Computing generators of the unit group of an integral abelian group ring

Paolo Faccin [a], Willem A. de Graaf [a,*], Wilhelm Plesken [b]

[a] *Dipartimento di Matematica, Università di Trento, Italy*
[b] *Lehrstuhl B für Mathematik, RWTH Aachen University, Germany*

A B S T R A C T

We describe an algorithm for obtaining generators of the unit group of the integral group ring $\mathbb{Z}G$ of a finite abelian group G. We used our implementation in MAGMA of this algorithm to compute the unit groups of $\mathbb{Z}G$ for G of order up to 110. In particular for those cases we obtained the index of the group of Hoechsmann units in the full unit group. At the end of the paper we describe an algorithm for the more general problem of finding generators of an arithmetic group corresponding to a diagonalisable algebraic group.

1. Introduction

Let G be a finite abelian group. For a ring R we let RG be the group ring over R, consisting of sums $\sum_{g \in G} a_g g$, with $a_g \in R$. We take $R = \mathbb{Z}$ and consider the unit group

$$(\mathbb{Z}G)^* = \{u \in \mathbb{Z}G \mid \text{there is a } v \in \mathbb{Z}G \text{ with } vu = 1\}.$$

Higman [14] showed that $(\mathbb{Z}G)^* = \pm G \times F$, where F is a free abelian group. Moreover, Ayoub and Ayoub [1] have established that the rank of F is $\frac{1}{2}(|G| + 1 + t_2 - 2l)$, where t_2 is the number of elements of G of order 2, and l is the number of cyclic subgroups of G.

Hoechsmann [15] described a construction of a set of generators of a finite-index subgroup of $(\mathbb{Z}G)^*$, called the group of constructable units. Regarding this construction he wrote "Does this method ever yield all units if $n = |G|$ is not a prime power? The answer seems to be affirmative for

* Corresponding author.
E-mail addresses: faccin@science.unitn.it (P. Faccin), degraaf@science.unitn.it (W.A. de Graaf), plesken@momo.math.rwth-aachen.de (W. Plesken).

all $n < 74$." In [15] this question is not dealt with any further. When $n = 74$ it is known that the group of constructable units is of index 3 in the full unit group (see [16]). So the question remains whether the constructable units generate the full unit group if $|G| < 74$.

In this paper we develop algorithms for computing generators of the unit group $(\mathbb{Z}G)^*$. Using our implementation of these algorithms in the computer algebra system MAGMA [4] we have computed the unit groups for all abelian groups of order $\leqslant 110$. We found 12 groups G of order less than 74 whose unit group is not generated by the Hoechsmann units (namely, the groups of order 40, 48, 60, 63 and 65).

In the next section we start by collecting some well-known facts and immediate observations concerning lattices, groups, and associative algebras. Also, in the second half of the section (Section 2.4) we describe our approach to computing the unit group of the maximal order in a cyclotomic field. This is achieved by combining a construction by Greither [12] of a finite-index subgroup of the unit group, along with a MAGMA program by Fieker for "saturating" a subgroup at a given prime p. The latter algorithm and its implementation will be described elsewhere.

Section 3 contains the main algorithm of this paper, namely an algorithm for computing the unit group of an order $\mathcal{O}$ in a toral algebra A. The main idea is to split A into its simple ideals $e_i A$, where the e_i are orthogonal primitive idempotents. The $e_i A$ are number fields with orders $e_i \mathcal{O}$. So in order to compute their unit groups we can use the effective version of the Dirichlet unit theorem (cf. [5,19]). The basic step of the algorithm is, given two orthogonal idempotents ϵ_1, ϵ_2, to obtain the unit group of $(\epsilon_1 + \epsilon_2)\mathcal{O}$ given the unit groups of $\epsilon_i \mathcal{O}$, $i = 1, 2$.

In Section 4 we describe our method for obtaining generators of unit groups of integral abelian group rings. Its main ingredients are the construction of the unit groups of cyclotomic fields, and the algorithm of Section 3. We comment on the running times of the implementation of the algorithm in MAGMA, and we give a table containing all abelian groups of orders up to 110, where the constructable (or Hoechsmann-) units do not generate the full unit group. For all these groups we give the index of the group of constructable units in the full unit group.

Finally in the last section we indicate an algorithm to obtain generators of the arithmetic group corresponding to a connected diagonalisable algebraic group defined over $\mathbb{Q}$. Again the main ingredient is the algorithm of Section 3.

In our main algorithms and implementations we make essential use of Fieker's implementation in MAGMA of an algorithm by Ge [10] to obtain a basis of the lattice

$$\left\{ (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n \mid u_1^{\alpha_1} \cdots u_n^{\alpha_n} = 1 \right\}$$

of multiplicative relations of given elements $u_1, \ldots, u_n$ in a number field.

2. Preliminaries

2.1. Lattices

In this paper we use the term "lattice" for a finitely generated subgroup of $\mathbb{Z}^m$. A lattice $\Lambda \subset \mathbb{Z}^m$ has a basis, that is a subset $u_1, \ldots, u_r$ such that every $u \in \Lambda$ can uniquely be written as $u = \sum_{i=1}^{r} \alpha_i u_i$, with $\alpha_i \in \mathbb{Z}$. The lattice $\Lambda \subset \mathbb{Z}^m$ is called *pure* if $\mathbb{Z}^m / \Lambda$ is torsion-free. (See [6, §III.16].)

Let $\Lambda \subset \mathbb{Z}^m$ be a lattice with basis $u_1, \ldots, u_r$. We form the $r \times m$-matrix B with rows consisting of the coefficients of the u_i with respect to the standard basis of $\mathbb{Z}^m$. By computing the Smith normal form of B we can effectively compute the homomorphism $\psi : \mathbb{Z}^m \to \mathbb{Z}^m / \Lambda$ (cf. [21, §8.3]). Let T denote the torsion submodule of $\mathbb{Z}^m / \Lambda$. Then $\psi^{-1}(T)$ is the smallest pure lattice containing Λ. So in particular, the Smith normal form algorithm gives a method to compute a basis of the lattice $V \cap \mathbb{Z}^m$, where V is a subspace of $\mathbb{Q}^m$. For example, we can compute the intersection of lattices this way.

As observed in [6, §III.16], a lattice Λ is pure if and only if it is a direct summand of $\mathbb{Z}^m$. So in that case, by computing a Smith normal form, we can compute a basis of $\mathbb{Z}^m$ such that the first r basis elements form a basis of Λ.

