LATTICES WITH SYMMETRY

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

Abstract. 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.

1. Introduction

Let G be a finite abelian group and let $u \in G$ be a fixed element of order 2. Define a G-lattice to be an integral lattice L with an action of G on L that preserves the inner product, such that u acts as -1. The *standard* G-lattice is the modified group ring $\mathbb{Z}\langle G\rangle = \mathbb{Z}[G]/(u+1)$, equipped with a natural inner product; we refer to Sections 2, 5, and 6 for more precise definitions. Our main result reads as follows:

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

We call a G-lattice L *invertible* if it is unimodular and 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 (see Definition 9.4 and Theorem 11.1). For example, the standard G-lattice is invertible. The following result is a consequence of Theorem 1.1.

Theorem 1.2. *There is a deterministic polynomial-time algorithm that, given a finite abelian group G equipped with an element of order 2, and invertible G-lattices L and M, decides whether L and M are isomorphic as G-lattices, and if they are, exhibits such an isomorphism.*

Deciding whether two lattices are isomorphic is a notorious problem. Our results show that it admits a satisfactory solution if the lattices are equipped with sufficient structure.

Our algorithms and runtime estimates draw upon an array of techniques from algorithmic algebraic number theory, commutative algebra, lattice basis reduction,

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 and by the Alfred P. Sloan Foundation. 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.

and analytic number theory. We develop techniques from commutative algebra that have not yet been fully exploited in the context of cryptology.

An important ingredient to our algorithm is a powerful novel technique that was invented by C. Gentry and M. Szydlo in Section 7 of [4]. We recast their method in the language of commutative algebra, replacing the "polynomial chains" that they used to compute powers of ideals in certain rings by tensor powers of modules. A number of additional changes enabled us to obtain a *deterministic* polynomial-time algorithm, whereas the Gentry-Szydlo algorithm is at best probabilistic.

The technique of Gentry and Szydlo has seen several applications in cryptography, as enumerated in [9]. By placing it in an algebraic framework, we have already been able to generalize the method significantly, replacing the rings $\mathbb{Z}[X]/(X^n-1)$ (with n an odd prime) used by Gentry and Szydlo by the larger class of modified group rings that we defined above, and further extensions appear to be possible. In addition, we hope that our reformulation will make it easier to understand the method and improve upon it. This should help to make it more widely applicable in a cryptographic context.

1.1. **Overview of algorithm proving Theorem 1.1.** The algorithm starts by testing whether the given G-lattice L is *invertible*, which is a necessary condition for being isomorphic to the standard G-lattice. Invertibility is a concept with several attractive properties. For example, it is easy to test. Secondly, every invertible G-lattice has rank $\#G/2$ and determinant 1, and therefore can be specified using a small number of bits (Proposition 3.4 below, and the way it is used to prove Theorem 14.5). Thirdly, an invertible G-lattice L is isomorphic to the standard one if and only if there is a *short* element $e \in L$, that is, an element of length 1.

Accordingly, most of the algorithm consists of looking for short elements in invertible G-lattices, or proving that none exists. The main tool for this is a further property of invertible G-lattices, which concerns *multiplication*. As the name suggests, any invertible G-lattice L has an *inverse* $\overline{L}$, which is also an invertible G-lattice, and any two invertible G-lattices L and M can be *multiplied* using a tensor product operation, which yields again an invertible G-lattice. For example, the product of L and $\overline{L}$ is the standard G-lattice $\mathbb{Z}\langle G\rangle$.

No sequence of multiplications will ever give rise to coefficient blow-up since, as remarked above, every invertible G-lattice can be specified using a small number of bits. It suffices to take the simple precaution of performing a lattice basis reduction after every multiplication (as in Algorithm 15.1). It is a striking consequence that even very high powers L^r of L can be efficiently computed!

Each short element $e \in L$ gives rise to a short element $e^r \in L^r$, which may be thought of as the r-th power of e. If r is well-chosen ($r = k(\ell)$, in the notation of Algorithm 19.1), then e^r will satisfy a congruence condition (modulo ℓ), and if we take ℓ large enough this enables us to determine e^r (or show that no e exists). However, passing directly from e^r to e is infeasible due to the large size of r. Thus, one also finds $e^s \in L^s$ for a second well-chosen large number s ($= k(m)$, in Algorithm 19.1), and a multiplicative combination of e^r and e^s yields $e^{\gcd(r,s)} \in L^{\gcd(r,s)}$. A result from analytic number theory shows that r and s can be chosen such that $\gcd(r,s)$ ($= k$, in Algorithm 19.1) is so small that e, if it exists, can be found from $e^{\gcd(r,s)}$ by a relatively easy root extraction. The latter step requires techniques (Proposition 17.3) of a nature entirely different from those in the present paper, and is therefore delegated to a separate publication [11].

While we believe that the techniques introduced here could lead to practical algorithms, we did not attempt an actual implementation. Also, any choices and recommendations we made were inspired by the desire to give a clean proof of our theorem rather than efficient algorithms.

1.2. **Structure of the paper.** Sections 2–4 contain background on integral lattices. In particular, we derive a new bound for the entries of a matrix describing an automorphism of a unimodular lattice with respect to a reduced basis (Proposition 3.4). Sections 5–7 contain basic material about G-lattices and modified group rings. Important examples of G-lattices are the ideal lattices introduced in Section 8. In Remark 8.6 we explain how to recover the Gentry-Szydlo algorithm from Theorem 1.2. In Sections 9–11 we begin our study of invertible G-lattices, giving several equivalent definitions and an algorithm for recognizing invertibility. Section 12 is devoted to the following pleasing result: a G-lattice is G-isomorphic to the standard one if and only if it is invertible and has a vector of length 1. In Sections 13–14 we show how to multiply invertible G-lattices and we introduce the Witt-Picard group of $\mathbb{Z}\langle G\rangle$, of which the elements correspond to G-isomorphism classes of invertible G-lattices. It has properties reminiscent of the class group in algebraic number theory; in particular, it is a finite abelian group (Theorems 14.2 and 14.5). We also show how to do computations in the Witt-Picard group. In Section 16 we treat the extended tensor algebra Λ, which is in a sense the hero of story: it is a single algebraic structure that comprises all rings and lattices occurring in our main algorithm. Section 17 shows how Λ can be used to assist in finding vectors of length 1. In Section 18 we use Linnik's theorem from analytic number theory in order to find auxiliary numbers in our main algorithm, and our main algorithm is presented in Section 19.

1.3. **Notation.** For the purposes of this paper, commutative rings have an identity element 1, which may be 0. If R is a commutative ring, let R^* denote the group of elements of R that have a multiplicative inverse in R.

2. Integral lattices

We begin with some background on lattices and on lattice automorphisms (see also [8]).

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 a group, L is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{Z}_{\geq 0}$, which is called the **rank** of L and is denoted $\operatorname{rank}(L)$. 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 $\{b_1, \ldots, b_n\}$ and an element of a lattice is specified by its coefficient vector on the same basis. The inner product $\langle\,\cdot\,,\,\cdot\,\rangle$ extends to a real-valued inner product on $L \otimes_{\mathbb{Z}} \mathbb{R}$ and makes $L \otimes_{\mathbb{Z}} \mathbb{R}$ into a Euclidean vector space.

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

Definition 2.3. The determinant $\det(L)$ of a lattice L is the determinant of the Gram matrix of L; equivalently, $\det(L)$ is the order of the cokernel of the map $L \to \mathrm{Hom}(L, \mathbb{Z})$, $x \mapsto (y \mapsto \langle x, y\rangle)$. A lattice L is **unimodular** if this map is bijective, i.e., if $\det(L) = 1$.

Definition 2.4. An **isomorphism** $L \xrightarrow{\sim} M$ of lattices is a group isomorphism φ from L to 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 to itself. The set of automorphisms of L is a finite group $\mathrm{Aut}(L)$ whose center contains -1.

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, we have $\mathrm{Aut}(\mathbb{Z}^n) \cong \{\pm 1\}^n \rtimes S_n$. (The standard basis vectors can be permuted, and signs changed.)
(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.

3. Reduced bases and automorphisms

The main result of this section is Proposition 3.4, in which we obtain some bounds for LLL-reduced bases of unimodular lattices. We will use this result to give bounds on the complexity of our algorithms and to show that the Witt-Picard group (Definition 14.1 below) is finite. If L is a lattice and $a \in L \otimes_{\mathbb{Z}} \mathbb{R}$, let $|a| = \langle a, a\rangle^{1/2}$.

Definition 3.1. If $\{b_1, \ldots, b_n\}$ is a basis for a lattice L, and $\{b_1^*, \ldots, b_n^*\}$ 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 $\{b_1, \ldots, b_n\}$ is **LLL-reduced** if

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

Remark 3.2. The LLL basis reduction algorithm [7] takes as input a lattice, and produces an LLL-reduced basis of the lattice, in polynomial time.

Lemma 3.3. *If $a = (\mu_{ij})_{ij} \in \mathrm{M}(n, \mathbb{R})$ is a lower-triangular real matrix with $\mu_{ii} = 1$ for all i and $|\mu_{ij}| \le 1/2$ for all $j < i$, and $a^{-1} = (\nu_{ij})_{ij}$, then*

$$|\nu_{ij}| \le \begin{cases} 0 & \text{if } i < j \\ 1 & \text{if } i = j \\ \frac{1}{3}\left(\frac{3}{2}\right)^{i-j} & \text{if } i > j. \end{cases}$$

Proof. Define $e \in \mathrm{M}(n,\mathbb{R})$ by $e_{ij} = 0$ if $j \geq i$ and $e_{ij} = \frac{1}{2}$ if $j < i$. Define $h \in \mathrm{M}(n,\mathbb{R})$ by $h_{i+1,i} = 1$ for $i = 1,\dots,n-1$ and $h_{ij} = 0$ otherwise. Then

$$e = \sum_{j=1}^{\infty} \frac{1}{2} h^j = \frac{h}{2(1-h)}.$$

Thus, $1 - e = (1 - 3h/2)/(1-h)$ and

$$\begin{aligned}(1-e)^{-1} &= (1-h)/(1-3h/2) \\ &= (1-h)\sum_{j=0}^{\infty} \left(\frac{3}{2}\right)^j h^j = \sum_{j=0}^{\infty} \left(\frac{3}{2}\right)^j h^j - \sum_{j=0}^{\infty} \left(\frac{3}{2}\right)^j h^{j+1} = \\ &\begin{pmatrix} 1 & 0 & \cdots & 0 \\ \frac{3}{2} & 1 & \cdots & 0 \\ (\frac{3}{2})^2 & \frac{3}{2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ (\frac{3}{2})^{n-1} & (\frac{3}{2})^{n-2} & \cdots & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ \frac{3}{2} & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ (\frac{3}{2})^{n-2} & (\frac{3}{2})^{n-3} & \cdots & \frac{3}{2} & 1 & 0 \end{pmatrix},\end{aligned}$$

which has ij entry 0 if $i < j$, and 1 if $i = j$, and $\frac{1}{3}\left(\frac{3}{2}\right)^{i-j}$ if $i > j$.

Since $e^n = 0 = (1-a)^n$, we have

$$(1-e)^{-1} = \sum_{i=0}^{n-1} e^i \quad \text{and} \quad a^{-1} = \sum_{i=0}^{n-1} (1-a)^i.$$

If $c = (c_{ij})_{ij} \in \mathrm{M}(n,\mathbb{R})$, let $|c|$ denote $(|c_{ij}|)_{ij}$. If $c, d \in \mathrm{M}(n,\mathbb{R})$, then $c \leq d$ means that $c_{ij} \leq d_{ij}$ for all i and j. We have

$$|a^{-1}| \leq \sum_{i=0}^{n-1} |1-a|^i \leq \sum_{i=0}^{n-1} e^i = (1-e)^{-1}.$$

This gives the desired result. □

Proposition 3.4. *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*

(i) $2^{1-i} \leq |b_i^*|^2 \leq 2^{n-i}$,
(ii) $|b_i|^2 \leq 2^{n-1}$ *for all* $i \in \{1,\dots,n\}$,
(iii) $|\langle b_i, b_j\rangle| \leq 2^{n-1}$ *for all* i *and* j,
(iv) *if* $\sigma \in \mathrm{Aut}(L)$, *and for each* i *we have* $\sigma(b_i) = \sum_{j=1}^{n} a_{ij} b_j$ *with* $a_{ij} \in \mathbb{Z}$, *then* $|a_{ij}| \leq 3^{n-1}$ *for all* i *and* j.

Proof. It follows from Definition 3.1 that for all $1 \leq j \leq i \leq n$ we have $|b_i^*|^2 \leq 2^{j-i}|b_j^*|^2$, so for all i we have

$$2^{1-i}|b_1^*|^2 \leq |b_i^*|^2 \leq 2^{n-i}|b_n^*|^2.$$

Since L is integral we have

$$|b_1^*|^2 = |b_1|^2 = \langle b_1, b_1\rangle \geq 1,$$

so $|b_i^*|^2 \geq 2^{1-i}$. Letting $L_i = \sum_{j=1}^{i} \mathbb{Z} b_j$, we have

$$|b_i^*| = \det(L_i)/\det(L_{i-1}).$$

Since L is integral and unimodular, we have

$$|b_n^*| = \det(L_n)/\det(L_{n-1}) = 1/\det(L_{n-1}) \leq 1,$$

so $|b_i^*|^2 \leq 2^{n-i}$, giving (i).

Since $\{b_i^*\}$ is orthogonal we have

$$\begin{aligned} |b_i|^2 = |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2 &\leq 2^{n-i} + \frac{1}{4} \sum_{j=1}^{i-1} 2^{n-j} \\ &= 2^{n-i} + (2^{n-2} - 2^{n-i-1}) = 2^{n-2} + 2^{n-i-1} \leq 2^{n-1}, \end{aligned}$$

giving (ii). Now (iii) follows by applying the Cauchy-Schwarz inequality $|\langle b_i, b_j \rangle| \leq |b_i||b_j|$ and (ii).

