisors modulo P, P' and other small auxiliary primes; we require no analogous condition on ℓ and m, since by Definition 3.4(iii), when L is invertible then for *all* m, the $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$-module L/mL is free of rank one.)

Proposition 4.5. (i) *Suppose L is an integral lattice, $3 \leq m \in \mathbb{Z}$, and $C \in L/mL$. Then C contains at most one element x with $\langle x, x\rangle = 1$.*

(ii) *There is a deterministic polynomial time algorithm that, given a rank n integral lattice L, $m \in \mathbb{Z}$ such that $m \geq 2^{n/2} + 1$, and $C \in L/mL$, finds all $x \in C$ with $\langle x, x\rangle = 1$ (and the number of them is 0 or 1).*

Proof. For (i), suppose $x, y \in C$, $\langle x, x\rangle = \langle y, y\rangle = 1$, and $x \neq y$. Since $x - y \in mL$ and L is an integral lattice, we have

$$m \leq \langle x - y, x - y\rangle^{1/2} \leq \langle x, x\rangle^{1/2} + \langle y, y\rangle^{1/2} = 1 + 1 = 2$$

by the triangle inequality. This contradicts $m \geq 3$, giving (i).

For (ii), using LLL to solve the closest vector problem, one can find (in polynomial time) $y \in C$ such that $\langle y, y\rangle < (2^n - 1)\langle x, x\rangle$ for all $x \in C$. Suppose $x \in C$ with $\langle x, x\rangle = 1$. Since $x, y \in C$, there exists $w \in L$ such that $x - y = mw$. Then

$$m\langle w, w\rangle^{1/2} = \langle x - y, x - y\rangle^{1/2} \leq \langle x, x\rangle^{1/2} + \langle y, y\rangle^{1/2} < (1 + 2^{n/2})\langle x, x\rangle^{1/2} \leq m.$$

Therefore $1 > \langle w, w\rangle^{1/2} \in \mathbb{Z}$, so $w = 0$, and thus $y = x$. Compute $\langle y, y\rangle$. If $\langle y, y\rangle = 1$, output y. If $\langle y, y\rangle \neq 1$, there is no $x \in C$ with $\langle x, x\rangle = 1$. □

The n of [6] is an odd prime, so $k = 2n$ and $\mathbb{Z}\langle G\rangle$ embeds in $\mathbb{Q}(\zeta_n) \times \mathbb{Q}$. Since the latter is a product of only two number fields, the number of zeros of $X^{2n} - v^{2n}$ is at most $(2n)^2$, and the Gentry-Szydlo method for finding v from v^{2n} is sufficiently efficient. If one wants to generalize [6] to the case where n is not prime, then the smallest t such that $\mathbb{Z}\langle G\rangle$ embeds in $F_1 \times \ldots \times F_t$ with number fields F_i can be large. Given ν, the number of zeros of $X^k - \nu$ could be as large as k^t. Finding e such that $\nu = e^k$ then requires a more efficient algorithm, which we attain with Proposition 4.8 below.

An **order** is a commutative ring A whose additive group is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$. We specify an order by saying how to multiply any two vectors in a given basis. Let $\mu(A)$ denote the group of roots of unity in A.

Proposition 4.6. *There is a deterministic polynomial time algorithm that, given an order A, determines a set of generators for $\mu(A)$.*

Proof. The proof is a bit intricate, involving commutative algebra and algorithmic algebraic number theory. A sketch is given in the appendix. □

Proposition 4.7. *Suppose L is an invertible G-lattice, $r \in \mathbb{Z}_{>0}$, and ν is a short vector in the G-lattice L^r. Let $A = \Lambda/(\nu - 1)$. Identifying $\bigoplus_{i=0}^{r-1} L^i \subset \Lambda$ with its image in A, we can view $A = \bigoplus_{i=0}^{r-1} L^i$ as a $\mathbb{Z}/r\mathbb{Z}$-graded ring. Then:*

(i) $G \subseteq \mu(A) \subseteq \bigcup_{i=0}^{r-1} L^i$,

(ii) $\{e \in L : e \cdot \bar{e} = 1\} = \mu(A) \cap L$,

(iii) $|\mu(A)|$ *is divisible by* $2n$ *and divides* $2nr$*, and*
(iv) *there exists* $e \in L$ *for which* $e \cdot \bar{e} = 1$ *if and only if* $|\mu(A)| = 2nr$*.*

