TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 344, Number 2, August 1994

THE ALGORITHMIC THEORY OF FINITELY GENERATED METABELIAN GROUPS

GILBERT BAUMSLAG, FRANK B. CANNONITO, AND DEREK J. S. ROBINSON

ABSTRACT. Algorithms are constructed which, when an explicit presentation of a finitely generated metabelian group G in the variety $\mathscr{A}^2$ is given, produce finitary presentations for the derived subgroup G', the centre $Z(G)$, the Fitting subgroup $\operatorname{Fit}(G)$, and the Frattini subgroup $\varphi(G)$. Additional algorithms of independent interest are developed for commutative algebra which construct the associated set of primes $\operatorname{Ass}(M)$ of a finitely generated module M over a finitely generated commutative ring R, and the intersection $\varphi_R(M)$ of the maximal submodules of M.

1. INTRODUCTION

It is now well known that the classical decision problems of group theory are insoluble even for the class of finitely presented soluble groups. Indeed it was shown by Harlampovič [9], and also by Baumslag, Gildenhuys and Strebel [4], that the word problem is insoluble for finitely presented soluble groups of derived length at most 3. However, despite this negative result, the prospects for a successful algorithmic theory for specific types of soluble group which are finitely presented, perhaps in some variety, remain favourable.

For example, a rather complete algorithmic theory for polycyclic-by-finite groups has been developed in recent works by the authors and D. Segal [3, 15]. There it was shown that many of the standard group theoretic constructions are effective for polycyclic-by-finite groups, and that subgroups such the centre, Fitting Subgroup and Frattini Subgroup are constructible. In addition Segal [15] has proved that the isomorphism problem for polycyclic-by-finite groups has a positive solution.

Our purpose here is to show that there is a satisfactory algorithmic theory for another well-known class of finitely generated soluble groups, namely those that are metabelian. Finitely generated metabelian groups have been studied intensively since the publication of P. Hall's fundamental papers in the 1950s, which first drew attention to the importance of commutative algebra in the theory of finitely generated soluble groups. For example, it follows from Hall's work that a finitely generated metabelian group satisfies $\max -n$, the maximal condition on normal subgroups, and is finitely presented in the variety $\mathscr{A}^2$ of

Received by the editors November 22, 1991 and, in revised form, February 8, 1993.
1991 *Mathematics Subject Classification.* Primary 20F10, 13L05.

The third author was a guest of the National University of Singapore and the University of Warwick during the preparation of this paper.

©1994 American Mathematical Society
0002-9947/94 $1.00 + $.25 per page

metabelian groups. The last result makes our class of groups a natural target for algorithmic methods.

Because of the connection with commutative algebra, it is to be expected that results and techniques from constructive commutative algebra will intervene in our theory. Our sources for these are papers by Seidenberg [16, 17] and Baumslag, Cannonito and Miller [2]. In addition it will be necessary to develop some apparently new algorithms for finitely generated modules over finitely generated commutative rings. It will be assumed throughout that all rings have identity and all modules are unital.

Results

To simplify the language we shall say that a finitely generated metabelian group is *given* if a finite presentation of the group in the variety $\mathscr{A}^2$ of finitely generated metabelian groups is furnished. Similar explanations apply when a finitely generated commutative ring, or a finitely presented module is "given". Also we shall say that a subgroup, or more generally an operator subgroup, can be *found* or *constructed* if there is an algorithm which produces a finite set of generators for it. Since a finitely generated metabelian group satisfies $\max -n$, it is meaningful to ask if a normal subgroup can be found.

At the heart of any finitely generated metabelian group G is its derived subgroup G'; this, of course, is a module over the finitely generated commutative ring $\mathbf{Z}G_{ab}$. Since this ring is noetherian, G' is finitely presented as a $\mathbf{Z}G_{ab}$-module. Thus a finite description of G' exists, even if it is not finitely generated as a group. It is a fundamental result for the entire paper that such a description can be found.

Theorem 3.1. *There is an algorithm which, when a finitely generated metabelian group G is given, finds a finite presentation of the $\mathbf{Z}G_{ab}$-module G'.*

There are many consequences of this theorem; we quote some of the more immediate ones.

Theorem 3.5. *There is an algorithm which, when a finitely generated metabelian group G is given, finds the centre $Z(G)$, and also a finite presentation of $Z(G)$.*

Theorem 4.1. *There is an algorithm which, when a finitely generated metabelian group G is given, finds (a finite subset whose normal closure is) the Fitting subgroup* $\mathrm{Fit}(G)$.

Another use of Theorem 3.1 is to get information about elements of finite order.

Corollary 4.4. *There is an algorithm to decide if a finitely generated metabelian group is torsion-free.*

It is also possible to decide if a given element has finite order, and to enumerate the possible orders of elements in a finitely generated metabelian group.

We have found it useful to introduce the following technical concept. A subgroup H of a finitely generated metabelian group G is said to be *nearly normal* in G if $H \cap G' \lhd G$. From our point of view the important feature of nearly normal subgroups is that they are determined by finite subsets. Thus it is meaningful to ask if a nearly normal subgroup can be constructed.