For (iv), define $\{c_1, \ldots, c_n\}$ to be the basis of L that is dual to $\{b_1, \ldots, b_n\}$, i.e., $\langle c_i, b_j \rangle = \delta_{ij}$ for all i and j, where δ_{ij} is the Kronecker delta symbol. Then $a_{ij} = \langle c_j, \sigma(b_i) \rangle$ so

$$|a_{ij}| \leq |c_j||\sigma(b_i)| = |c_j||b_i|. \tag{3.1}$$

Define $\mu_{ii} = 1$ for all i and $\mu_{ij} = 0$ if $i < j$, and let

$$M = (\mu_{ij})_{ij} \in \mathrm{M}(n, \mathbb{R}).$$

Then

$$(b_1 \ b_2 \ \cdots \ b_n) = (b_1^* \ b_2^* \ \cdots \ b_n^*) M^t.$$

For $0 \neq x \in L \otimes_{\mathbb{Z}} \mathbb{R}$, define

$$x^{-1} = \frac{x}{\langle x, x \rangle}.$$

This inverse map is characterized by the properties that $\langle x, x^{-1} \rangle = 1$ and $\mathbb{R}x^{-1} = \mathbb{R}x$; so $(x^{-1})^{-1} = x$. Since the basis dual to $\{b_i^*\}_i$ is $\{(b_i^*)^{-1}\}_i$, and M gives the change of basis from $\{b_i^*\}_i$ to $\{b_i\}_i$, it follows that the matrix $(M^t)^{-1}$ gives the change of basis from $\{(b_i^*)^{-1}\}_i$ to $\{c_i\}_i$. Thus,

$$(c_1 \ \cdots \ c_n) = ((b_1^*)^{-1} \ \cdots \ (b_n^*)^{-1}) M^{-1}.$$

Letting $(\nu_{ij})_{ij} = M^{-1}$, by Lemma 3.3 we have

$$c_j = \sum_{i \geq j} (b_i^*)^{-1} \nu_{ij}$$

with $\nu_{ii} = 1$ and $|\nu_{ij}| \leq \frac{1}{3} \left(\frac{3}{2}\right)^{i-j}$ if $i > j$. By (i) we have

$$|(b_i^*)^{-1}|^2 \leq 2^{i-1}.$$

Thus,

$$\begin{aligned}
|c_j|^2 &\le \sum_{i\ge j} 2^{i-1}\nu_{ij}^2 \\
&\le 2^{j-1} + \frac{1}{9}\sum_{i>j} 2^{i-1}\left(\frac{9}{4}\right)^{i-j} \\
&\le 2^{j-1} + \frac{2^{j-1}}{9}\sum_{k=1}^{n-j}\left(\frac{9}{2}\right)^{k} \\
&= 2^{j-1} + \frac{2^j}{63}\left[\left(\frac{9}{2}\right)^{n-j+1} - \frac{9}{2}\right] \\
&= \frac{2^{j-1}}{7}\left[\left(\frac{9}{2}\right)^{n-j} + 6\right] \\
&\le \frac{1}{7}\left(\frac{9}{2}\right)^{n-1} + \frac{6}{7}\left(\frac{9}{2}\right)^{n-1} = \left(\frac{9}{2}\right)^{n-1}.
\end{aligned}$$

Now by (ii) and (3.1) we have $|a_{ij}|^2 \le 9^{n-1}$, as desired. □

Remark 3.5. It is easier to get the weaker bound $|a_{ij}| \le 2^{\binom{n}{2}}$, as follows. Write $b_j = b_j^{\#} + y$ with $y \in \sum_{i\ne j}\mathbb{R}b_i$ and $b_j^{\#}$ orthogonal to $\sum_{i\ne j}\mathbb{R}b_i$. With c_j as in the proof of Proposition 3.4, we have $c_j = (b_j^{\#})^{-1}$, by the characterizations of $(b_j^{\#})^{-1}$ and c_j. Since

$$1 = \det(L) = \det(\sum_{i\ne j}\mathbb{Z}b_i)|b_j^{\#}|$$

we have

$$|c_j| = |\det(\sum_{i\ne j}\mathbb{Z}b_i)| \le \prod_{i\ne j}|b_i| \le 2^{(n-1)^2/2}$$

by Hadamard's inequality and Proposition 3.4(ii). By (3.1) and Proposition 3.4(ii) we have $|a_{ij}| \le 2^{\binom{n}{2}}$.

4. Short vectors in lattice cosets

We show how to find the unique vector of length 1 in a suitable lattice coset, when such a vector exists.

Proposition 4.1. *Suppose L is an integral lattice, $3 \le m \in \mathbb{Z}$, and $C \in L/mL$. Then the coset C contains at most one element $x \in L$ with $\langle x, x\rangle = 1$.*

Proof. Suppose $x, y \in C$, with $\langle x, x\rangle = \langle y, y\rangle = 1$. Since $x, y \in C$, there exists $w \in L$ such that $x - y = mw$. Using the triangle inequality, we have

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

Since $m \ge 3$ and $\langle w, w\rangle \in \mathbb{Z}_{\ge 0}$, we have $w = 0$, and thus $y = x$. □

Algorithm 4.2. Given a rank n integral lattice L, an integer m such that $m \ge 2^{n/2} + 1$, and $C \in L/mL$, the algorithm computes all $y \in C$ with $\langle y, y\rangle = 1$.

(i) Compute an LLL-reduced basis for mL and use it as in §10 of [8] 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., to find an approximate solution to the nearest vector problem.
(ii) Compute $\langle y, y\rangle$.
(iii) If $\langle y, y\rangle = 1$, output y.
(iv) If $\langle y, y\rangle \neq 1$, output "there is no $y \in C$ with $\langle y, y\rangle = 1$".

Proposition 4.3. *Algorithm 4.2 is a deterministic polynomial-time algorithm that, given a integral lattice L, an integer m such that $m \geq 2^{n/2} + 1$ where $n = \operatorname{rank}(L)$, and $C \in L/mL$, outputs all $y \in C$ with $\langle y, y\rangle = 1$. The number of such y is 0 or 1.*

Proof. Suppose $x \in C$ with $\langle x, x\rangle = 1$. Since $x, y \in C$, there exists $w \in L$ such that $x - y = mw$. Using the triangle inequality, we have

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

so $\langle w, w\rangle^{1/2} < 1$. Since $\langle w, w\rangle \in \mathbb{Z}_{\geq 0}$, we have $w = 0$, and thus $y = x$. If $\langle y, y\rangle \neq 1$, there is no $x \in C$ with $\langle x, x\rangle = 1$. □

5. G-lattices

We introduce G-lattices and G-isomorphisms. From now on, suppose that G is a finite abelian group equipped with a fixed element u of order 2, and that $n = \#G/2 \in \mathbb{Z}$.

Definition 5.1. 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 $1 \in S$.

Definition 5.2. A **G-lattice** is a lattice L together with a group homomorphism $f : G \to \operatorname{Aut}(L)$ 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 5.3. 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.

6. 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 $A = \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Q}$ and $\mathbb{C}$.

If H is a group and A is a commutative ring, the group ring $A[H]$ is the set of formal sums $\sum_{\sigma\in H} a_\sigma\sigma$ with $a_\sigma \in A$, with addition defined by

$$\sum_{\sigma\in H} a_\sigma\sigma + \sum_{\sigma\in H} b_\sigma\sigma = \sum_{\sigma\in H} (a_\sigma + b_\sigma)\sigma$$

and multiplication defined by

$$(\sum_{\sigma\in H} a_\sigma\sigma)(\sum_{\tau\in H} b_\tau\tau) = \sum_{\rho\in H} (\sum_{\sigma\tau=\rho} a_\sigma b_\tau)\rho.$$

For example, if H is a cyclic group of order m and h is a generator, then as rings we have

$$\mathbb{Z}[X]/(X^m - 1) \cong \mathbb{Z}[H]$$

via the map

$$\sum_{i=0}^{m-1} a_i X^i \mapsto \sum_{i=0}^{m-1} a_i h^i.$$

Definition 6.1. 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 L is a $\mathbb{Z}\langle G\rangle$-module, where one uses the G-action on L to define ax whenever $x \in L$ and $a \in \mathbb{Z}\langle G\rangle$. This is why we consider $A\langle G\rangle$ rather than the standard group ring $A[G]$. Considering groups equipped with an element of order 2 allows us to include the cyclotomic rings $\mathbb{Z}[X]/(X^{2^k}+1)$ in our theory.

Definition 6.2. Define the **scaled trace function** $t : A\langle G\rangle \to A$ by

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

This is well defined since the restriction of t to $(u+1)A[G]$ is 0. The map t is the A-linear map satisfying $t(1) = 1$, $t(u) = -1$, and $t(\sigma) = 0$ if $\sigma \in G$ and $\sigma \neq 1, u$.

Definition 6.3. 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 ring automorphism that is its own inverse.) One can think of this map as mimicking complex conjugation (cf. Lemma 7.3(i)).

Remark 6.4. If L is a G-lattice and $x, y \in L$, then

$$\langle \sigma x, \sigma y\rangle = \langle x, y\rangle$$

for all $\sigma \in G$ by Definition 2.4. It follows that

$$\langle ax, y\rangle = \langle x, \overline{a} y\rangle$$

for all $a \in \mathbb{Z}\langle G\rangle$. This "hermitian" property of the inner product is the main reason for introducing the involution.

Definition 6.5. For $x, y \in \mathbb{Z}\langle G\rangle$ define $\langle x, y\rangle_{\mathbb{Z}\langle G\rangle} = t(x\overline{y})$.

Recall that $n = \#G/2$ and S is a set of coset representatives of $G/\langle u\rangle$. The following two results are straightforward.

Lemma 6.6. *Suppose A is a commutative ring. Then:*

(i) $A\langle G\rangle = \{\sum_{\sigma\in S} a_\sigma \sigma : a_\sigma \in A\} = \bigoplus_{\sigma\in S} A\sigma$;
(ii) *if $a = \sum_{\sigma\in S} a_\sigma \sigma \in A\langle G\rangle$, then*
  (a) $t(a) = a_1$,
  (b) $t(\overline{a}) = t(a)$,
  (c) $t(a\overline{a}) = \sum_{\sigma\in S} a_\sigma^2$,
  (d) $a = \sum_{\sigma\in S} t(\sigma^{-1}a)\sigma$,

(e) *if* $t(ab) = 0$ *for all* $b \in A\langle G\rangle$, *then* $a = 0$.

Proposition 6.7. (i) *The additive group of the ring* $\mathbb{Z}\langle G\rangle$ *is a* G*-lattice of rank* n, *with lattice structure defined by* $\langle\,\cdot\,,\,\cdot\,\rangle_{\mathbb{Z}\langle G\rangle}$ *and* G*-action defined by* $\sigma x = \sigma x$ *where the right hand side is ring multiplication in* $\mathbb{Z}\langle G\rangle$.

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

Definition 6.8. We call $\mathbb{Z}\langle G\rangle$ the **standard** G**-lattice**.

The set S of coset representatives for $G/\langle u\rangle$ is an orthonormal basis for the standard G-lattice.

Example 6.9. 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, sending X to $-X$, we have

$$\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[X]/(X^n - 1) \cong \mathbb{Z}[X]/(X^n + 1).$$

Example 6.10. If G is cyclic, then $\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[X]/(X^n + 1)$, identifying X with a generator of G. If G is cyclic of order 2^r, then

$$\mathbb{Z}\langle G\rangle \cong \mathbb{Z}[X]/(X^{2^{r-1}} + 1) \cong \mathbb{Z}[\zeta_{2^r}],$$

where ζ_{2^r} is a primitive 2^r-th root of unity.

Remark 6.11. The ring $\mathbb{Z}\langle G\rangle$ is an integral domain if and only if G is cyclic and n is a power of 2 (including $2^0 = 1$). (If $g \in G$ is an element whose order is odd or 2, and $g \notin \{1, u\}$, then $g - 1$ is a zero divisor.)

7. The modified group ring over fields

The main result of this section is Lemma 7.3, which we will use repeatedly in the rest of the paper. Recall that G is a finite abelian group of order $2n$ equipped with an element u of order 2. If R is a commutative ring, then a commutative R-algebra is a commutative ring A equipped with a ring homomorphism from R to A.

If K is a subfield of $\mathbb{C}$ and E is a commutative K-algebra with $\dim_K(E) < \infty$, let Φ_E denote the set of K-algebra homomorphisms from E to $\mathbb{C}$. Then $\mathbb{C}^{\Phi_E}$ is a $\mathbb{C}$-algebra with coordinate-wise operations. The next result is not only useful for studying modified group rings, but also comes in handy in Proposition 16.2 below.

Lemma 7.1. *Suppose* K *is a subfield of* $\mathbb{C}$ *and* E *is a commutative* K*-algebra with* $\dim_K(E) < \infty$. *Assume* $\#\Phi_E = \dim_K(E)$. *Then:*

(i) *identifying* Φ_E *with*

$$\{\mathbb{C}\text{-algebra homomorphisms } E_{\mathbb{C}} = \mathbb{C} \otimes_K E \to \mathbb{C}\},$$

the map $E_{\mathbb{C}} \to \mathbb{C}^{\Phi_E}$, $x \mapsto (\varphi(x))_{\varphi\in\Phi_E}$ *is an isomorphism of* $\mathbb{C}$*-algebras;*

(ii) $\bigcap_{\varphi\in\Phi_E} \ker(\varphi) = 0$ *in* E;

(iii) *there is a finite collection* $\{K_j\}_{j=1}^d$ *of finite extension fields of* K *such that*

$$E \cong K_1 \times \cdots \times K_d$$

as K*-algebras.*

Proof. By the Corollaire to Proposition 1 in V.6.3 of [2], the set Φ_E is a $\mathbb{C}$-basis for $\mathrm{Hom}_K(E,\mathbb{C}) = \mathrm{Hom}_{\mathbb{C}}(E_{\mathbb{C}},\mathbb{C})$, so the $\mathbb{C}$-algebra homomorphism in (i) is an isomorphism. Part (ii) follows immediately from (i).

