ALGORITHMS FOR POLYCYCLIC-BY-FINITE GROUPS

BY GRETCHEN OSTHEIMER

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Mathematics

Written under the direction of

Professor Charles C. Sims

and approved by

New Brunswick, New Jersey

October, 1996

ABSTRACT OF THE DISSERTATION

Algorithms for Polycyclic-by-Finite Groups

by Gretchen Ostheimer

Dissertation Director: Professor Charles C. Sims

Let R be a number field. We present several algorithms for working with polycyclic-by-finite subgroups of $\mathrm{GL}(n, R)$. Let G be a subgroup of $\mathrm{GL}(n, R)$ given by a finite generating set of matrices. We describe an algorithm for deciding whether or not G is polycyclic-by-finite. For polycyclic-by-finite G, we describe an algorithm for deciding whether or not a given matrix is an element of G.

We prove that an abstract group G has a faithful representation as a triangularizable subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n if and only if G is polycyclic and the commutator subgroup of G is torsion-free nilpotent. Suppose G is a polycyclic group given by a consistent polycyclic presentation. We describe an algorithm for deciding whether or not G has a faithful representation as a triangularizable subgroup of $\mathrm{GL}(n, \mathbf{Z})$, as well as an algorithm for constructing such a representation if it exists.

Preliminary experiments indicate that the algorithms described in this thesis are suitable for computer implementation. Further experimentation is needed to determine the range of input for which the algorithms are practical with current technology.

Acknowledgements

My sincere thanks go to my advisor, Charles Sims, for the immense help which he has given me over the last four years. Even when he was inundated with his other professional obligations, he always found time to meet with me and to give careful attention to my work. I have the deepest respect for him and the high standards which he sets for himself in his research, teaching and professional relationships, and I consider myself very lucky to have had this opportunity to work closely with him.

I am very grateful to my officemate, friend and colleague Eddie Lo. Often, an idle question unfolded into an afternoon of brainstorming about group theory, and without these conversations my research would not have been the same. He was there in good times as well as bad with a delightful mix of philosophical insight and humor. I would also like to thank John Shareshian for his consistent support as a friend and colleague.

Many mathematicians and computer scientists helped me make the most of graduate school. David Johnson at Bell Labs has been a mentor for me throughout the last seven years. Richard Lyons helped see me through a particularly challenging time. Jerry Tunnell taught me to love number theory and helped me apply it in my research. John Dixon passed along a reference that allowed me to obtain a significant generalization. Ann Yasuhara helped me analyze the complexity of one of my bounds. I am grateful to the members of my committee for their careful reading and thoughtful feedback about this thesis.

Finally, I'd like to thank my friends and family for their support throughout my graduate career. I'd like to thank my father for telling me I could do it when I was still young enough to believe everything that he said. And most of all, I'd like to thank my partner, Emmi Schatz, for her consistent love, encouragement and patience, not to mention all the fun we have had along the way.

Dedication

This thesis is dedicated to Emmi Schatz.

Table of Contents

Algorithms for Polycyclic-by-Finite Groups

Gretchen Ostheimer

August 12, 1996

Chapter 1

Introduction

In 1911, Dehn formulated three fundamental decision problems for finitely presented groups :

- the word problem (given a finite presentation and a word W in the generators, decide whether or not W defines the identity element),
- the conjugacy problem (given a finite presentation and two words, W_1 and W_2, decide whether or not W_1 and W_2 define conjugate elements of the group), and
- the isomorphism problem (given two finite presentations, decide whether or not they define isomorphic groups).

The word problem is undecidable and it remains undecidable even if it is known that the finite presentation defines a solvable group.

One obstacle to computation with a finitely presented solvable group is that the group might have subgroups which are not finitely generated. If it is known that the group G is solvable and that all subgroups of G are finitely generated, i.e., if it is known that G is polycyclic, then all three of Dehn's problems are decidable. (For a history of these decidability results, consult the introductory remarks in [BCRS] and [Se1].) If the presentation is a consistent polycyclic presentation, then there exist practical algorithms for the word problem, but practical algorithms for the conjugacy and isomorphism problems have yet to be found. (In Section 1.2 we discuss what is meant by a a consistent polycyclic presentation.) The assumption that the group is given by a consistent polycyclic presentation can sometimes be dropped: although it is an undecidable problem to determine whether or not a given finitely presented group is polycyclic, if the group is polycyclic, the algorithm in [Lo2] for finding a consistent polycyclic presentation is practical enough to be useful in some interesting examples. The search for a practical algorithm for the conjugacy problem has motivated the research described in this thesis.

We will now try to illustrate the close relationship between the conjugacy problem and several basic problems concerning solvable matrix groups. It is natural to look for such a relationship since an abstract group is polycyclic if and only if it is isomorphic to a solvable subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n (Corollary 1, Chapter 2 and Theorem 5, Chapter 5 of [Se2]).

Let G be an infinite polycyclic group. There exists a normal subgroup N of G such that N is infinite free abelian (Lemma 6, Chapter 1 of [Se2]). Suppose that x and y are elements of N and that we want to decide whether or not x and y are conjugate in G. Since G acts by conjugation on N, there exists a homomorphism

$$G \to \mathrm{Aut}(N) \cong \mathrm{GL}(n, \mathbf{Z}),$$

where n is the rank of N as a free abelian group. Thus we are led to the consideration of the so-called *orbit problem* for polycyclic groups: given $a_1, \ldots, a_k \in \mathrm{GL}(n, \mathbf{Z})$ such that $G = \langle a_1, \ldots, a_k \rangle$ is polycyclic and given $u, v \in \mathbf{Z}^n$, decide whether or not there exists a g in G such that $ug = v$. This problem appears to be difficult. It was solved for nilpotent-by-finite groups in [Di1], but computing in nilpotent groups is much easier than computing in general polycyclic groups.

Let us consider the orbit problem in the special case when G is abelian. In this case the orbit problem is easily reduced to the so-called *membership problem* for abelian matrix groups: given $G = \langle a_1, \ldots, a_k \rangle \leq \mathrm{GL}(n, \mathbf{Z})$ such that G is abelian and given $a \in \mathrm{GL}(n, \mathbf{Z})$, decide whether or not $a \in G$. We now sketch the algorithm by which this reduction is achieved. Let U be the smallest G-invariant subgroup of $\mathbf{Z}^n$ containing u. Find a basis $\mathcal{B} = \{b_1, \ldots, b_r\}$ for U such that each b_i is of the form $uf_i(a_1, \ldots, a_k)$ for some polynomial $f_i \in \mathbf{Z}[x_1, \ldots, x_k]$. Let $\mathcal{C} = \{c_1, \ldots, c_r\}$ where $c_i = vf_i(a_1, \ldots, a_k)$. The reader can check that there exists a g in G such that $ug = v$ if and only if

- $\mathcal{C}$ is also a basis for U,

- if $m_1, \ldots, m_r$ are elements of $\mathbf{Z}$ such that $u = m_1 b_1 + \cdots + m_r b_r$, then $v = m_1 c_1 + \cdots + m_r c_r$, and
- the $r \times r$ change of basis matrix from $\mathcal{B}$ to $\mathcal{C}$ is an element of the restriction of G to U.

Thus we see how consideration of the conjugacy problem quickly leads to consideration of such questions as the membership problem for abelian matrix groups. In Chapter 2 we describe a set of algorithms for working with polycyclic-by-finite matrix groups. This includes an algorithm for solving the membership problem.

Another approach to working with a polycyclic-by-finite group G given by a finite presentation is to obtain a faithful representation of G as a subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n and then to work with the representation instead. (One reason that such an approach might be fruitful is that in this latter context we can often exploit the fact that the group is embedded in a finite-dimensional matrix algebra.) In Chapter 3 we describe an algorithm which, when given a finite presentation for a polycyclic group G, constructs an embedding of G into $\mathrm{GL}(n, \mathbf{Z})$ in the special case when the commutator G' of G is torsion-free nilpotent. Every polycyclic-by-finite G contains a normal subgroup H of finite index in G such that H' is torsion-free nilpotent. (This is a consequence of the linearity of G and Theorem 3, Chapter 2 of [Se2].) Therefore, it is reasonable to expect that it will be possible to extend this algorithm to the case when the group is polycyclic-by-finite.

There is debate within the computational group theory community about whether to focus on polynomial-time algorithms (algorithms for which the worst-case run-time is bounded by a polynomial in the length of the input) or practical algorithms (algorithms which are efficient enough to answer reasonable questions in a reasonable amount of time with the current technology). Although it is unlikely that the algorithms described in this thesis are polynomial, preliminary experiments suggest that they are in fact practical. In each of these experiments, one of the algorithms was simulated using sample input, and in most cases an answer was obtained fairly quickly.

1.1 Notation and definitions

Throughout this thesis let $\mathbf{Z}$ denote the ring of integers, $\mathbf{Q}$ the field of rationals, and $\mathbf{C}$ the field of complex numbers. Let R denote either $\mathbf{Z}$ or $\mathbf{Q}$. If p is a prime, then the field of p-adic numbers is denoted by $\mathbf{Q}_p$, its algebraic closure by $\overline{\mathbf{Q}_p}$, and the ring of p-adic integers by $\mathbf{Z}_p$. The field with p elements is denoted by F_p. If n is a positive integer, the group of $n \times n$ matrices invertible over R is denoted by $\mathrm{GL}(n, R)$ or by $\mathrm{GL}(V)$, where V is a free R-module of rank n. If G is a subgroup of $\mathrm{GL}(n, R)$, then the *enveloping algebra* of G, $\mathrm{Env}(G)$, is defined to be the smallest $\mathbf{Q}$-subalgebra A of the algebra of $n \times n$ matrices over $\mathbf{Q}$ such that $A \supset G$.

Let F be any field, and let E be an extension field of F. If G is a subgroup of $\mathrm{GL}(n, F)$, then G is *triangularizable over E* if there is a basis for E^n relative to which every matrix in G is upper triangular, and G is *triangularizable* if it is triangularizable over the algebraic closure of F. If G is a subgroup of $\mathrm{GL}(n, F)$ and if G is triangularizable over some extension field E of F, then there exists a finite extension L of F over which G is triangularizable. (See p. 33 of [Se2].) Therefore, a subgroup G of $\mathrm{GL}(n, \mathbf{Q})$ is triangularizable if and only if it is triangularizable over $\mathbf{C}$.

Let $\mathrm{Tr}_1(n, R)$ denote the group of upper triangular matrices with entries in R and 1's along the diagonal. Elements of $\mathrm{Tr}_1(n, R)$ are called *unitriangular*. An element of $\mathrm{GL}(n, R)$ is *unipotent* if all of its eigenvalues are 1. If $G < \mathrm{GL}(n, R)$ consists entirely of unipotent elements, then G is said to be *unipotent*. In this case there is a basis for R^n with respect to which G is unitriangular. (The case when $R = \mathbf{Q}$ is proved as Corollary 1.21 in [We], and the case when $R = \mathbf{Z}$ follows easily.) In Lemma 7 of Chapter 5 of [Se2], an alternative condition is given for guaranteeing the existence of such a basis, namely, that G act nilpotently on R^n: the group G *acts nilpotently* on R^n if there exists a chain

$$0 \leq V_0 \leq V_1 \leq \cdots \leq V_k = R^n$$

of G-invariant subgroups of R^n such that the induced action of G on each factor V_i/V_{i-1} is trivial. If G is a subgroup of $\mathrm{GL}(n, R)$, then there is a unique normal unipotent subgroup of G which is maximal among all such subgroups of G. (See 13.40 of [We].)

This subgroup is called the *unipotent part* of G.

If $x \in \mathbf{Z}^k$ and $g_1, \ldots, g_k \in \mathrm{GL}(n, R)$, then g^x denotes $g_1^{x_1} \cdots g_k^{x_k}$. The identity element of $\mathrm{GL}(n, R)$ is denoted by 1.

The i-th term in the lower central series for G is denoted by $\gamma_i(G)$. (For example, $\gamma_2(G) = G'$, the commutator subgroup of G.) The Fitting subgroup of a group G, $\mathrm{Fitt}(G)$, is defined to be

$$\langle N \mid N \triangleleft G \text{ and } N \text{ nilpotent} \rangle.$$

1.2 Basic algorithms for polycyclic groups

Chapter 9 in [Si] gives a good introduction to polycyclic groups. A group G is *polycyclic* if there is a sequence of subgroups $G_1, \ldots, G_{k+1}$ for G such that

$$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_k \triangleright G_{k+1} = 1,$$

where for each i, G_i/G_{i+1} is cyclic. In this case, if $g_i G_{i+1}$ is a generator for G_i/G_{i+1}, then $g_1, \ldots, g_k$ is called a *polycyclic generating sequence* for G. A group G is polycyclic if and only if G is solvable and all of the subgroups of G are finitely generated.

Polycyclic groups are finitely presented. It is often convenient to assume that a polycyclic group is given by a special presentation known as a *consistent polycyclic presentation*. Intuitively, a consistent polycyclic presentation is one from which the polycyclic structure of the group is easily gleaned. In particular, the generators in a consistent polycyclic presentation form a polycyclic generating sequence for G. (See Section 9.6 of [Si] for a precise definition.)

Throughout this thesis we rely on the following algorithms in [Si] for working with a polycyclic group G given by a consistent polycyclic presentation. These include:

- testing membership in a subgroup of G,
- finding the normal closure of a subgroup of G,
- finding generating sets for the terms in the lower central series of G, and
- finding a consistent polycyclic presentation for a section of G.

We also rely on the fact that a polycyclic group satisfies the ascending chain condition on subgroups. In Chapter 1, we will refer in some detail to two algorithms in Section 9.6 of [Si] for testing membership in a subgroup H of G: POLY_SUBGROUP and POLY_MEMBER. POLY_SUBGROUP calculates a polycyclic generating sequence for H. POLY_MEMBER uses such a sequence to test membership in H. POLY_MEMBER is constructive; that is, given a polycyclic generating sequence $h_1, \ldots, h_l$ for H and $y \in H$, POLY_MEMBER can find an x in $\mathbf{Z}^l$ such that $h^x = y$.

For a polycyclic group G define the *torsion subgroup* of G, $T(G)$, to be

$$\langle N \mid N \triangleleft G \text{ and } N \text{ finite} \rangle.$$

It follows from the ascending chain condition that $T(G)$ is finite. In Section 3.3 we will need a practical algorithm to find the torsion subgroup of a nilpotent group given by a consistent nilpotent presentation. In Theorem 3.11 of [BCRS], the authors describe an algorithm for finding $T(G)$ for polycyclic G. In the case when G is actually nilpotent, their algorithm (modified only slightly) appears to be practical. The modified algorithm is described as follows. Begin by finding the last nontrivial term $A = \gamma_c(G)$ in the lower central series for G. By induction on the class of G, we can find the torsion subgroup of G/A and hence its preimage C under the map $G \to G/A$. We can then find the torsion subgroup of C/C' and its preimage T under the map $C \to C/C'$. It is obvious that $T(G) \leq T$. Since A is central in G, A is contained in $Z(C)$, the center of C. Therefore $|C : Z(C)| \leq |C : A| < \infty$. By a theorem of Schur (Corollary 10.1.4 in [Ro]), it follows that C' is finite. Therefore, T is finite and $T = T(G)$.

1.3 Algorithms for the group ring

In Chapter 3 we describe an algorithm for constructing an embedding of a polycyclic group G (given by a consistent polycyclic presentation) into $\mathrm{GL}(n, \mathbf{Z})$ (for some n) in the special case when the commutator subgroup G' of G is torsion-free nilpotent. This is done by letting G act on the group ring $\mathbf{Z}[H]$ for various subgroups H of G. In this section we recall some basic facts about group rings. We also discuss the recent work of Lo in which the Gröbner basis method of commutative ring theory is generalized to the group ring of a polycyclic group. (See [Lo2].)