Remark 2.1. Computing a basis of the lattice $V \cap \mathbb{Z}^m$, where V is a subspace of $\mathbb{Q}^m$, is called *saturation*. There are methods known for this, based on computing a Hermite normal form, that are more efficient than the approach outlined above. Going into these matters would lead us too far from the subject of this paper.

2.2. Toral algebras

We say that an associative algebra A over $\mathbb{Q}$ is *toral* if it is semisimple, abelian and has an identity element, which we will denote by e. For example the group algebra $\mathbb{Q}G$ of a finite abelian group G is toral.

By the Wedderburn structure theorem (cf. [18, §3.5]) a toral algebra A is a direct sum $A = A_1 \oplus \cdots \oplus A_s$, where the A_i are ideals that are isomorphic (as associative algebras) to field extensions of $\mathbb{Q}$. A nonzero element $e_0 \in A$ is said to be an idempotent if $e_0^2 = e_0$. Two idempotents e_1, e_2 are called orthogonal if $e_1 e_2 = 0$. Furthermore, an idempotent is called primitive if it is not the sum of orthogonal idempotents. Now the decomposition of A into a direct sum of simple ideals corresponds to a decomposition of the identity element $e \in A$ as a sum of primitive orthogonal idempotents, $e = e_1 + \cdots + e_s$. Here e_i is the identity element of A_i, and vice versa, $A_i = e_i A$. We remark that there are algorithms to compute the e_i, given a basis of A (cf. [8,9]).

When $A = \mathbb{Q}G$, with G a finite abelian group, there is a very efficient way to compute the primitive idempotents. Let $\chi : G \to \mathbb{C}^*$ be an irreducible character of G. Then

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g$$

is an idempotent in $\mathbb{C}G$. Moreover, the e_χ, as χ runs over all irreducible characters, are primitive orthogonal idempotents with sum e (cf. [6, Theorem 33.8]). In particular, they form a basis of $\mathbb{C}G$. Let m denote the exponent of G, then all irreducible characters χ have values in the cyclotomic field $\mathbb{Q}(\zeta_m)$. So the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ acts on the irreducible characters. Now we sum the e_χ, for χ in an orbit of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, and obtain the primitive orthogonal idempotents of $\mathbb{Q}G$.

A subset $\mathcal{O}$ of a toral algebra A, containing the identity of A, is said to be an *order* (or, more precisely, a $\mathbb{Z}$-order) if there is a basis $a_1, \ldots, a_m$ of A such that $\mathcal{O} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_m$ and $a_i a_j \in \mathcal{O}$ for $1 \leqslant i, j \leqslant m$. For example, $\mathbb{Z}G$ is an order in $\mathbb{Q}G$. The unit group of $\mathcal{O}$ is

$$\mathcal{O}^* = \{a \in \mathcal{O} \mid \text{there is } b \in \mathcal{O} \text{ with } ab = e\}.$$

We consider the problem of obtaining a basis of the lattice of multiplicative relations

$$L = \{(\alpha_1, \ldots, \alpha_r) \in \mathbb{Z}^r \mid a_1^{\alpha_1} \cdots a_r^{\alpha_r} = e\},$$

where $a_1, \ldots, a_r$ are given elements of $\mathcal{O}^*$. Note that $e_i A$ are number fields. So using Ge's algorithm [10] we can compute bases of the lattices

$$L_j = \{(\alpha_1, \ldots, \alpha_r) \in \mathbb{Z}^r \mid (e_j a_1)^{\alpha_1} \cdots (e_j a_r)^{\alpha_r} = e_j\}.$$

Moreover, $L = \bigcap_j L_j$ so we can compute a basis of L (see Section 2.1).

2.3. Standard generating sets

Let U be a finitely-generated abelian group. We say that a set of generators $g_1, \ldots, g_r$ of U is *standard* if

(1) for $1 \leqslant i \leqslant s$ the order of g_i is d_i,

Table 1

Runtimes (in seconds) for the algorithm to compute generators of $(\mathbb{Z}G)^*$. The first column lists the isomorphism type of G, and the second the value of the Euler φ-function on the exponent of G. The third column has the average number of digits of the coefficients of the units output by the algorithm (with respect to the standard basis of $\mathbb{Z}G$). The fourth column displays the time spent to compute multiplicative relations in cyclotomic fields. The last column has the total time spent by the algorithm.

G	$\varphi(\exp(G))$	|digits|	t_m	t_{tot}
C_{70}	24	7.4	314	328
C_{80}	32	63.4	1131	1183
C_{90}	24	159.5	1043	1078
C_{91}	72	3.7	2352	2446
C_{96}	32	31.2	2322	2373
$C_2 \times C_{48}$	16	181.3	1575	1781
$C_2 \times C_2 \times C_{24}$	8	54.6	1031	1267
$C_2 \times C_4 \times C_{12}$	4	22.5	537	725
C_{100}	40	217.6	3822	3942
$C_2 \times C_{50}$	20	66 352.6	414 569	426 654
$C_5 \times C_{20}$	8	379.7	1227	1425
$C_{10} \times C_{10}$	4	275.2	1131	1332

(2) for $s + 1 \leqslant i \leqslant r$ the order of g_i is infinite,

(3) $d_i | d_{i+1}$ for $i < s$,

and there are no other relations. So a standard set of generators immediately gives an isomorphism of U to $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z} \oplus \mathbb{Z}^{r-s}$.

Giving finitely-generated abelian groups by standard generating sets yields straightforward algorithms for several computational tasks concerning these groups, such as computing the index of a subgroup, and computing the kernel of a homomorphism.

If an abelian group is given by a non-standard set of generators, then we can compute a standard one by computing the lattice of all relations of the generators, followed by a Smith normal form computation (cf. [21, §8.3]). So, using the algorithm indicated in the previous section, we can compute a standard set of generators for a finitely-generated subgroup of $\mathcal{O}^*$, where $\mathcal{O}$ is an order in a toral algebra.

Remark 2.2. For many computational problems regarding finitely-generated abelian groups it suffices to compute a Hermite normal form of the relation lattice. However, in our applications the main computational problem is to obtain the relation lattice (see Table 1), the subsequent computation of the Smith normal form does not bear heavily on the running time. Therefore, for our purposes, a Smith normal form is the most convenient.

