journal of Groups, Complexity, Cryptology
Volume 16, Issue 1, 2024, pp. 6:1–6:16
https://gcc.episciences.org/

Submitted May 11, 2024
Published Jul. 29, 2024

COMPUTING THE UNIT GROUP OF A COMMUTATIVE FINITE $\mathbb{Z}$-ALGEBRA

MARTIN KREUZER AND FLORIAN WALSH

(Martin Kreuzer) Fakultät für Informatik und Mathematik, Universität Passau, D-94032 Passau, Germany
e-mail address: martin.kreuzer@uni-passau.de

(Florian Walsh) Fakultät für Informatik und Mathematik, Universität Passau, D-94032 Passau, Germany
e-mail address: florian.walsh@uni-passau.de

Abstract. For a commutative finite $\mathbb{Z}$-algebra, i.e., for a commutative ring R whose additive group is finitely generated, it is known that the group of units of R is finitely generated, as well. Our main results are algorithms to compute generators and the structure of this group. This is achieved by reducing the task first to the case of reduced rings, then to torsion-free reduced rings, and finally to an order in a reduced ring. The simplified cases are treated via a calculation of exponent lattices and various algorithms to compute the minimal primes, primitive idempotents, and other basic objects. All algorithms have been implemented and are available as a `SageMath` package. Whenever possible, the time complexity of the described methods is tracked carefully.

1. Introduction

In the study of the structure of a commutative ring, one important aspect is its group of units. A famous result in this direction dating back to 1846 is L.G. Dirichlet's unit theorem (see [7]) which says that the group of units of the ring of integers of a number field is a finitely generated abelian group. Much later, in 1972, this was generalized to orders in such rings by H. Zassenhaus (see [30]). With the advance of computer algebra, the computation of an actual system of generators of such a unit group and its set of relations have become feasible, and algorithms achieving these tasks have been developed (see, for example, [6, 3]). Also for other types of rings, for which the group of units is known to be finitely generated, explicit algorithms for computing their generators or their presentations have been described, including for orders in (not necessarily commutative) finite dimensional $\mathbb{Q}$-algebras (see [4]), for integral group rings over finite abelian groups (see [10]), and for the affine coordinate rings of rational normal curves and elliptic curves (see [5]).

In this paper we improve on many of these results and consider the general case of a commutative finite $\mathbb{Z}$-algebra, i.e., a commutative ring which is a finitely generated $\mathbb{Z}$-module.

Key words and phrases: finite Z-algebra, unit group, exponent lattice, explicitly given algebra.
2020 *Mathematics Subject Classification.* 68W30, 20F05, 13P99, 16Z05.

DOI:10.46298/jgcc.2024.16.1.13875

In [24], P. Samuel proved that the unit groups of such rings are finitely generated. The main results of this paper are algorithms for computing a system of generators of these unit groups, as well as for calculating their structure.

Let us describe the path we follow to reach these goals. After recalling some basic results about finite $\mathbb{Z}$-algebras in Section 2, we devise algorithms for computing *exponent lattices* in such a ring R, i.e., lattices of the type $\Lambda = \{(a_1, \ldots, a_k) \in \mathbb{Z}^k \mid f_1^{a_1} \cdots f_k^{a_k} = 1\}$ where $f_1, \ldots, f_k \in R$. Using several techniques from our previous paper [19], we reduce the calculation of exponent lattices to the cases of 0-dimensional algebras over the fields $\mathbb{Q}$ and $\mathbb{F}_p$ with a prime p. For this characteristic p part, we solve the problem first modulo p and then refine the answer modulo higher powers of p with a method resembling the well-known technique of Hensel lifting (see Proposition 3.6). Altogether, we obtain Algorithm 3.8 and discuss several methods to improve its implementation (see Remark 3.9).

The next step is taken in Section 4 where we consider the case of a reduced finite $\mathbb{Z}$-algebra. If the algebra is even integral, algorithms for computing its unit group are known (see Remark 4.1). The general case is treated by calculating the primitive idempotents and computing the unit group of an order via reduction to the case of orders in number fields (see Lemma 4.4 and Algorithm 4.5). This solves the torsion-free reduced case (see Corollary 4.7) and allows us to deal with the general reduced case using a version of the Chinese Remainder Theorem (see Lemma 4.9 and Algorithm 4.10).

Finally, in Section 5, we attack the general case of a finite $\mathbb{Z}$-algebra. The main additional task is to find generators of $1 + \mathrm{Rad}(0)$ (see Lemma 5.1). We provide two different solutions (Algorithm 5.3 and Lemma 5.4). All in all, we are able to compute a system of generators of the unit group of a finite $\mathbb{Z}$-algebra (see Algorithm 5.3) and also its structure in terms of its rank and invariant factors (see Corollary 5.6).

Throughout the paper we tried to keep track of the complexity of the presented algorithms. First of all, this depends on the way the algebra R is given: either explicitly (via generators and relations of R^+ plus the structure constants) or through a presentation $R = \mathbb{Z}[x_1, \ldots, x_n]/I$ with an ideal I given by explicit generators. In the first case, many steps of the algorithms can be performed in probabilistic polynomial time plus (possibly) one integer factorization. In the second case, we may have to first compute a strong Gröbner basis to get going. After we reduce everything to the case of an order in a number field, we have to rely on previous work whose precise complexity estimates are apparently not known.

All algorithms in this paper are illustrated by explicit examples. They were computed using an implementation by the second author in the software system `SageMath` [27]. The complete package is available freely from his GitHub page [28]. As for the basic definitions and notation, we adhere to the terminology given in the books [17] and [18].

2. Preliminaries on Finite $\mathbb{Z}$-Algebras

In this section we collect basic properties of finite $\mathbb{Z}$-algebras, i.e., $\mathbb{Z}$-algebras which are finitely generated as a $\mathbb{Z}$-module. Given such an algebra R, we denote its underlying $\mathbb{Z}$-module by R^+. Subsequently, we assume that a $\mathbb{Z}$-algebra R is either given by an ideal I in $P = \mathbb{Z}[x_1, \ldots, x_n]$ such that $R = P/I$ or that it is given as follows.

Remark 2.1. A $\mathbb{Z}$-algebra R is said to be **explicitly given** if it is given by the following information.

(a) A set of generators $\mathcal{G} = \{g_0, \dots, g_n\}$ of the $\mathbb{Z}$-module R^+, together with a matrix $A = (a_{\ell k}) \in \mathrm{Mat}_{m,n+1}(\mathbb{Z})$ whose rows generate the syzygy module $\mathrm{Syz}_{\mathbb{Z}}(\mathcal{G})$ of $\mathcal{G}$.
(b) Structure constants $c_{ijk} \in \mathbb{Z}$ such that $g_i g_j = \sum_{k=0}^{n} c_{ijk} g_k$ for $i, j = 0, \dots, n$.

Notice that we may assume $g_0 = 1$ and encode this information as an ideal

$$I = \left\langle x_i x_j - \sum_{k=0}^{n} c_{ijk} x_k,\ \sum_{k=0}^{n} a_{\ell k} g_k \mid i, j = 1, \dots, n,\ \ell = 1, \dots, m \right\rangle$$

in $P = \mathbb{Z}[x_1, \dots, x_n]$ such that $R \cong P/I$.

If $R = P/I$ is not explicitly given, then we can obtain an explicit representation from a strong Gröbner basis of I.

Definition 2.2. Given an ideal $I \subseteq P$ and a term ordering σ, a set of polynomials $G = \{g_1, \dots, g_r\}$ in I is called a **strong σ-Gröbner basis** of I if, for every non-zero polynomial $f \in I$, there exists an index $i \in \{1, \dots, r\}$ such that $\mathrm{LM}_\sigma(f)$ is a multiple of $\mathrm{LM}_\sigma(g_i)$.

Strong Gröbner bases can be computed using a generalization of Buchberger's algorithm (see for example [1, Ch. 4] or [9]). For some ideal-theoretic operations which can be performed effectively using strong Gröbner bases, we refer to [1, Ch. 4] and [17, Ch. 3]. Generators of the $\mathbb{Z}$-module R^+ can be deduced from a strong Gröbner basis as follows.