The motivation for the introduction of nearly normal subgroups is the observation that centralizers in finitely generated metabelian groups are nearly normal. Using this fact and the theory of nearly normal subgroups developed in §5, we are able to prove

Theorem 6.1. *There is an algorithm which, when given a finitely generated metabelian group G and finite subsets X and Y, finds the centralizer $C_{\langle Y\rangle}(X)$ as a nearly normal subgroup of $\langle Y\rangle$.*

An algorithm is devised in §7 to decide membership in a product of nearly normal subgroups. As a consequence of this, we obtain a positive solution of a generalization of the conjugacy problem.

Theorem 7.2. *There is an algorithm which, when given a finitely generated metabelian group G and two sequences $x_1, \dots, x_n$ and $y_1, \dots, y_n$ of elements of G, decides if there exists an element g of G such that $x_i^g = y_i$ for $i = 1, 2, \dots, n$.*

The conjugacy problem for finitely generated metabelian groups was originally shown to be soluble by Noskov [11].

The remaining sections of the paper call for the development of some constructive commutative algebra that does not seem to appear in the literature, although it may well be known to experts in the field. In §8 it is shown how to construct the associated set of primes of a finitely generated module over a finitely generated commutative ring. This is applied in §9 to establish

Theorem 9.1. *There is an algorithm which, when given a finitely generated metabelian group, finds the limit of its lower central series.*

Here it should be borne in mind that the lower central series of a finitely generated metabelian group terminates after at most ω steps (see for example [13, Chapter 15]). Thus the algorithm of Theorem 9.1 will tell us if the group is residually nilpotent. (It is noteworthy that the corresponding question for polycyclic groups is still open).

The last main result of the paper is

Theorem 10.1. *There is an algorithm which, when a finitely generated metabelian group G is given, finds the Frattini subgroup $\varphi(G)$.*

The Frattini subgroup is usually the hardest subgroup to construct because of the highly nonconstructive nature of its definition. The bulk of the proof of Theorem 10.1 consists in constructing the intersection of the maximal submodules of a finitely generated module over a finitely generated commutative ring, a result of independent interest.

It should be emphasized that our concern in this paper has been with the existence of algorithms for finitely generated metabelian groups, but not the practicability of such algorithms. The next step is of course to determine whether some of the algorithms can be implemented. For this purpose it will be necessary to have at hand some practical algorithms from commutative algebra. In recent years there has been considerable interest in the implementation of programs to perform such standard operations as finding the primary decomposition of an ideal in a polynomial ring—see for example [7] where further references are given. The well-known concept of a Gröbner basis comes into play in many such algorithms.

Some algorithmic problems for finitely generated metabelian groups remain open, notably the isomorphism problem and the conjugacy problem for finitely generated subgroups. Also unresolved is the possible constructibility of normalizers, and intersections of finitely generated subgroups.

2. Preliminary results

Here we list some known results which will be used frequently in subsequent sections.

Theorem 2.1 (The word problem). *There is an algorithm which, when given a finitely generated metabelian group G and a word w in the generators of G, decides if w equals the identity element of G.*

This may be proved by observing that G is residually finite, by a result of P. Hall (see [13, Chapter 15]), and finitely presented in the variety $\mathscr{A}^2$. The algorithm consists of two procedures; the first enumerates finite quotients of G and checks to see if the image of w is nontrivial; the second enumerates the consequences of the defining relations of G and looks for the word w.

Theorem 2.2 (The generalized word problem). *There is an algorithm which, when given a finitely generated metabelian group G and a finite sequence of elements $x, x_1, \dots, x_n$ of G, decides whether x belongs to the subgroup $\langle x_1, \dots, x_n \rangle$.*

This result is due to Romanovskiĭ [14].

Theorem 2.3 (The conjugacy problem). *There is an algorithm which, when given a finitely generated metabelian group G and elements x and y, decides if x and y are conjugate in G.*

We owe this theorem to Noskov [11]. The proof utilizes an algorithm for rings which is of great importance to us.

Proposition 2.4 (Noskov's Lemma). *There is an algorithm which, when given a finitely generated commutative ring R and a finite subset X of the group of units $U(R)$, finds a finite presentation of the subgroup $\langle X \rangle$.*

This depends ultimately on work of Borevič and Šafarevič on the unit group of an algebraic number field. We show in §3 how to deduce Theorem 2.3 rapidly from Noskov's Lemma.

We shall make use of some important algorithms for finitely generated modules over finitely generated commutative rings. Keep in mind that such rings and modules are noetherian, and the modules finitely presented.

Theorem 2.5 [2, Theorem 2.7]. *Every finitely generated commutative ring is submodule computable.*

Here a ring R is said to be *submodule computable* if it is computable and right noetherian, and if, given a finitely generated R-module M and a finite subset X of M, there are effective procedures to find a finite R-module presentation of XR, the R-submodule of M generated by X, and to solve the membership problem for XR.