By Proposition 2 in V.6.3 of [2], the K-algebra E is what Bourbaki calls an étale K-algebra, and (iii) then follows from Theorem 4 in V.6.7 of [2]. □

Definition 7.2. Let Ψ denote the set of ring homomorphisms from $\mathbb{Q}\langle G\rangle$ to $\mathbb{C}$. We identify Ψ with the set of K-algebra homomorphisms from $K\langle G\rangle$ to $\mathbb{C}$, where K is any subfield of $\mathbb{C}$. The set Ψ can also be identified with the set of group homomorphisms $\psi : G \to \mathbb{C}^*$ such that $\psi(u) = -1$.

We have $\#\Psi = n$, since $\#\mathrm{Hom}(G,\mathbb{C}^*) = \#G = 2n$ and the restriction map $\mathrm{Hom}(G,\mathbb{C}^*) \to \mathrm{Hom}(\langle u\rangle,\mathbb{C}^*)$ is surjective. This allows us to apply Lemma 7.1 with $E = K\langle G\rangle$. If $a \in \mathbb{C}\langle G\rangle$, then a acts on the $\mathbb{C}$-vector space $\mathbb{C}\langle G\rangle$ by multiplication, and for $\psi \in \Psi$ the $\psi(a)$ are the eigenvalues for this linear transformation. Lemma 7.3(ii) justifies thinking of the map t of Definition 6.2 as a scaled trace function.

Lemma 7.3. (i) *If $\psi \in \Psi$, then $\overline{\psi(\alpha)} = \psi(\bar{\alpha})$ for all $\alpha \in \mathbb{R}\langle G\rangle$.*

(ii) *If $a \in \mathbb{C}\langle G\rangle$, then $t(a) = \frac{1}{n}\sum_{\psi\in\Psi}\psi(a)$.*

(iii) *If K is a subfield of $\mathbb{C}$, then $\bigcap_{\psi\in\Psi}\ker(\psi) = 0$ in $K\langle G\rangle$.*

(iv) *The map $\mathbb{C}\langle G\rangle \to \mathbb{C}^{\Psi}$, $x \mapsto (\psi(x))_{\psi\in\Psi}$ is an isomorphism of $\mathbb{C}$-algebras.*

(v) *There are number fields $K_1,\dots,K_d$ such that*

$$\mathbb{Q}\langle G\rangle \cong K_1 \times \cdots \times K_d$$

as $\mathbb{Q}$-algebras.

(vi) *Suppose K is a subfield of $\mathbb{C}$ and $\alpha \in K\langle G\rangle$. Then $\alpha \in K\langle G\rangle^*$ if and only if $\psi(\alpha) \neq 0$ for all $\psi \in \Psi$.*

(vii) *If $z \in \mathbb{R}\langle G\rangle$ is such that $\psi(z) \in \mathbb{R}$ for all $\psi \in \Psi$ and $\sum_{\psi\in\Psi}\psi(x\overline{x}z) \geq 0$ for all $x \in \mathbb{R}\langle G\rangle$, then $\psi(z) \geq 0$ for all $\psi \in \Psi$.*

Proof. For (i), since G is finite, $\psi(\sigma)$ is a root of unity for all $\sigma \in G$. Thus,

$$\overline{\psi(\sigma)} = \psi(\sigma)^{-1} = \psi(\sigma^{-1}) = \psi(\bar{\sigma}).$$

The $\mathbb{R}$-linearity of ψ and of $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ now imply (i).

We have

$$\frac{1}{n}\sum_{\psi\in\Psi}\psi(1) = 1 = t(1),$$

and

$$\frac{1}{n}\sum_{\psi\in\Psi}\psi(u) = -1 = t(u),$$

and for each $\sigma \notin \langle u\rangle$ we have

$$\sum_{\psi\in\Psi}\psi(\sigma) = -\sum_{\substack{\psi\in\mathrm{Hom}(G,\mathbb{C}^*)\\ \psi(u)=1}}\psi(\sigma) = -\sum_{\psi\in\mathrm{Hom}(G/\langle u\rangle,\mathbb{C}^*)}\psi(\sigma \bmod \langle u\rangle) = 0 = nt(\sigma).$$

Extending $\mathbb{C}$-linearly gives (ii).

If K is a subfield of $\mathbb{C}$, then $\#\Psi = n = \dim_K K\langle G\rangle$. Thus we can apply Lemma 7.1, giving (iii), (iv), and (v).

By (iv) we have $\mathbb{C}\langle G\rangle^* \xrightarrow{\sim} (\mathbb{C}^*)^\Psi$. This gives (vi) when $K = \mathbb{C}$. If K is a subfield of $\mathbb{C}$ and $x \in K\langle G\rangle \cap \mathbb{C}\langle G\rangle^*$ then multiplication by x is an injective map from $K\langle G\rangle$ to itself, so is also surjective, so $x \in K\langle G\rangle^*$. Thus

$$K\langle G\rangle^* = K\langle G\rangle \cap \mathbb{C}\langle G\rangle^*,$$

and (vi) follows.

For (vii), applying Lemma 7.1(iii) with $K = \mathbb{R}$ gives an $\mathbb{R}$-algebra isomorphism

$$\mathbb{R}\langle G\rangle \xrightarrow{\sim} \mathbb{R}^r \times \mathbb{C}^s.$$

The set $\Psi = \{\psi_j\}_{j=1}^{r+2s}$ consists of the r projection maps $\psi_j : \mathbb{R}\langle G\rangle \to \mathbb{R} \subset \mathbb{C}$ for $1 < j \le r$, along with the s projection maps $\psi_j : \mathbb{R}\langle G\rangle \to \mathbb{C}$ and their complex conjugates $\psi_{s+j} = \overline{\psi_j}$ for $r+1 \le j \le r+s$. By (i), if

$$x = (x_1, \dots, x_r, y_1, \dots, y_s) \in \mathbb{R}^r \times \mathbb{C}^s,$$

then

$$\overline{x} = (x_1, \dots, x_r, \overline{y_1}, \dots, \overline{y_s}).$$

Taking x to have 1 in the j-th position and 0 everywhere else, we have

$$0 \le \sum_{\psi\in\Psi} \psi(x\overline{x}z) = \begin{cases} \psi_j(z) & \text{if } 1 \le j \le r \\ 2\psi_j(z) & \text{otherwise,} \end{cases}$$

giving (vii). □

8. Ideal lattices

As before, G is a finite abelian group of order $2n$ equipped with an element u of order 2. Theorem 8.2 below gives a way to view certain ideals I in $\mathbb{Z}\langle G\rangle$ as G-lattices, and Theorem 8.5 characterizes the ones that are G-isomorphic to $\mathbb{Z}\langle G\rangle$.

Definition 8.1. A *fractional $\mathbb{Z}\langle G\rangle$-ideal* is a finitely generated $\mathbb{Z}\langle G\rangle$-module in $\mathbb{Q}\langle G\rangle$ that spans $\mathbb{Q}\langle G\rangle$ over $\mathbb{Q}$. An *invertible* fractional $\mathbb{Z}\langle G\rangle$-ideal is a fractional $\mathbb{Z}\langle G\rangle$-ideal I such that there is a fractional $\mathbb{Z}\langle G\rangle$-ideal J with $IJ = \mathbb{Z}\langle G\rangle$, where IJ is the fractional $\mathbb{Z}\langle G\rangle$-ideal generated by the products of elements from I and J.

Theorem 8.2. *Suppose $I \subset \mathbb{Q}\langle G\rangle$ is a fractional $\mathbb{Z}\langle G\rangle$-ideal and $w \in \mathbb{Q}\langle G\rangle$. Suppose that $I\overline{I} \subset \mathbb{Z}\langle G\rangle \cdot w$ and $\psi(w) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$. Then:*

(i) $\overline{w} = w$;
(ii) $w \in \mathbb{Q}\langle G\rangle^*$;
(iii) *I is a G-lattice, with G-action defined by multiplication in $\mathbb{Q}\langle G\rangle$, 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 6.2.

Proof. By Lemma 7.3(i) we have

$$\psi(w) = \overline{\psi(w)} = \psi(\bar{w})$$

for all $\psi \in \Psi$. Now (i) follows from Lemma 7.3(iii). Lemma 7.3(vi) implies (ii). Note that $\frac{x\overline{y}}{w} \in \mathbb{Z}\langle G\rangle$, since $I\overline{I} \subset \mathbb{Z}\langle G\rangle \cdot w$. Part (iii) now follows from (i) and (ii) of Lemma 7.3. □

Notation 8.3. Let I and w be as in Theorem 8.2. Define $L_{(I,w)}$ to be the G-lattice I with lattice structure defined by $\langle x, y\rangle_{I,w} = t(x\overline{y}/w)$.

Example 8.4. We have $L_{(\mathbb{Z}\langle G\rangle,1)} = \mathbb{Z}\langle G\rangle$.

Theorem 8.5. *Suppose that I_1 and I_2 are fractional $\mathbb{Z}\langle G\rangle$-ideals, that $w_1, w_2 \in \mathbb{Q}\langle G\rangle$, that $I_1\overline{I_1} \subset \mathbb{Z}\langle G\rangle \cdot w_1$ and $I_2\overline{I_2} \subset \mathbb{Z}\langle G\rangle \cdot w_2$, and that $\psi(w_1), \psi(w_2) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$. Let $L_j = L_{(I_j,w_j)}$ for $j = 1, 2$. Then sending v to multiplication by v gives a bijection from*

$$\{v \in \mathbb{Q}\langle G\rangle : I_1 = vI_2, w_1 = v\overline{v}w_2\} \quad \text{to} \quad \{G\text{-isomorphisms } L_2 \xrightarrow{\sim} L_1\}$$

and gives a bijection from

$$\{v \in \mathbb{Q}\langle G\rangle : I_1 = v\mathbb{Z}\langle G\rangle, w_1 = v\overline{v}\} \quad \text{to} \quad \{G\text{-isomorphisms } \mathbb{Z}\langle G\rangle \xrightarrow{\sim} L_1\}.$$

In particular, L_1 is G-isomorphic to $\mathbb{Z}\langle G\rangle$ if and only if there exists $v \in \mathbb{Q}\langle G\rangle$ such that $I_1 = (v)$ and $w_1 = v\overline{v}$.

Proof. Every $\mathbb{Z}\langle G\rangle$-module isomorphism $\varphi : L_2 \xrightarrow{\sim} L_1$ extends to a $\mathbb{Q}\langle G\rangle$-module isomorphism

$$L_2 \otimes \mathbb{Q} = \mathbb{Q}\langle G\rangle \to L_1 \otimes \mathbb{Q} = \mathbb{Q}\langle G\rangle,$$

and any such map is multiplication by some $v \in \mathbb{Q}\langle G\rangle^*$. Conversely, for $v \in \mathbb{Q}\langle G\rangle$, multiplication by v defines a $\mathbb{Z}\langle G\rangle$-module isomorphism from L_2 to L_1 if and only if $I_1 = vI_2$. When $I_1 = vI_2$, multiplication by v is a G-isomorphism from L_2 to L_1 if and only if $w_1 = v\overline{v}w_2$; this follows from Lemma 6.6(ii)(e), since for all $a, b \in I_2$ we have

$$\langle a, b\rangle_{I_2,w_2} = t\left(\frac{a\overline{b}}{w_2}\right) \quad \text{and} \quad \langle av, bv\rangle_{I_1,w_1} = t\left(\frac{a\overline{b}v\overline{v}}{w_1}\right).$$

This gives the first desired bijection. Taking $I_2 = \mathbb{Z}\langle G\rangle$ and $w_2 = 1$ gives the second bijection. □

Remark 8.6. We next show how to recover the Gentry-Szydlo algorithm from Theorem 1.1. The goal of the Gentry-Szydlo algorithm is to find a generator v of a principal ideal I of finite index in the ring $R = \mathbb{Z}[X]/(X^n - 1)$, given $v\overline{v}$ and a $\mathbb{Z}$-basis for I. 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 6.9, 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 in Notation 8.3. Then L is the "implicit orthogonal lattice" in §7.2 of [4]. Once one knows w and a $\mathbb{Z}$-basis for I, then one knows L. Theorem 1.1 produces a G-isomorphism $\varphi : \mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ in polynomial time, and thus (as in Theorem 8.5) gives a generator $v = \varphi(1)$ in polynomial time.

9. Invertible G-lattices

Recall that G is a finite abelian group of order $2n$, with a fixed element u of order 2, and S is a set of coset representatives for $G/\langle u\rangle$. In Definition 9.4 we introduce the concept of an invertible G-lattice. The inverse of such a lattice L is the G-lattice $\overline{L}$ given in Definition 9.1.

Definition 9.1. If L is a G-lattice, then the G-lattice $\overline{L}$ is a lattice equipped with a lattice isomorphism

$$L \xrightarrow{\sim} \overline{L}, \qquad x \mapsto \overline{x}$$

and a group homomorphism $G \to \mathrm{Aut}(\overline{L})$ defined by

$$\sigma\overline{x} = \overline{\sigma^{-1}x}$$

for all $\sigma \in G$ and $x \in L$, i.e.,

$$\overline{\sigma x} = \overline{\sigma}\,\overline{x}.$$

Existence follows by taking $\overline{L}$ to be L with the appropriate G-action. The G-lattice $\overline{L}$ is unique up to G-isomorphism, and we have $\overline{\overline{L}} = L$.

Definition 9.2. If L is a G-lattice, define the **lifted inner product**

$$\cdot : L \times \overline{L} \to \mathbb{Z}\langle G\rangle$$

by

$$x \cdot \overline{y} = \sum_{\sigma\in S} \langle x, \sigma y\rangle \sigma \in \mathbb{Z}\langle G\rangle.$$

This lifted inner product is independent of the choice of the set S, and is $\mathbb{Z}\langle G\rangle$-bilinear; in fact, it extends $\mathbb{Q}$-linearly, and for all $x, y \in L \otimes_{\mathbb{Z}} \mathbb{Q}$ and for all $a \in \mathbb{Q}\langle G\rangle$ we have

$$(ax) \cdot \overline{y} = x \cdot (a\overline{y}) = a(x \cdot \overline{y}), \tag{9.1}$$

$$\langle x, y\rangle = t(x \cdot \overline{y}), \tag{9.2}$$

and $x \cdot \overline{y} = \overline{y \cdot \overline{x}}$.