2.4. Units of cyclotomic fields

Let n be a positive integer. We consider the cyclotomic field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. The ring of integers of this field is $\mathbb{Z}[\zeta_n]$. By Dirichlet's unit theorem the unit group $\mathbb{Z}[\zeta_n]^*$ is equal to $T \times F$, where F is a free abelian group of rank $\frac{1}{2}\varphi(n) - 1$, and T is the group of roots of unity in $\mathbb{Q}(\zeta_n)$. The problem considered in this section is to obtain generators of the unit group, $\mathbb{Z}[\zeta_n]^*$. There are algorithms for this that work for any number field (cf. [5,19]); but their complexity is such that it is only practical to use them for n up to about 20 (depending on the hardware one uses, of course). For this reason we sketch a different approach, using several results from the literature. The situation is straightforward when n is a prime power, see Section 2.4.1. Then in Section 2.4.2 we describe what can be done when n is not a prime power. Using these methods we obtained a list of the generators of the unit groups $\mathbb{Z}[\zeta_n]^*$, for $n < 130$. However, for several n the correctness of this list depends on the Generalised Riemann Hypothesis, that is for n prime between 67 and 127, and for $n = 115, 119, 121, 123, 125, 129$ (so 19 cases in total).

Throughout we set $\mathbb{Q}(\zeta_n)^+ = \mathbb{R} \cap \mathbb{Q}(\zeta_n)$; then $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. By h_n^+ we denote the class number of $\mathbb{Q}(\zeta_n)^+$.

2.4.1. When n is a prime power

Suppose that $n = p^m$ is a prime power. For $1 < a < \frac{n}{2}$ with $\gcd(a, p) = 1$ set

$$\xi_a = \zeta_n^{\frac{1-a}{2}} \frac{1 - \zeta_n^a}{1 - \zeta_n}.$$

Then ξ_a lies in the unit group of $\mathbb{Q}(\zeta_n)^+$. Let U_n be the group generated by -1, ζ_n and all ξ_a. Then for the index we have $[\mathbb{Z}[\zeta_n]^* : U_n] = h_n^+$ (this is obtained by combining Corollary 4.13, Lemma 8.1 and Theorem 8.2 in [22]). It is known that $h_n^+ = 1$ if $\varphi(n) < 66$, and assuming the Generalised Riemann Hypothesis, we have $h_n^+ = 1$ when $\varphi(n) < 162$ (see Appendix in [22]). So for those n we have generators of the unit group.

2.4.2. When n is not a prime power

Here the situation is more difficult. First of all we assume that $n \not\equiv 2 \bmod 4$, as for $n = 2 \bmod 4$ we have that $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_{\frac{n}{2}})$ are isomorphic. By E^+ denote the unit group of $\mathbb{Q}(\zeta_n)^+$. We use a finite-index subgroup of E^+ defined by Greither [12]. Here we briefly describe his construction.

Let $\mathcal{G} = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, and write the elements of $\mathcal{G}$ as σ_a, where $\gcd(a, n) = 1$ and $\sigma_a(\zeta_n) = \zeta_n^a$. For $\alpha = \sum_a m_a \sigma_a \in \mathbb{Z}\mathcal{G}$ and $x \in \mathbb{Q}(\zeta_n)$ define

$$x^\alpha = \prod_a \sigma_a(x)^{m_a}.$$

Let $n = \prod_{i=1}^{s} p_i^{e_i}$ be the factorisation of n in distinct prime powers. Set $S = \{1, \ldots, s\}$ and $P_S = \{I \subset S \mid I \neq S\}$. For $I \in P_S$ we set $n_I = \prod_{i \in I} p_i^{e_i}$.

We consider arbitrary maps $\beta : S \to \mathbb{Z}\mathcal{G}$, which we extend to maps (denoted by the same symbol) $\beta : P_S \to \mathbb{Z}\mathcal{G}$ by $\beta(\emptyset) = 1$, $\beta(\{i\}) = \beta(i)$, and $\beta(I \cup J) = \beta(I)\beta(J)$ if $I \cap J = \emptyset$. Now let $z \in \mathbb{Q}(\zeta_n)$. For $I \in P_S$ set $z_I = 1 - z^{n_I}$, and $z(\beta) = \prod_{I \in S} z_I^{\beta(I)}$. Set $t = -\sum_{I \in S} n_I \beta(I) \in \mathbb{Z}\mathcal{G}$. Then for a with $1 < a < \frac{n}{2}$ and $\gcd(a, n) = 1$ we consider

$$\xi_a(\beta) = \zeta_n^{d_a} \frac{\sigma_a(z(\beta))}{z(\beta)}, \quad \text{where } d_a = \frac{(1 - \sigma_a)t}{2}.$$

(Note that for n odd, $\zeta_n^{\frac{1}{2}}$ lies in $\mathbb{Z}[\zeta_n]$, whereas for n even we have a odd and hence $\frac{1-a}{2}$ is an integer.)

Following Greither we describe a good choice for β. First a small piece of notation: if g is an element of order m of a group, then we set $N_g = 1 + g + \cdots + g^{m-1}$, which lies in the corresponding integral group ring. Now consider an $i \in S$. Let $\mathcal{G}_i$ denote the Galois group of $\mathbb{Q}(\zeta_{n/p_i^{e_i}})^+$ over $\mathbb{Q}$. This group contains the Frobenius automorphism F_i (by definition: $F_i(\zeta_{n/p_i^{e_i}}) = \zeta_{n/p_i^{e_i}}^{p_i}$). This yields the element N_{F_i} in $\mathbb{Z}\mathcal{G}_i$. Now we define $\beta(i)$ to be a lift of N_{F_i} to $\mathbb{Z}\mathcal{G}$.

Let C_β be the subgroup of E^+ generated by -1 and the $\xi_a(\beta)$. Greither proved that C_β does not depend on the choice for the lifts of the N_{F_i}, and that it is of index $h_n^+ i_\beta$ in E^+, where

$$i_\beta = \prod_{i=1}^{s} e_i^{g_i-1} f_i^{2g_i-1};$$

here e_i, f_i and g_i are respectively the ramification, inertial and decomposition degree of p_i in $\mathbb{Q}(\zeta_n)^+$ (so that $e_i f_i g_i = \frac{1}{2}\varphi(n)$).

Now let U_n denote the group generated by ζ_n and C_β. Then using [22, Corollary 4.13], we get that $[\mathbb{Z}[\zeta_n]^* : U_n] = 2h_n^+ i_\beta$.