Another result of a similar character which is important for us is

Theorem 2.6 [2, Theorem 2.14]. *Let there be given a finitely generated abelian group Q, a subgroup H of Q, a finitely generated $\mathbf{Z}Q$-module M, and a finite subset X of M. Then there is an algorithm to find a finite $\mathbf{Z}H$-module presentation of $(X)\mathbf{Z}H$.*

In fact this is the key to the solubility of the generalized word problem. Finally, we shall make use of the following result of Seidenberg [17, Theorems 5 and 6].

Proposition 2.7. *There is an algorithm which, when given a finitely generated commutative ring R and a finite subset X, determines a primary decomposition of the ideal XR, and hence can decide if XR is prime.*

3. The derived subgroup

Our first task is to construct a finite presentation of the derived subgroup of a finitely generated metabelian group. To expedite this we recall from [1] the definition of preferred presentation, although in a slightly different form.

A *preferred presentation* of a finitely generated metabelian group G is a finite $\mathscr{A}^2$-presentation $G = \langle g_1, \dots, g_t | R_1 \cup R_2 \rangle$ where

(a) R_1 is a finite set of words of the form

$$w = \prod_{1 \leq i < j \leq t} [g_i, g_j]^{u_{ij}},$$

the u_{ij} being words of the sort $g_1^{m_1} \cdots g_t^{m_t}$;

(b) R_2 is a finite set of words uw where u has the form $g_1^{m_1} \dots g_t^{m_t}$ and

$$w = \prod_{1 \leq i < j \leq t} [g_i, g_j]^{v_{ij}}$$

with v_{ij} of the form $g_1^{n_1} \cdots g_t^{n_t}$. Thus the words in R_1 determine a finite $\mathbf{Z}G_{ab}$-presentation of G' while those in R_2 yield a finite presentation of G_{ab}.

It is clear that every finitely generated metabelian group has a preferred presentation, and that there is a recursive enumeration of all preferred presentations of finitely generated metabelian groups.

Theorem 3.1. *There is an algorithm which, when a finitely generated metabelian group G is given, finds a finite presentation of the $\mathbf{Z}G_{ab}$-module G'.*

Proof. Enumerate all the preferred presentations of finitely generated metabelian groups, and let the groups determined by these be $G_1, G_2, \dots$. Then $G \simeq G_i$ for some i. For $i = 1, 2, \dots$ we enumerate all homomorphisms $\theta \colon G \to G_i$ and $\varphi \colon G_i \to G$, and determine if $\theta\varphi$ and $\varphi\theta$ are identity functions by using the given presentations of G and G_i. Such a triple (i, θ, φ) will eventually appear. Then $G \simeq G_i$ and we can read off from the preferred presentation of G_i a finite $\mathbf{Z}G_{ab}$-presentation of G'.

Corollary 3.2. *For each $i > 0$ there is an algorithm which, when given a finitely generated metabelian group G, finds a finite $\mathbf{Z}G_{ab}$-presentation of $\gamma_{i+1}(G)$, the $(i+1)$th term of the lower central series.*

Since we can certainly find generators for the module $\gamma_{i+1}(G)$, the assertion follows from submodule computability of $\mathbf{Z}G_{ab}$.

The next result indicates that one can really get hold of the finitely generated subgroups of a finitely generated metabelian group.

Theorem 3.3. *There is an algorithm which, when a finitely generated metabelian group G is given, together with a finite subset X, finds a finite $\mathscr{A}^2$-presentation of the subgroup $\langle X \rangle$.*

Proof. Let $K = \langle X \rangle$. Starting with a finite presentation of $Q = G_{ab}$, we find one for $H = KG'/G'$, and hence obtain a finite set of $\mathbf{Z}H$-module generators for $K \cap G'$. By Theorem 2.6 we can obtain a finite presentation of this module. It is now routine to combine this with the finite presentation of H to obtain a finite $\mathscr{A}^2$-presentation of K.

The centre. Our next objective is the construction of the centre of a finitely generated metabelian group. To pave the way we first establish

Proposition 3.4. *There is an algorithm which, when given a finitely generated metablian group G, finds a maximal abelian normal subgroup of G containing G'.*

Proof. Let $Q = G_{ab}$. By 3.1 we can find a finite $\mathbf{Z}Q$-presentation of $A = G'$, with generators $a_1, \dots, a_m$ say. Since $\mathbf{Z}Q$ is submodule computable, we can also find a finite $\mathbf{Z}Q$-presentation of each a_i^G, and so a finite set of generators of an ideal I_i such that $a_i^G \simeq \mathbf{Z}Q/I_i$. Then Noskov's Lemma (2.4) enables us to find a finite presentation of the group $Q + I_i/I_i$. Now the obvious homomorphism $Q \to Q + I_i/I_i$ has kernel $C_G(a_i)/A$. Thus we can find a finite set of generators for the latter group, and hence for $\bigcap_{i=1}^m C_G(a_i)/A = C_G(A)/A$. If $C_G(A) = A$, then A is a maximal abelian normal subgroup. Otherwise we can find $b_1 \in C_G(A) \backslash A$; then $A_1 = \langle A, b_1 \rangle$ is an abelian normal subgroup properly containing A. It is clear how to obtain a finite $\mathbf{Z}Q$-presentation of A_1.