Proposition 2.3. (Macaulay's Basis Theorem for Finite $\mathbb{Z}$-Algebras)
Let $I \subseteq P$ be an ideal such that P/I is a finite $\mathbb{Z}$-algebra, let σ be a term ordering on $\mathbb{T}^n$, and let $L = \{m \in \mathrm{LM}_\sigma(I) \mid \mathrm{LC}_\sigma(m) = 1\}$ be the set of all monic leading monomials of I. Then the residue classes of the terms in $\mathcal{O}_\sigma = \mathbb{T}^n \setminus L$ form a generating set of the $\mathbb{Z}$-module P/I.

Proof. See Proposition 6.6 in [20]. □

Given generators of R^+ as in the preceding lemma, it is also possible to determine an explicit presentation of R (see Algorithm 6.7 and Corollary 6.8 in [20]). From such a presentation we can then determine the structure of R^+.

Remark 2.4. By the structure theorem for finitely generated modules over a principal ideal domain there exist r and $k_1, \dots, k_u$ in $\mathbb{N}$ such that k_i divides k_j for $i < j$ and such that

$$R^+ \cong \mathbb{Z}^r \oplus \mathbb{Z}/k_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/k_u\mathbb{Z}.$$

The numbers r and $k_1, \dots, k_u$ are uniquely determined by R^+. We call r the **rank** and $k_1, \dots, k_u$ the **invariant factors** of R^+. The largest invariant factor k_u is the exponent of the torsion subgroup of R^+. We call it the **torsion exponent** τ of R^+.

The rank, the invariant factors, and the torsion exponent can be determined using a Smith normal form computation (for details we refer to Section 2 in [20]). Algorithms which compute the Smith normal form of an integer matrix can for example be found in [13] or [26]. If an explicit presentation is given or has been determined from a strong Gröbner basis, many computations that we need in the following sections can be performed efficiently, i.e., in (probabilistic) polynomial time in the bit complexity of the input. More precisely, we have the following complexity results.

Remark 2.5. Assume that R is an explicitly given finite $\mathbb{Z}$-algebra.

(a) The minimal prime ideals of R can be computed in zero-error probabilistic polynomial time except for the factorization of one integer (see Algorithm 4.2 in [20]).
(b) The primitive idempotents of R can be obtained from its minimal prime ideals in polynomial time using Algorithm 5.8 in [20].
(c) The intersection of ideals in R can be determined in polynomial time using Proposition 2.9 in [20].

3. Exponent Lattices in Finitely Generated $\mathbb{Z}$-Algebras

Let $R = P/I$ be a finitely generated $\mathbb{Z}$-algebra. In the following we present an algorithm which computes the multiplicative relations between units in R. We emphasize that in this section we do not require that R is a finite $\mathbb{Z}$-algebra.

Definition 3.1. Let R be a ring and let $f_1, \ldots, f_k \in R^\times$. Then the lattice

$$\Lambda = \{(a_1, \ldots, a_k) \in \mathbb{Z}^k \mid f_1^{a_1} \cdots f_k^{a_k} = 1\}$$

is called the **exponent lattice** of $(f_1, \ldots, f_k)$ in R.

The goal of this section is to provide an algorithm which computes a basis of the exponent lattice of the tuple $(f_1, \ldots, f_k)$ in a finitely generated $\mathbb{Z}$-algebra. In the following we refer to this task simply as computing an exponent lattice. Let us recall how this task is solved in affine K-algebras, i.e., in finitely generated algebras over a field K.

Remark 3.2. (Computing Exponent Lattices in Affine K-Algebras)
The problem of computing the exponent lattices has been considered by many authors. For units in a number field algorithms can be found in [11], in Section 7.3 of [14], in Section 3 of [15], or in [31]. Based on these algorithms, a method for computing the exponent lattice in zero-dimensional $\mathbb{Q}$-algebras is presented in [21]. Recently, we generalized these results and presented a method (see Algorithm 5.3 in [19]) for computing exponent lattices in arbitrary affine K-algebras where K is a field such that exponent lattices in finite extensions of K can be effectively computed. Note, that this includes the cases $K = \mathbb{Q}$ and $K = \mathbb{F}_p$.

Now the main idea is to reduce the problem of computing an exponent lattice in R to computing exponent lattices in affine $\mathbb{Q}$- and $\mathbb{F}_p$-algebras.

Lemma 3.3. *Let R be a ring, I an ideal in R, and $f \in R$. If $m \in \mathbb{N}$ is such that $I : f^\infty = I : f^m$, then*

$$I = (I : f^m) \cap \langle I, f^m \rangle.$$

Proof. See [12], Lemma 3.3.6. □

Together with the following proposition this lemma is the main tool for reducing the exponent lattice computation to $\mathbb{Q}$- and $\mathbb{F}_p$-algebras.

Proposition 3.4. *Let I be an ideal in P, let $G = \{g_1, \ldots, g_s\}$ be a minimal strong Gröbner basis of I, and let $N \in \mathbb{Z}$ be the least common multiple of the leading coefficients of the elements of G. Then the following holds.*
(a) $I = (I : \langle N \rangle) \cap (I + \langle N \rangle)$
(b) *If $I \cap \mathbb{Z} = \langle 0 \rangle$, then $I\mathbb{Q}[x_1, \ldots, x_n] \cap P = I : \langle N \rangle$.*

Proof. See [16], Proposition 4.3. □

The following example given in Section 4 of [16] illustrates the fact that the least common multiple N of the leading coefficients of a strong Gröbner basis as in the proposition is in general not the smallest number satisfying $I : \langle N\rangle = I : \langle N\rangle^\infty$.

Example 3.5. Consider the ideal $I = \langle x^2, y^2, z^2, xz + yz, xy, 2x - y, 3z\rangle \subseteq \mathbb{Z}[x, y, z]$. The generators form a strong Gröbner basis of I and the least common multiple of the leading coefficients is 6. But we have $I : \langle 3\rangle = I : \langle 6\rangle = I : \langle 6\rangle^\infty$.

Let $\{g_1, \dots, g_k\}$ be a strong Gröbner basis of I and let N be the least common multiple of the leading coefficients of the g_i. Then we have $I = I : \langle N\rangle \cap \langle I, N\rangle$. The property $I : \langle N\rangle = I\mathbb{Q}[x_1, \dots, x_n] \cap P$ then allows us to compute the exponent lattice modulo $I : \langle N\rangle$. This can be done using Remark 3.2. The ideal $\langle I, N\rangle$ can be further split into $\langle I, N\rangle = \bigcap_{i=1}^r \langle I, p_i^{e_i}\rangle$ where $N = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of N. Let $p \in \mathbb{N}$ be a prime number. The exponent lattice modulo an ideal of the form $\langle I, p\rangle$ can be computed using the fact that the polynomial $f_1^{c_1} \cdots f_k^{c_k} - 1$ is in I if and only if its canonical residue class is in $I\mathbb{F}_p[x_1, \dots, x_n]$. We can therefore again apply Remark 3.2. It remains to handle ideals of the form $\langle I, p^e\rangle$ with $e > 1$.

Proposition 3.6. *Let I be an ideal such that $I \cap \mathbb{Z} = \{0\}$. Consider the finitely generated $\mathbb{Z}$-algebra $R = P/I$, and let $f_1, \dots, f_k \in R^\times$. Let p be a prime number, let e be a positive integer, and let $b_1, \dots, b_m \in \mathbb{Z}^k$ be a basis of the exponent lattice Λ of $(\bar{f}_1, \dots, \bar{f}_k)$ in $P/\langle I, p^e\rangle$. Then the following conditions are equivalent.*

(a) *The $\mathbb{Z}$-linear combination $c = a_1 b_1 + \cdots + a_m b_m \in \Lambda$ with $a_1, \dots, a_m \in \mathbb{Z}$ is in the exponent lattice of $(\bar{f}_1, \dots, \bar{f}_k)$ in $P/\langle I, p^{e+1}\rangle$.*

(b) *The tuple $(a_1, \dots, a_m)$ is a solution of the linear equation over $\mathbb{Z}$ in the indeterminates $y_1, \dots, y_m$ given by*

$$\bar{h}_1 y_1 + \cdots + \bar{h}_m y_m = 0 \qquad \text{in } P/\langle I, p\rangle, \tag{i}$$

where $h_i = (f_1^{b_{i1}} \cdots f_k^{b_{ik}} - 1)/p^e \in R$ and $\bar{h}_i$ is its residue class modulo $\langle I, p\rangle$.