We used a program that Claus Fieker has written in MAGMA, V2.17-2 (see [2] for some of the background). This program, given a finite-index subgroup V of $\mathbb{Z}[\zeta_n]^*$, and a prime p, computes a subgroup $\widetilde{V}$ of $\mathbb{Z}[\zeta_n]^*$, containing V, and such that the index $[\mathbb{Z}[\zeta_n]^* : \widetilde{V}]$ is not divisible by p. We used this starting with the group U_n. For $n < 130$ and $\varphi(n) \leqslant 72$ we have $h_n^+ = 1$, and assuming the Generalised Riemann Hypothesis, we have $h_n^+ = 1$ for all $n < 130$ [22, Appendix]. Therefore we can compute $[\mathbb{Z}[\zeta_n]^* : U_n]$, and get all primes dividing it. So at the end we arrived at the full unit group $\mathbb{Z}[\zeta_n]^*$ for all $n < 130$.

3. Unit groups of orders in toral matrix algebras

Let A be a toral algebra with identity e, and $\mathcal{O} \subset A$ an order. In this section we consider the problem of computing a set of generators of $\mathcal{O}^*$. First we consider some special cases.

3.1. A simple toral algebra

Let A be a simple toral algebra. In other words, it is isomorphic to a finite extension of $\mathbb{Q}$. Now there are algorithms for computing generators of an order in a number field (the effective version of the Dirichlet unit theorem, see [5,19]). We use these to compute generators of $\mathcal{O}^*$ as well.

3.2. Two idempotents

Let A be a toral algebra with identity e, and $e_1, e_2 \in A$ orthogonal (but not necessarily primitive) idempotents with $e_1 + e_2 = e$. Set $A_i = e_i A$, then $A = A_1 \oplus A_2$. Let $\mathcal{O}$ be an order in A, then $\mathcal{O}_i = e_i \mathcal{O}$ is an order in A_i. Here we suppose that we have generators of $\mathcal{O}_i^*$, $i = 1, 2$, and the problem is to find generators of $\mathcal{O}^*$.

Set $J = (e_1 \mathcal{O} \cap \mathcal{O}) + (e_2 \mathcal{O} \cap \mathcal{O})$. Since this is an ideal in $\mathcal{O}$ we can form the quotient $R = \mathcal{O}/J$. Consider the maps $\varphi_i : e_i \mathcal{O} \to R$ defined by $\varphi_i(e_i a) = a + J$, for $a \in \mathcal{O}$. (Note that this is well-defined: if $e_1 a = e_1 b$ then $a - b = e_2(a - b)$ so it lies in J.) These are surjective ring homomorphisms with respective kernels $e_i \mathcal{O} \cap \mathcal{O}$.

Lemma 3.1. $\mathcal{O} = \{a_1 + a_2 \mid a_i \in e_i \mathcal{O} \text{ and } \varphi_1(a_1) = \varphi_2(a_2)\}$.

Proof. Let $a \in \mathcal{O}$ and set $a_i = e_i a$ then $a = a_1 + a_2$ and $a_i \in e_i \mathcal{O}$. Moreover $\varphi_1(a_1) = a + J = \varphi_2(a_2)$. Conversely, let $a, b \in \mathcal{O}$ be such that $\varphi_1(a_1) = \varphi_2(a_2)$, where $a_1 = e_1 a$ and $a_2 = e_2 b$. Then $a - b \in J$, whence $a = b + u_1 + u_2$ where $u_i \in e_i \mathcal{O} \cap \mathcal{O}$. Therefore $e_1 a = e_1 b + u_1$ so that $a_1 + a_2 = e_1 a + e_2 b = e_1 b + e_2 b + u_1 = b + u_1$ which lies in $\mathcal{O}$. $\square$

Corollary 3.2. $\mathcal{O}^* = \{a_1 + a_2 \mid a_i \in (e_i \mathcal{O})^* \text{ and } \varphi_1(a_1) = \varphi_2(a_2)\}$.

So in order to compute generators of $\mathcal{O}^*$ we perform the following steps:

(1) Compute bases of $\mathcal{O}_i = e_i \mathcal{O}$.
(2) Compute bases of $\mathcal{O}_i \cap \mathcal{O}$, of $J = (\mathcal{O}_1 \cap \mathcal{O}) + (\mathcal{O}_2 \cap \mathcal{O})$, and set $R = \mathcal{O}/J$.
(3) Compute generators of the groups $H_i = \varphi_i(\mathcal{O}_i^*) \subset R^*$ and $H = H_1 \cap H_2$.
(4) Compute generators of the groups $M_i = \varphi_i^{-1}(H) \subset \mathcal{O}_i^*$.
(5) Compute generators of the group $\mathcal{O}^* = \{a_1 + a_2 \mid a_i \in M_i \text{ and } \varphi_1(a_1) = \varphi_2(a_2)\}$.

3.2.1. Implementation

We comment on the implementation of the steps of the algorithm. Step (1) is done by a Hermite normal form computation. The intersections in step (2) are computed using the techniques indicated in Section 2.1. Note that a basis of J is obtained by concatenating the bases of $\mathcal{O}_i \cap \mathcal{O}$. The ring $R = \mathcal{O}/J$ can be constructed by a Smith normal form computation.

For step (3) we assume that $e_2 A$ is isomorphic to a number field (in other words, that e_2 is a primitive idempotent). When using the algorithm, this can always be arranged (see Section 3.3). Then $e_2 \mathcal{O}$ is an order in it. We set $I = e_2 \mathcal{O} \cap \mathcal{O}$ and use the isomorphism $R \cong (e_2 \mathcal{O})/I$. Subsequently we use algorithms described in [13,17] to compute a standard generating set of $(e_2 \mathcal{O}/I)^*$. So computing H_1, H_2 as subgroups of $(e_2 \mathcal{O}/I)^*$ we can perform the operations of step (3).

In step (4) we view φ_i as a homomorphism $\mathcal{O}_i^* \to H_i$. We use this to compute generators of the kernel of φ_i as well as pre-images of the generators of H. Together these generate the group M_i. As remarked in Section 2.3, we can compute standard generating sets of the groups $\mathcal{O}_i^*$. Using these, it is straightforward to obtain a standard generating set for the subgroups M_i. Then we restrict φ_i to obtain a homomorphism $\varphi_i : M_i \to H$.