The same procedure may be repeated for A_1. In this way an ascending chain $A = A_0 < A_1 < \cdots$ of abelian normal subgroups is produced. Since Q is finitely generated, we shall eventually find a v such that $A_v = A_{v+1}$. Then A_v will be a maximal abelian normal subgroup of G.

It is now straightforward to find the centre.

Theorem 3.5. *There is an algorithm which, when a finitely generated metabelian group G is given, finds the centre $Z(G)$, and also a finite presentation of $Z(G)$.*

Proof. Let $Q = G_{ab}$. We find a finite $\mathbf{Z}G$-presentation of a maximal abelian normal subgroup A containing G', using 3.4. Of course $Z(G) \leq A$. Let $x_1, \dots, x_n$ be the generators of G. Then $a \mapsto [a, x_i]$ is a $\mathbf{Z}Q$-endomorphism of A, so by [2, §2] we can find a finite set of generators for its kernel $C_A(x_i)$. By [2, §2] again we can then find a finite set of $\mathbf{Z}Q$-generators for $\bigcap_{i=1}^n C_A(x_i) = Z(G)$; of course these elements will generate $Z(G)$ as a group. Finally apply 3.3 to get a finite presentation of $Z(G)$.

Corollary 3.6. *There is an algorithm which finds the terms of the upper central series of a given finitely generated metabelian group.*

The conjugacy problem. We present next a proof of the solubility of the conjugacy problem which, although it stills depends on Noskov's Lemma, is somewhat simpler than the proof given in [11]. The main step in the argument is

Lemma 3.7. *There is an algorithm which, when given a finitely generated abelian group Q, a finitely generated $\mathbf{Z}Q$-module M, and elements a, b of M, decides if a and b are Q-conjugate, i.e., if there is an element q of Q such that $b = aq$.*

Proof. Put $R = \mathbf{Z}Q$. A finite presentation of the R-module aR is obtainable by the submodule computability of R. It is decidable whether $b \in aR$, and we can certainly assume that this is the case. We may further assume that $M = aR$, and identify M with R/I where I is the annihilator of a in R. A finite set of generators of the ideal I is known. Of course we assume that $a = 1 + I$ and $b = r + I$ where r can be found by enumeration. It is necessary to decide if $b \in \overline{Q} = Q + I/I$.

The first step is to decide whether $b \in U(R/I)$, or equivalently if $R = Rr + I$; submodule computability of R shows that this is possible. Assuming that $b \in U(R/I)$, we can then apply Noskov's Lemma to obtain a finite presentation of the subgroup $\langle b, \overline{Q}\rangle$. This presentation allows us to decide if $b \in \overline{Q}$.

Proof of Theorem 2.3. Let $Q = G_{ab}$. Obviously we can assume that $xA = yA$. Next observe that x and y are conjugate if and only if they are conjugate modulo $[A, x]$. For if the latter is true, $y^g = x[x, a] = x^a$ for some $g \in G$ and $a \in A$. Since we can obtain a finite set of $\mathbf{Z}Q$-generators of $[A, x]$, a finite presentation of $G/[A, x]$ in the variety $\mathscr{A}^2$ is at hand. Since we can pass to the group $G/[A, x]$, we may as well assume that $[A, x] = 1$. Hence $M = \langle A, x\rangle$ is a $\mathbf{Z}Q$-module via conjugation. Now it is easy to obtain a finite presentation of the module M. Also $y \in M$ since $yA = xA$. Lemma 3.7 can therefore be applied to give the result.

4. The Fitting subgroup

The main result of this section is

Theorem 4.1. *There is an algorithm which, when a finitely generated metabelian group G is given, finds its Fitting subgroup* $\mathrm{Fit}(G)$.

The proof depends upon a useful construction for modules.

Lemma 4.2. *There is an algorithm which, when given a finitely generated commutative ring R and a finitely R-module M, constructs a series of submodules $0 = M_0 < M_1 < \cdots < M_l = M$ and prime ideals $P_1, \dots, P_l$ such that $M_{i+1}/M_i \overset{R}{\simeq} R/P_i$.*

Proof. We can assume that $M \neq 0$. Enumerate the nonzero elements a_1 of M, and, using submodule computability of R, find a finite R-module presentation of a_1R, and hence a finite set of generators for the annihilator $P_1 = \mathrm{Ann}_R(a_1)$. Seidenberg's algorithm (see Proposition 2.7) can then be used to test P_1 for primeness. Eventually an a_1 will appear for which P_1 is prime. Put $M_1 = a_1R \overset{R}{\simeq} R/P_1$. If $M_1 \neq M$, repeat the procedure for the module M/M_1. Since M is noetherian, a finite chain of submodules M_i of the type sought will be obtained.