Proof. Since all tuples b_i are in Λ we have $f_1^{b_{i1}} \cdots f_k^{b_{ik}} = 1$ modulo $\langle I, p^e\rangle$. Therefore there exists $g_i \in P$ such that $f_1^{b_{i1}} \cdots f_k^{b_{ik}} = 1 + p^e g_i$ in R for $i = 1, \dots, m$. This shows $h_i = g_i$. Now the tuple c is in the exponent lattice of $(\bar{f}_1, \dots, \bar{f}_k)$ in $P/\langle I, p^{e+1}\rangle$ if and only if

$$f^c = f^{a_1 b_1} \cdots f^{a_m b_m} = (1 + p^e g_1)^{a_1} \cdots (1 + p^e g_m)^{a_m} = 1 + a_1 p^e g_1 + \cdots + a_m p^e g_m = 1$$

in $P/\langle I, p^{e+1}\rangle$. This is equivalent to $a_1 \bar{h}_1 + \cdots + a_m \bar{h}_m = 0$ in $P/\langle I, p\rangle$, which is satisfied if and only if $(a_1, \dots, a_m)$ is a solution of the linear equation (i). □

At this point we are ready to compute the exponent lattice of $(f_1, \dots, f_k)$ modulo an ideal of the form $\langle I, p^e\rangle$. This is achieved by first computing the exponent lattice of $(f_1, \dots, f_k)$ modulo $I\mathbb{F}_p[x_1, \dots, x_n]$ and then iteratively applying Proposition 3.6 to obtain the exponent lattice modulo $\langle I, p^i\rangle$ for $i = 2, \dots, e$.

Example 3.7. Let $I = \langle x^2 + x + 1, y^2 + y + 1, 8\rangle$, and consider the finite $\mathbb{Z}$-algebra $R = \mathbb{Z}[x, y]/I$. For $f_1 = 2x + 1$, $f_2 = 4y + 1$ and $f_3 = -2y - 1$ let us compute the exponent lattice of $(\bar{f}_1, \bar{f}_2, \bar{f}_3)$ in R. To compute the exponent lattice modulo $\langle I, 2\rangle$ we form the zero-dimensional $\mathbb{F}_2$-algebra $\mathbb{F}_2[x, y]/I\mathbb{F}_2[x, y]$, and obtain the exponent lattice $\Lambda_1 = \mathbb{Z}^3$. We then solve the linear equation in the indeterminates z_1, z_2, z_3 given by $xz_1 + 2yz_2 - (y + 1)z_3 = 0$

modulo $\langle I, 2\rangle$, and obtain the solution space $M_1 = \langle (0,1,0),(2,0,0),(0,0,2)\rangle$. Since $\Lambda_1 = \mathbb{Z}^3$, this yields $\Lambda_2 = M_1$. Then we solve the linear equation in the indeterminates z_1, z_2, z_3 given by $yz_1 - z_2 - z_3 = 0$ modulo $\langle I, 2\rangle$ and obtain the solution space $M_2 = \langle b_1, b_2, b_3\rangle$ with $b_1 = (0,1,1)$, $b_2 = (0,-1,1)$ and $b_3 = (2,0,0)$. Finally, we compute the exponent lattice

$$\Lambda_3 = \{c_1b_1 + c_2b_2 + c_3b_3 \mid c \in M_2\} = \langle (0,2,0),(2,0,2),(-2,0,2)\rangle.$$

Combining the previous results we now obtain the following algorithm.

Algorithm 3.8. (Computing Exponent Lattices in Finitely Generated $\mathbb{Z}$-Algebras) Let $R = P/I$ be a $\mathbb{Z}$-algebra, and let $f_1, \dots, f_k \in R^\times$. Consider the following sequence of instructions.

1: Compute $I \cap \mathbb{Z} = \langle q\rangle$.
2: **if** $q = 0$ **then**
3: Using Remark 3.2, compute the exponent lattice $\Lambda \subseteq \mathbb{Z}^k$ of $(f_1, \dots, f_k)$ in the $\mathbb{Q}$-algebra $\mathbb{Q} \otimes_{\mathbb{Z}} R$.
4: Compute a strong Gröbner basis $\{g_1, \dots, g_\ell\}$ of I.
5: Let $N = \mathrm{lcm}(\mathrm{LC}(g_1), \dots, \mathrm{LC}(g_\ell))$.
6: **if** $N = 1$ **then**
7: **return** Λ
8: **else**
9: Recursively apply the algorithm to compute the exponent lattice $M \subseteq \mathbb{Z}^k$ of $(f_1, \dots, f_k)$ in $P/(I + \langle N\rangle)$.
10: **return** $\Lambda \cap M$
11: **end if**
12: **else**
13: Compute the prime factorization $q = p_1^{e_1} \cdots p_r^{e_r}$.
14: **for** $i = 1, \dots, r$ **do**
15: Using Remark 3.2, compute the exponent lattice $M_i \subseteq \mathbb{Z}^k$ of $(f_1, \dots, f_k)$ in the $\mathbb{F}_p$-algebra $\mathbb{F}_p \otimes_{\mathbb{Z}} R$.
16: **for** $j = 1, \dots, e_i - 1$ **do**
17: Assume that M_i is generated by $\{b_1, \dots, b_m\} \subseteq \mathbb{Z}^k$.
18: For $s = 1, \dots, m$ form the elements $h_r = (f_1^{b_{s1}} \cdots f_k^{b_{sk}} - 1)/p_i^j \in R$.
19: Compute the solution space $M' \subseteq \mathbb{Z}^m$ of the linear equation over $\mathbb{Z}$ in the indeterminates $y_1, \dots, y_m$ given by
$$\bar{h}_1 y_1 + \cdots + \bar{h}_m y_m = 0 \quad \text{in } P/\langle I, p_i\rangle.$$
20: Replace M_i by the lattice $\{c_1b_1 + \cdots + c_mb_m \mid (c_1, \dots, c_m) \in M'\} \subseteq \mathbb{Z}^k$.
21: **end for**
22: **end for**
23: **return** the lattice $M_1 \cap \cdots \cap M_r$
24: **end if**

This is an algorithm which computes the exponent lattice of $(f_1, \dots, f_k)$ in R.

Proof. A tuple $a = (a_1, \dots, a_k) \in \mathbb{Z}^k$ is in the exponent lattice of $(f_1, \dots, f_k)$ if and only if $f_1^{a_1} \cdots f_k^{a_k} - 1 \in I$. By Proposition 3.4 we have $I = (I : \langle N\rangle) \cap \langle I, N\rangle$. In the case $I \cap \mathbb{Z} = \langle 0\rangle$, we have $I : \langle N\rangle = I\mathbb{Q}[x_1, \dots, x_n] \cap P$ by the same proposition. Line 3 therefore yields the exponent lattice of $(f_1, \dots, f_k)$ in $P/(I : \langle N\rangle)$. It remains to prove that lines 12–24 determine the exponent lattice of $(f_1, \ldots, f_k)$ in $P/\langle I, N\rangle$. Since we have $\langle I, N\rangle = \bigcap_{i=1}^{r} \langle I, p_i^{e_i}\rangle$, it is enough to show that lines 15–21 compute the exponent lattice of $(f_1, \ldots, f_k)$ in $P/\langle I, p_i^{e_i}\rangle$. Line 15 yields the exponent lattice of $(f_1, \ldots, f_k)$ in $P/\langle I, p_i\rangle$. It then follows from Proposition 3.6 that the j-th iteration of the for loop in lines 16–21 correctly computes the exponent lattice of $(f_1, \ldots, f_k)$ in $P/\langle I, p_i^{j+1}\rangle$. □

Let us collect some remarks about the implementation of this algorithm.

Remark 3.9. Suppose we are in the setting of Algorithm 3.8.

(a) A non-zero generator q of the ideal $I \cap \mathbb{Z}$ in line 1 is given by the unique integer contained in a reduced strong Gröbner basis of I. If R is a finite $\mathbb{Z}$-algebra, then q is zero if and only if the rank of R^+ is non-zero. The rank of an explicitly given finite $\mathbb{Z}$-algebra can be determined in polynomial time using a Smith normal form computation.

(b) As illustrated in Example 3.5 there can be a proper divisor M of N satisfying $I : \langle M\rangle = I : \langle M\rangle \cap \langle I, M\rangle$. By determining the smallest number with this property, unnecessary iterations in the else-branch of this algorithm can be avoided. If R is a finite $\mathbb{Z}$-algebra, then the smallest number with this property is given by the torsion exponent of R. It can be determined in polynomial time using a Smith normal form computation if R is explicitly given.