Example 9.3. If I, w, and $L_{(I,w)}$ are as in Theorem 8.2 and Notation 8.3, then $\overline{L_{(I,w)}} = L_{(\overline{I},w)}$, and applying Lemma 6.6(ii)(d) with $a = \frac{x\overline{y}}{w}$ shows that $x \cdot \overline{y} = \frac{x\overline{y}}{w}$. In particular, if $L = \mathbb{Z}\langle G\rangle$, then $\overline{L} = \mathbb{Z}\langle G\rangle$ with $^-$ having the same meaning as in Definition 6.3 for $A = \mathbb{Z}$, and with $\cdot$ being multiplication in $\mathbb{Z}\langle G\rangle$. Note that when $w \neq 1$, ideals I in $\mathbb{Z}\langle G\rangle$ do not inherit their lifted inner product from that of $\mathbb{Z}\langle G\rangle$.

Definition 9.4. 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.

It is clear from the definition that invertibility is preserved under G-lattice isomorphisms. Definition 9.4 implies 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 9.4 is easy algorithmically; see Algorithm 10.3 below.

Lemma 9.5. *If L is a G-lattice and L is G-isomorphic to the standard G-lattice, then L is invertible.*

Proof. Parts (i) and (ii) of Definition 9.4 are easy. 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. □

10. Determining invertibility

Fix as before a finite abelian group G of order $2n$ equipped with an element u of order 2.

Algorithm 10.3 below determines whether a G-lattice is invertible. In Proposition 10.4 we show that Algorithm 10.3 produces correct output and runs in polynomial time.

In [10] we obtain 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 $R = \mathbb{Z}\langle G\rangle/(m)$ and $M = L/mL$ gives the algorithm in the following result.

Proposition 10.1. *There is a deterministic polynomial-time algorithm that, given G, u, 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 there is, finds one.

Lemma 10.2. *Suppose that L is a G-lattice, $m \in \mathbb{Z}_{>1}$, and $e \in L$. Then:*

(i) *$\{\sigma e + mL : \sigma \in G\}$ generates L/mL as an abelian group if and only if $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is finite of order coprime to m;*
(ii) *if $\operatorname{rank}(L) = n$ and $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is finite, then the map*

$$\mathbb{Z}\langle G\rangle \to \mathbb{Z}\langle G\rangle \cdot e, \qquad a \mapsto ae$$

is an isomorphism of $\mathbb{Z}\langle G\rangle$-modules.

Proof. The set $\{\sigma e + mL : \sigma \in G\}$ generates L/mL as an abelian group if and only if $L = \mathbb{Z}\langle G\rangle e + mL$, and if and only if multiplication by m is surjective as a map from $L/(\mathbb{Z}\langle G\rangle \cdot e)$ to itself. Since $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is a finitely generated abelian group, this holds if and only if $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is finite of order coprime to m. This gives (i).

Now suppose that $\operatorname{rank}(L) = n$ and $L/(\mathbb{Z}\langle G\rangle \cdot e)$ is finite. The map in (ii) is clearly $\mathbb{Z}\langle G\rangle$-linear and surjective. Since $\mathbb{Z}\langle G\rangle$ and $\mathbb{Z}\langle G\rangle e$ both have rank n over $\mathbb{Z}$, the map is injective. □

Algorithm 10.3. Given G, u, and a G-lattice L, the algorithm decides whether L is invertible.

(i) If $\operatorname{rank}(L) \neq n$, output "no" (and stop).
(ii) Compute the determinant of the Gram matrix for L. If it is not 1, output "no" (and stop).

(iii) Use Proposition 10.1 to determine if e_2 (in the notation of Definition 9.4(iii)) exists. If no e_2 exists, output "no" and stop. Otherwise, use Proposition 10.1 to compute $e_2 \in L$.
(iv) Compute the order q of the group $L/(\mathbb{Z}\langle G\rangle \cdot e_2)$.
(v) Use Proposition 10.1 to determine if e_q exists. If no e_q exists, output "no". Otherwise, output "yes".

Proposition 10.4. *Algorithm 10.3 is a deterministic polynomial-time algorithm that, given G, u, and a G-lattice L, decides whether L is invertible.*

Proof. If Step (ii) outputs "no" then L is not unimodular so it is not invertible. We need to check Definition 9.4(iii) for all m's in polynomial time. We show that it suffices to check two particular values of m, namely $m = 2$ and q. By Lemma 10.2(i), the group $L/(\mathbb{Z}\langle G\rangle \cdot e_2)$ is finite of odd order q. If no e_q exists, L is not invertible. 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 1 over $\mathbb{Z}\langle G\rangle/(mm')$ if and only if L/mL is free of rank 1 over $\mathbb{Z}\langle G\rangle/(m)$ and $L/m'L$ is free of rank 1 over $\mathbb{Z}\langle G\rangle/(m')$. Lemma 10.2(i) now allows us to reduce to the case $m = p$. If p does not divide q, we can take $e_p = e_2$. If p divides q, we can take $e_p = e_q$. □

11. Equivalent conditions for invertibility

In this section we prove Theorem 11.1, which gives equivalent conditions for invertibility.

Theorem 11.1. *If L is a G-lattice, then the following statements are equivalent:*

(a) *L is invertible;*
(b) *the map $\varphi : L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} \to \mathbb{Z}\langle G\rangle$ defined by $\varphi(x \otimes \overline{y}) = x \cdot \overline{y}$ is an isomorphism of $\mathbb{Z}\langle G\rangle$-modules, where $\cdot$ is defined in Definition 9.2;*
(c) *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 as a lattice L is unimodular;*
(d) *L is G-isomorphic to $L_{(I,w)}$ for some fractional $\mathbb{Z}\langle G\rangle$-ideal I and some $w \in \mathbb{Q}\langle G\rangle^*$ such that $I\overline{I} = \mathbb{Z}\langle G\rangle \cdot w$ and $\psi(w) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, with $L_{(I,w)}$ as in Notation 8.3.*

We will prove Theorem 11.1 in a series of lemmas. The equivalence of (a) and (c) says that being invertible as a G-lattice is equivalent to being both unimodular as a lattice and invertible as a $\mathbb{Z}\langle G\rangle$-module.

Definition 11.2. Suppose R is a commutative ring. An R-module is **projective** if it is a direct summand of a free R-module. An R-module M is **flat** if whenever $N_1 \hookrightarrow N_2$ is an injection of R-modules, then the induced map

$$M \otimes_R N_1 \to M \otimes_R N_2$$

is injective.

Lemma 11.3. *Suppose that L is a $\mathbb{Z}$-free $\mathbb{Z}\langle G\rangle$-module of rank $\#G/2$, and 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. Then:

(i) *there is a* $\mathbb{Z}\langle G\rangle$*-module* M *such that* $L\oplus M$ *and* $\mathbb{Z}\langle G\rangle\oplus\mathbb{Z}\langle G\rangle$ *are isomorphic as* $\mathbb{Z}\langle G\rangle$*-modules, and*
(ii) L *is projective and flat as a* $\mathbb{Z}\langle G\rangle$*-module.*

Proof. Let $q = (L : \mathbb{Z}\langle G\rangle e_2)$. By Lemma 10.2(i), we have that q is finite and odd. Let $r = (L : \mathbb{Z}\langle G\rangle e_q)$. By Lemma 10.2(i), we have that r is finite and coprime to q. Take $a, b \in \mathbb{Z}$ such that $ar + bq = 1$. Let $N = \mathbb{Z}\langle G\rangle e_2 \oplus \mathbb{Z}\langle G\rangle e_q$. By Lemma 10.2(ii) we have $N \cong \mathbb{Z}\langle G\rangle \oplus \mathbb{Z}\langle G\rangle$ as $\mathbb{Z}\langle G\rangle$-modules. Define

$$p : N \to L \quad \text{by} \quad (x, y) \mapsto x + y$$

and

$$s : L \to N \quad \text{by} \quad x \mapsto (bqx, arx).$$

Then $p \circ s$ is the identity on L. Thus,

$$L \oplus \ker(p) \cong N \cong \mathbb{Z}\langle G\rangle \oplus \mathbb{Z}\langle G\rangle$$

as $\mathbb{Z}\langle G\rangle$-modules. So (i) holds with $M = \ker(p)$. Since L is a direct summand of a free module, L is projective. All projective modules are flat (by Example (1) in I.2.4 of [3]). □

Recall that the notions of fractional $\mathbb{Z}\langle G\rangle$-ideal and invertible fractional $\mathbb{Z}\langle G\rangle$-ideal were defined in Definition 8.1.

Lemma 11.4. *If* I *is an invertible fractional* $\mathbb{Z}\langle G\rangle$*-ideal, then:*

(i) *if* $m \in \mathbb{Z}_{>0}$*, then* I/mI *is isomorphic to* $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$ *as a* $\mathbb{Z}\langle G\rangle$*-module;*
(ii) I *is flat;*
(iii) *if* I' *is a fractional* $\mathbb{Z}\langle G\rangle$*-ideal, then the natural surjective map*

$$I \otimes_{\mathbb{Z}\langle G\rangle} I' \to II'$$

is an isomorphism.

Proof. Since I is an invertible fractional $\mathbb{Z}\langle G\rangle$-ideal, there is a fractional $\mathbb{Z}\langle G\rangle$-ideal J such that $IJ = \mathbb{Z}\langle G\rangle$. Let $\mathcal{F}$ denote the partially ordered set of fractional $\mathbb{Z}\langle G\rangle$-ideals. The maps from $\mathcal{F}$ to itself defined by $f_1 : N \mapsto NI$ and $f_2 : N \mapsto NJ$ are inverse bijections that preserve inclusions. Since $f_1(\mathbb{Z}\langle G\rangle) = I$, it follows that the maximal $\mathbb{Z}\langle G\rangle$-submodules of I are exactly the $\mathfrak{m}I$ such that $\mathfrak{m}$ is a maximal ideal of $\mathbb{Z}\langle G\rangle$. By the Chinese Remainder Theorem, the map $I \to \prod_{\mathfrak{m}} I/\mathfrak{m}I$ is surjective, where the product runs over the (finitely many) maximal ideals $\mathfrak{m}$ that contain m. It follows that there exists $x \in I$ that is not contained in any $\mathfrak{m}I$. Since $\mathbb{Z}\langle G\rangle x + mI$ is a fractional ideal that is not contained in any proper submodule of I, it equals I. Thus, I/mI is isomorphic to $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$ as a $\mathbb{Z}\langle G\rangle$-module. This proves (i).

For (ii), apply (i) and Lemma 11.3(ii).

Since I is flat, the natural map

$$I \otimes_{\mathbb{Z}\langle G\rangle} I' \to I \otimes_{\mathbb{Z}\langle G\rangle} \mathbb{Q}\langle G\rangle \cong I \otimes_{\mathbb{Z}\langle G\rangle} \mathbb{Z}\langle G\rangle \otimes_{\mathbb{Z}} \mathbb{Q} \cong I \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}\langle G\rangle$$

is injective, giving (iii). □

Let $L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$. Then the inner product $\langle\ ,\ \rangle$ on L extends $\mathbb{Q}$-bilinearly to a $\mathbb{Q}$-bilinear, symmetric, positive definite inner product on $L_{\mathbb{Q}}$, and the lifted inner product $\cdot$ extends $\mathbb{Q}$-bilinearly to a $\mathbb{Q}\langle G\rangle$-bilinear map $\cdot$ from $L_{\mathbb{Q}} \times \overline{L_{\mathbb{Q}}}$ to $\mathbb{Q}\langle G\rangle$.

Lemma 11.5. *Suppose* L *is an invertible* G*-lattice. Then* $L_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle\gamma$ *for some* $\gamma \in L_{\mathbb{Q}}$*. For such a* γ*, letting* $z = \gamma \cdot \overline{\gamma} \in \mathbb{Q}\langle G\rangle$ *we have:*

(i) $\langle a\gamma, b\gamma\rangle = t(a\bar{b}z)$ *for all* $a, b \in \mathbb{Q}\langle G\rangle$,
(ii) $z \in \mathbb{Q}\langle G\rangle^*$,
(iii) *for all* $\psi \in \Psi$ *we have* $\psi(z) \in \mathbb{R}_{>0}$,
(iv) $L \cdot \overline{L} = \mathbb{Z}\langle G\rangle$,
(v) *if* $I = \{x \in \mathbb{Q}\langle G\rangle : x\gamma \in L\}$, *then* $I\overline{I} = \mathbb{Z}\langle G\rangle z^{-1}$ *and as* G*-lattices we have* $L_{(I,z^{-1})} \cong L$.

Proof. By Definition 9.4(iii) and Lemma 10.2(i) we have that for all $m \in \mathbb{Z}_{>1}$ there exists $e_m \in L$ such that the index $i(m) = (L : \mathbb{Z}\langle G\rangle e_m)$ is finite and coprime to m. It follows that $\mathbb{Q}\langle G\rangle \cong L_{\mathbb{Q}}$ as $\mathbb{Q}\langle G\rangle$-modules. Let $\gamma \in L_{\mathbb{Q}}$ be the image of 1 under such an isomorphism $\mathbb{Q}\langle G\rangle \xrightarrow{\sim} L_{\mathbb{Q}}$. Then $L_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle\gamma$. Let

$$z = \gamma \cdot \overline{\gamma} \in \mathbb{Q}\langle G\rangle.$$

By (9.1) and (9.2), for all $a, b \in \mathbb{Q}\langle G\rangle$ we have

$$(a\gamma) \cdot (\overline{b\gamma}) = a(\gamma \cdot (\overline{b}\overline{\gamma})) = a\overline{b}(\gamma \cdot \overline{\gamma}) = a\overline{b}z$$

and thus

$$\langle a\gamma, b\gamma\rangle = t((a\gamma) \cdot (\overline{b\gamma})) = t(a\overline{b}z),$$

giving (i). Since the inner product on $L_{\mathbb{Q}}$ is symmetric, using Lemma 6.6(ii)(e) we have $\bar{z} = z$. Thus for all $\psi \in \Psi$ we have

$$\psi(z) = \psi(\bar{z}) = \overline{\psi(z)}$$

by Lemma 7.3(i), so $\psi(z) \in \mathbb{R}$. For all $a \in \mathbb{Q}\langle G\rangle$ we have

$$0 \leq \langle a\gamma, a\gamma\rangle = t(a\overline{a}z) = \frac{1}{n}\sum_{\psi\in\Psi} \psi(a\overline{a}z)$$

by Lemma 7.3(ii). By Lemma 7.3(vii) it follows that $\psi(z) \geq 0$ for all $\psi \in \Psi$. If $a \in \mathbb{Q}\langle G\rangle$ and $za = 0$, then

$$\langle a\gamma, a\gamma\rangle = t(a\overline{a}z) = 0,$$

so $a = 0$. Therefore multiplication by z is an injective, and thus surjective, map from $\mathbb{Q}\langle G\rangle$ to itself. Thus $z \in \mathbb{Q}\langle G\rangle^*$ and $\psi(z) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, by Lemma 7.3(vi). This gives (ii) and (iii).