The ideals that arise in Chapter 3 are two-sided. Henceforth, the term *ideal* will refer to a two-sided ideal of a ring. However, the algorithms in [Lo2] work with right ideals. Therefore, all ideals will be described by a finite set of right ideal generators. (Recall that each right ideal in the group ring of a polycyclic-by-finite group is finitely generated as a right ideal. For a proof of this, see [Lo2] or p. 93 of [Se2].) Note that if R is any ring and $\mathcal{A}$ and $\mathcal{B}$ are ideals of R generated as right ideals by sets A and B respectively, then $\mathcal{AB}$ is generated as a right ideal by $\{ab \mid a \in A,\, b \in B\}$.

The *augmentation ideal* $\mathcal{G}$ of $\mathbf{Z}[G]$ is the kernel of the ring homomorphism of $\mathbf{Z}[G]$ to $\mathbf{Z}$ taking $\sum n_g g$ to $\sum n_g$. If G is generated by $a_1, \ldots, a_k$ as a group, then the set $\{a_1 - 1, \ldots, a_k - 1\}$ generates $\mathcal{G}$ as a right ideal. To see this, let $\mathcal{J}$ be the right ideal generated by $\{a_1 - 1, \ldots, a_k - 1\}$. Since $\mathcal{G}$ is generated by

$$\{g - 1 \mid g \in G,\ g \neq 1\}$$

as an abelian group, it suffices to show that for all g in G, $g - 1 \in \mathcal{J}$. But suppose that $w \in G$ and $w - 1 \in \mathcal{J}$. Then $wa_i - 1 = (w-1)a_i + (a_i - 1) \in \mathcal{J}$, and $wa_i^{-1} - 1 = ((w-1) - (a_i - 1))a_i^{-1} \in \mathcal{J}$. Therefore, for all $g \in G$, $g - 1 \in \mathcal{J}$, and hence $\mathcal{J} = \mathcal{G}$.

Let G be a polycyclic group and let $\mathcal{I}$ be an ideal of $\mathbf{Z}[G]$. Suppose we are given a consistent polycyclic presentation for G and a finite set of elements in the group ring that generates $\mathcal{I}$ as a right ideal. Lo has implemented algorithms for solving the following problems.

- Decide whether or not a given element of the group ring is an element of $\mathcal{I}$.
- Decide whether or not $\mathbf{Z}[G]/\mathcal{I}$ is finitely generated as an abelian group.
- If so, find a finite set of elements of $\mathbf{Z}[G]$ whose images generate $\mathbf{Z}[G]/\mathcal{I}$ as an abelian group, and find a finite set of elements of $\mathbf{Z}[G]$ whose images generate the torsion subgroup of $\mathbf{Z}[G]/\mathcal{I}$ (considered as an abelian group).

If, in addition, $\mathbf{Z}[G]/\mathcal{I}$ is a free abelian group, then Lo's algorithms can be used to solve the following problems.

- Find a set of elements of $\mathbf{Z}[G]$ whose images form a basis for $\mathbf{Z}[G]/\mathcal{I}$.

- Given an element x of the group ring, express $x + \mathcal{I}$ in terms of that basis.

Let H be a finitely generated group acting on $\mathbf{Z}[G]/\mathcal{I}$ by $\mathbf{Z}$-automorphisms, where $\mathbf{Z}[G]/\mathcal{I}$ is finitely generated free abelian. In Chapter 3 we will consider several situations in which we start with a concrete description of the action of H; that is, if h is a given element of H and if x is a given element of $\mathbf{Z}[G]$, then we can find an element y of $\mathbf{Z}[G]$ such that the image of $x+\mathcal{I}$ under h is $y+\mathcal{I}$. In such situations Lo's algorithms can be used to find a matrix representation for H as follows. Find elements $b_1, \ldots, b_n$ of $\mathbf{Z}[G]$ whose images form a basis for $\mathbf{Z}[G]/\mathcal{I}$. Then for each generator h of H, find a matrix representing the action of h on $\mathbf{Z}[G]/\mathcal{I}$ by expressing the image of each $b_i + \mathcal{I}$ (under the action of h) as a $\mathbf{Z}$-linear combination of $b_1 + \mathcal{I}, \ldots, b_n + \mathcal{I}$.

1.4 Facts about $\mathbf{GL}(n, \mathbf{Z}_p)$

We first establish a connection between finitely generated subgroups of $\mathrm{GL}(n, \mathbf{Q})$ and subgroups of $\mathrm{GL}(n, \mathbf{Z}_p)$. If G is a finitely generated subgroup of $\mathrm{GL}(n, \mathbf{Q})$, then the subring S of $\mathbf{Q}$ generated by the entries of the elements of G is finitely generated as a ring. Therefore, there exists a prime p such that if $r \in S$, then $r = \frac{u}{v}$, where $u, v \in \mathbf{Z}$ and $(v, p) = 1$. Notice that G can be embedded in $\mathrm{GL}(n, \mathbf{Z}_p)$: the obvious embedding of $\mathbf{Q}$ into $\mathbf{Q}_p$ maps S into $\mathbf{Z}_p$, and thus there exists a group embedding of G into $\mathrm{GL}(n, \mathbf{Z}_p)$. As we saw in Section 1.1, G is triangularizable over $\overline{\mathbf{Q}_p}$ if and only if G is triangularizable over $\mathbf{C}$.

In [Di1] Dixon gives a sufficient condition for a subgroup of $\mathrm{GL}(n, \mathbf{Z}_p)$ to be triangularizable over $\overline{\mathbf{Q}_p}$. Consider the ring homomorphism

$$\mathbf{Z}_p \to \mathbf{Z}_p/p\mathbf{Z}_p \cong F_p$$

and its extension to a group homomorphism $\theta : \mathrm{GL}(n, \mathbf{Z}_p) \to \mathrm{GL}(n, F_p)$. The kernel of this homomorphism is called the *principal p-congruence subgroup* of $\mathrm{GL}(n, \mathbf{Z}_p)$.

Lemma 1.4.1 *Let p be an odd prime, and let C be the principal p-congruence subgroup of $GL(n, \mathbf{Z}_p)$. If H is a subgroup of C, and H is solvable-by-finite, then H is* *triangularizable (over* $\overline{\mathbf{Q}_p}$*).*

Proof. In [Di1] Dixon shows that H is connected in the Zariski topology of $\mathrm{M}(n, \overline{\mathbf{Q}_p})$. By the Lie-Kolchin theorem (as stated in Lemma 8.6 of [Di2]), H is triangularizable over $\overline{\mathbf{Q}_p}$. □

Chapter 2

Algorithms for Matrix Groups

2.1 Introduction

In this chapter we describe algorithms for solving the following problems concerning polycyclic-by-finite matrix groups. Refer to Section 1.1 for definitions and a description of the notation. Let G be a subgroup of $\mathrm{GL}(n, \mathbf{Q})$ given by a finite set of generators. We can decide whether or not G is

- triangularizable (Section 2.5.1),
- polycyclic-by-finite (Section 2.6.2),
- solvable-by-finite (Section 2.6.2).

If G is polycyclic-by-finite, we can do the following.

- Find a finite set of generators for a normal subgroup H of finite index in G such that H is triangularizable (Section 2.6.2).
- Given an element a in $\mathrm{GL}(n, \mathbf{Q})$, decide whether or not $a \in G$ (Section 2.6.3).

If G is triangularizable, we can find a finite set of generators for the unipotent part of G (Section 2.5.2). In the case when $G = \langle g_1, g_2, \ldots, g_k \rangle$ and G is abelian, we can also do the following.

- Given an element a in $\mathrm{GL}(n, \mathbf{Q})$ such that $a \in G$, find an $x \in \mathbf{Z}^k$ such that $a = g^x$ (Section 2.4).
- Find a presentation for G, i.e., find generators for the subgroup H of $\mathbf{Z}^k$ consisting of elements x such that $g^x = 1$ (Section 2.4).

Preliminary experiments suggest that the algorithms described in this chapter are practical. (See Section 2.8.) Further experiments are needed to determine the kinds of input for which the algorithms will terminate in a reasonable amount of time.

If F is a number field such that $[F : \mathbf{Q}] = d$, then the elements of F can be represented as $d \times d$ matrices over $\mathbf{Q}$. Therefore, all of the algorithms above can also be used to study subgroups of $\mathrm{GL}(n, F)$.

Throughout this chapter, R will denote either $\mathbf{Z}$ or $\mathbf{Q}$. The algorithms depend on two structure theorems concerning subgroups of $\mathrm{GL}(n, R)$: one describes the structure of triangularizable matrix groups (Section 2.5.1), and the other describes the structure of polycyclic-by-finite matrix groups (Section 2.6.1). In both cases, we show that through a change of basis over R, the groups have a certain block upper triangular form.

2.2 Abelian groups embedded in fields

In order to develop an algorithm to find a presentation for an abelian subgroup G of $\mathrm{GL}(n, \mathbf{Q})$, we consider two special cases. Let A be the enveloping algebra of G. In the first case A is a field, and in the second case $G \leq \mathrm{Tr}_1(n, \mathbf{Q})$. In Section 2.4 we prove a structure theorem for abelian matrix groups that shows that these two cases are sufficient. The first case is discussed in this section, and the second case is discussed in Section 2.3.

Let G be an abelian subgroup of $\mathrm{GL}(n, \mathbf{Q})$ given by a finite set $\{g_1, \ldots, g_k\}$ of generators. Suppose that A, the enveloping algebra of G, is a field. We want to find generators for the subgroup H of $\mathbf{Z}^k$ consisting of elements x such that $g^x = 1$. This problem was solved in [Ge]. Ge assumes that the field is described by d^3 structure constants, where d is the dimension of A as a vector space over $\mathbf{Q}$. More precisely, in order to use his algorithm, first find a basis $b_1, \ldots, b_d$ for A over $\mathbf{Q}$, and then find constants c_{ijk} such that for all i, j,

$$b_i b_j = \sum_k c_{ijk} b_k.$$

Ge proves that the run-time of his algorithm is polynomial in the length of the input.

Once we have an algorithm to find H, we can test membership in G constructively, i.e., we can decide whether or not $a \in G$ and, if so, we can express a in terms of the given generators for G. To do so, first verify that a commutes with $g_1, \ldots, g_k$. Then rename a as g_{k+1} and find generators for $\widetilde{H}$, the subgroup of vectors x in $\mathbf{Z}^{k+1}$ such that $g^x = 1$. If there exists an element x of $\widetilde{H}$ such that $x_{k+1} = -1$, then let y be the vector consisting of the first k components of x for then $a = g^y$. Otherwise, $a \notin G$.

Ge makes no claims concerning the practicality of his algorithm. However, we independently discovered an algorithm to find a presentation in the special case when $G \leq \mathrm{GL}(n, \mathbf{Z})$. Our algorithm is similar to that of Ge, and preliminary experiments suggest that our algorithm is practical.

We continue the notation established at the beginning of this section, but now we assume furthermore that $G < \mathrm{GL}(n, \mathbf{Z})$. Let O_A be the ring of algebraic integers of A, and let O_A^* be the group of units of O_A. If r is the number of real embeddings of A, and $2c$ is the number of complex embeddings of A, then the usual logarithmic homomorphism ρ maps O_A^* to $\mathbf{R}^s$, where $s = r + c$. The image of G under ρ is a lattice L in a hyperplane of $\mathbf{R}^s$. (See Theorem 4.9.7 of [Co].) Let K be the subgroup of $\mathbf{Z}^k$ consisting of elements x such that $\rho(g^x) = 1$. An algorithm for finding generators for K is described in [BP]. The algorithm requires as input a lower bound M for the length of the shortest nonzero vector in L. If A is a low degree extension of $\mathbf{Q}$, then accurate bounds on the length of a shortest nonzero vector can be obtained by finding a system of fundamental units for the group of units for O_A. (See Section 6.5 of [Co].) When this is impractical, the following lemma from [Do] can be used to obtain a lower bound.

Lemma 2.2.1 *Let α be a nonzero algebraic integer of degree d. Let $\{\alpha_1, \ldots, \alpha_d\}$ be the algebraic conjugates of α. If*

$$\prod_1^d max\{1, |\alpha_j|\} \leq 1 + \frac{1}{1200}\left(\frac{\log\log d}{\log d}\right)^3,$$

then α is a root of unity.

The run-time of the algorithm in [BP] is polynomial in $s + k$ and the size of the input data. The authors illustrate the practicality of their algorithm by finding (for real quartic fields with discriminants below 100000) a multiplicative relation between four given units.

Having found a presentation for $\rho(G)$ (that is, having found generators $k_1, \ldots, k_j$ for K), let us turn our attention back to the problem of finding a presentation for G (that is, of finding generators for H). The kernel of ρ is the torsion subgroup T of O_A^*. Let $m = |T|$, and suppose $T = \langle t \rangle$. Let ϕ be the Euler ϕ-function. The minimal polynomial f of t has degree $\phi(m)$. Therefore, $\phi(m) \leq n$, and the following lemma (suggested to the author by Jerrold Tunnell) gives a simple bound on the order of T.

Lemma 2.2.2 $m \leq 2.4\phi(m)^{4/3}$.

Proof. Let $m = p_1^{\alpha_1} \cdots p_j^{\alpha_j}$ be the prime factorization of m. If $j = 1$, then

$$\begin{aligned} \phi(m) &= m(1 - 1/p_1) \\ &\geq m/2. \end{aligned}$$

If $j > 1$, then

$$\begin{aligned} \phi(m) &= m(1 - 1/p_1) \cdots (1 - 1/p_j) \\ &= m^{3/4}(1 - 1/p_1)p_1^{\alpha_1/4} \cdots (1 - 1/p_j)p_j^{\alpha_j/4} \\ &\geq m^{3/4}(1 - 1/2)2^{1/4}(1 - 1/3)3^{1/4}. \end{aligned}$$

In either case, the result now follows. □

Therefore, T is a cyclic group of small order. A finite set of generators for $T \cap G$ is now easily found:

$$T \cap G = \langle g^{k_i} : i = 1, \ldots, j \rangle.$$

It is not hard in practice to find a cyclic generator for $T \cap G$. Since H is the kernel of the map from K to $T \cap G$ taking x to g^x, we can use the techniques of Section 9.6 of [Si] to find generators for H.

Ge uses a technique which is similar to that described above, but he uses complex logarithms instead of real logarithms. He shows that the length of the shortest nonzero vector in the resulting lattice is bounded below by $1/16$.

2.3 Unitriangular groups

2.3.1 Unitriangular subgroups of $\mathbf{GL}(n, \mathbf{Z})$

Let G be a subgroup of $\mathrm{Tr}_1(n, \mathbf{Z})$ given by a finite set $\{g_1, \ldots, g_k\}$ of generators. In order to test membership in G, we rely on algorithms which have been developed for working with polycyclic groups given by consistent polycyclic presentations. (See Section 1.2 for a description of POLY_SUBGROUP and POLY_MEMBER.) Since $\mathrm{Tr}_1(n, \mathbf{Z})$ is a finitely generated nilpotent group, it is also polycyclic. (See Example 2.1 and Proposition 3.4 in Chapter 9 of [Si].) It is easy to find a consistent polycyclic presentation $\langle X | R \rangle$ for $\mathrm{Tr}_1(n, \mathbf{Z})$: Example 4.1 in Chapter 9 of [Si] is easily generalized. It is also easy to express a given unitriangular matrix in terms of the generators in X. Use POLY_SUBGROUP to calculate a polycyclic generating sequence $h_1, \ldots, h_l$ for G and POLY_MEMBER to then test membership in G. In order to test our algorithm on examples, we implemented versions of POLY_SUBGROUP and POLY_MEMBER for this specific context. See Section 2.8 for further information.