(c) If R is a finite $\mathbb{Z}$-algebra, then the $\mathbb{Q}$-algebra in line 3 and the $\mathbb{F}_p$-algebra in line 15 are zero-dimensional. Exponent lattices in an explicitly given zero-dimensional $\mathbb{Q}$-algebra can be computed in polynomial time (see Algorithm 8.3 in [21]). For zero-dimensional $\mathbb{F}_p$-algebras, the problem can be reduced to the discrete logarithm problem in finite fields (see Algorithm 3.20 in [19]).

(d) In line 19 we need to compute the solution space of the linear equation over $\mathbb{Z}$ in the indeterminates $y_1, \ldots, y_m$ given by

$$g_1 y_1 + \cdots + g_m y_m = 0$$

in $P/\langle I, p_i\rangle$. This can be achieved by checking for all $(a_1, \ldots, a_m) \in \mathbb{Z}^m$ with $0 \le a_\ell \le p_i$ for $\ell = 1, \ldots, m$ whether $a_1 g_1 + \cdots + a_m g_m \in \langle I, p_i\rangle$. Alternatively, one can perform a syzygy calculation using Gröbner basis techniques. In particular, for large p_i, this might be more efficient. If R is an explicitly given finite $\mathbb{Z}$-algebra, we can use [20, Prop. 2.6] to solve this linear equation efficiently.

The following example illustrates how Algorithm 3.8 can be applied to compute exponent lattices in finite $\mathbb{Z}$-algebras.

Example 3.10. Let $I = \langle x^2 + x + 1,\ y^2 + y + 1,\ 6z^2,\ z^3\rangle$, and consider the finite $\mathbb{Z}$-algebra $R = \mathbb{Z}[x, y, z]/I$. Let $f_1 = -xyz - xz + 1$, $f_2 = y + 1$ and $f_3 = xy + x + y + 1$. We apply Algorithm 3.8 to compute the exponent lattice of $(\bar{f}_1, \bar{f}_2, \bar{f}_3)$ in R.

1: Since R is a finite $\mathbb{Z}$-algebra, we compute its rank given by 8.
2: The rank of R is non-zero, which implies $I \cap \mathbb{Z} = \langle 0\rangle$.
3: Using Remark 3.2, we compute the exponent lattice $\Lambda = \langle (0, 6, 0), (0, 0, 3)\rangle$ in the zero-dimensional $\mathbb{Q}$-algebra $\mathbb{Q} \otimes_{\mathbb{Z}} R$.
4,5: Since R is a finite $\mathbb{Z}$-algebra, we compute its torsion exponent given by 6.
9: We recursively apply the Algorithm to compute the exponent lattice of $(\bar{f}_1, \bar{f}_2, \bar{f}_3)$ in $P/\langle I, 6\rangle$.
1: We have $q = 6$.
13: We determine the factorization $6 = 2 \cdot 3$.

15: Using Remark 3.2, we compute generators $(4,0,0)$, $(0,3,0)$ and $(0,0,3)$ of the exponent lattice M_1 of $(\bar{f}_1, \bar{f}_2, \bar{f}_3)$ modulo $I\mathbb{F}_2[x,y,z]$ and generators $(3,0,0)$, $(0,6,0)$, and $(0,0,3)$ of the exponent lattice M_2 modulo $I\mathbb{F}_3[x,y,z]$.
20: The exponent lattice of $(\bar{f}_1, \bar{f}_2, \bar{f}_3)$ in R is given by $\Lambda \cap M_1 \cap M_2 = \langle (0,6,0), (0,0,3) \rangle$.

It is an open question to what extent Algorithm 3.8 can be generalized to the non-commutative case. A straightforward generalization does not seem to be possible, since in this case the multiplicative relations between units are in general not computable. This follows from the fact that the subgroup membership problem is undecidable for 4×4 integral matrices (see [23]). Also note that multiplicative relations in general do not form a lattice in the non-commutative case.

4. The Unit Group of Reduced Finite $\mathbb{Z}$-Algebras

Let us begin by considering the case of integral finite $\mathbb{Z}$-algebras, i.e, algebras of the form $P/\mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal in P.

Remark 4.1. (Computing the Unit Group of Integral Finite $\mathbb{Z}$-Algebras)
Let $\mathfrak{p}$ be a prime ideal in P such that $R = P/\mathfrak{p}$ is a finite $\mathbb{Z}$-algebra.

(a) If $\mathfrak{p} \cap \mathbb{Z} = \langle 0 \rangle$, then $K = \mathbb{Q} \otimes_{\mathbb{Z}} R$ is a number field. Since $P/\mathfrak{p}$ is integral over $\mathbb{Z}$ and its rank equals $\dim_{\mathbb{Q}}(K)$, the ring R is an order in K. Generators of the unit group of R can therefore be computed using for example the algorithms given in [6] or [3]. These algorithms require that the field K is given by a primitive element. Such an element can be determined using one of the methods described in [29] or Algorithm 6.3 in [21].
(b) If $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ for a prime number p, then $P/\mathfrak{p}$ is isomorphic to the finite field $K = \mathbb{F}_p \otimes_{\mathbb{Z}} R$. The problem therefore reduces to computing a primitive root of K. Algorithms for this task can be found in [25] or in [8].

Let us now consider the case of a reduced finite $\mathbb{Z}$-algebra $R = P/I$. If $I \cap \mathbb{Z} = \langle n \rangle$ for some $n \in \mathbb{Z} \setminus \{0\}$, then the minimal prime ideals of R are maximal ideals and therefore pairwise coprime. By the Chinese Remainder Theorem computing the unit group then reduces to the case discussed above. If $I \cap \mathbb{Z} = \langle 0 \rangle$, then the minimal prime ideals of R need not be pairwise coprime.

Example 4.2. Consider the ideal $I = \langle x^2 + x + 1, y^2 + y + 1 \rangle$. Its minimal prime ideals are given by $\mathfrak{p}_1 = \langle x - y, y^2 + y + 1 \rangle$ and $\mathfrak{p}_2 = \langle x + y + 1, y^2 + y + 1 \rangle$ and we have $\mathfrak{p}_1 + \mathfrak{p}_2 = \langle x + 2, y + 2, 3 \rangle$.

This example demonstrates that we cannot directly reduce to the integral case. Instead we notice, that if R is torsion-free, then R is an order in the reduced zero-dimensional $\mathbb{Q}$-algebra $\mathbb{Q} \otimes_{\mathbb{Z}} R$.

Definition 4.3. Let A be a zero-dimensional reduced $\mathbb{Q}$-algebra. A subring $\mathcal{O}$ of A is called an **order** if there is a basis $a_1, \dots, a_m$ of A such that $\mathcal{O} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_m$.

The unit group of an order in a zero-dimensional reduced $\mathbb{Q}$-algebra, can be computed using the algorithm presented in Section 3 of [10]. In the following we present a modified version of this algorithm.

Lemma 4.4. *Let A be a reduced zero-dimensional $\mathbb{Q}$-algebra and let e_1, e_2 be orthogonal idempotents with $e_1 + e_2 = 1$. Let $\mathcal{O}$ be an order in A. Consider the ideal $J = (e_1\mathcal{O} \cap \mathcal{O}) + (e_2\mathcal{O} \cap \mathcal{O})$ and form the ring $S = \mathcal{O}/J$. Consider the ring homomorphisms $\varphi_i : e_i\mathcal{O} \to S$ given by $\varphi_i(e_i a) = a + J$ for $a \in \mathcal{O}$. Then we have*

$$\mathcal{O} = \{a_1 + a_2 \mid a_i \in e_i\mathcal{O} \text{ and } \varphi_1(a_1) = \varphi_2(a_2)\}$$

Proof. See [10], Lemma 3.1. □

Given an order $\mathcal{O}$ in a reduced zero-dimensional $\mathbb{Q}$-algebra A and primitive idempotents $e_1, \ldots, e_k$ of A, we can compute generators of $(e_i\mathcal{O})^\times$ since $e_i\mathcal{O}$ is an order in the number field e_iA. We can then iteratively apply Lemma 4.4 to determine $\mathcal{O}^\times$.

Algorithm 4.5. (Computing the Unit Group of an Order)
Let A be a reduced zero-dimensional $\mathbb{Q}$-algebra, and let $\mathcal{O}$ be an order in A. Consider the following sequence of instructions.