Proof of Theorem 4.1. Let $Q = G_{ab}$; first construct the $\mathbf{Z}Q$-module $A = G'$. Then find a series of submodules M_i of A and prime ideals P_i of $\mathbf{Z}Q$ as specified in Lemma 4.2. Let $g \in G$ and put $\overline{g} = gG'$. If $g \in \mathrm{Fit}(G)$, then some $(\overline{g} - 1)^k$, $k > 0$, annihilates each M_{i+1}/M_i. Since P_i is prime, this means that $\overline{g} - 1$ annihilates M_{i+1}/M_i and $\overline{g} \in 1 + P_i$. Consequently

$$\mathrm{Fit}(G)/A = \bigcap_{i=1}^{l} \mathrm{Ker}(Q \to Q + P_i/P_i).$$

By Noskov's Lemma a finite presentation of $Q+P_i/P_i$ may be found, and hence a finite set of generators for the kernel of $Q \to Q+P_i/P_i$. Thus we can find finitely many generators for $\mathrm{Fit}(G)/A$. By adding the $\mathbf{Z}G$-generators of A, we obtain a finite subset whose normal closure in G is $\mathrm{Fit}(G)$.

The elements of finite order. Another use of Lemma 4.2 is to obtain information about the elements of finite order in a finitely generated metabelian group G. First note that since G satisfies $\max -n$, there is an upper bound for the finite orders of elements of G. On the other hand, the set of elements of finite order may be infinite. As the following result indicates, this set is well behaved algorithmically; in particular it is recursive.

Theorem 4.3. *There are algorithms which, when a finitely generated metabelian group G is given, do the following:*

(i) *determine if a given element has finite order, and if so find the order;*

(ii) *find elements $u_1, \dots, u_k$ of G and finite subsets $X_1, \dots, X_k$ of G' such that the set of elements with finite order in G is $u_1\langle X_1^G\rangle \cup \cdots \cup u_k\langle X_k^G\rangle$;*

(iii) *find the set of finite orders of elements of G.*

Corollary 4.4. *There is an algorithm which can decide if a given finitely generated metabelian group is torsion-free.*

Proof. Let $Q = G_{ab}$ and $A = G'$. The first step is to find the torsion-subgroup of Q; let this be $\{s_1A, \dots, s_tA\}$. Next, using Lemma 4.2, we construct a series of $\mathbf{Z}Q$-modules $0 = A_0 \subset A_1 \subset \cdots \subset A_m = A$, and prime ideals $P_0, \dots, P_{m-1}$ such that $A_{i+1}/A_i \simeq \mathbf{Z}Q/P_i$. For each i compute the characteristic of the domain $\mathbf{Z}Q/P_i$ by finding the (additive) order of $1+P_i$; this is possible by Theorem 2.6.

Let q denote the product of all the nonzero characteristics and t. Then it is clear that every finite order of an element of G divides q. If $g \in G$ is given, we can decide if g has finite order by determining if $g^q = 1$. Should this be true, we can then find the order of g by identifying the smallest positive divisor d of q such that $g^d = 1$.

Let $g \in G$ and write $g = s_ia$ with $a \in A$. Then $g^q = s_i^q a^{\eta_{iq}}$ where η_{iq} is the $\mathbf{Z}Q$-endomorphism of A which sends x to $x^{1+s_i+\cdots+s_i^{q-1}}$. Thus g has finite order if and only if $s_i^q = a^{-\eta_{iq}}$. To obtain all the elements of finite order, first decide for each i whether $s_i^q \in \mathrm{Im}(\eta_{iq})$. If this is the case, find by enumeration an a_{iq} in A such that $s_i^q = a_{iq}^{-\eta_{iq}}$. Then $(s_ia)^q = 1$ if and only if $a \in a_{iq}K_{iq}$ where $K_{iq} = \mathrm{Ker}(\eta_{iq})$. Now we can find a finite set of generators X_{iq} for the $\mathbf{Z}Q$-module K_{iq} (by [2, Lemma 2.3]). Then the elements of finite order are those in the set $\bigcup(s_ia_{iq})\langle X_{iq}\rangle^G$, the union begin taken over all i for which $s_i^q \in \mathrm{Im}(\eta_{iq})$. This completes the proof of (i) and (ii).

Finally, let d be a positive divisor of q. There is an element with order exactly d if and only if for some i we have $s_i^d \in \mathrm{Im}(\eta_{id})$ and also $(s_ia_{id}k)^e \neq 1$ for every proper positive divisor e of d and all $k \in K_{id}$. The second condition is equivalent to $s_i^e a_{id}^{\eta_{ie}} \notin K_{id}^{\eta_{ie}}$. This can be checked for all e dividing d.