When G is both unitriangular and abelian, we can also find a presentation for G in terms of $g_1, \ldots, g_k$, i.e., we can find generators for the subgroup H of $\mathbf{Z}^k$ consisting of elements z such that $g^z = 1$. We do so as follows. Since G is free abelian, we can use POLY_SUBGROUP to find a basis $h_1, \ldots, h_l$ for G. There is a homomorphism μ from $\mathbf{Z}^k$ to $\mathbf{Z}^l$ taking u in $\mathbf{Z}^k$ to the vector v in $\mathbf{Z}^l$ such that $h^v = g^u$. An integer matrix representing μ can be computed as follows: if e_i is the i-th vector in the usual basis for $\mathbf{Z}^k$, then POLY_MEMBER can be used to find $\mu(e_i)$, the vector in $\mathbf{Z}^l$ such that $g_i = h^{\mu(e_i)}$. The kernel H of μ is then easy to compute. As we saw in Section 2.2, if we can find a presentation for G, then it follows that our membership test for G can be made constructive.

2.3.2 Unitriangular subgroups of $\mathbf{GL}(n, \mathbf{Q})$

Let G be a finitely generated subgroup of $\mathrm{Tr}_1(n, \mathbf{Q})$. We reduce the problem of testing membership in G to the problem of testing membership in a subgroup of $\mathrm{Tr}_1(n, \mathbf{Z})$. In [Se2] (Lemma 2, Chapter 6), Segal shows that if $G = \langle g_1, \ldots, g_k \rangle$ is a finitely generated subgroup of $\mathrm{Tr}_1(n, \mathbf{Q})$, then it is easy to find an x in $\mathrm{GL}(n, \mathbf{Q})$ such that $x^{-1}Gx \leq \mathrm{Tr}_1(n, \mathbf{Z})$: find a natural number m such that mg_i is an integer matrix for all $1 \leq i \leq k$, and then let

$$x = \begin{pmatrix} 1 & 0 & \cdot & \cdot & 0 & 0 \\ 0 & m & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & m^{n-1} \end{pmatrix}.$$

Thus, membership testing in a finitely generated subgroup of $\mathrm{Tr}_1(n, \mathbf{Q})$ is reduced to the analagous problem in $\mathrm{Tr}_1(n, \mathbf{Z})$. As with subgroups of $\mathrm{Tr}_1(n, \mathbf{Z})$, if G is also abelian, then we can make our membership test constructive, and we can find a presentation for G. Alternative methods for working with abelian subgroups of $\mathrm{Tr}_1(n, \mathbf{Q})$ are described in [BBCIL].

2.4 Abelian groups

The following proposition indicates how the problem of finding presentations for finitely generated abelian groups can be reduced to the corresponding problems for abelian groups embedded in fields and finitely generated abelian unitriangular groups.

Proposition 2.4.1 *Let G be an abelian subgroup of $GL(n, R)$. There exist a basis B for R^n and positive integers $n_1, \ldots, n_r$ such that $n_1 + \cdots + n_r = n$ and all matrices in G have the following block structure with respect to B:*

$$g = \begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix},$$

where for $1 \leq i \leq r$, a_i is an $n_i \times n_i$ matrix, and if G_i is the image of G under the map that takes g to a_i, then the enveloping algebra of G_i is a field.

Proof. Let A be the enveloping algebra of G, and suppose A is not a field. There exists a zero divisor a of A. (If $R = \mathbf{Z}$, then ensure $a \in M(n, \mathbf{Z})$ by clearing denominators.) Let $V = \{v \in R^n \mid va = 0\}$. Since $0 < V < R^n$ and V is invariant under G, by induction we can choose a basis D for V relative to which $G|_V$ has the desired form. There is a complement W to V in R^n. (If $R = \mathbf{Z}$, then R^n/V is torsion-free.) Choose a basis for W and thereby a basis for R^n/V. Consider the map τ that takes an element of G to the matrix representing its action on R^n/V relative to this basis. By induction again, we can find a basis C for W such that relative to the corresponding basis for R^n/V, $\tau(G)$ has the desired form. Then C, D is a basis for R^n that satisfies the criteria of the proposition. □

The problem of computing a basis B satisfying the criteria of Proposition 2.4.1 is closely related to the problem of finding the primary decomposition of the radical $J(A)$ of A, where A is the enveloping algebra of G. Given a basis B satisfying the criteria of Proposition 2.4.1, we can compute vector space generators for M_i, the kernel of the map that takes a matrix g to a_i. Then M_i is a maximal ideal, and

$$J(A) = \bigcap_{i=1}^{r} M_i.$$

Conversely, if we are given ideal generators for the maximal ideals $M_1, \ldots, M_l$ in the primary decomposition of $J(A)$, then it follows from the uniqueness of the primary decomposition and Proposition 2.4.1 that there exists an i such that the nullspace V_i of M_i is a nontrivial, invariant subspace on which the enveloping algebra of G is a field.

The development of practical algorithms for finding primary decompositions is an active area of research. In [FR], for example, the authors show that there exists a polynomial time algorithm for computing the primary decomposition of the radical of a matrix algebra. In [EHV], the authors discuss the problem of finding a practical algorithm for computing the primary decomposition of an ideal in a polynomial ring. IBM's symbolic computation package AXIOM has a function for finding the primary decomposition for a zero-dimensional ideal in a polynomial ring. Further research on practical algorithms for computing the primary decomposition will shed light on how best to achieve the reduction we seek here. One method is to mimic the proof of

Proposition 2.4.1, relying on methods in [EHV] or [FR] for deciding whether or not A is a field and, if it is not, for finding a zero divisor a in A. Note that when $R = \mathbf{Z}$, we find a basis for $\mathbf{Z}^n$ relative to which G has the desired form.

Now let us assume that G is an abelian subgroup of $\mathrm{GL}(n, R)$ given by a finite set $\{g_1, \ldots, g_k\}$ of generators, and that we have found a basis for R^n satisfying the criteria of Proposition 2.4.1. We now show that we can obtain a presentation for G, i.e., we can find generators for the subgroup H of $\mathbf{Z}^k$ consisting of elements z such that $g^z = 1$. Let ψ be the group homomorphism given below.

$$g = \begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix} \longmapsto \begin{pmatrix} a_1 & 0 & \cdot & \cdot & 0 & 0 \\ 0 & a_2 & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix}$$

Let π_i be the group homomorphism that takes g to a_i. As we saw in Section 2.2, we can find generators for the subgroup K_i of $\mathbf{Z}^k$ consisting of elements z such that $\pi_i(g^z) = 1$, and hence we can find a basis $k_1, \ldots, k_s$ for

$$K = \bigcap_{i=1}^{r} K_i = \{x \in \mathbf{Z}^k \mid \psi(g^x) = 1\}.$$

Let S be the $s \times k$ matrix whose i-th row is k_i. The image of K (under the map that takes x to g^x) is an abelian subgroup of $Tr_1(n, \mathbf{Z})$ and hence is free. As described in Section 2.3, we can use POLY_SUBGROUP to find a basis $h_1, \ldots, h_l$ for the image of K. Let μ be the homomorphism from $\mathbf{Z}^s$ to $\mathbf{Z}^l$ that takes the standard basis vector $e_i \in \mathbf{Z}^s$ to the vector $v \in \mathbf{Z}^l$ such that $g^{k_i} = h^v$. An integer matrix representing μ can be found by using POLY_MEMBER to compute $\mu(e_i)$. Use Hermite normal form calculations to find a matrix T whose rows form a basis for the kernel of μ. The rows of TS then form a generating set for H. As described in Section 2.2, it follows that we can also test membership in G constructively.

2.5 Triangularizable groups

2.5.1 A structure theorem

Recall that an abelian subgroup G of $\mathrm{GL}(n, R)$ is triangularizable. (See p. 29 of [Se2].) We can use this fact to construct other examples of triangularizable subgroups. Let $n = n_1 + \cdots + n_r$, and let G_i be an abelian subgroup of $\mathrm{GL}(n_i, R)$. Choose as our generators for G matrices that have the following block structure:

$$\begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix},$$

where $a_i \in G_i$ for all i. Clearly, G is triangularizable. In this section we show that given a finite set of generators for a triangularizable subgroup G of $\mathrm{GL}(n, R)$, we can find a basis for R^n relative to which G has this form. Furthermore, we describe an algorithm for deciding whether or not a subgroup of $\mathrm{GL}(n, R)$ given by a finite set of generators is triangularizable.

Clearly, a triangularizable subgroup is unipotent-by-abelian: after a change of basis over $\mathbf{C}$ the group is upper triangular, and the commutator of two upper triangular matrices is an upper triangular matrix with 1's on the diagonal. We will now show that all unipotent-by-abelian subgroups have the desired form.

For any positive integer n and for any subgroup L of $\mathrm{GL}(n, R)$, let

$$V(L) = \{v \in R^n \mid vl_1l_2 = vl_2l_1 \,\forall\, l_1,\, l_2 \in L\}.$$

The following lemma establishes some obvious properties of $V(L)$.

Lemma 2.5.1 *Let L be a subgroup of $GL(n, R)$. Then $V(L) \leq R^n$ is an R-submodule of R^n invariant under L, the image of L under the map to $GL(V(L))$ is abelian, and $V(L)$ has a complement in R^n.*

Proof. $V(L)$ is invariant under the action of L since if $v \in V(L)$ and $x, g, h \in L$, then

$$vx(gh - hg) = v((xg)h - h(xg)) + (v(hx - xh))g = 0.$$

If $R = \mathbf{Z}$, then $\mathbf{Z}^n/V(L)$ is torsion-free. Hence for $R = \mathbf{Z}$ or $\mathbf{Q}$, $V(L)$ has a complement in R^n. The rest follows easily. □

Let $V_0(L) = 0$. Inductively, define a chain

$$0 = V_0(L) \leq V_1(L) \leq V_2(L) \leq \cdots$$

of L-invariant R-submodules of R^n as follows. Let $\overline{L}$ be the image of the map taking L to $\mathrm{GL}(R^n/V_i(L))$. Let $V_{i+1}(L)$ be the pullback of $V(\overline{L})$ under the map $R^n \to R^n/V_i(L)$. Then $V_{i+1}(L)$ is L-invariant. To see this, let $x \in V_{i+1}(L)$ and $g \in L$. Then $x + V_i(L) \in V(\overline{L})$. By Lemma 2.5.1 $xg + V_i(L) \in V(\overline{L})$ and hence $xg \in V_{i+1}(L)$.

For unipotent-by-abelian matrix groups, more can be said.

Lemma 2.5.2 *Let G be a unipotent-by-abelian subgroup of $GL(n, R)$. Then $V(G) \neq 0$.*

Proof. Recall (from Section 1.1) that since G' is unipotent, there is a basis for R^n with respect to which G' is unitriangular. Therefore, there exists a nonzero element x of R^n such that $xg = x$ for all $g \in G'$. For all g, h in G,

$$x(gh - hg) = x(ghg^{-1}h^{-1} - 1)hg = 0.$$

□

Lemma 2.5.3 *Let G be a unipotent-by-abelian subgroup of $GL(n, R)$. There exists a positive integer r such that $V_r(G) = R^n$. For all $0 \leq i \leq r - 1$, $V_i(G) < V_{i+1}(G)$, $V_i(G)$ has a complement in R^n, and the image of G under the map to $GL(V_{i+1}(G)/V_i(G))$ is abelian.*

Proof. Assume that $V_i(G) \neq R^n$. Let $\overline{G}$ be the image of the map taking G to $\mathrm{GL}(R^n/V_i(G))$. Then $\overline{G}$ is unipotent-by-abelian since $\overline{G'} = \overline{G}'$ is unipotent. Since $V(\overline{G}) \neq 0$, $V_i(G) < V_{i+1}(G)$. Therefore, there exists a positive integer r such that $V_r(G) = R^n$. The quotient $R^n/V_{i+1}(G)$ is isomorphic to $(R^n/V_i(G))/V(\overline{G})$, and this latter quotient is free since $V(\overline{G})$ has a complement in $R^n/V_i(G)$. Therefore $V_{i+1}(G)$

has a complement in R^n. It follows from the definition of $V_{i+1}(G)$ that the image of G under the map to $\mathrm{GL}(V_{i+1}(G)/V_i(G))$ is abelian. □

Our structure theorem for unipotent-by-abelian matrix groups now follows immediately.

Proposition 2.5.4 *Let G be a unipotent-by-abelian subgroup of $GL(n, R)$. There exist a basis B for R^n and positive integers $n_1, \ldots, n_r$ such that $n_1 + \cdots + n_r = n$ and all matrices in G have the following block structure with respect to B:*

$$g = \begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix},$$

where for $1 \leq i \leq r$, a_i is an $n_i \times n_i$ matrix, and the image of G under the map that takes g to a_i is abelian.

Note that when $R = \mathbf{Z}$, we find a basis for $\mathbf{Z}^n$ relative to which G has the desired form.

The following corollary is an immediate consequence.

Corollary 2.5.5 *Let G be a subgroup of $GL(n, R)$. Then G is triangularizable if and only if G is unipotent-by-abelian.*

Let A be the enveloping algebra of G, where G is a triangularizable subgroup of $\mathrm{GL}(n, R)$. Just as in the case of abelian matrix groups (Section 2.4), the problem of computing a basis for R^n satisfying the criteria of Proposition 2.5.4 is closely related to the problem of expressing the radical $J(A)$ as the intersection of maximal ideals. Let π_i be the map that takes g to a_i. As we saw in Section 2.4, we may assume that for each i, the enveloping algebra of $\pi_i(G)$ is a field. In this case, the kernel M_i of the algebra homomorphism extending π_i is a maximal ideal, and

$$J(A) = \bigcap_{i=1}^{r} M_i.$$

Further research into practical algorithms for finding primary decompositions will shed light on how best to compute a desired basis for R^n. One possibility is to use an algorithm based on Lemma 2.5.3 both to decide whether or not a subgroup G of $\mathrm{GL}(n, R)$ (given by a finite set of generators) is triangularizable, and, if so, to find a desired basis for R^n. We can do so as follows. Find a basis $\{b_1, \ldots, b_d\}$ for A as a vector space over $\mathbf{Q}$. (If $R = \mathbf{Z}$, then choose the b_i's in $\mathrm{GL}(n, \mathbf{Z})$.) Then $V(G) = \bigcap_{i,j} W_{i,j}$, where $W_{i,j} = \{v \in R^n \mid v(b_i b_j - b_j b_i) = 0\}$. If $V(G) = 0$, then G is not triangularizable. Otherwise, find a complement W to $V(G)$ in R^n. Now proceed inductively to decide whether or not $\overline{G}$, the image of the map taking G to $\mathrm{GL}(R^n/V(G))$, is triangularizable, and, if so, to find a basis $v_1, \ldots, v_j$ for W such that $\overline{G}$ has the desired form with respect to $v_1 + V(G), \ldots, v_j + V(G)$.

2.5.2 Testing membership

Let G be a triangularizable, polycyclic subgroup of $\mathrm{GL}(n, R)$, and let $a \in \mathrm{GL}(n, R)$. We will now reduce the problem of deciding whether or not $a \in G$ to two cases considered previously, namely, when G is finitely generated and abelian, or when G is finitely generated and unitriangular. It is important that we assume that G is polycyclic, since this does not automatically hold for triangularizable subgroups of $\mathrm{GL}(n, \mathbf{Q})$. For example, let G be the subgroup of $\mathrm{GL}(2, \mathbf{Q})$ generated by

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then G' is abelian. Furthermore,

$$G' = \left\{ \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \mid r \in \mathbf{Z}[1/2] \right\}.$$

Therefore, G' is not finitely generated.