Define

$$L^{-1} = \{\overline{y} \in \overline{L}_{\mathbb{Q}} : L \cdot \overline{y} \subset \mathbb{Z}\langle G\rangle\}$$

and let $m \in \mathbb{Z}_{>1}$. We have

$$L \supset \mathbb{Z}\langle G\rangle e_m \supset i(m)L,$$

so $e_m \in \mathbb{Q}\langle G\rangle^*\gamma$ and therefore $e_m \cdot \overline{e_m} \in \mathbb{Q}\langle G\rangle^*$. Now

$$i(m)(e_m \cdot \overline{e_m})^{-1}\overline{e_m} \in L^{-1},$$

because for all $x \in L$ one has

$$i(m)x \cdot (e_m \cdot \overline{e_m})^{-1}\overline{e_m} \subset \mathbb{Z}\langle G\rangle e_m \cdot (e_m \cdot \overline{e_m})^{-1}\overline{e_m} = \mathbb{Z}\langle G\rangle.$$

Therefore

$$i(m) = e_m \cdot i(m)(e_m \cdot \overline{e_m})^{-1}\overline{e_m} \in L \cdot L^{-1} \subset \mathbb{Z}\langle G\rangle.$$

This is true for all $m \in \mathbb{Z}_{>1}$, so $1 \in L \cdot L^{-1}$ and $L \cdot L^{-1} = \mathbb{Z}\langle G\rangle$.

Now for $\overline{y} \in \overline{L}_{\mathbb{Q}}$ one has $\overline{y} \in \overline{L}$ if and only if $y \in L$, if and only if for all $x \in L$ one has $\langle x, y\rangle \in \mathbb{Z}$, if and only if for all $x \in L$ and $\sigma \in G$ one has $\langle x, \sigma y\rangle = \langle \sigma^{-1}x, y\rangle \in \mathbb{Z}$,

if and only if for all $x \in L$ one has $x \cdot \overline{y} \in \mathbb{Z}\langle G\rangle$, if and only if $\overline{y} \in L^{-1}$. So $\overline{L} = L^{-1}$. Thus $L \cdot \overline{L} = \mathbb{Z}\langle G\rangle$, giving (iv).

If $I \subset \mathbb{Q}\langle G\rangle$ is such that $L = I\gamma$, then $I \xrightarrow{\sim} L$, $x \mapsto x\gamma$ as $\mathbb{Z}\langle G\rangle$-modules. Then

$$\mathbb{Z}\langle G\rangle = L \cdot \overline{L} = I\overline{I}\gamma \cdot \overline{\gamma} = I\overline{I}z,$$

so $I\overline{I} = \mathbb{Z}\langle G\rangle z^{-1}$. Now

$$\langle x\gamma, y\gamma\rangle = t(x\gamma \cdot \overline{y\gamma}) = t(x\overline{y}z) = \langle x, y\rangle_{I,z^{-1}}$$

for all $x, y \in I$. Thus, $L_{(I,z^{-1})} \cong L$ as G-lattices. This gives (v). □

We are now ready to prove Theorem 11.1.

For (a) ⇒ (d), apply Lemma 11.5 with $w = z^{-1}$.

For (d) ⇒ (b), by (d) we have $L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} = I \otimes_{\mathbb{Z}\langle G\rangle} \overline{I}$. Using Lemma 11.4(iii) we have that the composition

$$I \otimes \overline{I} \xrightarrow{\sim} I\overline{I} = \mathbb{Z}\langle G\rangle w \xrightarrow{\sim} \mathbb{Z}\langle G\rangle$$

is an isomorphism, where the first map sends $x \otimes y$ to $x\overline{y}$ and the last map sends α to α/w. Since $x \cdot \overline{y} = x\overline{y}/w$, this gives (b).

For (b) ⇒ (c), suppose (b) holds, i.e., the map

$$\varphi : L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} \to \mathbb{Z}\langle G\rangle, \quad x \otimes \overline{y} \mapsto x \cdot \overline{y}$$

is an isomorphism of $\mathbb{Z}\langle G\rangle$-modules. Then L is unimodular, as follows. Consider the maps:

$$L \to \mathrm{Hom}_{\mathbb{Z}\langle G\rangle}(\overline{L}, \mathbb{Z}\langle G\rangle) \to \mathrm{Hom}(\overline{L}, \mathbb{Z}) \to \mathrm{Hom}(L, \mathbb{Z})$$

where the left-hand map is the $\mathbb{Z}\langle G\rangle$-module isomorphism induced by φ, defined by $x \mapsto (\overline{y} \mapsto x \cdot \overline{y})$, the middle map is $f \mapsto t \circ f$, and the right-hand map is $g \mapsto (y \mapsto g(\overline{y}))$. The latter two maps are group isomorphisms; for the middle map note that its inverse is

$$\hat{f} \mapsto (\overline{x} \mapsto \sum_{\sigma \in S} \hat{f}(\sigma^{-1}\overline{x})\sigma).$$

The composition, which takes x to

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

is therefore a bijection, so L is unimodular. Then (c) holds by taking $M = \overline{L}$.

For (c) ⇒ (a), by Lemma 7.3(v) we have $\mathbb{Q}\langle G\rangle \cong \prod_{j\in J} K_j$ with $\#J < \infty$ and fields K_j. Each $\mathbb{Q}\langle G\rangle$-module V is $V = \prod_{j\in J} V_j$ with each V_j a K_j-vector space. With $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$ and $W = M \otimes_{\mathbb{Z}} \mathbb{Q}$ we have

$$\prod_{j\in J}(V_j \otimes_{K_j} W_j) = V \otimes_{\mathbb{Q}\langle G\rangle} W \cong \mathbb{Q}\langle G\rangle \cong \prod_j K_j.$$

This holds if and only if for all j we have

$$(\dim_{K_j} V_j)(\dim_{K_j} W_j) = 1,$$

which holds if and only if for all j we have

$$\dim_{K_j} V_j = \dim_{K_j} W_j = 1.$$

This holds if and only if $V \cong W \cong \mathbb{Q}\langle G\rangle$ as $\mathbb{Q}\langle G\rangle$-modules. Thus, L and M may be viewed as fractional $\mathbb{Z}\langle G\rangle$-ideals in $\mathbb{Q}\langle G\rangle$, and LM is principal, so L and M are invertible fractional $\mathbb{Z}\langle G\rangle$-ideals. By Lemma 11.4(i), if I is an invertible fractional $\mathbb{Z}\langle G\rangle$-ideal, then I/mI is cyclic as a $\mathbb{Z}\langle G\rangle$-module, for every positive integer m. Thus L/mL is cyclic as a $\mathbb{Z}\langle G\rangle$-module, so (a) holds.

This concludes the proof of Theorem 11.1.

12. Short vectors in invertible lattices

Recall that G is a group of order $2n$ equipped with an element u of order 2. The main result of this section is Theorem 12.4, which shows in particular that a G-lattice is G-isomorphic to the standard G-lattice if and only if it is invertible and has a short vector (i.e., a vector of length 1).

Definition 12.1. We will say that a vector e in an integral lattice L is **short** if $\langle e, e\rangle = 1$.

Example 12.2. 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 12.3. *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*

$$\langle e, \sigma e\rangle = \begin{cases} 1 & \text{if } \sigma = 1, \\ -1 & \text{if } \sigma = u, \\ 0 & \text{for all other } \sigma \in G; \end{cases}$$

(iii) *$e \in L$ is short if and only if $e \cdot \overline{e} = 1$, with inner product $\cdot$ defined in Definition 9.2.*

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 $m = \#H$.

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

$$a \in \left(\sum_{\tau \in H} \tau\right) (\mathbb{Z}/m\mathbb{Z})\langle G\rangle.$$

By Definition 9.4, Theorem 11.1, and Lemma 11.4, there is a $\mathbb{Z}[H]$-module isomorphism

$$L/mL \cong (\mathbb{Z}/m\mathbb{Z})\langle G\rangle.$$

Since $e + mL$ is fixed by H, we have

$$e + mL \in \left(\sum_{\tau \in H} \tau \right) (L/mL),$$

so $e_m \in mL + (\sum_{\tau \in H} \tau)L$. Write

$$e = m\varepsilon_1 + \left(\sum_{\tau \in H} \tau \right) \varepsilon_2$$

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 9.2. □

This enables us to prove the following result.

Theorem 12.4. *Suppose L is a G-lattice. Then:*

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

$$\{G\text{-isomorphisms } \mathbb{Z}\langle G \rangle \to L\} \to \{\text{short vectors of } L\}$$

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*

$$G \to \{\text{short vectors of } L\}, \qquad \sigma \mapsto \sigma e$$

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 12.3(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 Lemma 9.5. Part (iv) is trivial for $\mathbb{Z}\langle G \rangle$, and L is G-isomorphic to $\mathbb{Z}\langle G \rangle$, so we have (iv). □

13. Tensor products of G-lattices

Recall that G is a finite abelian group with an element u of order 2. We will define the tensor product of invertible G-lattices, and derive some properties. See [1, 6] for background on tensor products.

Definition 13.1. Suppose that L and M are invertible G-lattices. Define the $\mathbb{Z}\langle G \rangle$-bilinear map

$$\cdot : (L \otimes_{\mathbb{Z}\langle G \rangle} M) \times (\overline{L} \otimes_{\mathbb{Z}\langle G \rangle} \overline{M}) \to \mathbb{Z}\langle G \rangle, \quad (a, \overline{b}) \mapsto a \cdot \overline{b}$$

by letting

$$(x \otimes v) \cdot (\overline{y} \otimes \overline{w}) = (x \cdot \overline{y})(v \cdot \overline{w})$$

for all $x, y \in L$ and $v, w \in M$ and extending $\mathbb{Z}\langle G\rangle$-bilinearly. Take

$$\overline{L \otimes_{\mathbb{Z}\langle G\rangle} M}$$

to be $\overline{L} \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}$, with

$$\overline{x \otimes v} = \overline{x} \otimes \overline{v}.$$

Example 13.2. Let $L = L_{(I_1,w_1)}$ and $M = L_{(I_2,w_2)}$ where I_1, I_2 are fractional $\mathbb{Z}\langle G\rangle$-ideals, $w_1, w_2 \in \mathbb{Q}\langle G\rangle^*$ are such that $\psi(w_i) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, and $I_i\overline{I_i} = \mathbb{Z}\langle G\rangle w_i$ for $i = 1, 2$. Then $L \otimes_{\mathbb{Z}\langle G\rangle} M$ may be identified with I_1I_2 via Lemma 11.4, and $\overline{L \otimes_{\mathbb{Z}\langle G\rangle} M}$ may be identified with $\overline{I_1I_2}$, and the dot product

$$I_1I_2 \times \overline{I_1I_2} \to \mathbb{Z}\langle G\rangle$$

from Definition 13.1 becomes $a \cdot \overline{b} = a\overline{b}/(w_1w_2)$ as in Example 9.3. This is precisely the lifted inner product of the G-lattice $L_{(I_1I_2,w_1w_2)}$ (which is invertible by Theorem 11.1). We thus have

$$L_{(I_1,w_1)} \otimes_{\mathbb{Z}\langle G\rangle} L_{(I_2,w_2)} = L_{(I_1I_2,w_1w_2)}. \tag{13.1}$$

Theorem 13.3. *Let L and M be invertible G-lattices. Then $L \otimes_{\mathbb{Z}\langle G\rangle} M$ is an invertible G-lattice with inner product*

$$\langle a, b\rangle = t(a \cdot \overline{b}),$$

where the dot product is defined in Definition 13.1 and equals the lifted inner product for this G-lattice.

Proof. By Theorem 11.1 we may assume that $L = L_{(I_1,w_1)}$ and $M = L_{(I_2,w_2)}$ where I_1, I_2 are fractional $\mathbb{Z}\langle G\rangle$-ideals, $w_1, w_2 \in \mathbb{Q}\langle G\rangle^*$ are such that $\psi(w_i) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, and $I_i\overline{I_i} = \mathbb{Z}\langle G\rangle w_i$ for $i = 1, 2$. In this case, we already checked the theorem in Example 13.2. □

Proposition 13.4. *Suppose that L, M, and N are invertible G-lattices. Then we have the following G-isomorphisms:*

(i) $L \otimes_{\mathbb{Z}\langle G\rangle} M \cong M \otimes_{\mathbb{Z}\langle G\rangle} L$,
(ii) $(L \otimes_{\mathbb{Z}\langle G\rangle} M) \otimes_{\mathbb{Z}\langle G\rangle} N \cong L \otimes_{\mathbb{Z}\langle G\rangle} (M \otimes_{\mathbb{Z}\langle G\rangle} N)$,
(iii) $L \otimes_{\mathbb{Z}\langle G\rangle} \mathbb{Z}\langle G\rangle \cong L$,
(iv) $L \otimes_{\mathbb{Z}\langle G\rangle} \overline{L} \cong \mathbb{Z}\langle G\rangle$.