Proof. Since the ideal $(\overline{\nu}-1) = (\nu^{-1}-1) = (1-\nu) = (\nu-1)$, the map $a \mapsto \overline{a}$ induces an involution on A. Since the lattice's inner product is symmetric and positive definite, for all ring homomorphisms $\psi : A \to \mathbb{C}$ we have $\psi(\overline{a}) = \overline{\psi(a)}$ for all $a \in A$, and $\bigcap_\psi \ker \psi = 0$. Let $E = \{e \in A : e\overline{e} = 1\}$, a subgroup of A^*.

Suppose $e \in \mu(A)$. Then for all ring homomorphisms $\psi : A \to \mathbb{C}$ we have $1 = \psi(e)\overline{\psi(e)} = \psi(e)\psi(\overline{e}) = \psi(e\overline{e})$, so $e\overline{e} = 1$. Thus, $\mu(A) \subseteq E$.

Conversely, suppose $e \in E$. Write $e = \sum_{i=0}^{r-1} \varepsilon_i$ with $\varepsilon_i \in L^i$, so $\overline{e} = \sum_{i=0}^{r-1} \overline{\varepsilon}_i$ with $\overline{\varepsilon}_i \in L^{-i} = L^{r-i}$ in A. We have $1 = e\overline{e} = \sum_{i=0}^{r-1} \varepsilon_i\overline{\varepsilon}_i$ (the degree 0 piece of $e\overline{e}$). Applying the map t of Definition 2.9 and using (1) we have $1 = \sum_{i=0}^{r-1} \langle \varepsilon_i, \varepsilon_i \rangle$. It follows that there exists j such that $\langle \varepsilon_j, \varepsilon_j \rangle = 1$, and $\varepsilon_i = 0$ if $i \neq j$. Thus, $E \subseteq \bigcup_{i=0}^{r-1} \{e \in L^i : \langle e, e \rangle = 1\}$, giving (i). By Proposition 3.9(iii) and Example 3.8 we have $E \cap \mathbb{Z}\langle G \rangle = G$, so $\mu(\mathbb{Z}\langle G \rangle) = G$.

The degree map from E to $\mathbb{Z}/r\mathbb{Z}$ that takes $e \in E$ to j such that $e \in L^j$ is a group homomorphism with kernel $E \cap \mathbb{Z}\langle G \rangle = G$. Therefore, $|E|$ divides $|G| \cdot |\mathbb{Z}/r\mathbb{Z}| = 2nr$. Thus, $E \subseteq \mu(A) \subseteq E$, so $E = \mu(A)$ and we have (ii,iii). The degree map is surjective if and only if $|\mu(A)| = 2nr$, and if and only if 1 is in the image, i.e., if and only if $\mu(A) \cap L \neq \emptyset$. Part (iv) now follows from (ii). □

Proposition 4.8. *There is a deterministic polynomial time algorithm that, given* G *of exponent* k*, an invertible* G*-lattice* L*, and* $\nu \in L^k$*, determines whether there exists* $e \in L$ *such that* $\nu = e^k$ *and* $e \cdot \bar{e} = 1$*, and if so, finds one.*

Proof. Check whether $\nu\overline{\nu} = 1$. If so, let $A = \Lambda/(\nu - 1)$ and apply Proposition 4.6 to compute generators for $\mu(A)$. Using Proposition 4.7 with $r = k$, apply the degree map $\mu(A) \to \mathbb{Z}/k\mathbb{Z}$ to the generators, check whether the images generate $\mathbb{Z}/k\mathbb{Z}$, and if they do, compute an element $e \in \mu(A)$ whose image is 1. Then $e \in \mu(A) \cap L = \{e \in L : e \cdot \bar{e} = 1\}$. Check whether $\nu = e^k$. If any step fails, no such e exists (by Remark 4.1). The algorithm runs in polynomial time since $2nk \leq (2n)^2$. □

5. The Algorithm

We present the main algorithm, followed by a fuller explanation. As before, k is the exponent of the group G and $k(j)$ is the exponent of $(\mathbb{Z}\langle G \rangle/(j))^*$ if $j \in \mathbb{Z}_{>1}$.