5. Nearly normal subgroups

Let G be a finitely generated metabelian group, and write $A = G'$. A subgroup H of G is said to be *nearly normal* if $H \cap A \lhd G$. Nearly normal subgroups of G are distinguished by the fact that they are finitely describable. If H is nearly normal, then $H \cap A$ is finitely generated as a $\mathbf{Z}G_{ab}$-module, say by the finite subset V. Also $H/H \cap A$ is generated as a group by $U(H \cap A)$ where U is finite. Hence $H = \langle U \rangle \langle V^G \rangle$, so that H is determined by the pair of finite subsets U and V where $V \subseteq A$. If there is an effective procedure to construct U and V, we shall say that the nearly normal subgroup H *can be found.*

On the other hand, Baumslag, Stammbach and Strebel [5] have shown that the free metabelian group of rank 2 has continuously many nonisomorphic subgroups. Thus a finitely generated metabelian group can have subgroups which are not constructible by any algorithm.

We proceed now to develop some elementary results about nearly normal subgroups.

Lemma 5.1. *If a nearly normal subgroup H of a finitely generated metabelian group G is given in the form $H = \langle U \rangle \langle V^G \rangle$ where U and V are finite and $V \subseteq G' = A$, then we can find the $\mathbf{Z}G_{ab}$-module $H \cap A$.*

Proof. Clearly $H \cap A = (\langle U \rangle \cap A)\langle V^G \rangle$. We can find a finite presentation of the group $\langle U \rangle A/A \simeq \langle U \rangle / \langle U \rangle \cap A$, and hence a finite set of $\langle U \rangle$-generators for $\langle U \rangle \cap A$. The result follows on adjoining to this set the elements of V.

Lemma 5.2. *There is an algorithm which, when given a finitely generated metabelian group G, a nearly normal subgroup H, and an element x of G, decides if x belongs to H.*

Proof. Let H be given in the usual form, $H = \langle U \rangle \langle V^G \rangle$. Since a finite $\mathscr{A}^2$-presentation of the group $\overline{G} = G/\langle V^G \rangle$ is available, we can pass to this group. We have to decide if $x\langle V^G \rangle \in \overline{H} = H/\langle V^G \rangle$. This is possible by Theorem 2.2, since $\overline{H}$ is finitely generated.

Corollary 5.3. *There is an algorithm which, when given two nearly normal subgroups H_1 and H_2 of a finitely generated metabelian group G, decides if $H_1 \subseteq H_2$.*

Proof. Let $H_i = \langle U_i \rangle \langle V_i^G \rangle$ in the usual form, $i = 1, 2$. Then $H_1 \subseteq H_2$ if and only if $U_1 \subseteq H_2$ and $V_1 \subseteq H_2$; for $V_1 \subseteq H_2$ implies that $V_1^G \subseteq (H_2 \cap A)^G = H_2 \cap A$. Now apply Lemma 5.2.

Intersections. The intersection of two nearly normal subgroups is obviously nearly normal. The next result shows that such an intersection is constructible.

Theorem 5.4. *There is an algorithm which, when given a finitely generated metabelian group G and finite subsets of G that define two nearly normal subgroups H and K, finds finite subsets that define $H \cap K$.*

During the proof we shall need

Lemma 5.5. *There is an algorithm which, when given a finitely generated abelian group Q, a finitely generated $\mathbf{Z}Q$-module M, and a derivation $\delta \colon Q \to M$, finds the subgroup* $\operatorname{Ker}(\delta)$.

Proof. Of course δ is given by means of its effect on the generators of Q. We follow the method of [3, 6.2]. Let $M_1 = M \oplus \mathbf{Z}$, and define a $\mathbf{Z}Q$-module structure on M by the rule $(x, n) \cdot q = (xq + q^{\delta}n, n)$ where $x \in M$, $q \in Q$,

$n \in \mathbf{Z}$. Starting from a finite presentation of M, we can easily write down a finite $\mathbf{Z}Q$-presentation of M_1. Since $\operatorname{Ker}(\delta) = C_Q(b)$ where $b = (0, 1)$, it is sufficient to show how to find $C_Q(b)$.

By submodule computability we can find a finite presentation of $(b)\mathbf{Z}Q$, and hence a finite set of generators for the ideal $I = \operatorname{Ann}_{\mathbf{Z}Q}(b)$, since $(b)\mathbf{Z}Q \simeq \mathbf{Z}Q/I$. Noskov's Lemma allows us to find a finite presentation of the group $Q{+}I/I$. Since $C_Q(b)$ is the kernel of the natural homomorphism $Q \to Q{+}I/I$, a finite set of generators for $C_Q(b)$ is at hand.

Proof of Theorem 5.4. (i) First we find $A = G'$. By Lemma 5.1 we can find sets of generators for the $\mathbf{Z}G_{ab}$-modules $H \cap A$ and $K \cap A$. Then by submodule computability we can find $\mathbf{Z}G_{ab}$-generators for $H \cap K \cap A$.

(ii) *If* $A \leq H$ *or* $A \leq K$, *then we can find* $H \cap K$.