Now we come to step (5). Let $h_1, \ldots, h_r, a_1, \ldots, a_s, b_1, \ldots, b_t$ be standard generating sets of H, M_1 and M_2 respectively. Set

$$\Lambda = \big\{ (\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t) \in \mathbb{Z}^{s+t} \mid \varphi_1\big(a_1^{\alpha_1} \cdots a_s^{\alpha_s}\big) = \varphi_2\big(b_1^{\beta_1} \cdots \beta_t^{e_t}\big) \big\}.$$

Then

$$\mathcal{O}^* = \big\{ a_1^{\alpha_1} \cdots a_s^{\alpha_s} + b_1^{\beta_1} \cdots b_t^{\beta_t} \mid (\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t) \in \Lambda \big\}.$$

Moreover, Λ is a lattice, hence has a finite basis. Furthermore, the elements of $\mathcal{O}^*$ corresponding to the elements of a basis of Λ generate $\mathcal{O}^*$. So the problem of finding a generating set of $\mathcal{O}^*$ is reduced to finding a basis of Λ.

Define $\mu_{ij}, \nu_{ij} \in \mathbb{Z}$ by

$$\varphi_1(a_i) = \prod_{j=1}^{r} h_j^{\mu_{ij}},$$

$$\varphi_2(b_i) = \prod_{j=1}^{r} h_j^{\nu_{ij}}.$$

A small calculation shows that $(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t) \in \Lambda$ if and only if

$$\sum_{i=1}^{s} \mu_{ij} \alpha_i - \sum_{k=1}^{t} \nu_{kj} \beta_k = 0 \quad \mathrm{mod}\ \mathrm{ord}(h_j) \tag{1}$$

for $1 \leqslant j \leqslant r$ (and where $\mathrm{ord}(h_j)$ denotes the order of h_j). Let S be the integral matrix with columns

$$\big(\mu_{1j}, \ldots, \mu_{sj}, -\nu_{1j}, \ldots, -\nu_{tj}, \mathrm{ord}(h_j) \big)$$

for $1 \leqslant j \leqslant r$. We compute a basis of the integral kernel of S, which is the set of all $v \in \mathbb{Z}^{s+t+1}$ such that $vS = 0$. For each v in this basis we take the vector consisting of the first $s+t$ coordinates. This way we obtain a basis of Λ.

3.3. The general case

Now let A be a toral algebra, $e_1, \ldots, e_m$ its primitive orthogonal idempotents with sum e, and $A_i = e_i A$ the corresponding simple ideals. Let $\mathcal{O}$ be an order in A; then $e_i \mathcal{O}$ is an order in A_i, and as indicated in Section 3.1, we can compute generators of the unit groups $(e_i \mathcal{O})^*$. Then for $j = 2, 3, \ldots$ we set $\epsilon_j = e_1 + \cdots + e_j$ and we apply the algorithm of Section 3.2 to the algebra $\epsilon_j A$ with its order $\epsilon_j \mathcal{O}$, and two idempotents ϵ_{j-1} and e_j, yielding the unit group $(\epsilon_j \mathcal{O})^*$. When the algorithm terminates we have the unit group $\mathcal{O}^*$.

4. Units of integral abelian group rings

Let G be an abelian group. As seen in Section 2.2, it is straightforward to compute primitive orthogonal idempotents $e_1, \ldots, e_r \in \mathbb{Q}G$ such that $e_i(\mathbb{Q}G)$ is isomorphic to a field extension of $\mathbb{Q}$. Let m denote the exponent of G, then (cf. [1])

$$\mathbb{Q}G \cong \bigoplus_{d \mid m} \bigoplus_{i=1}^{t_d} \mathbb{Q}(\zeta_d),$$

where $\mathbb{Q}(\zeta_d)$ is the cyclotomic field of order d, and t_d is the number of cyclic subgroups of G of order d. In particular, $e_i(\mathbb{Q}G) \cong \mathbb{Q}(\zeta_{d_i})$. We consider the order $\mathbb{Z}G$ in $\mathbb{Q}G$. We have that $e_i(\mathbb{Z}G)$ is isomorphic to $\mathbb{Z}[\zeta_{d_i}]$, and by the results of Section 2.4, we have generators of $\mathbb{Z}[\zeta_{d_i}]^*$ for $d_i < 130$. So for small groups G we can apply the algorithm of Section 3 to obtain generators of the unit group $(\mathbb{Z}G)^*$. Using our implementation of the algorithms in Magma, we have carried this out for all abelian groups of orders up to 110. In Table 1 we collect some timings and other data related to the algorithm.

From Table 1 we see that the running time is dominated by the time needed to compute multiplicative relations in cyclotomic fields (Ge's algorithm). This algorithm needs to work harder if the degrees of the fields that occur are higher. Indeed, the running times generally increase when $\varphi(\exp(G))$ increases (note that this is the highest degree of a cyclotomic field occurring in the decomposition of $\mathbb{Q}G$). However, also the size of the elements of which we need to compute multiplicative relations plays a role. For some groups the average number of digits of a unit, as output by the algorithm, is very high. This is seen most dramatically for $C_2 \times C_{50}$. Note also that the size (i.e., the average number of digits of their coefficients) of the units output by the algorithm is far from being optimal; indeed, for $G = C_2 \times C_{50}$, the unit group $(\mathbb{Z}G)^*$ is also generated by the Hoechsmann units (see below).

Various constructions of finite index subgroups of $(\mathbb{Z}G)^*$ have appeared in the literature (see [20] for an overview). Among these a construction by Hoechsmann [15] seems to yield subgroups of particularly small index. As an application of our algorithm, we have compared the full unit groups with the groups of Hoechsmann units, for G of size up to 110.

We briefly describe Hoechsmann's construction. First, let C be a cyclic group of order n, generated by the element x. For $i \geqslant 0$ and $y \in C$ we set

$$s_i(y) = 1 + y + \cdots + y^{i-1}.$$

Let i, j be integers with $0 < i, j < n$ and $\gcd(i, n) = \gcd(j, n) = 1$. Let k, l be positive integers with $li = 1 + kn$. Set

$$u_{i,j}(x) = s_l(x^i) s_i(x^j) - k s_n(x).$$

Then $u_{i,j}(x)$ is a unit in $(\mathbb{Z}C)^*$. Let $\Theta(C)$ denote the set of all units constructed in this way. We let $\mathcal{H}$ be the group of units in $(\mathbb{Z}G)^*$ generated by all $\Theta(C)$, where C ranges over the cyclic subgroups of G of order > 2, along with $\pm G$. It is called the group of *constructable units* of $\mathbb{Z}G$. By [15, Theorem 2.5], $\mathcal{H}$ is a subgroup of finite index of $(\mathbb{Z}G)^*$.