Compute the primitive idempotents $e_1, \ldots, e_m$ of A.
Compute $U = (e_1\mathcal{O})^\times$.
for $j = 2, \ldots, m$ **do**
  Set $f = e_1 + \cdots + e_{j-1}$.
  Compute generators of $f\mathcal{O}\cap\mathcal{O}$ and $e_j\mathcal{O}\cap\mathcal{O}$ and form the ideal $J = (f\mathcal{O}\cap\mathcal{O}) + (e_j\mathcal{O}\cap\mathcal{O})$ in $\mathcal{O}$.
  Compute generators $e_jh_1, \ldots, e_jh_\ell$ of $(e_j\mathcal{O})^\times$.
  Assume that $U = \{fg_1, \ldots, fg_k\}$.
  Compute a set of generators $B \subseteq \mathbb{Z}^{k+\ell}$ of the exponent lattice Λ of the tuple $\big(g_1, \ldots, g_k, h_1^{-1}, \ldots, h_\ell^{-1}\big)$ in $\mathcal{O}/J$.
  Set $U = \Big\{ fg_1^{b_1} \cdots g_k^{b_k} + e_jh_1^{b_{k+1}} \cdots h_\ell^{b_{k+\ell}} \mid b \in B \Big\}$.
end for
return U.

This is an algorithm which computes a set of generators of $\mathcal{O}^\times$.

Proof. It suffices to show that after the j-th iteration U generates the unit group of the order $(e_1 + \cdots + e_j)\mathcal{O}$ in $(e_1 + \cdots + e_j)A$. Let $r \in \mathcal{O}$ and consider the group homomorphisms $\varphi_f : f\mathcal{O} \to \mathcal{O}/J$ given by $\varphi_f(fr) = r + J$ and $\varphi_{e_j} : e_j\mathcal{O} \to \mathcal{O}/J$ given by $\varphi_{e_j}(e_jr) \mapsto r + J$. Let $g = fg_1^{c_1} \cdots g_k^{c_k}$ in U and $h = e_jh_1^{c_{k+1}} \cdots h_\ell^{c_{k+\ell}}$ in $(e_j\mathcal{O})^\times$. Then by Lemma 4.4 the element $g - h$ is in the unit group of $(e_1 + \cdots + e_j)\mathcal{O}$ if and only if

$$\varphi_f(g) = g_1^{c_1} \cdots g_k^{c_k} + J = h_1^{c_{k+1}} \cdots h_\ell^{c_{k+\ell}} + J = \varphi_{e_j}(e_jh).$$

This is equivalent to $(c_1, \ldots, c_{k+\ell}) \in \Lambda$. □

Let $R = P/I$ be a finite $\mathbb{Z}$-algebra. If R is torsion-free and reduced, then it is an order in the zero-dimensional $\mathbb{Q}$-algebra $A = \mathbb{Q} \otimes_{\mathbb{Z}} R$. Consequently, Algorithm 4.5 can be applied to compute the unit group of the order R in A. In this case the steps of this algorithm can be performed as follows.

Lemma 4.6. *Let $R = P/I$ be a reduced torsion-free finite $\mathbb{Z}$-algebra, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the minimal prime ideals of I.*

(a) *The $\mathbb{Q}$-algebra $A = \mathbb{Q} \otimes_{\mathbb{Z}} R$ is zero-dimensional and its maximal ideals are given by $\mathfrak{m}_i = \mathfrak{p}_i\mathbb{Q}[x_1, \ldots, x_n]$ for $i = 1, \ldots, m$. We can therefore compute elements $q_i \in \bigcap_{i \neq j} \mathfrak{m}_j$*

and $p_i \in \mathfrak{m}_i$ such that $q_i + p_i = 1$. The residue classes $\bar{q}_1, \dots, \bar{q}_m$ in A then form the primitive idempotents of A

(b) *The ideal $\bar{q}_i R$ in A is isomorphic to $\bar{q}_i(P/\mathfrak{p}_i)$.*

(c) *We have $\bar{q}_i R \cap R = \bigcap_{j \neq i} \mathfrak{p}_i / I$.*

(d) *For $f = \sum_{i \neq j} q_i$ we have $\bar{f} R \cap R = \mathfrak{p}_j / I$.*

Proof. Part (a) is a direct consequence of the Chinese Remainder Theorem (see Lemma 3.7.4 in [17]), and (b) follows from the fact that $\bar{q}_i A$ is isomorphic to $A/\mathfrak{m}_i$.

To proof (c), we notice that the ideal $\bar{q}_i R \cap R$ is contained in the right-hand side, since $q_i \in \bigcap_{i \neq j} \mathfrak{m}_j$. To show the opposite inclusion, let $f \in P$ such that $\bar{f} \in \bigcap_{i \neq j} \mathfrak{p}_j / I$. Then we have $f = q_i f + p_i f$. Since $p_i \in \mathfrak{m}_i$, this implies $p_i f \in \bigcap_{i=1,\dots,m} \mathfrak{p}_i = I$. Hence, $\bar{f} = \bar{q}_i \bar{f} \in \bar{q}_i R \cap R$. Part (d) follows analogously. □

Using these observations, we can adapt Algorithm 4.5 as follows.

Corollary 4.7. (Computing the Unit Group of a Reduced Torsion-Free Finite $\mathbb{Z}$-Algebra)
Let $R = P/I$ be a reduced torsion-free finite $\mathbb{Z}$-algebra. Consider the following sequence of instructions.

1: *Compute the minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ of I.*
2: ***for** $i = 1, \dots, m$ **do***
3:     *Compute elements $q_i \in \bigcap_{i \neq j} \mathfrak{p}_j \mathbb{Q}[x_1, \dots, x_n]$ and $p_i \in \mathfrak{p}_i \mathbb{Q}[x_1, \dots, x_n]$ such that $q_i + p_i = 1$.*
4: ***end for***
5: *Using Remark 4.1, compute a set of polynomials U such that their residue classes generate $(P/\mathfrak{p}_1)^\times$.*
6: ***for** $j = 2, \dots, m$ **do***
7:     *Form the ideal $J = \bigcap_{1 \leq i \leq j-1} \mathfrak{p}_i + \mathfrak{p}_j$.*
8:     *Using Remark 4.1, compute polynomials $h_1, \dots, h_\ell$ such that their residue classes generate $(P/\mathfrak{p}_j)^\times$.*
9:     *Assume that $U = \{g_1, \dots, g_k\}$, and compute a set of generators $B \subseteq \mathbb{Z}^{k+\ell}$ of the exponent lattice of $\left(\bar{g}_1, \dots, \bar{g}_k, \bar{h}_1^{-1}, \dots, \bar{h}_\ell^{-1}\right)$ in P/J.*
10:     *Set $U = \left\{ f g_1^{b_1} \cdots g_k^{b_k} + q_j h_1^{b_{k+1}} \cdots h_\ell^{b_{k+\ell}} \mid b \in B \right\}$ where $f = q_1 + \cdots + q_{j-1}$.*
11: ***end for***
12: ***return** U.*

This is an algorithm which computes a set of polynomials such that their residue classes generate $R^\times$.

Proof. Since R is torsion-free and reduced, it is an order in the zero-dimensional $\mathbb{Q}$-algebra $\mathbb{Q} \otimes_{\mathbb{Z}} R$. Now we show that the steps of this algorithm correspond to the steps of Algorithm 4.5.

Assume that at the start of the j-th iteration of the for-loop in lines 6–11 the residue classes of the elements in U generate the unit group of $R_{j-1} = P/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{j-1})$. Consider the finite $\mathbb{Z}$-algebra $R_j = P/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_j)$. The residue classes of the elements $f = q_1 + \cdots + q_{j-1}$ and q_j form orthogonal idempotents in $\mathbb{Q} \otimes_{\mathbb{Z}} R_j$ with $\bar{f} + \bar{q}_j = 1$. By Lemma 4.6.b we then have $\bar{q}_j R_j \cong \bar{q}_j(P/\mathfrak{p}_j)$ and $\bar{f} R_j \cong \bar{f} R_{j-1}$. Furthermore Lemma 4.6.c yields $\bar{q}_j R_j \cap R_j = (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{j-1})/I$ and $\bar{f} R_j \cap R_j = \mathfrak{p}_j / I$. This shows that the ideal J in line 7 corresponds to the ideal J in line 5 of Algorithm 4.5. □

Let us apply this algorithm to a concrete example.

Example 4.8. Let $I = \langle x^2+x+1, y^2+y+1, z^2+z+1\rangle$, and consider the finite $\mathbb{Z}$-algebra $R = \mathbb{Z}[x,y,z]/I$. We follow the steps of Corollary 4.7 to compute generators of $R^\times$.