Proof. By Theorem 11.1 we may reduce to the case where the invertible G-lattices are of the form $L_{(I,w)}$. Then (13.1) immediately gives (i) and (ii). For (iii) and (iv), note that $\mathbb{Z}\langle G\rangle = L_{(\mathbb{Z}\langle G\rangle,1)}$, and if $L = L_{(I,w)}$ then

$$\overline{L} \cong L_{(\overline{I},w)} \cong L_{(\overline{I}w^{-1},w^{-1})} = L_{(I^{-1},w^{-1})}.$$

□

Remark 13.5. One can extend parts (i), (ii), and (iii) of Proposition 13.4 to general G-lattices, by replacing $L \otimes_{\mathbb{Z}\langle G\rangle} M$ by its image in $L_{\mathbb{Q}} \otimes_{\mathbb{Q}\langle G\rangle} M_{\mathbb{Q}}$. That image is a G-lattice with lifted inner product given by the same formula.

14. The Witt-Picard group

This section, which is mostly a digression, is devoted to what we call the Witt-Picard group $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$. The results of this section are not directly used later, with the exception of the proof of Theorem 14.5, but it may be said that the properties of $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$, in particular its finiteness, are what makes our algorithms possible. Also, several of our results admit an attractive reformulation in terms of $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$.

As before, G is a finite abelian group of order $2n$ equipped with an element u of order 2.

Definition 14.1. We define

$$\mathrm{WPic}_{\mathbb{Z}\langle G\rangle} = \{[L] : L \text{ is an invertible } G\text{-lattice}\},$$

where the symbols $[L]$ are chosen so that $[L] = [M]$ if and only if L and M are G-isomorphic.

Theorem 14.2. *The set* $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ *is an abelian group, 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*

$$[L]^{-1} = [\overline{L}].$$

Proof. This follows immediately from Theorem 13.3 and Proposition 13.4. □

Corollary 14.3. *Suppose that L and M are invertible G-lattices. Then L and M are G-isomorphic if and only if $L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}$ and $\mathbb{Z}\langle G\rangle$ are G-isomorphic.*

Proof. This follows immediately from Theorem 14.2. More precisely,

$$\begin{aligned} L \cong_G M &\iff [L] = [M] \\ &\iff [L][M]^{-1} = 1 = [\mathbb{Z}\langle G\rangle] \\ &\iff [L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}] = [\mathbb{Z}\langle G\rangle] \\ &\iff L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M} \cong_G \mathbb{Z}\langle G\rangle \end{aligned}$$

where $\cong_G$ means G-isomorphic. □

The following description of $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ is reminiscent of the definition of class groups in algebraic number theory.

Proposition 14.4. *Let $\mathcal{I}_{\mathbb{Z}\langle G\rangle}$ denote the group of invertible fractional $\mathbb{Z}\langle G\rangle$-ideals. Then the group* $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ *is isomorphic to the quotient of the group*

$$\{(I, w) \in \mathcal{I}_{\mathbb{Z}\langle G\rangle} \times \mathbb{Q}\langle G\rangle^* : I\overline{I} = \mathbb{Z}\langle G\rangle w \text{ and } \psi(w) \in \mathbb{R}_{>0} \text{ for all } \psi \in \Psi\}$$

by its subgroup $\{(\mathbb{Z}\langle G\rangle v, v\overline{v}) : v \in \mathbb{Q}\langle G\rangle^*\}$.

Proof. Define the map by $(I, w) \mapsto [L_{(I,w)}]$. Surjectivity follows from Theorem 11.1, and the kernel is the desired subgroup by Theorem 8.5. □

Just as for the class group, we have:

Theorem 14.5. *The group* $\mathrm{WPic}_{\mathbb{Z}\langle G\rangle}$ *is finite.*

Proof. If L is an invertible G-lattice and $\{b_1, \ldots, b_n\}$ is an LLL-reduced basis, and for $\sigma \in G$ we have $\sigma(b_i) = \sum_{j=1}^n a_{ij}^{(\sigma)} b_j$ with $a_{ij}^{(\sigma)} \in \mathbb{Z}$, then

$$|\langle b_i, b_j \rangle| \leq 2^{n-1} \quad \text{and} \quad |a_{ij}^{(\sigma)}| \leq 3^{n-1}$$

for all i, j, and σ, by Proposition 3.4(iii) and (iv). Thus there are only finitely many possibilities for

$$((\langle b_i, b_j \rangle)_{i,j=1}^n, (a_{ij}^{(\sigma)})_{i,j=1,\ldots,n;\sigma \in G}).$$

If L' is also an invertible G-lattice with LLL-reduced basis $\{b_1', \ldots, b_n'\}$, and if we have

$$\langle b_i, b_j \rangle = \langle b_i', b_j' \rangle \quad \text{and} \quad a_{ij}^{(\sigma)} = a_{ij}^{\prime(\sigma)}$$

for all i, j, and σ, then the group isomorphism

$$L \to L', \quad b_i \mapsto b_i'$$

is an isomorphism of G-lattices. The finiteness of $\mathrm{WPic}_{\mathbb{Z}\langle G \rangle}$ now follows. □

We call $\mathrm{WPic}_{\mathbb{Z}\langle G \rangle}$ the **Witt-Picard group** of $\mathbb{Z}\langle G \rangle$. The reason for the nomenclature lies in Theorem 11.1. If R is a commutative ring, an invertible R-module is an R-module L for which there exists an R-module M with $L \otimes_R M \cong R$. The Picard group Pic_R is the set of invertible R-modules up to isomorphism, where the group operation is tensoring over R. This addresses the module structure, while Witt rings reflect the structure as a unimodular lattice.

We remark that one can formulate algorithms for $\mathrm{WPic}_{\mathbb{Z}\langle G \rangle}$, as follows. Elements $[L] \in \mathrm{WPic}_{\mathbb{Z}\langle G \rangle}$ are represented as L with an LLL-reduced basis.

Proposition 14.6. *There are deterministic polynomial-time algorithms for:*

(i) *finding the unit element,*
(ii) *inverting,*
(iii) *multiplying,*
(iv) *exponentiation,*
(v) *equality testing.*

Proof. Part (i) is trivial, since $1 = [\mathbb{Z}\langle G \rangle]$. For (ii) we have $[L]^{-1} = [\overline{L}]$, and the algorithm is to replace each σ by $\overline{\sigma}$. For parts (iii), (iv), and (v) use Algorithms 15.2 and 15.3 below and Theorem 1.2, respectively. □

15. Multiplying and exponentiating invertible G-lattices

In this section we give algorithms for multiplying and exponentiating invertible G-lattices. We shall always assume that all G-lattices in inputs and outputs of algorithms are specified via an LLL-reduced basis. As we saw in the proof of Theorem 14.5, this prevents coefficient blow-up.

Algorithm 15.1. Given invertible G-lattices L and M equipped with LLL-reduced bases, the algorithm outputs $L \otimes_{\mathbb{Z}\langle G \rangle} M$ with an LLL-reduced basis and an $n \times n \times n$ array of integers to describe the multiplication map

$$L \times M \to L \otimes_{\mathbb{Z}\langle G \rangle} M.$$

(i) Realize L as $L_{(I,w)}$ as in Lemma 11.5, using $\gamma = e_2$, and likewise realize M as $L_{(J,v)}$.
(ii) Compute $IJ \subset \mathbb{Q}\langle G \rangle$ and an LLL-reduced basis for the G-lattice $L_{(IJ,wv)}$.

(iii) Output $L \otimes_{\mathbb{Z}\langle G\rangle} M = L_{(IJ,wv)}$ and the multiplication map

$$L \times M \to L \otimes_{\mathbb{Z}\langle G\rangle} M$$

coming from multiplication $I \times J \to IJ$ in the ring $\mathbb{Q}\langle G\rangle$.

An alternative (probably less efficient) option is to directly use the definition of tensor product, i.e., compute $L \otimes_{\mathbb{Z}\langle G\rangle} M$ as

$$(L \otimes_{\mathbb{Z}} M)/(\sum_{i,j,\sigma} \mathbb{Z}(\sigma b_i \otimes b'_j - b_i \otimes \sigma b'_j))$$

where

$$L \otimes_{\mathbb{Z}} M = \bigoplus_{i,j} \mathbb{Z}(b_i \otimes b'_j).$$

With either choice, Algorithm 15.1 runs in polynomial time. Using ideals works well for computing products and low powers (cf. Algorithm 19.1(vii) below). However, computing high powers of ideals cannot be done in polynomial time, but computing high tensor powers of G-lattices is possible. Likewise, the map $L \to L^{\otimes r}$, $d \mapsto d^{\otimes r}$ cannot be written down for large r, but one can compute the composition

$$L \to L^{\otimes r} \to L^{\otimes r}/mL^{\otimes r}$$

(see Algorithm 15.2), and thanks to Proposition 4.3 this suffices for our purposes.

Applying Algorithm 15.1 gives the following polynomial-time algorithm.

Algorithm 15.2. Given G and u as usual, invertible G-lattices L and L' equipped with LLL-reduced bases, a positive integer m, and elements $d \in L/mL$ and $d' \in L'/mL'$, the algorithm computes $L \otimes_{\mathbb{Z}\langle G\rangle} L'$ and the element

$$d \otimes d' \in (L \otimes L')/m(L \otimes L').$$

(i) Apply Algorithm 15.1 to compute $L \otimes_{\mathbb{Z}\langle G\rangle} L'$.
(ii) Lift d to L and d' to L', and then apply the composition

$$L \times L' \to L \otimes_{\mathbb{Z}\langle G\rangle} L' \to (L \otimes L')/m(L \otimes L').$$

For all G, u, and $m \in \mathbb{Z}_{>0}$, by the proof of Theorem 14.5 there is a bound on the runtime of the previous algorithm that holds uniformly for all L, L', d, and d', and this bound is polynomial in the length of the data specifying G, u, and m.

Applying basis reduction, and iterating Algorithm 15.2 using an addition chain for r, gives the following polynomial-time algorithm. It replaces the polynomial chains in §7.4 of the Gentry-Szydlo paper [4].

Algorithm 15.3. Given G, u, an invertible G-lattice L, positive integers m and r, and $d \in L/mL$, the algorithm computes $L^{\otimes r}$ and $d^{\otimes r} \in L^{\otimes r}/mL^{\otimes r}$.

Note that it is $\log(r)$ and not r that enters in the runtime. This means that very high powers of lattices can be computed without coefficient blow-up, thanks to the basis reduction that takes place in Algorithm 15.1(ii). The fact that this is possible was one of the crucial ideas of Gentry and Szydlo.

16. The extended tensor algebra Λ

The extended tensor algebra Λ is a single algebraic structure that comprises all rings and lattices that our main algorithm needs, including their inner products.

Suppose L is an invertible G-lattice. Letting $L^{\otimes 0} = \mathbb{Z}\langle G\rangle$ and letting

$$L^{\otimes m} = L \otimes_{\mathbb{Z}\langle G\rangle} \cdots \otimes_{\mathbb{Z}\langle G\rangle} L \quad \text{(with } m \text{ } L\text{'s)}$$

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

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

("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. For all $j \in \mathbb{Z}$ we have $\overline{L^j} = \overline{L}^j = L^{-j}$. Note that computing the G-lattice $L^{-1} = \overline{L}$ is trivial; just compose the G-action map $G \to \mathrm{GL}(n,\mathbb{Z})$ with the map $G \to G$, $\sigma \mapsto \overline{\sigma}$. The ring structure on Λ is defined as the ring structure on the tensor algebra, supplemented with the lifted inner product $\cdot$ of Definition 9.2. Let $\Lambda_{\mathbb{Q}} = \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 16.1. (i) *The extended tensor algebra Λ is a commutative ring containing $\mathbb{Z}\langle G\rangle$ as a subring;*

(ii) *for all $j \in \mathbb{Z}$, the action of G on L^j becomes multiplication in Λ;*

(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) *if $j \in \mathbb{Z}$, then the lifted inner product $\cdot : L^j \times \overline{L^j} \to \mathbb{Z}\langle G\rangle$ becomes multiplication in Λ, with $\overline{L^j} = \overline{L}^j$;*

(v) *if $j \in \mathbb{Z}$, then for all $x, y \in L^j$ we have $\langle x, y\rangle = t(x\overline{y})$;*

(vi) *if $j \in \mathbb{Z}$ and $e \in L^j$ is short, then $\overline{e} = e^{-1}$ in L^{-j};*

(vii) *if γ is as in Lemma 11.5, then $\gamma \in \Lambda_{\mathbb{Q}}^*$, one has $L^i_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle\gamma^i$ for all $i \in \mathbb{Z}$, and $\Lambda_{\mathbb{Q}}$ may be identified with the Laurent polynomial ring $\mathbb{Q}\langle G\rangle[\gamma,\gamma^{-1}]$.*

(viii) *if $e \in L$ is short, then $\Lambda = \mathbb{Z}\langle G\rangle[e,e^{-1}]$, where the right side is the subring of Λ generated by $\mathbb{Z}\langle G\rangle$, e, and e^{-1}, which is a Laurent polynomial ring.*

Proof. The proof is straightforward. It is best to begin with (vii). □

All computations in Λ and in $\Lambda/m\Lambda = \bigoplus_{i\in\mathbb{Z}} L^i/mL^i$ with $m \in \mathbb{Z}_{>0}$ that occur in our algorithms are done with homogeneous elements only, where the set of homogeneous elements of Λ is $\bigcup_{i\in\mathbb{Z}} L^i$.

If A is a commutative ring, let $\mu(A)$ denote the subgroup of A^* consisting of the roots of unity, i.e., the elements of finite order. The following result will allow us to construct a polynomial-time algorithm to find k-th roots of short vectors, when they exist.

Proposition 16.2. *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* $2nr$,
(iv) *the degree map* $\mu(A) \to \mathbb{Z}/r\mathbb{Z}$ *that takes* $e \in \mu(A)$ *to* j *such that* $e \in L^j$ *is surjective if and only if* $\mu(A) \cap L \neq \emptyset$, *and*
(v) *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.