In general the set consisting of the $u_{i,j}(x)$ is a heavily redundant generating set. We note, however, that [16, Theorem 1.1], gives a non-redundant generating set of $\mathcal{H}$, if the group $H_m = (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$ is cyclic, where m is the exponent of G. We remark that for small m the group H_m is cyclic with only few exceptions. The values of m up to 120, for which H_m is not cyclic, are 24, 40, 48, 56, 60, 63, 65, 72, 80, 84, 85, 88, 91, 96, 104, 105, 112, 117, 120.

We let $\text{Hind}(G)$ be the index of $\mathcal{H}$ in $(\mathbb{Z}G)^*$, and we call this number the Hoechsmann index. We have computed the Hoechsmann indices for all abelian groups of orders up to 110. For most groups the index is 1. The groups for which it is not 1 are listed in Table 2, along with the corresponding Hoechsmann indices.

Table 2
Hoechsmann indices for abelian groups of orders up to 110, for which this index is not 1.

G	Hind(G)	G	Hind(G)
C_{40}	2	C_{84}	2
$C_2 \times C_{20}$	2	$C_2 \times C_{42}$	2
$C_2 \times C_2 \times C_{10}$	2	C_{85}	2
C_{48}	2	C_{90}	3
$C_2 \times C_{24}$	2	$C_3 \times C_{30}$	3
$C_2 \times C_2 \times C_{12}$	2	C_{91}	3
$C_4 \times C_{12}$	4	C_{96}	8
C_{60}	2	$C_2 \times C_{48}$	16
$C_2 \times C_{30}$	2	$C_2 \times C_2 \times C_{24}$	32
C_{63}	3	$C_2 \times C_2 \times C_2 \times C_{12}$	16
$C_3 \times C_{21}$	3	$C_2 \times C_4 \times C_{12}$	64
C_{65}	2	$C_4 \times C_{24}$	64
C_{74}	3	C_{98}	7
C_{80}	4	$C_7 \times C_{14}$	343
$C_2 \times C_{40}$	8	C_{104}	2
$C_2 \times C_2 \times C_{20}$	16	$C_2 \times C_{52}$	2
$C_2 \times C_2 \times C_2 \times C_{10}$	32	$C_2 \times C_2 \times C_{26}$	2
$C_4 \times C_{20}$	8	C_{105}	4

From Table 2 we see that on many occasions when Hind$(G) \neq 1$ we have that $|G| = m$, with H_m not cyclic. Also, for the groups considered, if for one group G of order m we have Hind$(G) \neq 1$, then the same holds for all groups of that order (except when $(\mathbb{Z}G)^*$ has rank 0).

Remark 4.1. For the groups C_p, with p a prime between 67 and 120 the correctness of our computation depends on the Generalised Riemann Hypothesis (see Section 2.4).

5. Computing generators of arithmetic groups of diagonalisable algebraic groups

In this section we use the term *D-group* as short for diagonalisable algebraic subgroup of GL$(n, \mathbb{C})$, defined over $\mathbb{Q}$. We consider the problem to compute generators of the arithmetic group $G(\mathbb{Z}) = G \cap \mathrm{GL}(n, \mathbb{Z})$ for a given connected D-group G. We assume that the group G is given by its Lie algebra $\mathfrak{g} \subset \mathfrak{gl}(n, \mathbb{C})$ which in turn is given by a basis of matrices with coefficients in $\mathbb{Q}$. In the sequel such a basis will be called a $\mathbb{Q}$-*basis*.

We have two subsections: the first is devoted to characters, and in the second we outline our algorithm.

5.1. Computing the characters

We recall that a character of a group H is a homomorphism $\chi : H \to F^*$, where F^* denotes the multiplicative group of nonzero elements of a field F. In this section we let $G \subset H \subset \mathrm{GL}_m(\mathbb{C})$ be two connected D-groups defined over $\mathbb{Q}$. A well-known theorem (cf. [3, Proposition 8.2]) states that there are characters $\chi_1, \ldots, \chi_t : H \to \mathbb{C}^*$ such that G is the intersection of their kernels, i.e.,

$$G = \left\{ h \in H \mid \chi_i(h) = 1 \text{ for } 1 \leqslant i \leqslant s \right\}.$$

The problem considered in this section is to find a number field K, and characters $\chi_1, \ldots, \chi_t : H \to K^*$ such that G is the intersection of their kernels. We require that K and the χ_i be explicitly given, i.e., that we know the minimum polynomial of a primitive element of K, and that for a given $h \in H$ we can effectively compute $\chi_i(h)$. We assume that we are given the Lie algebras $\mathfrak{h}, \mathfrak{g}$ of H and G respectively, in terms of $\mathbb{Q}$-bases.

Proposition 5.1. *Let $X \in \mathrm{GL}_m(\mathbb{C})$ be such that $\widetilde{H} = XHX^{-1}$ consists of diagonal matrices. Set $\tilde{\mathfrak{h}} = X\mathfrak{h}X^{-1}$, $\tilde{\mathfrak{g}} = X\mathfrak{g}X^{-1}$. Then $\tilde{\mathfrak{h}}, \tilde{\mathfrak{g}}$ consist of diagonal matrices as well. Set*

$$\Lambda(\tilde{\mathfrak{h}}) = \left\{ (e_1, \ldots, e_m) \in \mathbb{Z}^m \;\middle|\; e_1\alpha_1 + \cdots + e_m\alpha_m = 0 \text{ for all } \mathrm{diag}(\alpha_1, \ldots, \alpha_m) \in \tilde{\mathfrak{h}} \right\},$$

and similarly define $\Lambda(\tilde{\mathfrak{g}})$. Then $\Lambda(\tilde{\mathfrak{h}}) \subset \Lambda(\tilde{\mathfrak{g}}) \subset \mathbb{Z}^m$ are pure lattices (cf. Section 2.1). Let $\underline{e}_i = (e_{i,1}, \ldots, e_{i,m}) \in \mathbb{Z}^m$, for $1 \leqslant i \leqslant s$, be a basis of $\Lambda(\tilde{\mathfrak{g}})$ such that $\underline{e}_{t+1}, \ldots, \underline{e}_s$ is a basis of $\Lambda(\tilde{\mathfrak{h}})$. For $1 \leqslant i \leqslant t$ define $\chi_i : H \to \mathbb{C}^*$ by $\chi_i(h) = \alpha_1^{e_{i,1}} \cdots \alpha_m^{e_{i,m}}$, where $XhX^{-1} = \mathrm{diag}(\alpha_1, \ldots, \alpha_m)$. Then G, as subgroup of H, is the intersection of the kernels of the χ_i.