As we saw in the previous section, we may assume that we have found a basis for R^n satisfying the criteria of Proposition 2.5.4. We may also assume that a has a block structure like that of G with respect to this basis. Let ψ be the map from $\langle G, a \rangle$ to

GL(n, R) given below.

$$\begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix} \longmapsto \begin{pmatrix} a_1 & 0 & \cdot & \cdot & 0 & 0 \\ 0 & a_2 & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix}$$

As we saw in Section 2.4, we can test membership in $\psi(G)$ constructively, i.e., we can decide whether or not $\psi(a) \in \psi(G)$, and, if so, we can find $g \in G$ such that $\psi(a) = \psi(g)$. Thus we are left with the problem of deciding whether or not ag^{-1} is in the intersection H of G and the kernel of ψ.

Notice that H is precisely the unipotent part U of G. Clearly, H is a normal, unipotent subgroup of G, and hence $H \leq U$. As before, let G_i be the image of G under the map π_i that takes a matrix to the i-th block along the block diagonal, and let n_i be the size of the matrices in G_i (so that $G_i \leq \mathrm{GL}(n_i, R)$). Suppose g is an element of U. Let $a_i = \pi_i(g)$. Since g is unipotent, $(a_i - 1)^{n_i} = 0$. But A_i, the enveloping algebra of G_i, is a field, and hence $a_i - 1 = 0$. Therefore, $g \in H$.

Find a finite set of generators for H as follows. Recall from Section 2.4 that we can find a presentation for $\psi(G)$ in terms of our given generators, i.e., we can find generators $k_1, \ldots, k_s$ for the subgroup K of vectors v in $\mathbf{Z}^k$ such that $\psi(g^v) = 1$. Let X be a finite set of normal generators for G', and let $\widetilde{H} = \langle g^{k_1}, \ldots, g^{k_s}, X\rangle$. Then H is the normal closure of $\widetilde{H}$ in G. By conjugating elements in $\widetilde{H}$ by $g_1, \ldots, g_k$, keep building up $\widetilde{H}$ until $\widetilde{H}$ is normal in G, in which case $\widetilde{H} = H$. (Since H satisfies the ascending chain condition on subgroups, we do not need to conjugate by $g_1^{-1}, \ldots, g_k^{-1}$.) This process is guaranteed to terminate since G is assumed to be polycyclic. Now we have generators for H, so we can use the methods of Section 2.3 to decide whether or not $ag^{-1} \in H$.

2.6 Polycyclic-by-finite groups

In this section we describe algorithms for working with polycyclic-by-finite subgroups of $\mathrm{GL}(n, R)$. We rely on the theorem of Dixon concerning the principal p-congruence subgroups of $\mathrm{GL}(n, \mathbf{Z})$ described in Section 1.4. In Section 2.6.3 we describe two algorithms for testing membership in a polycyclic-by-finite matrix group, one of which relies on the structure theorem described in the next section.

2.6.1 A structure theorem

Let G be a polycyclic-by-finite subgroup of $\mathrm{GL}(n, R)$. In this section we prove the following proposition concerning the structure of G.

Proposition 2.6.1 *Let G be a polycyclic-by-finite subgroup of $GL(n, R)$. There exist a basis B for R^n and positive integers $n_1, \ldots, n_r$ such that $n_1 + \cdots + n_r = n$ and all matrices in G have the following block structure with respect to B*

$$g = \begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix},$$

where for $1 \le i \le r$, a_i is an $n_i \times n_i$ matrix and the image of G under the map that takes g to a_i is abelian-by-finite.

Proof. There exists a subgroup $H \lhd G$ such that $|G : H| < \infty$ and H is triangularizable. (See Theorem 3, Chapter 2 of [Se2] as well as Lemma 1.4.1 of this thesis.) Let $V_0(H), \ldots, V_r(H)$ be defined as in Section 2.5.1. By Lemma 2.5.3, it suffices to show that each $V_i(H)$ is invariant under G. Since $V_i(H)$ is invariant under H, and $H \lhd G$, it follows easily that for all $g \in G$, $V_i(H)g$ is invariant under H.

Next we show that for all i, H is abelian on $V_i(H)g/V_{i-1}(H)g$. Let $x \in V_i(H)$ and $h_1, h_2 \in H$. Then there exist $h'_1, h'_2 \in H$ such that $gh_1 = h'_1 g$ and $gh_2 = h'_2 g$. Therefore

$$xgh_1h_2 - xgh_2h_1 = xh'_1gh_2 - xh'_2gh_1 = xh'_1h'_2g - xh'_2h'_1g \in V_{i-1}(H)g.$$

We now show by induction on i that $V_i(H)g = V_i(H)$. This is trivial in the case when $i = 0$. By induction we may assume that $V_{i-1}(H)g = V_{i-1}(H)$. Then H is abelian on $V_i(H)g/V_{i-1}(H)$. Therefore $V_i(H)g \leq V_i(H)$ (by our definition of $V_i(H)$), and hence $V_i(H)g = V_i(H)$. The proposition now follows. □

2.6.2 Deciding if a matrix group is polycyclic-by-finite

Let G be a subgroup of $\mathrm{GL}(n, R)$ given by a finite set $\{g_1, \ldots, g_k\}$ of generators. Let S be the subring of $\mathbf{Q}$ generated by the entries of $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$. Let p be an odd prime which does not divide the denominator of any of the entries of $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$. (For example, if $G \leq \mathrm{GL}(n, \mathbf{Z})$, then let $p = 3$.) Let θ be the homomorphism $\theta : \mathrm{GL}(n, \mathbf{Z}_p) \to \mathrm{GL}(n, F_p)$ defined in Section 1.4. Let K be the intersection of G with the kernel of θ. By Lemma 1.4.1, G is solvable-by-finite if and only if K is triangularizable. Furthermore, G is polycyclic-by-finite if and only if K is both triangularizable and polycyclic since if G is polycyclic-by-finite, then every subgroup of G is finitely generated. (See Propositions 1 and 4 in Chapter 1 of [Se2].) This allows us to reduce problems concerning solvable-by-finite groups to corresponding problems concerning triangularizable groups. We will now elaborate on how this reduction can be achieved.

First we must obtain a description of K. One way to do so (as in [Di1]) is to get a set T of coset representatives for G/K and to then use the Schreier construction to get a set of $1 + |T|(k-1)$ generators for K. (See Proposition 3.4 in Chapter 4 of [Si].) If we have a reasonable number of generators for K, then we can decide whether or not G is solvable-by-finite since we can decide whether or not K is triangularizable. (See Section 2.5.) Likewise, if G is solvable-by-finite, then we can decide whether or not G is polycyclic-by-finite: as proved in [Be3] (as a result of [BBR] and [Be2]), it is possible to decide whether or not a triangularizable group K is polycyclic.

The Schreier construction will be impractical in many cases since even if p is small, $|T|$ might be large: for example, $|\mathrm{GL}(10, F_3)| \sim 3 \times 10^{47}$. When $|T|$ is large, we can use techniques for working with matrix groups over finite fields to obtain a presentation for G/K and thereby obtain normal generators for K. One way to achieve this is to view G/K as a permutation group on the vectors in F_p^n and to use algorithms for finding presentations of permutation groups. If G is solvable, then we can instead use special methods for finding presentations for solvable subgroups of $\mathrm{GL}(n, F_p)$. (See [Lu].)

Suppose now that K is given by normal generators, i.e., suppose we have generators for $\widetilde{K}$ such that $\widetilde{K}^G = K$. We can decide whether or not $\widetilde{K}$ is triangularizable, and if it is, then we can test membership in $\widetilde{K}$. By conjugating elements in $\widetilde{K}$ by $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$, keep building up $\widetilde{K}$, stopping when either it is not triangularizable (in which case G is not solvable-by-finite) or $\widetilde{K}$ is both triangularizable and normal in G (in which case $\widetilde{K} = K$ and G is solvable-by-finite). If we let K_i be the approximation for K obtained after i iterations, then

$$K_1 \leq K_2 \leq \cdots,$$

and $\bigcup K_i = K$. Since K is finitely generated, there exists an i such that $K_i = K$, so the algorithm is guaranteed to terminate.

2.6.3 Testing membership

We now discuss the problem of deciding whether or not a given matrix a in $\mathrm{GL}(n, \mathbf{Q})$ is an element of G, where G is a polycyclic-by-finite matrix group given by a finite set $\{g_1, \ldots, g_k\}$ of generators. We describe two algorithms for this problem. (We have not yet compared the efficiency of these algorithms.)

We carry over our notation from Section 2.6.2: S is the subring of $\mathbf{Q}$ generated by the entries of $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$; p is an odd prime which does not divide the denominator of any of the entries of $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$; θ is the map from $\mathrm{GL}(n, \mathbf{Z}_p)$ to $\mathrm{GL}(n, F_p)$ defined in Section 1.4; K is the intersection of G with the kernel of θ; T is a set of coset representatives for G/K. We may assume that the entries of a are in S, and as we saw in the Section 2.6.2, we may assume that we have generators for K.

The first algorithm for deciding whether or not $a \in G$ relies on the algorithm in Section 2.5.2 for testing membership in a triangularizable matrix group. If $|G/K|$ is small, then find a set T of coset representatives for G/K and simply try each $t \in T$, testing whether or not $at^{-1} \in K$. If $|G/K|$ is large, then use techniques for matrices over finite fields to decide whether or not $\theta(a) \in \theta(G)$ and, if so, to find g in G such that $\theta(a) = \theta(g)$. Then $a \in G$ if and only if $ag^{-1} \in K$. This approach might be particularly efficient in the case when G is polycyclic, since then we can use algorithms developed for working with solvable matrix groups over finite fields. (See [Lu].)

The second algorithm for deciding whether or not $a \in G$ relies on the algorithms in [Be1] for working with abelian-by-finite matrix groups as well as the algorithm in Section 2.3 for testing membership in a unitriangular matrix group. Recall that $K \triangleleft G$, $|G : K| < \infty$, and K is triangularizable. Find a basis for R^n relative to which K has the block structure described in Proposition 2.5.4. With respect to this basis for R^n, G has the block structure described in Proposition 2.6.1. (This follows from the proof of Proposition 2.6.1.) Assume that a has the same block structure with respect to this basis. Let ψ be the map from $\langle G, a\rangle$ to $\mathrm{GL}(n, R)$ given below.

$$\begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix} \longmapsto \begin{pmatrix} a_1 & 0 & \cdot & \cdot & 0 & 0 \\ 0 & a_2 & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix}$$

We can obtain generators for the intersection H of G with the kernel of ψ much as we found the unipotent part of a triangularizable matrix group in Section 2.5.2. Use the algorithm in [Be1] to find a presentation for $\psi(G)$, and from that obtain a set $\{h_1, \ldots, h_l\}$ of normal generators for H. Let $\widetilde{H} = \langle h_1, \ldots, h_l\rangle$. Then H is the normal closure of $\widetilde{H}$ in G. By conjugating elements in $\widetilde{H}$ by $g_1, \ldots, g_k$, keep building up $\widetilde{H}$ until $\widetilde{H}$ is normal in G, in which case $\widetilde{H} = H$. (Since H satisfies the ascending chain condition on subgroups, we do not need to conjugate by $g_1^{-1}, \ldots, g_k^{-1}$.) This process is guaranteed to terminate since G is assumed to be polycyclic-by-finite. Use the algorithm in [Be1] to decide whether or not $\psi(a) \in \psi(G)$, and, if so, to find a $g \in G$ such that $\phi(a) = \psi(g)$. Then $a \in G$ if and only if $ag^{-1} \in H$.

2.7 Comparisons with other algorithms

Algorithms are given in [BCRS] for all of the problems discussed in this chapter in the key case when $R = \mathbf{Z}$. We will not describe those algorithms completely here; rather, we will simply highlight several particularly inefficient steps in the algorithms to illustrate their impracticality.

Suppose that G is a polycyclic-by-finite matrix group. In [BCRS] an algorithm is given to decide whether or not a given matrix a is an element of G. If m is a positive integer, let θ_m be the map from $\mathrm{GL}(n, \mathbf{Z})$ to $\mathrm{GL}(n, \mathbf{Z}/m\mathbf{Z})$. If a is not an element of G, then there exists an m such that $\theta_m(a)$ is not an element of $\theta_m(G)$ (Theorem 5 in Chapter 5 of [Se2]). In [BCRS], the authors verify that a is not an element of G by simply trying all positive integers m, testing whether or not $\theta_m(a)$ is an element of $\theta_m(G)$, and stopping if it is not. They verify that a is an element of G by enumerating the elements of G, stopping if a is found. These two procedures are then run in parallel. Eventually one of them stops, and then it is known whether or not $a \in G$. The algorithm in [BCRS] to decide whether or not a given matrix group is polycyclic-by-finite relies on this algorithm for testing membership in such a group.

In [BCRS] an algorithm is given to verify that G is triangularizable. This algorithm enumerates the algebraic number fields F and enumerates for each F the $n \times n$ non-singular matrices p over F, testing whether or not $p^{-1}Gp$ is upper-triangular, stopping if this is the case. If G is polycyclic, a triangularizable subgroup H of finite index in G is found by enumerating all the normal subgroups H of G, testing each H to see if it is triangularizable and stopping when such an H is found. The unipotent part of G is then found by triangulating the matrices in H over F. Note that one might have to consider number fields F whose degree over $\mathbf{Q}$ is as much as $n!$. It is clear that the algorithms in [BCRS] are not practical, even for simple examples.

Algorithms for testing membership in an abelian subgroup of $\mathrm{GL}(n, R)$, as well as algorithms to find a presentation for such a group, were discovered independently by the author and [BBCIL]. The algorithm in [BBCIL] is proved to have a run-time which is polynomial in the length of the input. While that algorithm is in some respects similar to the one presented here, the method for testing membership in a matrix group which is both unipotent and abelian is quite different since the algorithm described in this thesis works for all finitely generated unipotent groups.

In [Be1] Beals describes an algorithm for deciding whether or not a given finitely generated subgroup of $\mathrm{GL}(n, R)$ is solvable-by-finite. He proves that the run-time of his algorithm is polynomial in the length of input. His algorithm appears to be suitable for computer implementation. We described in Section 2.6.2 an alternative to Beals' algorithm. We make no claims regarding the asymptotic run-time of our algorithm, but our algorithm does also appear to be suitable for computer implementation.

As we saw in Section 2.6, our algorithms for solvable-by-finite matrix groups rely on Dixon's observation in [Di1] that solvable-by-finite subgroups of the p-congruence subgroup of $\mathrm{GL}(n, \mathbf{Z}_p)$ are triangularizable for p an odd prime. We also saw that it is an easy consequence of this result that problems concerning solvable-by-finite matrix groups can be reduced to problems about triangularizable matrix groups. Dixon illustrates this himself by using such a reduction to solve the stabilizer and orbit problems for a nilpotent-by-finite matrix group G: given u in R^n, find the stabilizer of u in G, and given u, v in R^n, decide whether or not u and v are in the same orbit under the action of G. We also rely on an algorithm of Beals ([Be3]) for deciding whether or not a given finitely generated triangularizable group is polycyclic.

In [Be1] Beals extends the work in [BBCIL] to the case when G is abelian-by-finite. In this thesis, we described two algorithms for testing membership in a polycyclic-by-finite subgroup of $\mathrm{GL}(n, R)$, one of which relies on these abelian-by-finite results and the other of which does not. Experimentation is needed to compare the efficiency of all of these algorithms in practice.

2.8 Experiments

In this section I describe two experiments in which I traced through the algorithm to test membership in a triangularizable subgroup of $\mathrm{GL}(n, \mathbf{Z})$. Some parts of the algorithm were implemented in Maple, but most were not implemented. Therefore, I stepped through the algorithm by hand using Maple as a tool and using heuristics when the capabilities of Maple were insufficient. These preliminary experiments suggest that this algorithm is practical, but they raise as many questions as they answer. These questions will be discussed at the end of this section.