Next we show that the natural map

$$\bigoplus_{i=0}^{r-1} L^i \to \Lambda/(\nu - 1) = A$$

is bijective. For surjectivity, by Proposition 16.1(vi) we have $\nu L^j = L^{j+r}$ for all $j \in \mathbb{Z}$, and thus L^{j+r} and L^j have the same image under the natural map $\Lambda \to \Lambda/(\nu - 1) = A$. For injectivity, suppose

$$0 \neq a = \sum_{i=h}^{j} a_i \in \Lambda$$

with $h \leq j$, with all $a_i \in L^i$, and with $a_h \neq 0$ and $a_j \neq 0$. Then

$$(\nu - 1)a = \sum_{i=h}^{j+r} b_i$$

with $b_i \in L^i$ where $b_h = -a_h \neq 0$ and $b_{j+r} = \nu a_j \neq 0$, and therefore

$$(\nu - 1)a \notin \bigoplus_{i=0}^{r-1} L^i.$$

Hence we have

$$(\nu - 1)\Lambda \cap \bigoplus_{i=0}^{r-1} L^i = \{0\}.$$

The injectivity now follows.

Recall that Ψ is the set of $\mathbb{C}$-algebra homomorphisms from $\mathbb{C}\langle G\rangle$ to $\mathbb{C}$. Letting $A_{\mathbb{Q}} = A \otimes_{\mathbb{Z}} \mathbb{Q}$, we have

$$A_{\mathbb{Q}} = \Lambda_{\mathbb{Q}}/(\nu - 1)\Lambda_{\mathbb{Q}} \quad \text{and} \quad \Lambda_{\mathbb{Q}} = \bigoplus_{i \in \mathbb{Z}} L^i_{\mathbb{Q}}.$$

Since L is invertible, by Lemma 11.5 there exists $\gamma \in L_{\mathbb{Q}}$ such that

$$L_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle \cdot \gamma$$

with $z = \gamma\overline{\gamma} \in \mathbb{Q}\langle G\rangle^*$ and $\psi(z) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$. By Proposition 16.1(vii) we have $\gamma \in L^*_{\mathbb{Q}}$, and

$$L^j_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle \cdot \gamma^j$$

for all $j \in \mathbb{Z}$, and

$$\Lambda_{\mathbb{Q}} = \bigoplus_{i \in \mathbb{Z}} L^i_{\mathbb{Q}} = \mathbb{Q}\langle G\rangle[\gamma, \gamma^{-1}].$$

Thus, there exists $\delta \in \mathbb{Q}\langle G\rangle^*$ such that $\nu = \delta\gamma^r$. The set of ring homomorphisms from A to $\mathbb{C}$ can be identified with the set of ring homomorphisms from $A_{\mathbb{Q}}$ to $\mathbb{C}$, which is

$$\{\text{ring homomorphisms } \varphi : \Lambda_{\mathbb{Q}} \to \mathbb{C} : \varphi(\nu) = 1\}.$$

The latter set can be identified with

$$\{(\psi, \zeta) : \psi \in \Psi, \zeta \in \mathbb{C}^*, \psi(\delta)\zeta^r = 1\}$$

via the map

$$\varphi \mapsto (\varphi|_{\mathbb{Q}\langle G\rangle}, \varphi(\gamma))$$

and its inverse

$$(\psi, \zeta) \mapsto (\sum_i a_i\gamma^i \mapsto \sum_i \psi(a_i)\zeta^i),$$

and has size $nr = \dim_{\mathbb{Q}}(A_{\mathbb{Q}})$. Since

$$1 = \nu\overline{\nu} = (\delta\gamma^r)\overline{(\delta\gamma^r)} = \delta\overline{\delta}z^r,$$

we have

$$\psi(\delta)\overline{\psi(\delta)}\psi(z)^r = 1 = \psi(\delta)\overline{\psi(\delta)}(\zeta\overline{\zeta})^r,$$

so $\psi(z)^r = (\zeta\overline{\zeta})^r$. Since $\psi(z) \in \mathbb{R}_{>0}$, we have $\psi(z) = \zeta\overline{\zeta}$. Since $\overline{\gamma} = z\gamma^{-1}$, we now have

$$\varphi(\overline{\gamma}) = \varphi(z)\zeta^{-1} = \overline{\zeta} = \overline{\varphi(\gamma)}.$$

By Lemma 7.3(i) we have $\psi(\bar{\alpha}) = \overline{\psi(\alpha)}$ for all $\alpha \in \mathbb{Q}\langle G\rangle$. Since $A_{\mathbb{Q}}$ is generated as a ring by $\mathbb{Q}\langle G\rangle$ and γ, it follows that $\varphi(\bar{\alpha}) = \overline{\varphi(\alpha)}$ for all $\alpha \in A_{\mathbb{Q}}$ and all ring homomorphisms $\varphi : A_{\mathbb{Q}} \to \mathbb{C}$.

Applying Lemma 7.1(ii) to the commutative $\mathbb{Q}$-algebra $A_{\mathbb{Q}}$ shows that

$$\bigcap_{\varphi} \ker\varphi = 0.$$

Let

$$E = \{e \in A : e\overline{e} = 1\},$$

a subgroup of A^*.

If $e \in \mu(A)$, then $\varphi(e)$ is a root of unity in $\mathbb{C}$ for all ring homomorphisms $\varphi : A \to \mathbb{C}$, so

$$1 = \varphi(e)\overline{\varphi(e)} = \varphi(e)\varphi(\overline{e}) = \varphi(e\overline{e}).$$

Since $\bigcap_{\varphi} \ker\varphi = 0$, we have $e\overline{e} = 1$. 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 6.2 and using (9.2) 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 12.3(iii) and Example 12.2 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 $\#G\#(\mathbb{Z}/r\mathbb{Z}) = 2nr$. Thus, $E \subseteq \mu(A) \subseteq E$, so $E = \mu(A)$ and we have (ii) and (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 $\mu(A) \cap L \neq \emptyset$. This gives (iv). Part (v) now follows from (ii). □

Remark 16.3. In the proof of Proposition 16.2 we showed that $\mu(\mathbb{Z}\langle G\rangle) = G$.

17. Short vectors

Recall that G is a finite abelian group of order $2n$ equipped with an element u of order 2. The main result of this section is Algorithm 17.4.

Definition 17.1. The exponent of a finite group H is the least positive integer k such that $\sigma^k = 1$ for all $\sigma \in H$.

The exponent of a finite group H divides $\#H$ and has the same prime factors as $\#H$.

Notation 17.2. Let k denote the exponent of G.

By Theorem 12.4, the G-isomorphisms $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ for a G-lattice L are in one-to-one correspondence with the short vectors of L, and if a short $e \in L$ exists, then the short vectors of L are exactly the $2n$ vectors $\{\sigma e : \sigma \in G\}$. With k the exponent of G, we have

$$(\sigma e)^k = \sigma^k e^k = e^k$$

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.

The n of [4] is an odd prime, so the group exponent $k = 2n$, and $\mathbb{Z}\langle G\rangle$ embeds in $\mathbb{Q}(\zeta_n) \times \mathbb{Q}$, where $\zeta_n \in \mathbb{C}^*$ is a primitive n-th root of unity. 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 [4] 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 as large as n. 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 Algorithm 17.4 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. In [11] we prove the following result, and give the associated algorithm.

Proposition 17.3. *There is a deterministic polynomial-time algorithm that, given an order A, determines a set of generators for the group $\mu(A)$ of roots of unity in A^*.*

Algorithm 17.4. Given G of exponent k, u, a fractional $\mathbb{Z}\langle G\rangle$-ideal I, an element $w \in \mathbb{Q}\langle G\rangle^*$ such that $I\overline{I} = \mathbb{Z}\langle G\rangle \cdot w$ and $\psi(w) \in \mathbb{R}_{>0}$ for all $\psi \in \Psi$, a short vector ν in the G-lattice $L_{(I^k, w^k)}$, and the order $A = \bigoplus_{i=0}^{k-1} I^i$ with multiplication

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

and

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

the algorithm determines whether there exists $\alpha \in L_{(I,w)}$ such that $\nu = \alpha^k$ in $L_{(I^k,w^k)}$ and $\alpha \cdot \overline{\alpha} = 1$, and if so, finds one.

(i) Apply Proposition 17.3 to compute generators for $\mu(A)$.
(ii) Apply the degree map $\mu(A) \to \mathbb{Z}/k\mathbb{Z}$ from Proposition 16.2(iv) to the generators, and check whether the images generate $\mathbb{Z}/k\mathbb{Z}$. If they do not, output "no e exists"; if they do, compute an element $\alpha \in \mu(A)$ whose image under the degree map is 1.
(iii) Check whether $\nu = \alpha^k$. If not, output "no α exists". If so, output α.

Proposition 17.5. *Algorithm 17.4 produces correct output and runs in polynomial time.*

Proof. We apply Proposition 16.2 with $r = k$. With $L = L_{(I,w)}$, our order A can be identified with the ring $\Lambda/(\nu - 1)$ of that proposition. Suppose Step (ii) produces $\alpha \in \mu(A)$ of degree 1. Then

$$\alpha \in \mu(A) \cap L_{(I,w)} = \{\varepsilon \in L_{(I,w)} : \varepsilon \cdot \bar{\varepsilon} = 1\}$$

by Proposition 16.2(ii). By Proposition 12.3(iii), this set is the set of short vectors in $L_{(I,w)}$. By Theorem 12.4(iv), if a short $\varepsilon \in L_{(I,w)}$ exists, then the short vectors in $L_{(I,w)}$ are exactly the $2n$ vectors $\{\sigma\varepsilon : \sigma \in G\}$, which all have the same k-th power since k is the exponent of G. By this and Proposition 16.2(iv), if any step fails then the desired α does not exist. The algorithm runs in polynomial time since

$$\#\mu(A) = 2nk \leq (2n)^2$$

by Proposition 16.2(v). □

18. Finding auxiliary prime powers

In this section we present an algorithm to find auxiliary prime powers ℓ and m. To bound the runtime, we use Heath-Brown's version of Linnik's theorem in analytic number theory.

Recall that G is a finite abelian group equipped with an element u of order 2, and k is the exponent of G.

Notation 18.1. For $m \in \mathbb{Z}_{>0}$ let $k(m)$ denote the exponent of the unit group $(\mathbb{Z}\langle G\rangle/(m))^*$.

Lemma 18.2. *Suppose p is a prime number and $j \in \mathbb{Z}_{>0}$. Then:*

(i) $(\mathbb{Z}/p^j\mathbb{Z})^* \subset (\mathbb{Z}\langle G\rangle/(p^j))^*$;
(ii) *if p is odd, then the exponent of $(\mathbb{Z}/p^j\mathbb{Z})^*$ is $(p-1)p^{j-1}$;*
(iii) *if $p \equiv 1 \bmod k$, then $k(p^j) = (p-1)p^{j-1}$.*

Proof. Parts (i) and (ii) are easy. For (iii), we proceed by induction on j. If $p \equiv 1 \bmod k$, then p is odd. We first take $j = 1$. The map $x \mapsto x^p$ is a ring endomorphism of $\mathbb{Z}\langle G\rangle/(p)$ and is the identity on G, since the exponent k divides $p - 1$. Since G generates the ring, the map is the identity and therefore $x^p = x$ for all $x \in \mathbb{Z}\langle G\rangle/(p)$ and $x^{p-1} = 1$ for all $x \in (\mathbb{Z}\langle G\rangle/(p))^*$.

Now suppose $j > 1$. Suppose $x \in \mathbb{Z}\langle G\rangle$ maps to a unit in $\mathbb{Z}\langle G\rangle/(p^j)$. By the induction hypothesis,

$$x^{(p-1)p^{j-2}} \equiv 1 \mod p^{j-1}.$$

Thus, $x^{(p-1)p^{j-2}} = 1 + p^{j-1}v$ for some $v \in \mathbb{Z}\langle G\rangle$. Since $(j-1)p \geq j$ we have

$$x^{(p-1)p^{j-1}} = (1+p^{j-1}v)^p = 1 + \binom{p}{1}p^{j-1}v + \cdots + p^{(j-1)p}v^p \equiv 1 \mod p^j.$$

Thus, $k(p^j)$ divides $(p-1)p^{j-1}$ for all $j \in \mathbb{Z}_{>0}$. Part (iii) now follows from (i) and (ii). □

Theorem 18.3 (Heath-Brown, Theorem 6 of [5])**.** *There is an effective constant $c > 0$ such that if $a, t \in \mathbb{Z}_{>0}$ and $\gcd(a,t) = 1$, then the smallest prime p such that $p \equiv a \mod t$ is at most $ct^{5.5}$.*

Algorithm 18.4. Given positive integers n and k with k even, the algorithm produces prime powers $\ell = p^r$ and $m = q^s$ with $\ell, m \geq 2^{n/2}+1$ such that $p \equiv q \equiv 1 \mod k$ and $\gcd(\varphi(\ell), \varphi(m)) = k$, where φ is Euler's phi function.

(i) Try $p = k+1, 2k+1, 3k+1, \ldots$ until the least prime $p \equiv 1 \mod k$ is found.
(ii) Find the smallest $r \in \mathbb{Z}_{>0}$ such that $p^r \geq 2^{n/2}+1$.
(iii) Try $q = p+k, p+2k, \ldots$ until the least prime $q \equiv 1 \mod k$ such that $\gcd((p-1)p, q-1) = k$ is found.
(iv) Find the smallest $s \in \mathbb{Z}_{>0}$ such that $q^s \geq 2^{n/2}+1$.
(v) Let $\ell = p^r$ and $m = q^s$.

Proposition 18.5. *Algorithm 18.4 runs in time $(n+k)^{O(1)}$.*

Proof. Algorithm 18.4 takes as input $n, k \in \mathbb{Z}_{>0}$ with k even, and computes positive integers r and s and primes p and q such that:

- $p \equiv q \equiv 1 \mod k$,
- $\gcd((p-1)p^{r-1}, (q-1)q^{s-1}) = k$,
- $p^r \geq 2^{n/2}+1$, and
- $q^s \geq 2^{n/2}+1$.