Proof. Note that $\tilde{\mathfrak{h}}$ is the Lie algebra of $\widetilde{H}$. Therefore, it consists of diagonal matrices. Since $\tilde{\mathfrak{g}} \subset \tilde{\mathfrak{h}}$ we get the same property for $\tilde{\mathfrak{g}}$. The lattices $\Lambda(\tilde{\mathfrak{h}})$, $\Lambda(\tilde{\mathfrak{g}})$ are obviously pure. So as noted in Section 2.1, the required basis of $\Lambda(\tilde{\mathfrak{g}})$ exists.

A character $\widetilde{\chi}$ of $\widetilde{H}$ is given by a sequence $(e_1, \ldots, e_m)$ of integers such that $\widetilde{\chi}(\mathrm{diag}(\alpha_1, \ldots, \alpha_m)) = \alpha_1^{e_1} \cdots \alpha_m^{e_m}$. This follows from the same statement for the full diagonal group D_m, along with the fact that a character of $\widetilde{H}$ extends to a character of D_m [3, Proposition 8.2]. Furthermore, the differential of $\widetilde{\chi}$ is given by $\mathrm{d}\widetilde{\chi}(\mathrm{diag}(\alpha_1, \ldots, \alpha_m)) = e_1\alpha_1 + \cdots + e_m\alpha_m$. So since $\tilde{\mathfrak{h}}$ consists of all $\mathrm{diag}(\alpha_1, \ldots, \alpha_m)$ with $e_1\alpha_1 + \cdots + e_m\alpha_m = 0$ for all $(e_1, \ldots, e_m) \in \Lambda(\tilde{\mathfrak{h}})$ we get that

$$\widetilde{H} = \left\{ \mathrm{diag}(\alpha_1, \ldots, \alpha_m) \;\middle|\; \alpha_1^{e_1} \cdots \alpha_m^{e_m} = 1 \text{ for all } (e_1, \ldots, e_m) \in \Lambda(\tilde{\mathfrak{h}}) \right\}.$$

Indeed, the latter is a connected algebraic group with the same Lie algebra as H. An analogous statement holds for $\widetilde{G} = XGX^{-1}$ and $\tilde{\mathfrak{g}}$. This implies the statement of the proposition. $\quad\square$

So in order to solve the problem of this section we need to say how the various objects in Proposition 5.1 can be computed.

Let $B \subset M_m(\mathbb{Q})$ be the associative algebra with one generated by the basis elements of $\mathfrak{h}$. Then, using the terminology of Section 2.2, B is toral (indeed: its elements can simultaneously be diagonalised). Now using algorithms given in for example [7,11] we can compute a *splitting element* $b_0 \in B$. This means that b_0 generates B (as associative algebra). By repeatedly factoring polynomials over number fields, we construct the splitting field K of the minimal polynomial of b_0 over $\mathbb{Q}$. After factoring this polynomial over K we find the eigenvalues and eigenvectors of b_0. From this we get a matrix $X \in \mathrm{GL}_m(K)$ such that Xb_0X^{-1} is diagonal. We note that this also implies that $X\mathfrak{h}X^{-1}$ consists of diagonal matrices. As this is the Lie algebra of $\widetilde{H} = XHX^{-1}$, we get the same for $\widetilde{H}$, as the latter group is connected.

Since we have given a basis of $\mathfrak{h}$ we can compute a basis of $X\mathfrak{h}X^{-1}$. Corresponding to a basis element $\mathrm{diag}(\alpha_1, \ldots, \alpha_m)$ we construct the linear equation $\alpha_1 x_1 + \cdots + \alpha_m x_m = 0$ in the unknowns x_i. We can express the α_i as vectors in $\mathbb{Q}^d$, where d is the degree of K. So by solving these equations we get a basis of the space

$$V(\tilde{\mathfrak{h}}) = \left\{ (a_1, \ldots, a_m) \in \mathbb{Q}^m \;\middle|\; a_1\alpha_1 + \cdots + a_m\alpha_m = 0 \text{ for all } \mathrm{diag}(\alpha_1, \ldots, \alpha_m) \in \tilde{\mathfrak{h}} \right\}.$$

Now $\Lambda(\tilde{\mathfrak{h}}) = V(\tilde{\mathfrak{h}}) \cap \mathbb{Z}^m$, so as seen in Section 2.1, we can compute a basis of $\Lambda(\tilde{\mathfrak{h}})$. Furthermore, using the methods outlined in the same section, we get a basis of $\Lambda(\tilde{\mathfrak{g}})$ that contains a basis of $\Lambda(\tilde{\mathfrak{h}})$. Then the characters χ_i are easily constructed as in Proposition 5.1.

5.2. Putting the pieces together

Now let $G \subset \mathrm{GL}_m(\mathbb{C})$ be a connected D-group, defined over $\mathbb{Q}$. We assume that we have given its Lie algebra $\mathfrak{g} \subset \mathfrak{gl}_m(\mathbb{C})$ by a $\mathbb{Q}$-basis. We describe an algorithm for obtaining a finite set of generators of the group $G(\mathbb{Z}) = G \cap \mathrm{GL}_m(\mathbb{Z})$.

Lemma 5.2. *Let $A \subset M_m(\mathbb{C})$ be the associative algebra with one generated by the basis elements of $\mathfrak{g}$. Let A^* denote the set of invertible elements of A. Then A^* is a D-group defined over $\mathbb{Q}$ with Lie algebra A. Furthermore, $G \subset A^*$.*

Proof. Note that A has a basis consisting of matrices with coefficients in $\mathbb{Q}$. Let $A(\mathbb{Q})$ denote the $\mathbb{Q}$-algebra spanned by such a basis. Consider the linear equations that define $A(\mathbb{Q})$ as a subspace of $M_m(\mathbb{Q})$. Then those equations define A^* as a subgroup of $GL_m(\mathbb{C})$. Since the basis elements of $\mathfrak{g}$ can simultaneously be diagonalised, the same holds for the elements of A^*. It follows that A^* is a D-group, defined over $\mathbb{Q}$.

