Journal of Algebra 373 (2013) 441–452

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

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

ARTICLE INFO

Article history:
Received 16 April 2012
Available online 22 October 2012
Communicated by Gunter Malle

Keywords:
Group rings
Units
Arithmetic groups

ABSTRACT

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).

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2012.09.031

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_iA, where the e_i are orthogonal primitive idempotents. The e_iA 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

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

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.