We next show that Algorithm 18.4 terminates, with correct output, in the claimed time. By Theorem 18.3 above, the prime p found by Algorithm 18.4 satisfies $p \leq ck^{5.5}$ with an effective constant $c > 0$. Primality testing can be done by trial division. 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

$$q \equiv 2 \mod p \quad \text{and} \quad q \equiv 1+k \mod k_1 \quad \text{and} \quad q \equiv 2 \mod k_2.$$

This gives a congruence

$$q \equiv a \mod p(p-1)$$

for some a with $\gcd(a, p(p-1)) = 1$. Theorem 18.3 implies that Algorithm 18.4 produces a prime q with the desired properties and satisfying

$$q \leq c(p^2)^{5.5} \leq c(ck^{5.5})^{11} = c^{12}k^{60.5}.$$

The upper bounds on p and q imply that Algorithm 18.4 runs in time $(n+k)^{O(1)}$. □

Remark 18.6. In practice, Algorithm 18.4 is *much* faster than implied by the proof of Proposition 18.5; Theorem 18.3 is unnecessarily pessimistic, and in practice one does not need to find a prime q that is congruent to 2 mod pk_2 and to $1+k$ mod k_1. In work in progress, we get better bounds for the runtime of our main algorithm,

and avoid using the theorem of Heath-Brown or Algorithm 18.4, by generalizing our theory to the setting of "CM orders".

Algorithm 18.4 immediately yields the following algorithm.

Algorithm 18.7. Given G and u, the algorithm produces prime powers ℓ and m such that

$$\ell, m \geq 2^{n/2} + 1 \quad \text{and} \quad \gcd(k(\ell), k(m)) = k,$$

where k is the exponent of G, and produces the values of $k(\ell)$ and $k(m)$.

(i) Compute n and k.

(ii) Run Algorithm 18.4 to compute prime powers $\ell = p^r$ and $m = q^s$ with

$$\ell, m \geq 2^{n/2} + 1$$

such that

$$p \equiv q \equiv 1 \bmod k \quad \text{and} \quad \gcd(\varphi(\ell), \varphi(m)) = k.$$

(iii) Compute $k(\ell) = (p-1)p^{r-1}$ and $k(m) = (q-1)q^{s-1}$.

By Lemma 18.2(iii), Algorithm 18.7 produces the desired output. It follows from Proposition 18.5 that Algorithm 18.7 runs in polynomial time (note that the input in Algorithm 18.7 includes the group law on G).

Remark 18.8. Our prime powers ℓ and m play the roles that in the Gentry-Szydlo paper [4] 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 $P'-1$. While the Gentry-Szydlo primes P and P' are found with at best a probabilistic algorithm, we can find ℓ and m in polynomial time with a deterministic algorithm. (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 9.4, when L is invertible then for *all* m, the $(\mathbb{Z}/m\mathbb{Z})\langle G\rangle$-module L/mL is free of rank 1.)

The next result will provide the proof of correctness for a key step in our main algorithm.

Lemma 18.9. *Suppose e is a short vector in an invertible G-lattice L, suppose $\ell, m \in \mathbb{Z}_{\geq 3}$, and suppose $e_{\ell m} \in L$ is such that $e_{\ell m} + \ell m L$ generates $L/\ell m L$ as a $(\mathbb{Z}/\ell m\mathbb{Z})\langle G\rangle$-module. Then $e^{k(m)}$ is the unique short vector in the coset*

$$e_{\ell m}^{k(m)} + mL^{k(m)},$$

and there is a unique $s \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$ such that

$$e^{k(m)} \equiv s e_{\ell m}^{k(m)} \mod \ell L^{k(m)}.$$

If further $b \in \mathbb{Z}_{>0}$ and $bk(m) \equiv k \bmod k(\ell)$, then e^k is the unique short vector in $s^b e_{\ell m}^k + \ell L^k$.

Proof. Since e is short, we have $\mathbb{Z}\langle G\rangle e = L$. Thus for all $r \in \mathbb{Z}_{>0}$, the coset $e + rL$ generates L/rL as a $\mathbb{Z}\langle G\rangle/(r)$-module. We also have that $e_{\ell m} + mL$ generates L/mL as a $\mathbb{Z}\langle G\rangle/(m)$-module, and $e_{\ell m} + \ell L$ generates $L/\ell L$ as a $\mathbb{Z}\langle G\rangle/(\ell)$-module. Thus, there exist $y_m \in (\mathbb{Z}\langle G\rangle/(m))^*$ and $y_\ell \in (\mathbb{Z}\langle G\rangle/(\ell))^*$ such that

$$e_{\ell m} = y_m e \bmod mL \quad \text{and} \quad e_{\ell m} = y_\ell e \bmod \ell L.$$

It follows that

$$e_{\ell m}^{k(m)} \equiv e^{k(m)} \bmod mL^{k(m)} \quad \text{and} \quad e_{\ell m}^{k(\ell)} \equiv e^{k(\ell)} \bmod \ell L^{k(\ell)}.$$

We have

$$(\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle e = L/\ell L = (\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle e_{\ell m}.$$

Thus

$$(\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle \cdot e^{k(m)} = L^{k(m)}/\ell L^{k(m)} = (\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle \cdot e_{\ell m}^{k(m)},$$

so

$$e^{k(m)} \equiv s e_{\ell m}^{k(m)} \bmod \ell L^{k(m)} \tag{18.1}$$

for a unique $s \in ((\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle)^*$. We have $e \cdot \bar{e} = 1$, so

$$e \in \Lambda^* \quad \text{and} \quad e + \ell\Lambda \in (\Lambda/\ell\Lambda)^*.$$

By (18.1) we have

$$(e + \ell\Lambda)^{k(m)} = s(e_{\ell m} + \ell\Lambda)^{k(m)}$$

in $\Lambda/\ell\Lambda = \bigoplus_{i\in\mathbb{Z}} L^i/\ell L^i$. It follows that

$$e_{\ell m} + \ell\Lambda \in (\Lambda/\ell\Lambda)^*.$$

If $ak(\ell) + bk(m) = k$ with $a \in \mathbb{Z}$, then

$$e^k = (e^{k(\ell)})^a (e^{k(m)})^b \equiv (e_{\ell m}^{k(\ell)})^a (s e_{\ell m}^{k(m)})^b \equiv s^b e_{\ell m}^k \bmod \ell\Lambda,$$

so $s^b e_{\ell m}^k + \ell L^k$ contains the short vector e^k of L^k. In both cases, uniqueness follows from Proposition 4.1. □

19. The main algorithm

Algorithm 19.1 below is the algorithm promised in Theorem 1.1. That it is correct and runs in polynomial time follows from the results above; see the discussion after the algorithm. As before, k is the exponent of the group G and $k(j)$ is the exponent of $(\mathbb{Z}\langle G\rangle/(j))^*$ if $j \in \mathbb{Z}_{>0}$.

Algorithm 19.1. Given G, u, and a G-lattice L, the algorithm determines whether there exists a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$, and if so, computes one.

(i) Apply Algorithm 10.3 to check whether L is invertible. If it is not, terminate with "no".
(ii) Apply Algorithm 18.7 to produce prime powers ℓ and m as well as $k(\ell)$ and $k(m)$.
(iii) Use Proposition 10.1 to compute $e_{\ell m}$ and e_2.
(iv) Use Algorithm 15.3 to compute the pair

$$(L^{k(m)}, e_{\ell m}^{k(m)} + \ell m L^{k(m)}).$$

Use Algorithm 4.2 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 $b \in \mathbb{Z}_{>0}$ such that

$$bk(m) \equiv k \bmod k(\ell).$$

(vii) Compute

$$I = \{x \in \mathbb{Q}\langle G\rangle : xe_2 \in L\}$$

and compute I^i for $i = 2, \ldots, k$.

(viii) Compute $s^b \in (\mathbb{Z}/\ell\mathbb{Z})\langle G\rangle$ and

$$s^b (e_{\ell m}/e_2)^k + \ell I^k \in I^k/\ell I^k.$$

Use Algorithm 4.2 to decide whether the coset

$$s^b (e_{\ell m}/e_2)^k + \ell I^k$$

contains a short vector ν for the lattice $L_{(I^k, w^k)}$ where

$$w = (e_2 \cdot \overline{e_2})^{-1},$$

and if so, compute it. Terminate with "no" if none exists.

(ix) Construct the order $A = \bigoplus_{i=0}^{k-1} I^i$ with multiplication

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

and

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

Apply Algorithm 17.4 to find $\alpha \in L_{(I,w)}$ such that $\nu = \alpha^k$ and $\alpha \cdot \overline{\alpha} = 1$ (or to prove there is no G-isomorphism). Let $e = \alpha e_2 \in L$, and let the map $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ send x to xe.

Proposition 19.2. *Algorithm 19.1 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, outputs a G-isomorphism $\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L$ or a proof that none exists.*

Proof. By Theorem 12.4(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. Algorithm 10.3 checks whether L is invertible. If it is, we look for an $e \in L$ such that $e\bar{e} = 1$.

Algorithm 18.7 produces prime powers $\ell, m \geq 2^{n/2} + 1$ such that

$$\gcd(k(\ell), k(m)) = k.$$

The algorithm in Proposition 10.1 produces $e_{\ell m}$, which then serves as both e_m and e_ℓ. Algorithm 4.2 finds a short vector ν_m (if it exists) in the coset

$$e_{\ell m} + mL^{k(m)} \in L^{k(m)}/mL^{k(m)}.$$

If $e \in L$ is short, then $\nu_m = e^{k(m)}$ by Lemma 18.9.

As in Lemma 11.5, the set I is an invertible $\mathbb{Z}\langle G\rangle$-ideal, and the map

$$L_{(I,w)} \xrightarrow{\sim} L, \qquad x \mapsto xe_2$$

is an isomorphism of G-lattices, so $L = Ie_2$. We next show that I^i for $i = 2, \dots, k$ can be computed in polynomial time. Let

$$q = (L : \mathbb{Z}\langle G\rangle e_2).$$

Then $L = \mathbb{Z}\langle G\rangle e_2 + \mathbb{Z}\langle G\rangle e_q$, so $I = \mathbb{Z}\langle G\rangle + \mathbb{Z}\langle G\rangle\beta$ where $\beta \in \mathbb{Q}\langle G\rangle$ and $\beta = e_q/e_2 \in \Lambda_{\mathbb{Q}}$. We claim that

$$I^i = \mathbb{Z}\langle G\rangle + \mathbb{Z}\langle G\rangle\beta^i$$

for all $i \in \mathbb{Z}_{>0}$. Namely, we have

$$L \supset \mathbb{Z}\langle G\rangle e_2 \supset qL,$$

so $L^i \supset \mathbb{Z}\langle G\rangle e_2^i \supset q^i L^i$. Since $L^i = I^i e_2^i$, we have

$$I^i \supset \mathbb{Z}\langle G\rangle \supset q^i I^i.$$

Similarly, letting $r = (L : \mathbb{Z}\langle G\rangle e_q)$ we have

$$I^i \supset \mathbb{Z}\langle G\rangle\beta^i \supset r^i I^i.$$

Since q and r are coprime by Lemma 10.2(i), we have

$$I^i \supset \mathbb{Z}\langle G\rangle + \mathbb{Z}\langle G\rangle\beta^i \supset q^i I^i + r^i I^i = I^i,$$

and the desired equality follows. Now $\beta, \beta^2, \dots, \beta^k$ are easily computable in polynomial time, since $k \le 2n$.

By Lemma 18.9, if $\alpha \in L_{(I^k, w^k)}$ is short then $\nu = \alpha^k$. Algorithm 17.4 then finds a short vector $\alpha \in L_{(I^k, w^k)}$, or proves that none exists. Then $e = \alpha e_2$ is a short vector in L, and the map $x \mapsto xe$ gives the desired G-isomorphism from $\mathbb{Z}\langle G\rangle$ to L. □

Remark 19.3. 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 $\mathbb{Z}\langle G\rangle$ by Lemma 9.5. At the end one would check whether $\langle e, e\rangle = 1$ and $\langle e, \sigma e\rangle = 0$ for all $\sigma \ne 1, u$. 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.

Thanks to Corollary 14.3, we can convert Algorithm 19.1 to an algorithm to test whether two G-lattices are G-isomorphic (and produce an isomorphism).

Algorithm 19.4. Given G, u, and two invertible G-lattices L and M, the algorithm determines whether there is a G-isomorphism $M \xrightarrow{\sim} L$, and if so, computes one.

(i) Compute $L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M}$.

(ii) Apply Algorithm 19.1 to find a G-isomorphism

$$\mathbb{Z}\langle G\rangle \xrightarrow{\sim} L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M},$$

or a proof that none exists. In the latter case, terminate with "no".

(iii) Using this map and the map

$$\overline{M} \otimes_{\mathbb{Z}\langle G\rangle} M \to \mathbb{Z}\langle G\rangle, \quad \overline{y} \otimes x \mapsto \overline{y} \cdot x,$$

output the composition of the (natural) maps

$$M \xrightarrow{\sim} \mathbb{Z}\langle G\rangle \otimes_{\mathbb{Z}\langle G\rangle} M \xrightarrow{\sim} L \otimes_{\mathbb{Z}\langle G\rangle} \overline{M} \otimes_{\mathbb{Z}\langle G\rangle} M \xrightarrow{\sim} L \otimes_{\mathbb{Z}\langle G\rangle} \mathbb{Z}\langle G\rangle \xrightarrow{\sim} L.$$

Acknowledgments: We thank Craig Gentry, Daniele Micciancio, René Schoof, Mike Szydlo, and all the participants of the 2013 Workshop on Lattices with Symmetry. We thank the reviewers for very helpful comments.

Note from the Editor in Chief: This paper was solicited by the editors, due to the extended abstract [9] on which it is based having been selected as one of the best papers at the conference Crypto 2014.

References

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

[2] N. Bourbaki, Eléments de mathématique. Algèbre. Chapitres 4 à 7, Springer, Berlin, 2007.

[3] N. Bourbaki, Elements of mathematics. Commutative algebra, Hermann, Paris; Addison-Wesley Publishing Co., Reading, Mass., 1972.

[4] 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`.

[5] 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.

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

[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., *Lattices*, in Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press, Cambridge, 2008, 127–181, `http://library.msri.org/books/Book44/files/06hwl.pdf`.

[9] 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.

[10] 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`.

[11] H. W. Lenstra, Jr. and A. Silverberg, *Roots of unity in orders*, Foundations of Computational Mathematics (2016), `http://doi.org/10.1007/s10208-016-9304-1`.

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

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