The first experiment will now be described in some detail. I constructed a triangularizable matrix group $H < \mathrm{GL}(6, \mathbf{Z})$ as follows. For $i = 1, 2, 3$, I started with the companion matrix h_i to an irreducible quadratic polynomial and then chose three nonzero matrices $h_{i,1}, h_{i,2}$ and $h_{i,3}$ in the enveloping algebra of $\langle h_i \rangle$. Thus, $\langle h_{i,1}, h_{i,2}, h_{i,3} \rangle$ was an abelian subgroup of $\mathrm{GL}(2, \mathbf{Z})$ for which the enveloping algebra was a field. I then constructed block upper triangular matrices $f_1, f_2, f_3 \in \mathrm{GL}(6, \mathbf{Z})$ by letting the block diagonal of f_i consist of the matrices $h_{1,i}, h_{2,i}$, and $h_{3,i}$ and by choosing random entries off the block diagonal. I obtained a change of basis matrix p by performing 20 random elementary row operations to the identity matrix. Let $m_i = p^{-1} f_i p$, and let $H = \langle m_1, m_2, m_3 \rangle$. The entries of m_1, m_2 and m_3 had up to six digits.

$$m_1 = \begin{pmatrix} 23613 & 9785 & -2290 & 5575 & 112261 & -3078 \\ -683 & -301 & 81 & 234 & -3640 & 100 \\ -2194 & -996 & 274 & 1007 & -11946 & 330 \\ -4682 & -1931 & 451 & -1136 & -22229 & 609 \\ -4757 & -1964 & 460 & -1106 & -22633 & 620 \\ -1376 & -279 & 80 & 369 & -7241 & 176 \end{pmatrix}$$

$$m_2 = \begin{pmatrix} -1497 & -1055 & 100 & -5945 & -1535 & 212 \\ 4838 & 1574 & -369 & 900 & 23254 & -625 \\ 19316 & 6287 & -1475 & 3554 & 92882 & -2495 \\ -222 & 37 & 21 & 1097 & -2204 & 25 \\ 312 & 210 & -20 & 1180 & 379 & -44 \\ 496 & -44 & 0 & -396 & 2876 & -63 \end{pmatrix}$$

$$m_3 = \begin{pmatrix} -22979 & -6901 & 1690 & -1219 & -113497 & 3005 \\ -9257 & -3338 & 819 & -567 & -45637 & 1192 \\ -37541 & -13512 & 3314 & -2339 & -185038 & 4835 \\ 5644 & 1757 & -431 & 288 & 27887 & -736 \\ 4619 & 1388 & -340 & 242 & 22817 & -604 \\ 936 & 316 & -80 & -36 & 4708 & -121 \end{pmatrix}$$

To put H back in the block upper triangular form of Proposition 2.5.4, I followed a short cut to the algorithm described in Section 2.5.1. Instead of calculating a basis for $\mathrm{Env}(H)$ over $\mathbf{Q}$ and then considering the Lie bracket of each pair of basis elements, I considered the single Lie bracket $l = m_1m_2 - m_2m_1$. I found that the nullspace V of l was a two-dimensional subgroup of $\mathbf{Z}^6$ invariant under the action of H such that the restriction of H to V was abelian. I found a complement W to V in $\mathbf{Z}^6$ and a basis for $\mathbf{Z}^6$ consisting of a basis for W and a basis for V. I used a similar approach with the restriction of H to $\mathbf{Z}^6/V$ to find a suitable basis for W. In this way I obtained a suitable basis for $\mathbf{Z}^6$. Let g_i be the matrix for m_i with respect to this basis. The entries of g_1, g_2 and g_3 had up to 60 digits. (The growth in the sizes of entries was unexpected and merits further attention.) Let $G = \langle g_1, g_2, g_3 \rangle$. Now G was in block upper triangular form with three 2×2 abelian matrix groups G_1, G_2, G_3 along the diagonal.

Test matrices t_1, t_2, t_3 were constructed as follows. For t_1 I computed a short word in the generators:

$$t_1 = g_3 g_1^2 g_2^{-2} g_3 g_1 g_2^{-1}.$$

For t_2 I constructed a matrix for which the block diagonal was the same as that of g_1^3 but for which the entries off the block diagonal were random. For t_3 I constructed a block diagonal matrix, the first block of which was like that of g_1, the second block of which was like that of g_1^3, and the third block of which was like that of g_1^5.

I set out to test whether or not t_1, t_2 and t_3 were elements of G. Rename t_1, t_2 and t_3 as g_4, g_5 and g_6 respectively, and let $\widetilde{G} = \langle g_1, \ldots, g_6 \rangle$. Let ψ be the map from $\widetilde{G}$ to $\mathrm{GL}(6, \mathbf{Z})$ given below:

$$g = \begin{pmatrix} a_1 & * & * \\ 0 & a_2 & * \\ 0 & 0 & a_3 \end{pmatrix} \longmapsto \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix}.$$

For $i = 1, 2, 3$, let π_i be the map that takes g to a_i. Let A_i be the enveloping algebra of G_i. I found that for each i and j, $\pi_i(t_j)$ was an element of A_i. For each i I found that A_i was a field. Rather than using the techniques of [EHV] or [FR] to prove this, I proceeded as follows. I found a primitive element p_i for A_i. (For each field, our first guess for a primitive element worked.) I showed that the characteristic polynomial for p_i was irreducible.

I used our primitive elements p_1, p_2 and p_3 to determine that A_1 had two real embeddings, A_2 had two complex embeddings, and A_3 had two real embeddings into $\mathbf{C}$. Let ρ_1 be the logarithmic homomorphism from A_1^* to $\mathbf{R}^2$, and let ρ_3 be the logarithmic homomorphism from A_3^* to $\mathbf{R}^2$. (Since $O_{A_2}^*$ is finite, I could ignore the logarithmic homomorphism for A_2^*.) Rather than considering A_1, A_2 and A_3 separately, as suggested in Section 2.4, I let σ be the map from $\widetilde{G}$ to $\mathbf{R}^4$ given by

$$\sigma : g \longmapsto (\rho_1(\pi_1(g)), \rho_3(\pi_3(g))).$$

I found the length of the shortest vector in $\sigma(\widetilde{G})$ using the tables in Appendix B of [Co] listing fundamental units for fields with low discriminant. The algorithm in [BP] was then used to find a basis for K, the subgroup of $\mathbf{Z}^6$ consisting of elements x such that $\sigma(g^x) = 0$.

Using our basis for K, I found for each j that $\sigma(t_j)$ was an element of $\sigma(G)$, and I found a matrix s_j in the kernel of σ such that $t_j \in G$ if and only if $s_j \in G$. From the basis elements for K, it was easy to find a presentation for $\sigma(G)$ in terms of $\sigma(g_1)$, $\sigma(g_2)$ and $\sigma(g_3)$. From this I found a $t \in G$ such that the kernel of σ was generated by t and G'. Hence the torsion subgroup T of $\psi(G)$ was given by $T = \langle\psi(t)\rangle$. The order of $\psi(t)$ was four, and hence the intersection I of the kernel of ψ and G was given by $I = \langle t^4, G'\rangle$. I found that $r_1 = s_1t^3$ and $r_2 = s_2$ were in the kernel of ψ, and that for $q = 0, 1, 2, 3$, s_3t^q was not in the kernel of ψ. This established that t_3 was not an element of G. At no time during these computations did I notice a significant delay while Maple performed the desired computations. I was left with the task of deciding whether or not r_1 and r_2 were in I.

I implemented in Maple a function NORMAL_CLOSURE to compute the normal closure of a subgroup of $\mathrm{Tr}_1(6, \mathbf{Z})$ (given by a finite set of generators) in a subgroup G of $\mathrm{GL}(6, \mathbf{Z})$ (also given by a finite set of generators). Subroutines included versions of POLY_SUBGROUP and POLY_MEMBER (from Section 9.6 of [Si]). Our algorithms were slightly different from those in [Si] because I was able to exploit the structure of $\mathrm{Tr}_1(6, \mathbf{Z})$ as a finitely generated nilpotent group.

I used NORMAL_CLOSURE to compute a polycyclic generating sequence for G'. This was the only point at which I found that time and space requirements became problematic. At times during the computation, I was raising group elements to powers consisting of 500 digits. For reasons that I still don't understand, memory became tight, and this problem was alleviated by saving intermediate results and then restarting. After approximately 50 minutes of CPU time, I did succeed in finding a polycyclic generating sequence for G'. Finally, I used our version of POLY_MEMBER and concluded that $r_1 \in I$ and that $r_3 \notin I$, and hence that $t_1 \in G$ and $t_3 \notin G$.

In the second example, $G < \mathrm{GL}(6, \mathbf{Z})$ was generated by two matrices, m_1 and m_2, and I was testing membership of a third matrix t in G. The original matrices had entries with up to nine digits.

$$m_1 = \begin{pmatrix} -1734 & -2649 & -691 & 2094 & 4948 & -5145 \\ 552 & 862 & 218 & -681 & -1597 & 1656 \\ 2193 & 3355 & 873 & -2653 & -6269 & 6518 \\ 153 & 245 & 62 & -192 & -438 & 449 \\ 1158 & 1758 & 462 & -1391 & -3296 & 3431 \\ 1174 & 1789 & 468 & -1416 & -3350 & 3485 \end{pmatrix}$$

$$m_2 = \begin{pmatrix} -990 & -95 & -903 & 730 & -805 & 964 \\ 303 & 56 & 282 & -243 & 271 & -340 \\ 1275 & 104 & 1162 & -913 & 1031 & -1229 \\ 79 & 33 & 83 & -64 & 97 & -141 \\ 661 & 52 & 594 & -490 & 517 & -601 \\ 664 & 60 & 599 & -502 & 524 & -615 \end{pmatrix}$$

The matrix t (obtained as a short word in the given generators) is given below:

$$\begin{pmatrix} 138788803 & -106263680 & 127387571 & 89189564 & 82651357 & -75800544 \\ -45285979 & 34788524 & -41508293 & -29058598 & -26764909 & 24364183 \\ -175901475 & 134670117 & -161455942 & -113042552 & -104768361 & 96098357 \\ -12601810 & 9830602 & -11475766 & -8029697 & -7182962 & 6299878 \\ -92106657 & 70389711 & -84606027 & -59239958 & -55084112 & 50726571 \\ -93732987 & 71659457 & -86086510 & -60275836 & -56009248 & 51536230 \end{pmatrix}$$

I used the same technique as in the first experiment to prove that G was triangularizable and to put G in the desired block upper triangular form. This time, the growth in the sizes of entries was not too bad: the largest entry had twelve digits. Unlike the first experiment, it was relatively easy to compute a polycyclic generating sequence for G': the largest exponent encountered had approximately 200 digits, and the computation took less than seven minutes.

An implementation and further experimentation are needed to determine the kinds of input for which this algorithm, as well as the other algorithms in this thesis, will terminate in a reasonable amount of time. Ideally, an implementation platform would include some primitives for working with finitely generated abelian groups, number fields and matrix groups over finite fields. Our preliminary experiments suggest two interesting questions to investigate.

1. Why did sizes of the matrix entries grow so much (sometimes) when putting the group into the desired block upper triangular form?

2. Why was it relatively difficult to compute a polycyclic generating sequence for G'? Why did I end up raising group elements to such high powers?

Recall from Section 2.5.1 that the problem of putting G into the desired block upper triangular form is closely related to that of finding the primary decomposition of a matrix algebra. There are polynomial-time algorithms for solving this latter problem. (See [FR].) Likewise, there are polynomial-time algorithms for working with nilpotent matrix groups like $\mathrm{Tr}_1(n, \mathbf{Z})$. (See [Be1].) As discussed in Section 9.5 of [Si], POLY_SUBGROUP can be viewed as a generalization of an algorithm to compute the Hermite normal form h of an integer matrix m. The powers to which we raise group elements in POLY_SUBGROUP correspond to the entries in a matrix p such that $pm = h$. When performing Hermite normal form calculations, it is not unusual to encounter alarmingly large entries in the matrix p. In [Ha] Havas describes very successful techniques for avoiding this problem. These techniques are based on the work in [HM] and [HMM]. It would be interesting to investigate whether his techniques can be adapted to our context.

Chapter 3

Finding Matrix Representations

3.1 Introduction

One approach to working with a polycyclic-by-finite group G given by a finite presentation is to obtain a faithful representation of G as a subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n and then to work with the representation instead. (One reason that such an approach might be fruitful is that, as we saw in the previous chapter, in this latter context we can often exploit the fact that the group is embedded in a finite-dimensional matrix algebra.) In this chapter we describe an algorithm which, when given a finite presentation for a polycyclic group G, constructs an embedding of G into $\mathrm{GL}(n, \mathbf{Z})$ in the special case when the commutator G' of G is torsion-free nilpotent.

In Chapter 5 of [Se2], Segal proves the existence of an embedding of an abstract polycyclic group G into $\mathrm{GL}(n, \mathbf{Z})$ for some n. In order to develop a practical algorithm for constructing that embedding, we would need a practical algorithm for finding the Fitting subgroup of a polycyclic group given by a finite presentation. While algorithms for this problem are known to exist, a practical algorithm has yet to be found. (See Section 3.7.) The algorithm we describe here is somewhat different from that in [Se2]: for example, it does not compute the Fitting subgroup. Preliminary experiments (reported in Section 3.8) suggest that our algorithm is practical for some interesting presentations. Further experiments are needed to determine the kinds of input for which the algorithm will terminate in a reasonable amount of time.

Every polycyclic-by-finite G contains a normal subgroup H of finite index in G such that H' is torsion-free nilpotent. (This is a consequence of the linearity of G and Theorem 3, Chapter 2 of [Se2].) Therefore, it is reasonable to expect that it will be possible to extend the algorithm presented in this chapter to the case when the group is polycyclic-by-finite. Indeed, if it were possible to find such a subgroup H (practically), then we could use our algorithm to construct an embedding of H into $\mathrm{GL}(m, \mathbf{Z})$ for some m and then use the algorithm suggested by Lemma 3.5.3 to construct an embedding of G into $\mathrm{GL}(md, \mathbf{Z})$, where $d = |G : H|$. This problem merits further investigation.

3.2 Existence of an embedding into $\mathbf{Tr}_1(n, \mathbf{Z})$

In Chapter 5 of [Se2], Segal proves the existence of an embedding of a finitely generated torsion-free nilpotent group into a unitriangular matrix group. In Section 3.3 we describe an algorithm for constructing this embedding. In this section we summarize the results from [Se2] to which we will need to refer when describing our construction.

Proposition 3.2.1 *Let $G = X \ltimes H$ be a semi-direct product. Then the action of H on $\mathbf{Z}[H]$ by right multiplication and the action of X on $\mathbf{Z}[H]$ by conjugation extend simultaneously to give an action of G on $\mathbf{Z}[H]$. Thus, there is a homomorphism*

$$^* : G \to Aut_{\mathbf{Z}}(\mathbf{Z}[H])$$

such that for h in H, x in X and $a = \sum_{c \in H} a_c c$ in $\mathbf{Z}[H]$,

$$a^{h^*} = ah, \text{ and } a^{x^*} = a^x = \sum_{c \in H} a_c c^x.$$

Now let H be a finitely generated torsion-free nilpotent group of class c. Segal defines the ideal $\mathcal{I}(H)$ of $\mathbf{Z}[H]$ as follows. Let $\mathcal{H}$ be the augmentation ideal of $\mathbf{Z}[H]$. Segal proves that $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ is finitely generated as an abelian group. Let T be the torsion subgroup of $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ (considered as an abelian group under addition). Then $\mathcal{I}(H)$ is defined to be the pullback of T under the quotient map that takes $\mathbf{Z}[H]$ to $\mathbf{Z}[H]/\mathcal{H}^{c+1}$. Segal proves the following theorem, thereby establishing the existence of a representation of $X \ltimes H$ in which H is represented by a unitriangular matrix group.