Algorithm 5.1. *Input a finite abelian group* G*, an element* $u \in G$ *of order* 2*, and a* G*-lattice* L*. Output a* G*-isomorphism* $\mathbb{Z}\langle G \rangle \xrightarrow{\sim} L$*, or a proof that none exists.*

(i) *Apply Proposition 4.3(ii) to check whether* L *is invertible. If it is not, terminate with "no".*
(ii) *Find* ℓ *and* m *as in Proposition 4.4.*
(iii) *Compute* $e_{\ell m}$ *as in Proposition 4.3(i).*
(iv) *Using an addition chain for* $k(m)$ *and the algorithms mentioned in §3.3, compute the pair* $(L^{k(m)}, e_{\ell m}^{k(m)} + mL^{k(m)})$*. Use Proposition 4.5(ii) to decide whether the coset* $e_{\ell m}^{k(m)} + mL^{k(m)}$ *contains a short vector* $\nu_m \in L^{k(m)}$*, and if so, compute it. Terminate with "no" if none exists.*
(v) *Compute* $s \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G \rangle)^*$ *such that* $\nu_m = s(e_{\ell m}^{k(m)} + \ell L^{k(m)})$ *in* $L^{k(m)}/\ell L^{k(m)}$*.*
(vi) *Use the extended Euclidean algorithm to find* $b \in \mathbb{Z}$ *such that* $bk(m) \equiv k \bmod k(\ell)$*.*
(vii) *Using an addition chain for* k *and the algorithms mentioned in §3.3, compute the pair* $(L^k, e_{\ell m}^k + \ell L^k)$ *and compute* $s^b(e_{\ell m}^k + \ell L^k)$*. Use Proposition 4.5(ii) to decide whether the latter coset contains a short vector* $\nu \in L^k$*, and if so, compute it. Terminate with "no" if none exists.*
(viii) *Apply Proposition 4.8 to find* $e \in L$ *such that* $\nu = e^k$ *and* $e \cdot \bar{e} = 1$ *(or to prove there is no* G*-isomorphism).*

We explain the algorithm in more detail. By Proposition 3.10(iii), the G-lattice L is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if L is invertible and has a short vector. Run the algorithm in Proposition 4.3(ii) to check whether L is invertible. If it is not, terminate with "no". If it is, we look for an $e \in L$ such that $e\bar{e} = 1$. Lattice basis reduction algorithms such as LLL can find fairly short vectors, but they are not nearly short enough for our purpose. We supplement LLL with computations modulo m. Any short e satisfies $\mathbb{Z}\langle G\rangle e = L$, which implies that for all $m \in \mathbb{Z}_{>0}$, the coset $e + mL$ generates L/mL as a $\mathbb{Z}\langle G\rangle/(m)$-module. Proposition 4.3(i) gives another generator e_m. Thus, $e_m = ye$ for some $y \in (\mathbb{Z}\langle G\rangle/(m))^*$. We have $e_m^{k(m)} \bmod m = e^{k(m)} \bmod m$ in $\Lambda/m\Lambda$.

Apply Proposition 4.4 to find prime powers $m, \ell \geq 2^{n/2} + 1$ such that $\gcd(k(\ell), k(m)) = k$. Compute $e_{\ell m}$ (which works as both e_m and e_ℓ) as in Proposition 4.3(i). Proposition 4.5(ii) applied to the coset $e_{\ell m} + mL^{k(m)} \in L^{k(m)}/mL^{k(m)}$ finds a short vector ν_m (if it exists). If $e \in L$ is short, then $\nu_m = e^{k(m)}$ by Proposition 4.5(i).