1: We compute the minimal prime ideals of I and obtain

$$\mathfrak{p}_1 = \langle y-z, x+z+1, z^2+z+1\rangle$$
$$\mathfrak{p}_2 = \langle y-z, x-z, z^2+z+1\rangle$$
$$\mathfrak{p}_3 = \langle y+z+1, x+z+1, z^2+z+1\rangle$$
$$\mathfrak{p}_4 = \langle y+z+1, x-z, z^2+z+1\rangle$$

2–4: We compute the primitive idempotents

$$e_1 = 1/3\bar{x}\bar{y} + 1/3\bar{x}\bar{z} - 1/3\bar{y}\bar{z} + 1/3\bar{x} + 1/3$$
$$e_2 = -1/3\bar{x}\bar{y} - 1/3\bar{x}\bar{z} - 1/3\bar{y}\bar{z} - 1/3\bar{x} - 1/3\bar{y} - 1/3\bar{z}$$
$$e_3 = -1/3\bar{x}\bar{y} + 1/3\bar{x}\bar{z} + 1/3\bar{y}\bar{z} + 1/3\bar{z} + 1/3$$
$$e_4 = 1/3\bar{x}\bar{y} - 1/3\bar{x}\bar{z} + 1/3\bar{y}\bar{z} + 1/3\bar{y} + 1/3$$

of the zero-dimensional $\mathbb{Q}$-algebra $\mathbb{Q}\otimes_{\mathbb{Z}} R$.

5: Using Remark 4.1, we determine a set of generators $U = \{\bar{z}+1\}$ of $(R/\mathfrak{p}_1)^\times$.

7: Form the ideal $J = \mathfrak{p}_1 + \mathfrak{p}_2 = \langle x+1, y+2, z+2, 3\rangle$.

8: Using Remark 4.1, we compute $(R/\mathfrak{p}_2)^\times = \langle \bar{z}+1\rangle$.

9: Using Remark 3.2, we compute generators $(1,1)$ and $(0,2)$ of the exponent lattice of $(\bar{z}+1, (\bar{z}+1)^{-1})$ in the finite field R/J.

10: Compute $e_1(\bar{z}+1) + e_2(\bar{z}+1) = \bar{z}+1$ and $e_1 + e_2(\bar{y}+1)^2 = -\bar{y}\bar{z} - \bar{y}$ and set $U = \{\bar{z}+1, -\bar{y}\bar{z}-\bar{y}\}$.

7: Form the ideal $J = (\mathfrak{p}_1 \cap \mathfrak{p}_2) + \mathfrak{p}_3 = \langle x+2, y+2, z+2, 3\rangle$.

8: Using Remark 4.1, we compute $(R/\mathfrak{p}_2)^\times = \langle \bar{z}+1\rangle$.

9: Using Remark 3.2, we compute generators $(1,0,1)$, $(0,1,0)$ and $(0,0,2)$ of the exponent lattice of $(\bar{z}+1, -\bar{y}\bar{z}-\bar{y}, (\bar{z}+1)^{-1})$ in R/J.

10: Set $U = \{\bar{z}+1, -\bar{y}\bar{z}-\bar{y}, \bar{x}\bar{z}+\bar{x}+\bar{z}+1\}$.

7: Form the ideal $J = (\mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3) + \mathfrak{p}_4 = \langle z^2+z+1, x+2z, y+z+1, 3\rangle$.

8: Using Remark 4.1, we compute $(R/\mathfrak{p}_2)^\times = \langle \bar{z}+1\rangle$.

9: Using Remark 3.2, we compute generators $(1,0,0,1)$, $(0,1,0,2)$, $(0,0,1,2)$ and $(0,0,0,6)$ of the exponent lattice in R/J of

$$\left(\bar{z}+1, -\bar{y}\bar{z}-\bar{y}, \bar{x}\bar{z}+\bar{x}+\bar{z}+1, (\bar{z}+1)^{-1}\right).$$

10: Set $U = \{\bar{z}+1, -\bar{y}\bar{z}-\bar{y}, \bar{x}\bar{z}+\bar{x}+\bar{z}+1, 1\}$.

12: The algorithm returns the generators $\bar{z}+1, -\bar{y}\bar{z}-\bar{y}, \bar{x}\bar{z}+\bar{x}+\bar{z}+1$ of $R^\times$.

A reduced finite $\mathbb{Z}$-algebra need not be torsion-free, but we can decompose it into a direct product of finitely many finite fields and a torsion-free algebra.

Lemma 4.9. *Let R be a reduced finite $\mathbb{Z}$-algebra. Let $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ be the minimal prime ideals of R of height n, let $\mathfrak{m}_1,\dots,\mathfrak{m}_s$ be the maximal ideals of R, and let $J = \mathfrak{p}_1\cap\dots\cap\mathfrak{p}_r$. Then R/J is torsion-free and we have $R \cong R/J \times R/\mathfrak{m}_1 \times \dots \times R/\mathfrak{m}_s$.*

Proof. As a reduced ring, R does not have embedded prime ideals. Therefore J is not contained in any $\mathfrak{m}_i$. Since $\mathfrak{m}_1,\dots,\mathfrak{m}_s$ are maximal ideals the isomorphism follows directly by the Chinese Remainder Theorem. To prove that R/J is torsion-free, we note that the prime ideals $\mathfrak{p}_i$ satisfy $\mathfrak{p}_i\mathbb{Q}[x_1,\dots,x_n]\cap P$. Now let $f \in P$ and assume there exists $k \in \mathbb{Z}\setminus\{0\}$ with $kf \in J$. Then we have $kf \in \mathfrak{p}_i$ and by the above observation $f \in \mathfrak{p}_i$ for all $i = 1,\dots,k$. This shows $f \in J$. $\square$

Thus we can now combine our results and obtain the following algorithm.

Algorithm 4.10. (Computing the Unit Group of a Reduced Finite $\mathbb{Z}$-Algebra) Let $R = P/I$ be a reduced finite $\mathbb{Z}$-algebra. Consider the following sequence of instructions.

1: Let $G = [\,]$.
2: Compute the prime decomposition $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s$ where $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ are prime ideals of height n and $\mathfrak{m}_1,\dots,\mathfrak{m}_s$ are maximal ideals.
3: Compute $J = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$.
4: Apply Algorithm 4.5 to compute a set of polynomials H such that their residue classes generate the unit group of the order P/J in $\mathbb{Q}[x_1,\dots,x_n]/J\mathbb{Q}[x_1,\dots,x_n]$.
5: Using the Chinese Remainder Theorem, compute $e_1,\dots,e_{s+1} \in P$ such that their residue classes form orthogonal idempotents of R with $R \cong \bar{e}_1R \times \cdots \times \bar{e}_{s+1}R$ and $\bar{e}_iR \cong P/\mathfrak{m}_i$ for $i = 1,\dots,s$ and $\bar{e}_{s+1}R \cong P/J$.
6: **for all** $h \in H$ **do**
7:    Add $\bar{e}_{s+1}\bar{h} + \sum_{i=1}^{s} \bar{e}_i$ to G.
8: **end for**
9: **for** $i = 1,\dots,s$ **do**
10:    Using Remark 4.1, compute $g_i \in P$ such that $\bar{g}_i$ generates $(P/\mathfrak{m}_i)^\times$.
11:    Add $\bar{e}_i\bar{g}_i + \sum_{j\neq i} \bar{e}_j$ to G.
12: **end for**
13: **return** G.

This is an algorithm which computes a generating set of the unit group $R^\times$.

Proof. By Lemma 4.9, we have $R^\times \cong (P/J)^\times \times (P/\mathfrak{m}_1)^\times \times \cdots \times (P/\mathfrak{m}_s)^\times$, and P/J is torsion-free. This shows that the units in R are given by the residue classes of elements of the form $e_1f_1 + \cdots + e_sf_s + e_{s+1}g$ where $\bar{f}_i$ is a unit in $(P/\mathfrak{m}_i)$ and $\bar{h}$ is a unit in (P/J). We therefore conclude that the elements computed in line 7 and in line 11 generate $R^\times$. $\square$

As noted in Remark 2.5, the computations in lines 2,3 and 5 can be performed efficiently if R is explicitly given.