Since A^*, as subgroup of $GL_m(\mathbb{C})$, is given by linear equations, its Lie algebra, as subalgebra of $\mathfrak{gl}_m(\mathbb{C})$, is given by the same equations. Hence the Lie algebra of A^* is A, where the Lie product is given by the commutator. So since $\mathfrak{g} \subset A$, we also have $G \subset A^*$, as G is connected. $\quad\square$

Now in order to compute generators of $G(\mathbb{Z})$ we have the following algorithm. As input we take a $\mathbb{Q}$-basis of $\mathfrak{g}$.

(1) Compute a $\mathbb{Q}$-basis of A (notation of Lemma 5.2).
(2) Let $\mathcal{O} = A \cap M_m(\mathbb{Z})$ and use the algorithm of Section 3 to compute generators $a_1, \ldots, a_r$ of $\mathcal{O}^*$.
(3) Use the algorithm of Section 5.1 to construct a number field K and characters $\chi_1, \ldots, \chi_s : A^* \to K^*$ such that G is given, as subgroup of A^*, by the intersection of their kernels.
(4) Use Ge's algorithm [10] to compute bases of the lattices

$$\Lambda_i = \left\{ (e_1, \ldots, e_r) \in \mathbb{Z}^r \;\middle|\; \chi_i(a_1)^{e_1} \cdots \chi_i(a_r)^{e_r} = 1 \right\}.$$

(5) Let $\underline{e}_k = (e_{k,1}, \ldots, e_{k,r})$, for $1 \leqslant k \leqslant t$, be a basis of the intersection of all Λ_i $(1 \leqslant i \leqslant s)$. Set $u_k = a_1^{e_{k,1}} \cdots a_r^{e_{k,r}}$. Then $u_1, \ldots, u_t$ is a set of generators of $G(\mathbb{Z})$.

Proposition 5.3. *The previous algorithm terminates correctly.*

Proof. Note that by Lemma 5.2, A is the Lie algebra of A^*, so that in step (3) we have the correct input for the algorithm of Section 5.1. A basis of $\mathcal{O}$ can be computed using the methods of Section 2.1. So all steps can effectively be carried out.

Observe that $A^*(\mathbb{Z}) = A^* \cap GL_m(\mathbb{Z})$ is equal to $\mathcal{O}^*$. Now $g \in G(\mathbb{Z})$ if and only if $g \in A^*(\mathbb{Z})$ and $\chi_i(g) = 1$ for $1 \leqslant i \leqslant s$. But this is equivalent to $g = a_1^{e_1} \cdots a_r^{e_r}$ for certain $e_i \in \mathbb{Z}$, and $\chi_i(g) = 1$ for $1 \leqslant i \leqslant s$. But the latter condition is equivalent to $(e_1, \ldots, e_r) \in \Lambda_i$ for $1 \leqslant i \leqslant s$. Hence $g \in G(\mathbb{Z})$ if and only if g is a product of the u_k. $\quad\square$

Acknowledgment

References

[1] R.G. Ayoub, C. Ayoub, On the group ring of a finite abelian group, Bull. Aust. Math. Soc. 1 (1969) 245–261.
[2] Jean-François Biasse, Claus Fieker, Improved techniques for computing the ideal class group and a system of fundamental units in number fields, in: Proceedings of ANTS 2012, in press.
[3] A. Borel, Linear Algebraic Groups, second edition, Springer-Verlag, Berlin, Heidelberg, New York, 1991.
[4] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symbolic Comput. 24 (3–4) (1997) 235–265.
[5] Henri Cohen, A Course in Computational Algebraic Number Theory, first edition, Grad. Texts in Math., vol. 138, Springer, Berlin, 1993.
[6] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Pure Appl. Math., vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York, London, 1962.
[7] W. Eberly, Decomposition of algebras over finite fields and number fields, Comput. Complexity 1 (2) (1991) 183–210.

[8] W. Eberly, Decomposition of algebras over R and C, Comput. Complexity 1 (1991) 211–234.
[9] W. Eberly, M. Giesbrecht, Efficient decomposition of associative algebras, in: Y.N. Lakshman (Ed.), Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation: ISSAC'96, ACM, New York, 1996, pp. 170–178.
[10] G. Ge, Algorithms related to multiplicative representations of algebraic numbers, PhD thesis, University of California, Berkeley, 1993.
[11] Willem A. de Graaf, Gábor Ivanyos, Finding splitting elements and maximal tori in matrix algebras, in: Interactions Between Ring Theory and Representations of Algebras, Murcia, in: Lect. Notes Pure Appl. Math., vol. 210, Dekker, New York, 2000, pp. 95–105.
[12] Cornelius Greither, Improving Ramachandra's and Levesque's unit index, in: Number Theory, Ottawa, ON, 1996, in: CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 111–120.
[13] Florian Hess, Sebastian Pauli, Michael E. Pohst, Computing the multiplicative group of residue class rings, Math. Comp. 72 (243) (2003) 1531–1548.
[14] Graham Higman, The units of group-rings, Proc. Lond. Math. Soc. (2) 46 (1940) 231–248.
[15] Klaus Hoechsmann, Constructing units in commutative group rings, Manuscripta Math. 75 (1) (1992) 5–23.
[16] Klaus Hoechsmann, Unit bases in small cyclic group rings, in: Methods in Ring Theory, Levico Terme, 1997, in: Lect. Notes Pure Appl. Math., vol. 198, Dekker, New York, 1998, pp. 121–139.
[17] Jürgen Klüners, Sebastian Pauli, Computing residue class rings and Picard groups of orders, J. Algebra 292 (1) (2005) 47–64.
[18] R.S. Pierce, Associative Algebras, Springer-Verlag, New York, Heidelberg, Berlin, 1982.
[19] M. Pohst, H. Zassenhaus, Algorithmic Algebraic Number Theory, Encyclopedia Math. Appl., vol. 30, Cambridge University Press, Cambridge, 1989.
[20] Sudarshan K. Sehgal, Units in Integral Group Rings, Pitman Monogr. Surv. Pure Appl. Math., vol. 69, Longman Scientific & Technical, Harlow, 1993. With an appendix by Al Weiss.
[21] C.C. Sims, Computation with Finitely Presented Groups, Cambridge University Press, Cambridge, 1994.
[22] Lawrence C. Washington, Introduction to Cyclotomic Fields, second edition, Grad. Texts in Math., vol. 83, Springer-Verlag, New York, 1997.