Since $e_{\ell m}^{k(m)}$ (by definition) and ν_m (by Proposition 3.10(ii)) each generate the $(\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle$-module $L^{k(m)}/\ell L^{k(m)}$, we can find $s \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$ such that $\nu_m = s(e_{\ell m}^{k(m)} + \ell L^{k(m)})$ in $L^{k(m)}/\ell L^{k(m)}$. Since $k = \gcd(k(\ell), k(m))$, we can use the extended Euclidean algorithm to find $a, b \in \mathbb{Z}$ such that $ak(\ell) + bk(m) = k$. Compute $s^b \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$ and $s^b e_{\ell m}^k \in L^k/\ell L^k$ and use Proposition 4.5(ii) to compute a short $\nu \in L^k$ in this coset or prove that none exists. If $e \in L$ is short, then $e^{k(m)} = \nu_m \equiv s e_{\ell m}^{k(m)} \bmod \ell\Lambda$, so $e^k \equiv \nu_m^b (e_{\ell m}^{k(\ell)})^a \equiv s^b e_{\ell m}^k \bmod \ell\Lambda$, so $s^b(e_{\ell m}^k + \ell L^k)$ contains the short vector e^k of L^k, and by Proposition 4.5(i) we have $\nu = e^k$. Proposition 4.8 then finds a short vector $e \in L$, or proves none exists. The map $x \mapsto xe$ gives the desired G-isomorphism from $\mathbb{Z}\langle G\rangle$ to L. This completes the proof of Theorem 1.1.

Remark 5.2. There is a version of the algorithm in which checking invertibility in step (i) is skipped. In this case, the algorithm may misbehave at other points, indicating that L is not invertible and thus not G-isomorphic to $\mathbb{Z}\langle G\rangle$. At the end one would check whether $\langle e, e\rangle = 1$ and $\langle e, \sigma e\rangle = 0$ for all $\sigma \neq 1, u$. If so, then $\{\sigma e\}_{\sigma \in S}$ is an orthonormal basis for L, and $x \mapsto xe$ gives the desired isomorphism; if not, no such isomorphism exists.

References

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

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

[3] C. Gentry, *Fully homomorphic encryption using ideal lattices*, in Proceedings of the 41st ACM Symposium on Theory of Computing—STOC 2009, ACM, New York (2009), 169–178.

[4] C. Gentry, *A fully homomorphic encryption scheme*, Stanford University PhD thesis, 2009, `http://crypto.stanford.edu/craig/craig-thesis.pdf`.

[5] C. Gentry, email, May 9, 2012.

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

[7] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), 265–338.

[8] S. Lang, Algebra, Third edition, Graduate Texts in Mathematics **211**, Springer-Verlag, New York, 2002.

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

[10] 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.

Appendix

See [1] for commutative algebra background.

A.1. **Sketch of proof of Proposition 4.2.** Suppose that A and B are finite commutative rings, that $R \twoheadrightarrow A \times B$ is a surjective ring homomorphism with nilpotent kernel, and that $y_B \in M$ is such that the map $B \to M_B = B \otimes_R M$, $b \mapsto b \otimes y_B$ is an isomorphism. Let I denote the kernel of the natural map $R \to B$ and let N denote the image of IM under the natural map $M \to M_A$.

Initially, take $A = R$, $B = 0$, and $y_B = 0$. As long as $A \neq 0$, do the following. If $N = 0$, stop and output "no". Otherwise, pick $x_A \in IM$ whose image $x \in N$ is nonzero. Compute $\boldsymbol{a} = \mathrm{Ann}_A x$, where Ann_A denotes the annihilator in A. Let $\boldsymbol{b} = \mathrm{Ann}_A \boldsymbol{a}$.

If $\boldsymbol{a} = \boldsymbol{a}^2$, then $A \xrightarrow{\sim} A/\boldsymbol{a} \times A/\boldsymbol{b}$ and $M_A \xrightarrow{\sim} M_{A/\boldsymbol{a}} \times M_{A/\boldsymbol{b}}$. The image of x is of the form $(x', 0)$. If x' does not generate $M_{A/\boldsymbol{a}}$, stop with "no". Otherwise, compute $\beta \in R$ that maps to $(0, 1)$ under the map $R \twoheadrightarrow A \times B$, and replace y_B, B, A by $\beta y_B + x_A$, $(A/\boldsymbol{a}) \times B$, $A/\boldsymbol{b}$, respectively. If $\boldsymbol{a} \neq \boldsymbol{a}^2$, then $\boldsymbol{a} \cap \boldsymbol{b}$ is a nonzero nilpotent ideal, and we replace A by $A/(\boldsymbol{a} \cap \boldsymbol{b})$ and leave y_B unchanged.