Suppose, for example, that $A \leq H$. Since we have finite sets of generators for H/A and KA/A, we can find $(H/A) \cap (KA/A) = (H \cap K)A/A$, and hence $H \cap K/H \cap K \cap A$. Therefore we have found $H \cap K$.

(ii) *We can assume that* $HA = KA$.

Write $\overline{H} = H \cap (KA)$ and $\overline{K} = K \cap (HA)$. Then $\overline{H}$ and $\overline{K}$ are nearly normal, and by (ii) we can find them. Also

$$HA \cap KA = \overline{H}A = \overline{K}A,$$

and $\overline{H} \cap \overline{K} = H \cap K$. Replace H and K by $\overline{H}$ and $\overline{K}$ respectively, to justify the assumption.

(iii) *We can assume that* $H \cap A = 1 = K \cap A$.

Since finite sets of $\mathbf{Z}G_{ab}$-generators for $H \cap A$ and $K \cap A$ can be found by Lemma 5.1, we can write down a finite $\mathscr{A}^2$-presentation of the group G/D where $D = (H \cap A)(K \cap A)$. Assume that we are able to find $HD/D \cap KD/D = (H \cap K)D/D$; thus we know $(H \cap K)D$ as a nearly normal subgroup.

Next enumerate finite subsets X of G and check to see if $X \subseteq H$ and $X \subseteq K$, using Lemma 5.2. Then determine if $\langle X \rangle D = (H \cap K)D$. Since $(H \cap K)D/D$ is finitely generated, such an X will eventually appear. When it does, we shall have

$$H \cap K = (H \cap K) \cap (\langle X \rangle D) = \langle X \rangle (H \cap K \cap A).$$

Since finitely many $\mathbf{Z}G_{ab}$-generators for $H \cap K \cap A$ are known, $H \cap K$ has been constructed.

These considerations allow us to assume that $H \cap A = 1 = K \cap A$. Thus finite generating sets for H and K are known.

(v) *The final step.*

We have now reached the position where $HA = KA$ and $H \cap A = 1 = K \cap A$. There is a derivation $\delta \colon H \to A$ such that $K = \{hh^\delta | h \in H\}$. Let $H = \langle h_1, \dots, h_m \rangle$, and put $a_i = h_i^\delta$. The a_i can be found by enumerating elements a of A and checking to see if $h_i a \in K$. Notice that $H \cap K = \operatorname{Ker}(\delta)$. Also $A_0 = \langle \operatorname{Im}(\delta) \rangle$ is a $\mathbf{Z}H$-submodule of A, and it is easy to see that $a_1, \dots, a_m$ generate the module A_0. A finite $\mathbf{Z}H$-module presentation of A_0 can be constructed by Theorem 2.6. Finally, Lemma 5.5 allows us to find $\operatorname{Ker}(\delta)$.

Next we present a second constructibility theorem for intersections which will be required in the construction of centralizers.

Theorem 5.6. *There is an algorithm which, when given a finitely generated metabelian group G, together with finite subsets defining a finitely generated subgroup H and a nearly normal subgroup N, finds $H \cap N$ as a nearly normal subgroup of H.*

Proof. As usual, write $A = G'$. In the first place $H \cap N$ is nearly normal in H since $(H \cap N) \cap H' = (N \cap A) \cap H' \lhd H$.

(i) *We can assume that* $N \leq HA$.

For we can find the normal subgroup HA, and then, using Theorem 5.4, find $\overline{N} = (HA) \cap N$ as a nearly normal subgroup of G. Observing that $H \cap \overline{N} = H \cap N$, we then replace N by $\overline{N}$, so that it is permissible to suppose that $N \leq HA$.

(ii) *We can find a finite set of generators for the* $\mathbf{Z}H_{ab}$*-module* $H \cap N \cap A$.

First find a finite set of $\mathbf{Z}G_{ab}$-generators for $N \cap A$, using Lemma 5.1. Then use this set to obtain a finite $\mathbf{Z}G_{ab}$-presentation of the module $A/N \cap A$. Find a finite presentation of the group $H/H \cap A$, and hence a finite set of $\mathbf{Z}(HG'/G')$-generators for $H \cap A$. Now apply Theorem 2.6 to construct a finite $\mathbf{Z}H_{ab}$-presentation of $(H \cap A)(N \cap A)/N \cap A$. From this we read off a finite set of generators for $H \cap N \cap A$.

(iii) *We can assume that* $N \cap A = 1$.

Since $N \cap A$ is known as a normal subgroup of G, a finite $\mathscr{A}^2$-presentation of $G/(N \cap A)$ is available. Suppose that we can find

$$(H(N \cap A)/(N \cap A)) \cap (N/(N \cap A)) = (H \cap N)(N \cap A)/(N \cap A)$$

as a nearly normal subgroup of $H(N \cap A)/(N \cap A)$. Since $[H \cap N \cap A, H] \leq N \cap A$, we actually have a finite set of generators for $(H \cap N)(N \cap A)/(N \cap A)$. A finite set of generators of $H \cap N \cap A/H' \cap N$ and a finite set of $\mathbf{Z}H_{ab}$-module generators of $H' \cap N = H' \cap (H \cap N \cap A)$ are also available. Combining all of these, we obtain the required description of $H \cap N$.