Theorem 3.2.2 *Let H be a finitely generated torsion-free nilpotent group. Then $\mathbf{Z}[H]/\mathcal{I}(H)$ is a finitely generated free abelian group. Let $X = Aut(H)$ and define the map*

$$^* : X \ltimes H \to Aut_{\mathbf{Z}}(\mathbf{Z}[H])$$

as in Proposition 3.2.1. Then $\mathcal{I}(H)$ is invariant under $(X \ltimes H)^*$, and $X \ltimes H$ acts faithfully via * on $\mathbf{Z}[H]/\mathcal{I}(H)$. Furthermore, there exists a basis for $\mathbf{Z}[H]/\mathcal{I}(H)$ relative to which H is represented by unitriangular matrices.

Recall that for all n, $\mathrm{Tr}_1(n, \mathbf{Z})$ is finitely generated torsion-free nilpotent. Therefore, it follows from Theorem 3.2.2 that an abstract group H can be embedded in $\mathrm{Tr}_1(n, \mathbf{Z})$ for some n if and only if H is finitely generated torsion-free nilpotent.

By examining Segal's proof of Theorem 3.2.2, we see that he could easily have given an explicit bound on the size of the representation.

Proposition 3.2.3 *Let H be a finitely generated torsion-free nilpotent group of class $c+1$. Then the rank of $\mathbf{Z}[H]/\mathcal{I}(H)$ as a free abelian group is less than or equal to $1 + k + \cdots + k^c$, where k is the number of generators for H/H'.*

Proof. In Lemma 2 of Chapter 5, Segal proves that $\mathcal{H}/\mathcal{H}^2$ is isomorphic to H/H' (as an abelian group). In the proof of Lemma 3, he notes that there is a a $\mathbf{Z}$-module epimorphism

$$\pi_i : \mathcal{H}^{i-1}/\mathcal{H}^i \otimes \mathcal{H}/\mathcal{H}^2 \to \mathcal{H}^i/\mathcal{H}^{i+1}$$

given by

$$(x + \mathcal{H}^i) \otimes (y + \mathcal{H}^2) \to xy + \mathcal{H}^{i+1}.$$

Therefore, if we have a generating set for $\mathcal{H}^{i-1}/\mathcal{H}^i$ consisting l elements, then we can find a generating set for $\mathcal{H}^i/\mathcal{H}^{i+1}$ consisting of lk elements. By induction it follows that there is a generating set for $\mathcal{H}^i/\mathcal{H}^{i+1}$ consisting of k^i elements. Since $\mathbf{Z}[H]/\mathcal{H}$ is a cyclic group, there is a generating set for $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ consisting of $1 + k + \cdots + k^c$ elements. □

3.3 Constructing an embedding into $\mathrm{Tr}_1(n, \mathbf{Z})$

Suppose we are given a consistent polycyclic presentation for H and that H is torsion-free nilpotent. Continue the notation from Section 3.2 in which $\mathcal{H}$ denotes the augmentation ideal of $\mathbf{Z}[H]$ and $\mathcal{I}(H)$ is defined as for Theorem 3.2.2. We can use the algorithms of Lo as described in Section 1.3 to construct the embedding described in

Theorem 3.2.2, provided that we can find a finite set of elements of the group ring that generate $\mathcal{I}$ as a right ideal. We will now show how to find such a generating set.

Let $\{a_1, \ldots, a_k\}$ be a set of generators for H. As we saw in Section 1.3, $a_1 - 1, \ldots, a_k - 1$ generate $\mathcal{H}$ as a right ideal, and hence we can obtain a set of k^{c+1} elements of $\mathbf{Z}[H]$ that generate $\mathcal{H}^{c+1}$ as a right ideal. Use the algorithms in [Lo2] to obtain a generating set

$$\{b_1 + \mathcal{H}^{c+1}, \ldots, b_r + \mathcal{H}^{c+1}\}$$

for the torsion subgroup of $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ (considered as an abelian group). Then $b_1, \ldots, b_r$ together with the right ideal generators for $\mathcal{H}^{c+1}$ generate $\mathcal{I}$ as a right ideal.

3.4 Testing for nilpotency

In Section 3.3 we saw that a group H can be embedded in $\mathrm{Tr}_1(n, \mathbf{Z})$ for some n if and only if H is finitely generated torsion-free nilpotent. Suppose we are given a consistent polycyclic presentation for a group H. In this section we describe an algorithm for deciding whether or not H is torsion-free nilpotent.

Before describing the algorithm, we prove the following lemma. (This lemma seems to be common knowledge, but I have been unable to find a reference for it.)

Lemma 3.4.1 *Let H be a finitely generated group such that $|\gamma_i(H) : \gamma_{i+1}(H)| < \infty$ for some i. Then $|\gamma_j(H) : \gamma_{j+1}(H)| < \infty$ for all $j \geq i$.*

Proof. Let r be the exponent of $\gamma_i(H)/\gamma_{i+1}(H)$. Let $g_1, \ldots, g_m$ be elements of $\gamma_i(H)$ whose images generate $\gamma_i(H)/\gamma_{i+1}(H)$. Suppose H is generated by $\{a_1, \ldots, a_k\}$. Then the image of

$$\{[g_i, a_j] \mid 1 \leq i \leq m,\ 1 \leq j \leq k\}$$

generates $\gamma_{i+1}(H)/\gamma_{i+2}(H)$. (See Proposition 9.2.6 of [Si].) Let $h = [g, a]$ for some g in $\{g_1, \ldots, g_m\}$ and a in $\{a_1, \ldots, a_k\}$. Using a commutator identity (Proposition 9.1.6 of [Si]), we see that

$$[g^m, a]\gamma_{i+2}(H) = [g^{m-1}, a][g^{m-1}, a, g][g, a]\gamma_{i+2}(H).$$

Since $\gamma_{i+1}(H)/\gamma_{i+2}(H)$ is abelian and $[g^{m-1}, a, g] \in \gamma_{i+2}$,

$$[g^m, a]\gamma_{i+2}(H) = [g^{m-1}, a][g, a]\gamma_{i+2}(H).$$

By induction it follows that

$$[g^r, a]\gamma_{j+2}(H) = h^r\gamma_{i+2}(H).$$

Since $g^r \in \gamma_{i+1}(H)$, $h^r \in \gamma_{i+2}(H)$. Therefore, $\gamma_{i+1}(H)/\gamma_{i+2}(H)$ is a finitely generated abelian group of finite exponent, and hence is finite. □

Lemma 3.4.1 gives us an algorithm for deciding whether or not H is torsion-free nilpotent. Begin by computing generators for each of the terms in the lower central series for H. If in so doing we find that for some i,

$$1 < |\gamma_i(H) : \gamma_{i+1}(H)| < \infty, \tag{3.1}$$

then we can deduce by Lemma 3.4.1 that either H is not nilpotent or $\gamma_i(H)$ is a nontrivial finite normal subgroup. If, on the other hand,

$$|\gamma_i(H) : \gamma_{i+1}(H)| = 1, \text{ and } \gamma_i(H) \neq 1, \tag{3.2}$$

then H is not nilpotent. If, for all i, neither 3.1 nor 3.2 occurs, then each time we move down the lower central series, the Hirsch number of $\gamma_i(H)$ decreases and in a finite number of steps we discover that for some c, $\gamma_{c+1}(H) = 1$, i.e., that H is class c nilpotent. Having found the last term in the lower central series for H, we can now compute the torsion subgroup of H (using the algorithm described in Section 1.2), and thereby decide whether or not H is torsion-free.

3.5 Existence of an embedding into a solvable matrix group

In Chapter 5 of [Se2], Segal proves the existence of an embedding of an abstract polycyclic group G into $\mathrm{GL}(n, \mathbf{Z})$ for some n. In Section 3.6 we describe an algorithm for constructing a similar embedding in the case when G' is torsion-free nilpotent. In this section, we summarize the results from [Se2] to which we will need to refer when describing our construction.

For the key step in the proof, Segal makes the following inductive assumption. Throughout this chapter we will refer to this assumption as Hypothesis (†).

Hypothesis (†) :

- *H and K are normal subgroups of a polycyclic group L,*
- *$H \leq K$ and L/H is abelian, and*
- *there is an embedding μ of K into $GL(m, \mathbf{Z})$ such that $\mu(H) \subseteq Tr_1(m, \mathbf{Z})$.*

He then shows that there is an integer n and an embedding ν of L into $\mathrm{GL}(n, \mathbf{Z})$ such that $\nu(H) \leq Tr_1(n, \mathbf{Z})$. We begin by considering the most difficult and interesting case – the case in which L/K is infinite cyclic and generated by aK.

Let L act on $\mathbf{Z}[K]$ as in Proposition 3.2.1. Since $\mathbf{Z}[K]$ isn't finitely generated as an abelian group, our first goal is to find an ideal $\mathcal{I}$ of $\mathbf{Z}[K]$ such that

1. $\mathcal{I}$ is invariant under the action of a, giving us an action of L on $\mathbf{Z}[K]/\mathcal{I}$, and
2. $\mathbf{Z}[K]/\mathcal{I}$ is a finitely generated free abelian group. (Thus we get a matrix representation for L.)

We begin by finding two ideals $\mathcal{J}$ and $\overline{\mathcal{K}}$, each of which satisfies one of these two criteria, and then we show how $\mathcal{I}$ can be constructed from $\mathcal{J}$ and $\overline{\mathcal{K}}$.

Our embedding μ of K into $\mathrm{GL}(m, \mathbf{Z})$ extends to a ring homomorphism of $\mathbf{Z}[K]$ to $M(m, \mathbf{Z})$. Let $\mathcal{J}$ be the kernel of this action. The quotient $\mathbf{Z}[K]/\mathcal{J}$ is a finitely generated free abelian group, but $\mathcal{J}$ might not be invariant under the action of a.

Let $\mathcal{H}$ be the augmentation ideal of $\mathbf{Z}[H]$. Since $\mathbf{Z}[H] \subseteq \mathbf{Z}[K]$, we can let $\overline{\mathcal{H}} = \mathcal{H}\,\mathbf{Z}[K]$. Since $H \triangleleft K$, $\overline{\mathcal{H}} = \mathbf{Z}[K]\,\mathcal{H}$. Not only is $\overline{\mathcal{H}}$ is invariant under the action of a, but a acts trivially on $\mathbf{Z}[K]/\overline{\mathcal{H}}$. To see this, let k be an element of K. Then

$$k^a - k = k([k, a] - 1) \in k(L' - 1) \subseteq k(H - 1) \subseteq \overline{\mathcal{H}}.$$

(Notice that we are using the fact that L/H is abelian here.) Unfortunately, $\mathbf{Z}[K]/\overline{\mathcal{H}}$ might not be finitely generated.

Let $\mathcal{S} = (\mathcal{J} + \overline{\mathcal{H}})^m$ and let T be the torsion subgroup of $\mathbf{Z}[K]/\mathcal{S}$, considered as an abelian group. Let $\mathcal{I}$ be the pullback of T under the map $\mathbf{Z}[K] \to \mathbf{Z}[K]/\mathcal{S}$. Clearly,

$\mathcal{I}$ is an ideal of $\mathbf{Z}[K]$. Segal proves that $\mathcal{I}$ satisfies the criteria above. By carefully examining the proof of Theorem 4 in Section 5.C, we see that Segal actually proves the following lemma. For completeness we include a proof, all of the ideas of which can be found in Segal's proof of Theorem 4.

Lemma 3.5.1 *Suppose that H, K and L satisfy Hypothesis (†) and that L/K is infinite cyclic and generated by aK. Let $\mathcal{I}$ be the ideal of $\mathbf{Z}[K]$ defined above. Then $\mathcal{I}$ is invariant under the action of a and $\mathbf{Z}[K]/\mathcal{I}$ is a finitely generated free abelian group. If τ is the homomorphism*

$$\tau : L \to Aut_{\mathbf{Z}}(\mathbf{Z}[K]/\mathcal{I})$$

induced from the homomorphism * in Proposition 3.2.1, then the kernel of τ is the centralizer $C_{\langle a\rangle}(K)$. There is a basis for $\mathbf{Z}[K]/\mathcal{I}$ with respect to which $\tau(H)$ is unitriangular.

Proof. Since (as we saw above) a acts trivially on $\mathbf{Z}[K]/\overline{\mathcal{H}}$, the ideal $\mathcal{J}+\overline{\mathcal{H}}$ is invariant under a. Therefore $\mathcal{I}$ is also invariant.

Since $\mathbf{Z}[K]/\mathcal{J}$ is finitely generated as an abelian group, so is $\mathbf{Z}[K]/(\mathcal{J}+\overline{\mathcal{H}})$. By Lemma 9 in Section 5.C of [Se2], $\mathbf{Z}[K]/\mathcal{S}$ is also finitely generated as an abelian group. Therefore $\mathbf{Z}[K]/\mathcal{I}$ is finitely generated free abelian.

Before finding the kernel of τ, we show that $(1+\mathcal{I})\cap K = 1$. Since μ is injective, $(1+\mathcal{J})\cap K = 1$. Therefore, it suffices to show that $\mathcal{I} \subseteq \mathcal{J}$. Since H is embedded in $\mathrm{Tr}_1(m,\mathbf{Z})$, $\mathcal{H}^m \subseteq \mathcal{J}$. Since $\mathcal{J}$ is an ideal of $\mathbf{Z}[K]$, it follows that $(\overline{\mathcal{H}})^m \subseteq \mathcal{J}$. Therefore,

$$\mathcal{S} = (\mathcal{J}+\overline{\mathcal{H}})^m \subseteq (\overline{\mathcal{H}})^m + \mathcal{J} \subseteq \mathcal{J}.$$

Since $\mathbf{Z}[K]/\mathcal{J}$ is torsion-free, $\mathcal{I} \subseteq \mathcal{J}$. Therefore, $(1+\mathcal{I})\cap K = 1$.

We are now ready to find the kernel of τ. Clearly, $C_{\langle a\rangle}(K)$ is contained in the kernel of τ. Suppose that $k \in K$ and r is a nonnegative integer such that ka^r is in the kernel of τ. Then $1+\mathcal{I}$ is fixed by $\tau(ka^r)$, and therefore $k^{a^r} \in (1+\mathcal{I})\cap K = 1$. Thus, $k = 1$. Now for all j in K, $j+\mathcal{I}$ is fixed by a^r. Therefore, $j^{a^r} - j \in \mathcal{I}$. But

$$j^{a^r} - j = j([j,a^r]-1).$$

Hence $[j, a^r] - 1 \in \mathcal{I}$ and $[j, a^r] \in (\mathcal{I} + 1) \cap K = 1$. Therefore, a^r centralizes K and the kernel of τ is precisely $C_{\langle a \rangle}(K)$.

Let $M = \mathbf{Z}[K]/\mathcal{I}$, considered as a $\mathbf{Z}[H]$-module. Then $M\mathcal{H}^m = 0$, since

$$\mathbf{Z}[K]\mathcal{H}^m \subseteq \overline{\mathcal{H}}^m \subseteq \mathcal{S} \subseteq \mathcal{I}.$$

Let M_i be the subgroup of M generated by $\{xy + \mathcal{I} : x \in \mathbf{Z}[K], y \in \mathcal{H}^i\}$. Then H stabilizes the following chain:

$$M \geq M_1 \geq M_2 \geq \cdots \geq M_m = 0.$$

Therefore, H acts nilpotently on M, and hence (see Section 1.1) there is a basis for M with respect to which $\tau(H)$ is unitriangular. □

With this key lemma in hand, it is now relatively easy to prove the existence of a matrix representation for a polycyclic-by-finite group. Segal first states the following lemma, leaving the proof to the reader.

Lemma 3.5.2 *Let G be a polycyclic-by-finite group. There exists a normal torsion-free subgroup G_1 with finite index in G such that $G_1/\mathit{Fitt}(G_1)$ is free abelian.*

Let $G_1 \lhd G$ as above. Lemma 8 of Section 5.C of [Se2] shows that in order to find an embedding of G, it suffices to find an embedding for G_1. Since we will use Segal's Lemma 8 in a somewhat different context, we give a more complete statement of it here. The proof given here is basically that sketched in [Se2].