When $A = 0$, then I is nilpotent; say $I^r = 0$. Then $By = M_B = M/IM$ for $y = (y_B \mod IM)$. Thus,

$$M = Ry_B + IM = Ry_B + I(Ry_B + IM) = Ry_B + I^2 M = \ldots = Ry_B + I^r M = Ry_B.$$

A.2. **Sketch of proof of Proposition 4.6.** One starts by computing the nilradical N of the $\mathbb{Q}$-algebra $A_{\mathbb{Q}} = A \otimes_{\mathbb{Z}} \mathbb{Q}$ as well as the unique subalgebra $E \subset A_{\mathbb{Q}}$ that maps isomorphically to $A_{\mathbb{Q}}/N$. One has $\mu(A) \subset E$, so replacing A by $A \cap E$ one reduces to the case in which the nilradical of A is 0, which we now assume. Next one determines the set $\mathrm{Spec}(E)$ of prime ideals $\mathfrak{m}$ of E. For each $\mathfrak{m}$ we compute $E/\mathfrak{m}$, which is an algebraic number field, and we also compute its subring $A/(\mathfrak{m} \cap A)$. One has $E \cong \prod_{\mathfrak{m} \in \mathrm{Spec}(E)} E/\mathfrak{m}$, and we identify A with a subring of finite additive index in the product ring $B = \prod_{\mathfrak{m} \in \mathrm{Spec}(E)} A/(\mathfrak{m} \cap A)$.

For each prime number p dividing $|\mu(A)|$ one has $p \leq 1 + \dim_{\mathbb{Q}} E$, so it will suffice to find, for each such p, a set of generators for the p-primary component $\mu(A)_p$ of $\mu(A)$. Fix now a prime number $p \leq 1 + \dim_{\mathbb{Q}} E$.

Since each $A/(\mathfrak{m} \cap A)$ is contained in a number field, $\mu(A/(\mathfrak{m} \cap A))_p$ is cyclic and easy to determine. This leads to a set of generators for $\mu(B)_p$.

Compute $C = \{x \in B : p^i x \in A \text{ for some } i \in \mathbb{Z}_{\geq 0}\}$; this is a subring of B containing A. The group C/A is finite of p-power order, and the group B/C is finite of order not divisible by p. We make $\mathrm{Spec}(E)$ into the set of vertices of a graph by connecting $\mathfrak{m}, \mathfrak{n} \in \mathrm{Spec}(E)$ with an edge if and only if $(\mathfrak{m} \cap C) + (\mathfrak{n} \cap C) \neq C$. For each connected component V of this graph, determine the image C_V of C in the product ring $\prod_{\mathfrak{m} \in V} A/(\mathfrak{m} \cap A)$. Then one can show that one has $C \cong \prod_V C_V$, with V ranging over the connected components, so that $\mu(C)_p \cong \prod_V \mu(C_V)_p$. In addition, one can show that for each V and each $\mathfrak{m} \in V$ the natural map $\mu(C_V)_p \to \mu(A/(\mathfrak{m} \cap A))_p$ is *injective*, so that $\mu(C_V)_p$ is cyclic; the proof also leads to an efficient algorithm for computing $\mu(C_V)_p$. Thus, at this point one knows a set of generators for $\mu(C)_p$.

To pass from $\mu(C)_p$ to $\mu(A)_p$, one starts by computing the intersection $\mathbf{r}$ of all maximal ideals of C that contain p, as well as $\mathbf{s} = \mathbf{r} \cap A$. One has $\mu(C)_p \subset 1 + \mathbf{r}$ and $\mu(A)_p = \mu(C)_p \cap (1 + \mathbf{s})$. To compute the latter intersection, one determines $t \in \mathbb{Z}_{>0}$ with $p^t C \subset A$ as well as a presentation for the finite abelian p-group $1 + (\mathbf{r}/p^t C)$, which is a subgroup of the unit group $(C/p^t C)^*$; to do this, one uses that $\mathbf{r}/p^t C$ is a nilpotent ideal of $C/p^t C$. The group $\mu(A)_p$ is now obtained as the kernel of the natural map $\mu(C)_p \to (1 + (\mathbf{r}/p^t C))/(1 + (\mathbf{s}/p^t C))$.

Mathematisch Instituut, Universiteit Leiden, The Netherlands
E-mail address: hwl@math.leidenuniv.nl

Department of Mathematics, University of California, Irvine, CA 92697
E-mail address: asilverb@math.uci.edu