Example 4.11. Consider the reduced finite $\mathbb{Z}$-algebra $R = \mathbb{Z}[x,y,z]/I$ where

$$I = \left\langle 3x,\, xz - x,\, y^2 + z,\, x^2 + xy,\, z^3 - 1 \right\rangle.$$

Let us apply Algorithm 4.10 to compute generators of $R^\times$.

1: Set $G = [\,]$.
2: We compute the minimal prime ideals of I and obtain $\mathfrak{p}_1 = \langle z-1, x, y^2+1\rangle$, $\mathfrak{p}_2 = \langle x, z^2+z+1, y^2+z\rangle$ and $\mathfrak{m} = \langle 3, z-1, x+y, y^2+1\rangle$.
3: Compute $J = \mathfrak{p}_1 \cap \mathfrak{p}_2$.
4: Using Algorithm 4.5, we obtain the following generators of $(P/J)^\times$.

$$h_1 = 9\bar{y}\bar{z}^2 - 17\bar{y}\bar{z} - 15\bar{z}^2 + 9\bar{y} + 15\bar{z}$$

$$h_2 = 15\bar{y}\bar{z} + 9\bar{z}^2 - 15\bar{y} - 17\bar{z} + 9$$

$$h_3 = -56\bar{y}\bar{z} - 32\bar{z}^2 + 56\bar{y} + 65\bar{z} - 32$$

5: Determine orthogonal idempotents $e_1 = \bar{x}\bar{y} + \bar{y}^2 + \bar{z}$ and $e_2 = -\bar{x}\bar{y} + 1$ of R such that $e_1 + e_2 = 1$, $e_1R \cong P/\mathfrak{m}$ and $e_2R \cong P/J$.
7: Add $e_1 + e_2h_1$, $e_1 + e_2h_2$ and $e_1 + e_2h_3$ to G.
10: Using Remark 4.1, we compute a generator $g = \bar{y} + 1$ of $(P/\mathfrak{m})^\times$.
11: Add $e_1g + e_2$ to G.
13: The generators of $R^\times$ are given by

$$\begin{aligned} e_1 + e_2h_1 &= 9\bar{y}\bar{z}^2 + \bar{x}\bar{y} - 17\bar{y}\bar{z} - 15\bar{z}^2 + \bar{x} + 9\bar{y} + 15\bar{z} \\ e_1 + e_2h_2 &= 15\bar{y}\bar{z} + 9\bar{z}^2 - 15\bar{y} - 17\bar{z} + 9 \\ e_1 + e_2h_3 &= -56\bar{y}\bar{z} - 32\bar{z}^2 + 56\bar{y} + 65\bar{z} - 32 \\ e_1g + e_2 &= -\bar{x} + 1. \end{aligned}$$

5. The Unit Group of Non-Reduced Finite $\mathbb{Z}$-Algebras

Using the results of the previous subsection, in particular Algorithm 4.10, we can now compute generators of the unit group of $R/\operatorname{Rad}(0)$. The next task is to lift these generators to a generating set of $R^\times$.

Lemma 5.1. *Let R be a finite $\mathbb{Z}$-algebra.*
(a) *The canonical homomorphism $\varphi\colon R \to R/\operatorname{Rad}(0)$ induces a surjective group homomorphism $\varphi^\times\colon R^\times \to (R/\operatorname{Rad}(0))^\times$.*
(b) *The kernel of $\varphi^\times$ is given by $1 + \operatorname{Rad}(0)$.*

Proof. See [22], Lemma 1.1.5. □

This lemma shows $R^\times/(1+\operatorname{Rad}(0)) \cong (R/\operatorname{Rad}(0))^\times$. Therefore, if we have generators of $(R/\operatorname{Rad}(0))^\times$ and generators of $1 + \operatorname{Rad}(0)$, we obtain generators of $R^\times$ using the following well-known result.

Remark 5.2. Let M be a $\mathbb{Z}$-module and $N \subseteq M$ a submodule. Assume that the residue classes of $m_1, \ldots, m_k \in M$ generate M/N, and let N be generated by $n_1, \ldots, n_\ell$. Then $m_1, \ldots, m_k, n_1, \ldots, n_\ell$ generate M.

Since we already saw how to determine generators of $R/\operatorname{Rad}(0)^\times$, it remains to compute generators of $1 + \operatorname{Rad}(0)$. If $\operatorname{Rad}(0)^2 = 0$, then elements $1 + f, 1 + g$ of $1 + \operatorname{Rad}(0)$ satisfy $(1+f)(1+g) \equiv 1+f+g$. In this case generators of the additive group of $\operatorname{Rad}(0)$, immediately yield generators of $1 + \operatorname{Rad}(0)$. If the nilpotency index of $\operatorname{Rad}(0)$ is greater than 2, we can inductively compute generators of $1 + \operatorname{Rad}(0)^{i-1}$ in $R/\operatorname{Rad}(0)^i$.

Algorithm 5.3. (Computing Generators of the Unit Group)
Let $R = P/I$ be a finite $\mathbb{Z}$-algebra. Consider the following sequence of instructions.

```
1: Let G = [ ].
2: Compute the nilradical Rad(0) of R.
3: Apply Algorithm 4.10 to compute elements in R such that their residue classes generate
   the unit group of R/Rad(0). Add these elements to G.
4: Compute the nilpotency index s of Rad(0) in R.
5: for i = 2, ..., s do
```

6: Compute $f_1, \dots, f_\ell \in R$ such that the residue classes $\bar{f}_1, \dots, \bar{f}_\ell$ in $R/\operatorname{Rad}(0)^i$ generate $1 + \operatorname{Rad}(0)^{i-1}$.
7: Add $f_1, \dots, f_\ell$ to G.
8: **end for**
9: **return** G.

This is an algorithm which computes a generating set of the unit group $R^\times$.

Proof. After line 3 has been executed the list G contains generators of the unit group of $R/\operatorname{Rad}(0)$. Now assume that the elements in G generate $R/\operatorname{Rad}(0)^{i-1}$ after iteration number $i-1$ of lines 5–8. By Lemma 5.1 the group homomorphism

$$\varphi_i^\times\colon \left(R/\operatorname{Rad}(0)^{i-1}\right)^\times \to \left(R/\operatorname{Rad}(0)^{i}\right)^\times$$

is surjective and its kernel is given by $1 + \operatorname{Rad}(0)^{i-1}$. This implies

$$\left(R/\operatorname{Rad}(0)^{i-1}\right)^\times / \left(1 + \operatorname{Rad}(0)^{i-1}\right) \cong \left(R/\operatorname{Rad}(0)^{i}\right)^\times .$$

The generators of $R/\operatorname{Rad}(0)^{i-1}$ together with the generators of $1 + \operatorname{Rad}(0)^{i-1}$ therefore generate $\left(R/\operatorname{Rad}(0)^{i}\right)^\times$. Hence, after iteration number s the list G contains generators of $(R/\operatorname{Rad}(0)^s)^\times = R^\times$. □

The loop in lines 5–8 can be avoided as follows.

Lemma 5.4. *Let $R = P/I$ be a finite $\mathbb{Z}$-algebra, and let $\mathcal{G} = \mathbb{T}^n \setminus L$ be a set of terms as in Lemma 2.3 such that the residue classes of the elements in $\mathcal{G}$ generate R^+. Let $f_1, \dots, f_k \in P$ such that their residue classes generate* $\operatorname{Rad}(0)$. *Then $\mathcal{H} = \left\{1 + \bar{t}\bar{f}_i \mid i = 1, \dots, k,\ t \in \mathcal{G}\right\}$ generates* $1 + \operatorname{Rad}(0)$.

Proof. Clearly, $\mathcal{H}$ is contained in $1 + \operatorname{Rad}(0)$. By the proof of Algorithm 5.3, it is then enough to show that there are $g_1, \dots, g_s \in H$ such that $\bar{g}_1, \dots, \bar{g}_s$ in $R/\operatorname{Rad}(0)^i$ generate $1 + \operatorname{Rad}(0)^{i-1}$. Every element in $\operatorname{Rad}(0)^{i-2}$ can be written as a $\mathbb{Z}$-linear combination of the residue classes of the terms in $\mathcal{G}$. Thus, every element in $\operatorname{Rad}(0)^{i-1}$ can be written as a $\mathbb{Z}$-linear combination of the terms in $\left\{\bar{t}\bar{f}_i \mid i = 1, \dots, k,\ t \in \mathcal{G}\right\}$. The claim now follows from the fact that $(1 + \bar{f})(1 + \bar{g}) = 1 + \bar{f} + \bar{g}$ for $f, g \in \operatorname{Rad}(0)^{i-1}$, since $fg \in \operatorname{Rad}(0)^i$. □

Let us apply Algorithm 5.3 using this simplification to a concrete example.