Lemma 3.5.3 *Let H be a subgroup of finite index d in a group G. Suppose that there exists an embedding μ of H into $GL(n, \mathbf{Z})$. Then there exists an embedding ν of G into $GL(nd, \mathbf{Z})$. If, furthermore, $K \leq H$, $K \lhd G$ and $\mu(K) \leq \mathit{Tr}_1(n, \mathbf{Z})$, then we can choose ν such that $\nu(K) \leq \mathit{Tr}_1(nd, \mathbf{Z})$.*

Proof. Let $M = \mathbf{Z}^n$, considered as a right $\mathbf{Z}[H]$-module via μ. Let $V = M \otimes \mathbf{Z}[G]$ (where $\otimes$ denotes $\otimes_{\mathbf{Z}[H]}$ and $\mathbf{Z}[G]$ is viewed as a left $\mathbf{Z}[H]$-module). Let $\{x_1, \ldots, x_d\}$ be a set of coset representatives for the right cosets of H in G. Then

$$V = M \otimes \mathbf{Z}[H]x_1 \oplus \cdots \oplus M \otimes \mathbf{Z}[H]x_d.$$

Let $b_1, \ldots, b_n$ be a basis for M over $\mathbf{Z}$. Then

$$\mathcal{B} = b_1 \otimes x_1,\ \ldots,\ b_n \otimes x_1,\ b_1 \otimes x_2,\ \ldots,\ b_n \otimes x_2,\ \ldots,\ b_1 \otimes x_d,\ \ldots,\ b_n \otimes x_d$$

is a basis for V over $\mathbf{Z}$. Fix g in G. Let $\sigma \in \Sigma_d$. Let $h_1, \ldots, h_d$ in H be given by $x_i g = h_i x_{\sigma(i)}$. Then define

$$\begin{aligned} \nu : G &\rightarrow \mathrm{Aut}_{\mathbf{Z}}(V) \\ g &\mapsto \nu(g) \end{aligned}$$

as follows:

$$(b_k \otimes x_i)\nu(g) = b_k \mu(h_i) \otimes x_{\sigma(i)}$$

for all $1 \leq k \leq n$ and $1 \leq i \leq d$. It is easy to check that ν is an embedding. Suppose $K \triangleleft G$. For all h in K, there exist $h_1, \ldots, h_d$ such that $x_i h = h_i x_i$, in which case the matrix for $\nu(h)$ with respect to the basis $\mathcal{B}$ is

$$\begin{pmatrix} \mu(h_1) & 0 & \cdot & \cdot & 0 & 0 \\ 0 & \mu(h_2) & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & \mu(h_d) \end{pmatrix}.$$

Therefore, if $\mu(K) \leq \mathrm{Tr}_1(n, \mathbf{Z})$, then $\nu(K) \leq \mathrm{Tr}_1(nd, \mathbf{Z})$. $\square$

Since $\mathrm{Fitt}(G_1)$ is finitely generated torsion-free nilpotent, it can be embedded in $\mathrm{Tr}_1(m, \mathbf{Z})$ for some m (as described above). Suppose that

$$G_1 \triangleright K \triangleright \mathrm{Fitt}(G_1)$$

where G_1/K is infinite cyclic and generated by xH. It is not hard to show that $\mathrm{Fitt}(K) = \mathrm{Fitt}(G_1)$. By induction, there exists a positive integer k and an embedding of K into $\mathrm{GL}(k, \mathbf{Z})$ mapping $\mathrm{Fitt}(G_1)$ into $\mathrm{Tr}_1(k, \mathbf{Z})$. It can be shown that $C_{\langle x \rangle}(K) = 1$. By Lemma 3.5.1, there exists positive integer n and an embedding $\tau : G_1 \rightarrow \mathrm{GL}(n, \mathbf{Z})$ such that $\tau(Fitt(G_1)) \leq \mathrm{Tr}_1(n, \mathbf{Z})$. By Lemma 3.5.3 it follows that there exists an embedding ν of G into $\mathrm{GL}(nd, \mathbf{Z})$ such that $\nu(G_1) \leq \mathrm{Tr}_1(nd, \mathbf{Z})$, where $|G : G_1| = d$.

3.6 Constructing an embedding into a triangularizable matrix group

In the previous section we sketched a proof of the existence of an embedding of a polycyclic group G into a (solvable) subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n. In this section we describe an algorithm for constructing a somewhat different embedding in the special case when G can be embedded in a triangularizable subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n. As discussed in Section 3.1, it is reasonable to expect that we will be able to extend our algorithm to the polycyclic case. In order to develop a practical algorithm for constructing the embedding of Section 3.5, we would need a practical algorithm for finding the Fitting subgroup of a polycyclic group given by a finite presentation. While algorithms for this problem are known to exist, a practical algorithm has yet to be found. (See Section 3.7.) The algorithm we describe here does not compute the Fitting subgroup.

The following proposition follows easily from well-known results.

Proposition 3.6.1 *Let G be any group. If there exists a positive integer n and an embedding $\psi : G \hookrightarrow GL(n, \mathbf{Z})$ mapping G into a triangularizable group, then G is polycyclic and G' is torsion-free nilpotent.*

Proof. If there exists a positive integer n and an embedding $\psi : G \hookrightarrow \mathrm{GL}(n, \mathbf{Z})$ mapping G into a triangularizable group, then $\psi(G)'$ is unipotent and hence (as noted in Section 1.1) there is a basis for $\mathbf{Z}^n$ with respect to which $\psi(G)'$ is unitriangular. Therefore $\psi(G)'$ is torsion-free nilpotent. Since $\psi(G)'$ is solvable, it follows that $\psi(G)$ is solvable, and Mal'cev showed that all solvable subgroups of $\mathrm{GL}(n, \mathbf{Z})$ are polycyclic. (For a proof of this see Section 2.B in [Se2].) $\square$

The converse of Proposition 3.6.1 also holds:

Proposition 3.6.2 *If G is a polycyclic group and G' is torsion-free nilpotent, then there exists a positive integer n and an embedding $\psi : G \hookrightarrow GL(n, \mathbf{Z})$ mapping G into a triangularizable group.*

Proposition 3.6.2 is proved in Section 3.6.2; the key lemma is proved in Section 3.6.1. As we develop these proofs we also describe an algorithm to construct the embedding.

Before doing so, notice that as a consequence of Propositions 3.6.1 and 3.6.2, we can decide whether or not G (given by a consistent polycyclic presentation) can be embedded in a triangularizable subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n: begin by finding generators for G' (see Section 1.2) and then use the methods in Section 3.4 to decide whether or not G' is torsion-free nilpotent. For the rest of this section, assume that G' is torsion-free nilpotent.

In Section 3.3 we showed that we can construct an embedding of G' into $\mathrm{Tr}_1(n, \mathbf{Z})$. Our plan is to refine the series $G \triangleright G'$ to a series

$$G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_l = G'$$

where for all i, H_i/H_{i+1} is either finite or infinite cyclic. We then pull our embedding of G' up to G one factor at a time (increasing the dimension of the representation as we go). When pulling the embedding up to an infinite cyclic extension, we use that fact that H_i/G' is abelian and that we have an embedding from G' into a unitriangular group.

Suppose that H, K and L satisfy Hypothesis (†). Suppose L/K is either finite, in which case we are given a set $\{x_1, \ldots, x_d\}$ of coset representatives for L/K, or L/K is infinite cyclic, in which case we are given a cyclic generator aK. We want to find a positive integer n and an embedding ν of L into $\mathrm{GL}(n, \mathbf{Z})$ such that $\nu(H) \subseteq \mathrm{Tr}_1(n, \mathbf{Z})$. In Section 3.6.1 we consider the case when L/K is infinite cyclic.

The case when L/K is finite is relatively easy. By Lemma 3.5.3 there exists an embedding ν of L into $\mathrm{GL}(md, \mathbf{Z})$ such that $\nu(H) \subseteq \mathrm{Tr}_1(md, \mathbf{Z})$. By examining the proof of Lemma 3.5.3, we see that for a given l in L, we find a matrix representing $\nu(l)$ as follows. Find σ in Σ_d and $h_1, \ldots, h_d$ in H such that $x_i l = h_i x_{\sigma(i)}$. Let $\mathcal{B}$ be the basis for $\mathbf{Z}^{nd}$ defined in the proof of Lemma 3.5.3. Then the matrix for $\nu(l)$ with respect to

$\mathcal{B}$ is ap, where a in $\mathrm{GL}(nd, \mathbf{Z})$ is given by

$$a = \begin{pmatrix} \mu(h_1) & 0 & \cdot & \cdot & 0 & 0 \\ 0 & \mu(h_2) & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & \mu(h_d) \end{pmatrix}$$

and p is obtained by taking the tensor product of the $n \times n$ identity matrix and the $d \times d$ permutation matrix associated with σ.

3.6.1 Infinite cyclic extensions

Throughout this section we will assume that H, K and L satisfy Hypothesis (†) and that L/K is infinite cyclic and generated by aK.

Lemma 3.6.3 *There exists a positive integer n and an embedding $\nu : L \to GL(n, \mathbf{Z})$ such that $\nu(H) \leq Tr_1(n, \mathbf{Z})$.*

Proof. If $C_{\langle a \rangle}(K)$ is trivial, then the homomorphism τ of Lemma 3.5.1 is an embedding. If instead $C_{\langle a \rangle}(K) = \langle a^r \rangle$ for some positive integer r, then refine the series $L \triangleright K$ as follows:

$$L \triangleright K\langle a^r \rangle \triangleright K.$$

Then $K\langle a^r \rangle$ is the direct product of $\langle a^r \rangle$ and K, and the map λ from $K\langle a^r \rangle$ to $\mathrm{GL}(m+2, \mathbf{Z})$ given by

$$\lambda : a^{ri}k \hookrightarrow \begin{pmatrix} \mu(k) & 0 \\ 0 & \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \end{pmatrix}$$

is an embedding such that $\lambda(H)$ is unitriangular. By Lemma 3.5.3, there exists an embedding ν from L to $\mathrm{GL}(n, \mathbf{Z})$ such that $\nu(H)$ is unitriangular. □

We now discuss the way in which Lemma 3.6.3 gives us an algorithm to construct our embedding of L into $\mathrm{GL}(n, \mathbf{Z})$. We begin by constructing the embedding τ of Lemma

3.5.1. Let us assume that we are given a consistent polycyclic presentation for K and an element a of L such that aK generates L/K. Assume that the embedding μ of K into $\mathrm{GL}(m, \mathbf{Z})$ is also given (by matrices representing $\mu(k)$ for each generator of K). If we can find a finite set of right ideal generators for $\mathcal{I}$, then we can use Lo's Gröbner basis algorithm (described in Section 1.3) to find $\tau(l)$ for each generator l of L.

We first show that we can find a finite set of right ideal generators for $\mathcal{J}$. Our embedding $\mu : K \to \mathrm{GL}(n, \mathbf{Z})$ can be extended to a ring homomorphism (which we also denote by μ) from $\mathbf{Z}[K]$ to the ring of $n \times n$ matrices over $\mathbf{Z}$. Suppose K is generated by $g_1, \ldots, g_s$. Since $\mu(g_1), \ldots, \mu(g_s)$ generate $\mu(\mathbf{Z}[K])$ as a ring (and since $\mu(\mathbf{Z}[K])$ is a free abelian group of rank less than or equal to m^2), we can find elements $x_1, \ldots, x_r$ of $\mathbf{Z}[K]$ whose images form a $\mathbf{Z}$-basis for $\mathbf{Z}[K]/\mathcal{J}$. Fix i such that $1 \leq i \leq s$. For $1 \leq j \leq s$, let $\alpha(i,j)$ be the integer such that $g_i - \sum_j \alpha(i,j)x_j \in \mathcal{J}$, and let $\beta(i,j)$ be the integer such that $g_i^{-1} - \sum_j \beta(i,j)x_j \in \mathcal{J}$. Next fix i, j such that $1 \leq i, j \leq s$. For $1 \leq k \leq s$, let $\gamma(i,j,k)$ be the integer such that $x_i x_j - \sum_k \gamma(i,j,k)x_k \in \mathcal{J}$. Now let

$$R = \{g_i - \sum_j \alpha(i,j)x_j,\ g_i^{-1} - \sum_j \beta(i,j)x_j,\ x_i x_j - \sum_k \gamma(i,j,k)x_k :\ 1 \leq i,j,k \leq s\}.$$

It is easy to see that R generates $\mathcal{J}$ as a right ideal.

Since $\overline{\mathcal{H}} = \mathcal{H}\,\mathbf{Z}[K]$ and (as we saw in Section 1.3) we can find generators for $\mathcal{H}$ as a right ideal of $\mathbf{Z}[H]$, it follows that we can find generators for $\overline{\mathcal{H}}$ as a right ideal of $\mathbf{Z}[K]$. Therefore, we can find a finite set Q of right ideal generators for $\mathcal{S} = (\mathcal{J} + \overline{\mathcal{H}})^m$. Then use the methods of Section 1.3 to find a finite set P of elements of $\mathbf{Z}[K]$ whose images generate the torsion subgroup of $\mathbf{Z}[K]/\mathcal{S}$. Then $Q \cup P$ generates $\mathcal{I}$ as a right ideal of $\mathbf{Z}[K]$.

Now we may assume that we have constructed the homomorphism τ of Lemma 3.5.1. We can determine the order of $\tau(a)$, whether it be finite or infinite. (This is an easy case of the algorithm in Section 2.4.) If $\tau(a)$ has infinite order, then $C_{\langle a \rangle}(K)$ is trivial and τ is actually an embedding satisfying all the desired properties.

When the order of $\tau(a)$ is a positive integer r, our construction is much simpler. Refine the series $L \triangleright K$ as in the proof of Lemma 3.6.3:

$$L \triangleright K\langle a^r \rangle \triangleright K.$$

It is easy to construct the embedding λ from $K\langle a\rangle$ to $\mathrm{GL}(m+2,\mathbf{Z})$ (defined in the proof of Lemma 3.6.3), and as we saw above, we can then construct an embedding ν from L to $\mathrm{GL}(n,\mathbf{Z})$ as needed.

We see that the size n of the embedding ν might depend on our choice of a coset representative for L/K. For example, suppose that the action of a is inner; i.e., there exists a $k \in K$ such that for all $x \in K$, $x^a = x^k$. Then ak^{-1} centralizes K. Therefore, with this choice of coset representative for L/K, we obtain a different (and probably considerably smaller) representation of L. This raises the following question: is there an algorithm to choose a coset representative for L/K that will result in a small matrix representation for L? This question warrants further thought.

3.6.2 The full algorithm

We are now ready to prove Proposition 3.6.2:

There exist subgroups $H_0, H_1, \ldots, H_r$ of G such that

$$G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_r = G',$$

where H_0/H_1 is finite and H_i/H_{i+1} is infinite cyclic for all i. By Theorem 3.2.2 there exists a positive integer m and an embedding $\mu : G' \to \mathrm{Tr}_1(m,\mathbf{Z})$. By repeated applications of Lemma 3.6.3, there exists a positive integer n' and an embedding $\nu' : H_1 \to \mathrm{GL}(n',\mathbf{Z})$ such that $\nu'(G') \leq \mathrm{Tr}_1(n',\mathbf{Z})$. By Lemma 3.5.3 it now follows that there exists a positive integer n and an embedding $\nu : G \to \mathrm{GL}(n,\mathbf{Z})$ such that $\nu(G') \leq \mathrm{Tr}_1(n,\mathbf{Z})$. $\square$

We now describe an algorithm for actually constructing the embedding posited in Proposition 3.6.2. Assume that G is a polycyclic group given by a consistent polycyclic presentation and that G' is torsion-free nilpotent of class c. Find generators for G'. (Let p be the number generators obtained for G'.) As we showed in Section 3.3, we can construct an embedding from G' into $\mathrm{Tr}_1(m,\mathbf{Z})$. Use the methods of Section 9.6 of [Si] to find a consistent polycyclic presentation for G/G'. Then find generators for subgroups $H_0, \ldots, H_r$ such that

$$G = H_0 \triangleright H_1 \triangleright \ldots \triangleright H_r = G',$$

H_0/H_1 is finite and H_i/H_{i+1} is infinite cyclic for all $1 \leq i < r$. Let d be the order of H_0/H_1. For i such that $1 \leq i < r$, use the methods of Section 3.6.1 to construct a representation for H_i from our representation for H_{i+1}. Use the methods of Lemma 3.5.3 to construct a representation for H_0 from our representation for H_1.

The size n of the resulting embedding depends on many factors, including the parameters p, c, d and r defined above. By examining the proofs of the results leading up to Proposition 3.6.2, it is not difficult to prove the existence of a primitive recursive function $B(p, c, d, r)$ such that $n < B(p, c, d, r)$. However, easily obtained bounds for n appear to grow very rapidly as a function of these parameters, and preliminary experiments suggest that such bounds vastly overestimate the actual size of the embedding obtained. (See section 3.8 for details about these experiements.) Further experimentation is needed to understand how the size of the embedding obtained for G depends on the structure of G.

3.7 Comparisons with earlier algorithms

In [GS], the authors describe an algorithm for finding an embedding of a finitely-generated torsion-free nilpotent group H into $\mathrm{Tr}_1(n, \mathbf{Z})$. Their embedding is the same as that described in Section 3.5. Recall that we found an ideal $\mathcal{I}(H)$ of $\mathbf{Z}[H]$ such that $\mathbf{Z}[H]/\mathcal{I}(H)$ is finitely generated free abelian and there is a faithful action of H on $\mathbf{Z}[H]/\mathcal{I}(H)$. We then used the Gröbner basis algorithms described in Section 1.3 to find a basis for $\mathbf{Z}[H]/\mathcal{I}(H)$ and thereby find a matrix representation for H. In [GS] the authors describe another method for finding a basis for $\mathbf{Z}[H]/\mathcal{I}(H)$. It is not clear which algorithm will be faster in practice. This question should be investigated further.

Let G be a polycyclic group given by a consistent polycyclic presentation. In Section 3.4 we described an algorithm for deciding whether or not G is torsion-free nilpotent. We are not the first to establish that this problem is decidable. In [BCRS] the authors describe an algorithm for deciding whether or not G is nilpotent as well as an algorithm for finding the maximal normal finite subgroup of T of G. As we discussed in Section 3.4, their algorithm for finding T appears to be practical for nilpotent G. Their algorithm to decide nilpotence depends on the following theorem. (See Section 1.C in [Se2].)

Theorem 3.7.1 *Let G be a polycyclic-by-finite group such that G is not nilpotent. Then there exists a finite quotient of G which is not nilpotent.*

Nilpotence can therefore be decided by a method which the authors of [BCRS] call the *local-global method.* Imagine two processes running simultaneously. The first process attempts to prove that G is nilpotent by computing the terms of the lower central series, stopping if it is discovered that $\gamma_k(G) = 1$. The second attempts to prove that G is not nilpotent by enumerating all the finite quotients $\overline{G}$ of G and stopping if it is discovered that $\overline{G}$ is not nilpotent. Eventually, one of these two processes stops, at which point it has been decided whether or not G is nilpotent. This algorithm is unlikely to be practical even for very simple examples.

In [Se1], Segal describes an algorithm for finding an embedding of a polycyclic group G (given by a finite presentation) into $\mathrm{GL}(n, \mathbf{Z})$. This embedding is based on the proof presented in Chapter 7 of [Se2] that every polycyclic-by-finite group can be embedded in $\mathrm{GL}(n, \mathbf{Z})$ for some n. The construction of this embedding is considerably more complicated than that described in Section 3.5 of this thesis.

In [Se1], no attempt was made to find a practical algorithm to construct the embedding. For example, at one point in the construction, Segal relies on an algorithm to solve the following problem, known as the *generalized conjugacy problem.*

- Let G be a polycyclic-by-finite group given by a finite presentation. Let A and B be subgroups of G (given by finite generating sets). Decide whether or not A and B are conjugate in G.

The following theorem (see Section 4.D in [Se2]) shows that the so-called local-global method can be used to decide whether or not A and B are conjugate.

Theorem 3.7.2 *Let G be a polycyclic-by-finite group and let A and B be two subgroups of G. If A and B have conjugate images in every finite quotient of G, then A and B are conjugate in G.*

In this case one process enumerates all the elements g of G, stopping if it finds that $A^g = B$, and the other process enumerates all the finite quotients $\overline{G}$ of G, stopping if it finds that $\overline{A}$ is not conjugate to $\overline{B}$. As with the algorithm to decide nilpotence, this algorithm is unlikely to be practical even for very simple examples. Moreover, the problem of finding a practical algorithm to solve the generalized conjugacy problem is generally believed to be quite difficult. It may yet be the case that there does exist a practical algorithm for finding the embedding described in [Se1], but we chose to model our embedding after that described in Section 3.5 of this thesis.

As we remarked in Section 3.6, we did not follow the construction in Section 3.5 exactly, because to do so we would have needed to find the Fitting subgroup of a polycyclic group G given by a consistent polycyclic presentation. An algorithm for finding the Fitting subgroup of a polycyclic-by-finite group given by a finite presentation is described in [BCRS]. Once again, the authors of [BCRS] were not trying to find a practical algorithm. For example, at one point in the algorithm they find a certain finite section F/T of the group, where $F \triangleleft G$ and $T \triangleleft F$. They then enumerate each of the subgroups of this section, computing for each its preimage L under the map $F \to F/T$ and then testing whether or not L is nilpotent and $L \triangleleft G$. The practicality of such a step is suspect. However, the problem of finding the Fitting subgroup appears to be more tractable than that of solving the generalized conjugacy problem and should be investigated further.

In addition to comparing the efficiency of various algorithms for finding a matrix representation for a polycyclic group, we should also compare the sizes of the matrices produced by such algorithms. The embedding described in [Se1] is canonical in the following sense. Segal defines, for a given polycyclic-by-finite group G, a positive integer n_G and an embedding β_G of G into $\mathrm{GL}(n_G, \mathbf{Z})$. Let G and H be isomorphic polycyclic groups, where $\theta : G \to H$ is an isomorphism. Then $n_G = n_H = n$, say, and there exists an inner automorphism γ of $\mathrm{GL}(n, \mathbf{Z})$ such that

$$\gamma(\beta_G(G)) = \beta_H(\theta(G)).$$

On the other hand, the sizes of the matrices produced by the algorithm described in

Table 3.1: Unitriangular Groups

Group	Size of embedding
$\mathrm{Tr}_1(2, \mathbf{Z})$	2
$\mathrm{Tr}_1(3, \mathbf{Z})$	7
$\mathrm{Tr}_1(4, \mathbf{Z})$	35
$\mathrm{Tr}_1(5, \mathbf{Z})$	132

Section 3.6 appear to vary depending on such things as the given generating set for the group. The problem of finding a relatively small matrix representation for a given polycyclic group should be investigated further.

3.8 Experiments

In this section we describe a series of experiments in which matrix representations were constructed from finite presentations using the algorithms described in this chapter. The work in this section was done jointly with Eddie Lo. We have not implemented the algorithms in this chapter. Therefore, we stepped through the algorithms by hand using as a tool Lo's implementation of the Gröbner basis method for the group ring of a polycyclic group. (See Section 1.3.) In all cases, the matrices obtained had small entries (at most two digits), and at no time did we experience unreasonable delays while the Gröbner basis calculations were performed.

In the first series of experiments, we constructed embeddings for the following torsion-free nilpotent groups. For $n = 2, 3, 4, 5$, we followed Example 4.1 in Chapter 9 of [Si] to obtain a presentation for $\mathrm{Tr}_1(n, \mathbf{Z})$. We then used the techniques in Section 3.3 to construct embeddings from these presentations. We indicate in Table 3.1 the sizes of the embeddings obtained.

Let $F(r, c)$ denote the free nilpotent group of rank r and class c. (The free nilpotent group $F(r, c)$ is defined to be $F(r)/\gamma_{c+1}(F(r))$, where $F(r)$ is the free group on r generators.) In the second series of experiments, we constructed embeddings for $F(2, 1)$, $F(2, 2)$, $F(2, 3)$ and $F(2, 4)$. We used Lo's polycyclic quotient algorithm to obtain presentations for these groups. (See [Lo2].) We then used the techniques in Section 3.3 to construct embeddings from these presentations. We indicate in Table 3.2 the sizes

Table 3.2: Free Nilpotent Groups

Group	Size of embedding
$F(2,1)$	3
$F(2,2)$	7
$F(2,3)$	15
$F(2,4)$	31

of the embeddings obtained. It is interesting to note that for these groups, the sizes of the embeddings obtained were equal to the bound calculated in Proposition 3.2.3.

In the next series of three experiments, we started with a presentation of a group L_i, an embedding μ_i for a subgroup K_i of L_i, and a subgroup H_i of K_i satisfying Hypothesis (†). In the first of these experiments,

$$L_1 = \langle a, b, c \mid bc = cb, b^a = b^2c, c^a = bc \rangle,$$

and $K_1 = H_1 = \langle b, c \rangle$. We embedded K_1 as follows:

$$b = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ and } c = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(Hence K_1 was a torsion-free abelian group of rank 2.)

In the second experiment,

$$\begin{aligned} L_2 = \langle a_1, a_2, a_3, a_4 \mid\ & a_2^{a_1} = a_3, a_3^{a_1} = a_4^{-2}a_3^3a_2^{-1}, a_4^{a_1} = a_4, \\ & a_3^{a_2} = a_4^{-1}a_3, a_4^{a_2} = a_4, a_4^{a_3} = a_4 \rangle, \end{aligned}$$

and $K_2 = H_2 = \langle a_2, a_3, a_4 \rangle$. We embedded K_2 into $\mathrm{Tr}_1(3, \mathbf{Z})$ by sending a_2, a_3, a_4 to the usual generators for $\mathrm{Tr}_1(3, \mathbf{Z})$.

In the third experiment,

$$L_3 = \langle a, b, c \mid b^a = c^3b, c^a = c^{-1}, c^b = c^{-1} \rangle.$$

We embedded $K_3 = \langle b, c \rangle$ as follows:

$$b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \text{ and } c = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Table 3.3: Infinite Cyclic Extensions

Size of K_i embedding	Size of L_i embedding
3	6
3	7
4	24

We let $H_3 = \langle c \rangle$. We then used the methods of Section 3.6.1 to construct embeddings for L_1, L_2 and L_3. (In the case of L_3 we found the size of the embedding, but we did not calculate the matrices.) We indicate in Table 3.3 the sizes of the embeddings obtained.

References

[BBCIL] L. Babai, R. Beals, J-y. Cai, G. Ivanyos, E. M. Luks, *Multiplicative equations over commuting matrices*, Manuscript (1994).

[BBR] L. Babai, R. Beals, D. Rockmore, *Deciding finiteness of matrix groups in deterministic polynomial time*, Proc. ISSAC'93, ACM Press (1993), 117–126.

[BCRS] G. Baumslag, F. B. Cannonito, D. J. Robinson, D. Segal, *The algorithmic theory of polycyclic-by-finite groups*, J. Algebra **142** (1991), 118–149.

[Be1] R. Beals, *Algorithms for matrix groups and the Tits alternative*, Proc. 36th IEEE FOCS (1995), 593-602.

[Be2] R. Beals, *Testing integrality of matrix groups*, manuscript.

[Be3] R. Beals, personal communication.

[BP] J. Buchmann, M. Pohst, *Computing a lattice basis from a system of generating vectors*, EUROCAL '87, Lecture Notes in Comput. Sci. 378, Springer (1989), 54–63.

[Co] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag (1995).

[Di1] J. D. Dixon, *The orbit-stabilizer problem for linear groups*, Can. J. Math. **37** (1985), 238–259.

[Di2] J. D. Dixon, *The Structure of Linear Groups*, Van Nostrand Reinhold (1971).

[Do] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.

[EHV] D. Eisenbud, C. Huneke, W. Vasconcelos, *Direct methods for primary decomposition*, Invent. Math. **110** (1992), 207–235.

[Fo] E. Formanek, *Conjugate separability of polycyclic groups*, J. Algebra **42** (1976), 1–10.

[FR] K. Friedl, L. Rónyai, *Polynomial time solutions of some problems in abstract algebra*, Proc. 17th ACM STOC (1985), 153–162.

[Ge] G. Ge, *Algorithms related to multiplicative representations of algebraic numbers*, Ph. D. Thesis, Math Dept., U. C. Berkeley (1993).

[GS] F. Grunewald, D. Segal, *Some general algorithms II: nilpotent groups*, Ann. of Math. **112** (1980), 585–617.

[Ha] G. Havas, personal communication.

[HM] G. Havas, B. S. Majewski, *Hermite normal form computation for integer matrices*, Congressus Numerantium **105** (1994), 87–96.

[HMM] G. Havas, B. S. Majewski, K. R. Matthews, *Extended gcd algorithms*, Technical Report **302**, The University of Queensland (1995).

[Lo1] E. H. Lo, *Finding intersection and normalizer in finitely generated nilpotent groups*, preprint.

[Lo2] E. H. Lo, *Polycyclic quotient algorithm*, Proc. DIMACS Workshop on Groups and Computation (1995), (to appear).

[Lu] E. M. Luks, *Computing in solvable matrix groups*, Proc. 33rd IEEE FOCS (1992), 111–120.

[Ro] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag (1982).

[Se1] D. Segal, *Decidable Properties of Polycyclic Groups*, Proc. London Math. Soc. (3) **61** (1990), 497–528.

[Se2] D. Segal, *Polycyclic Groups*, Cambridge University Press (1983).

[Si] C. C. Sims, *Computation with Finitely Presented Groups*, Cambridge University Press (1994).

[We] B. A. F. Wehrfritz, *Infinite Linear Groups*, Springer-Verlag (1973).

Vita

Gretchen Ostheimer

1975-79	Attended Wellesley College, Wellesley, Massachusetts. Majored in Mathematics.
1979	B.A., Wellesley College.
1979-80	Programmer, Intermetrics, Cambridge, Massachusetts.
1980-81	Attended Cambridge University, Cambridge, England. Studied Mathematics.
1980-81	Rotary Foundation Graduate Fellow, Rotary Club of America.
1981-85	Project leader, Applied Research of Cambridge, Cambridge, England.
1985-86	Graduate student in Biomechanics, University of Toronto, Toronto, Canada.
1986-89	Senior software engineer, Software Options, Cambridge, Massachusetts.
1987-88	Graduate student in Mathematics and Computer Science, Harvard University, Cambridge, Massachusetts.
1989-96	Graduate student in Mathematics, Rutgers University, New Brunswick, New Jersey.
1989-96	Grant recipient, Graduate Research Program for Women, AT&T Bell Labs, Murray Hill, New Jersey.
1989-92	National Needs Fellow, Mathematics, Rutgers University.
1992-95	Teaching assistant, Mathematics, Rutgers University.
1993	DIMACS Fellow, NSF Center for Discrete Mathematics and Computer Science, Rutgers University.
1995-96	Assistant instructor, Mathematics, Rutgers University.
1995	Fredman, Michael L., Johnson, David S., McGeoch, Lyle A., and Ostheimer, Gretchen, "Data structures for traveling salesmen," J. Algorithms 18 (1995), 432-479.
1996	Ostheimer, Gretchen, "Algorithms for polycyclic-by-finite matrix groups," Proceedings of the DIMACS Workshop on Groups and Computation, AMS-ACM (to appear).
1996	Ph. D. in Mathematics, Rutgers University.