Example 5.5. Consider the finite $\mathbb{Z}$-algebra $R = \mathbb{Z}[x,y]/I$, where $I = \left\langle x^3, 6x^2, y^2 + y + 1\right\rangle$.

1: Let $G = [\,]$.
2: Compute $\operatorname{Rad}(0) = \left\langle \bar{x}, \bar{y}^2 + \bar{y} + 1\right\rangle$.
3: Using Algorithm 4.10, we compute $(R/\operatorname{Rad}(0))^\times = \langle \bar{y} + 1\rangle$ and add $\bar{y} + 1$ to G.
4-8: Using Lemma 2.3, we determine $\mathbb{Z}$-module generators $\mathcal{G} = \left\{\bar{x}^2\bar{y}, \bar{x}\bar{y}, \bar{y}, \bar{x}^2, \bar{x}, 1\right\}$ of R. Then for every generator g of $\operatorname{Rad}(0)$ and for every term $t \in \mathcal{G}$ we calculate $1 + \operatorname{NF}_{\sigma,I}(tg)$ and obtain generators $1 + \bar{x}, 1 + \bar{x}^2, 1 + \bar{x}\bar{y}, 1 + \bar{x}^2\bar{y}$ of $1 + \operatorname{Rad}(0)$.
9: We obtain

$$R^\times = \left\langle 1 + \bar{y}, 1 + \bar{x}, 1 + \bar{x}^2, 1 + \bar{x}\bar{y}, 1 + \bar{x}^2\bar{y}\right\rangle .$$

The generating set produced by Algorithm 5.3 is in general not minimal. But we can compute the exponent lattice of these generators to identify redundant ones. Furthermore, the isomorphism type of the unit group can be determined by computing the Smith normal form of the exponent lattice.

Corollary 5.6. (Computing the Isomorphism Type of the Unit Group)
Let $R = P/I$ be a finite $\mathbb{Z}$-algebra. Consider the following sequence of instructions.

1: *Using Algorithm 5.3, compute generators $g_1, \ldots, g_k$ of $R^\times$.*
2: *Using Algorithm 3.8, compute generators $v_1, \ldots, v_m \in \mathbb{Z}^k$ which generate the exponent lattice of $(g_1, \ldots, g_k)$ in R.*
3: *Form the matrix whose rows are given by $v_1, \ldots, v_m$, and compute its Smith normal form S.*
4: *Let r be the number of diagonal entries of S equal to zero, and let $k_1, \ldots, k_u$ be the non-zero diagonal entries of S.*
5: ***return*** *r and $k_1, \ldots, k_u$.*

This is an algorithm which computes the rank and the invariant factors of the group $R^\times$.

Algorithm 5.3 for computing generators of the unit group of a finite $\mathbb{Z}$-algebra raises the natural question whether it can be extended to finitely generated $\mathbb{Z}$-algebras which are not necessarily finite $\mathbb{Z}$-modules. The unit group of such rings is finitely generated if and only if the Jacobson radical is finitely generated as an additive group (see [2, Thm. 1]). In particular, the unit group of a finitely generated, reduced $\mathbb{Z}$-algebra is a finitely generated group. However, the previous results cannot be directly applied to compute a set of generators. For example, in the integral case, the algebra no longer needs to be a finite field or an order in a number field. To the best of our knowledge, there exist no algorithms which compute generators of the unit group in this case. We leave this problem for future research.

References

[1] W.W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics **3**, Amer. Math. Soc., Providence, 1994.
[2] H. Bass, *Introduction to Some Methods of Algebraic K-Theory*, Amer. Math. Soc., Providence, 1974.
[3] J.-F. Biasse and C. Fieker, Subexponential class group and unit group computation in large degree number fields, *LMS J. Comput. Math.* **17A** (2014), 385–403.
[4] O. Braun, R. Coulangeon, G. Nebe, and S. Schönnenbeck, Computing in arithmetic groups with Voronoi's algorithm, *J. Algebra* **435** (2015), 263–285.
[5] J. Chen, S. Vemulapalli, and L. Zhang, Computing unit groups of curves, *J. Symbolic Comput.* **104** (2021), 236–255.
[6] H. Cohen, F. Diaz, and M. Olivier, Subexponential algorithms for class group and unit computations, *J. Symbolic Comput.* **24** (1997), 433–441.
[7] L.G. Dirichlet, *Zur Theorie der komplexen Einheiten* (1846) (in German), Werke, Vol. I, Dietrich Reimer Verlag, Berlin, 1889, pp. 639–644.
[8] J. Dubrois and J.-G. Dumas, Efficient polynomial time algorithms computing industrial-strength primitive roots, *Inform. Process. Lett.* **97**(2) (2006), 41–45.
[9] C. Eder, G. Pfister, and A. Popescu, Standard bases over Euclidean domains, *J. Symbolic Comput.* **102** (2021), 21–36.
[10] P. Faccin, W.A. de Graaf, and W. Plesken, Computing generators of the unit group of an integral abelian group ring, *J. Algebra* **373** (2013), 441–452.
[11] G. Ge, Algorithms related to multiplicative representations of algebraic numbers, PhD thesis, University of California, Berkeley, 1993.
[12] G.-M. Greuel and G. Pfister, *A Singular Introduction to Commutative Algebra*, Springer-Verlag, Berlin, Heidelberg, 2008.
[13] R. Kannan and A. Bachem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix, *SIAM J. Comput.* **8**(4) (1979), 499–507.
[14] M. Kauers, *Algorithms for nonlinear higher order difference equations*, PhD Thesis, RISC Institute, Linz, 2005.

[15] M. Kauers, P. Nuspl, and V. Pillwein, Order bounds for C^2-finite sequences, in: *ISSAC'23: Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, Association for Computing Machinery, New York, 2023, pp. 389–397.

[16] M. Kreuzer, A. Miasnikov, and F. Walsh, Decomposing finite $\mathbb{Z}$-algebras, preprint 2023, available at `arXiv:2308.01735`.

[17] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag, Berlin, Heidelberg, 2000.

[18] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 2*, Springer-Verlag, Berlin, Heidelberg, 2005.

[19] M. Kreuzer and F. Walsh, Computing the binomial part of a polynomial ideal, *J. Symbolic Comput.* **124** (2024), paper 102298.

[20] M. Kreuzer and F. Walsh, Efficient algorithms for finite $\mathbb{Z}$-algebras, *journal of Groups, Complexity, Cryptology* **15**(2) (2024).

[21] H.W. Lenstra and A. Silverberg, Algorithms for commutative algebras over the rational numbers, *Found. Comput. Math.* **18**(1) (2018), 159–180.

[22] E. Malek, On the group of units of a finite R-algebra, *J. Algebra* **23**(3) (1972), 538–552.

[23] K.A. Mihailova, The occurrence problem for free products of groups, *Math. USSR Sb.* **4**(2) (1968), 181–190.

[24] P. Samuel, *Algebraic Theory of Numbers: Translated from the French by Allan J. Silberger*, Hermann, Paris, 1970.

[25] V. Shoup, Searching for primitive roots in finite fields, *Math. Comp.* **58**(197) (1992), 369–380.

[26] A. Storjohann, Near optimal algorithms for computing smith normal forms of integer matrices, in: *Algorithms and Computation*, Proc. ISAAC'96 (Osaka 1996), LNCS **1178**, Springer-Verlag, Berlin, Heidelberg, 1996, pp. 267–274.

[27] The Sage Developers, Sagemath, the Sage Mathematics Software System, 2023.

[28] F. Walsh, Binomial part, a `Sagemath` package, Version 1.1, April 2024, available at `https://github.com/abacus42/binomial-part`.

[29] K. Yokoyama, M. Noro, and T. Takeshima, Computing primitive elements of extension fields, *J. Symbolic Comput.* **8**(6) (1989), 553–580.

[30] H. Zassenhaus, On the units of orders, *J. Algebra* **20** (1972), 368–395.

[31] T. Zheng and B. Xia, An effective framework for constructing exponent lattice basis of nonzero algebraic numbers, in: *ISSAC '19: Proceedings of the 2019 International Symposium on Symbolic and Algebraic Computation*, Association for Computing Machinery, New York, 2019, pp. 371–378.