Consequently we can suppose that $N \cap A = 1$, which means that we have finitely many generators for N, say $u_1, \dots, u_m$. A finite presentation of N in the u_i can then be found.

(iv) *The final step.*

This is a modification of the derivation argument used in the proof of the previous theorem. We have reached the situation where $N \leq HA$ and $N \cap A = 1$. Then $NA = NA \cap HA = (H \cap NA)A$. If $x \in N$, it follows that $xa_x \in H \cap NA$ for some $a_x \in A$; here a_x is uniquely determined modulo $H \cap A$. Note that $H \cap A$ is a $\mathbf{Z}N$-module since $N \leq HA$. Then $x \mapsto a_x(H \cap A)$ is a derivation from N to $A/(H \cap A)$, call it δ.

We can find elements $a_{u_1}, \dots, a_{u_m}$ by enumeration, and then a finite presentation of the $\mathbf{Z}(HA/A)$-module A_1 generated by these elements. Here use has been made of Theorem 2.6. A finite $\mathbf{Z}(HA/A)$-presentation of $\overline{A}_1 = A_1(H \cap A)/(H \cap A)$ is now at hand. Since $N \leq HA$, we can apply Theorem 2.6 once again to obtain a finite presentation of the $\mathbf{Z}N$-submodule A_2 generated by the elements $a_{u_i}(H \cap A) = u_i^\delta$. But A_2 is the $\mathbf{Z}N$-submodule generated by $\operatorname{Im}(\delta)$. Since $H \cap N = \operatorname{Ker}(\delta)$, the result follows via Lemma 5.5.

6. Centralizers

Our aim here is to construct arbitrary centralizers in finitely generated metabelian groups.

Theorem 6.1. *There is an algorithm which, when given a finitely generated metabelian group G, and finite subsets X and Y, finds the centralizer $C_{\langle Y\rangle}(X)$ as a nearly normal subgroup of $\langle Y\rangle$.*

This will follow quickly from a special case.

Lemma 6.2. *There is an algorithm which, when given a finitely generated metabelian group G and an element x of G, finds $C_G(x)$ as a nearly normal subgroup of G.*

Proof. Write $Q = G_{ab}$, $A = G'$ amd $C = C_G(x)$. Of course $C\cap A = C_A(x)\triangleleft G$, so C is nearly normal.

(i) *We can find a finite set of generators for the* $\mathbf{Z}Q$*-module* $C \cap A$.

Indeed $C \cap A$ is the kernel of the $\mathbf{Z}Q$-endomorphism $a \mapsto [a, x]$ of A. Since a finite $\mathbf{Z}Q$-presentation of $[A, x]$ is obtainable, we can find $C \cap A$.

(ii) *We may assume that* $[A, x] = 1$.

In the first place we can write down a finite $\mathscr{A}^2$-presentation of $G/[A, x]$. Now suppose that we have been able to find the centalizer of $x[A, x]$ in $G/[A, x]$, say $C_1/[A, x]$. Of course $A \leq C_1$, so we have a finite set of generators for C_1/A. If $u \in C_1$, then $[u, x] = [a, x]$ for some a in A, and $ua^{-1} \in C$. It follows that $C_1 = CA$.

To find C, we first enumerate finite subsets Y of G, and check to see if $Y \subset C$, i.e. if $[x, y] = 1$ for every y in Y. Then we decide if $C_1 = \langle Y\rangle A$. Such a Y is bound to appear; when it does, we shall have $C = C \cap (\langle Y\rangle A) = \langle Y\rangle(C \cap A)$. Because of (i) we have found C.

(iii) We now suppose that $[A, x] = 1$, so that $B = \langle x, A\rangle$ is a $\mathbf{Z}Q$-module. It is straightforward to construct a finite $\mathbf{Z}Q$-presentation of B from one of A. Next $\langle x^G\rangle \simeq \mathbf{Z}Q/I$ where I is the annihilator of x in $\mathbf{Z}Q$. Submodule computability enables us to construct a finite set of generators for the ideal I. Finally, C/A is the kernel of the natural map $Q \to Q + I/I$. The usual argument with Noskov's Lemma produces a finite set of generators for C/A. Therefore C has been found.

Proof of Theorem 6.1. This is now easy. Write $X = \{x_1, \dots, x_m\}$. By Lemma 6.2 we can find $C_G(x_i)$ as a nearly normal subgroup of G. Therefore we can find $C_G(X) = \bigcap_{i=1}^m C_G(x_i)$ by Theorem 5.4. Finally, Theorem 5.6 allows us to find $C_{\langle Y\rangle}(X) = \langle Y\rangle \cap C_G(X)$.

7. Deciding membership in a product of nearly normal subgroups

Our main result in this section is

Theorem 7.1. *There is an algorithm which, when given a finitely generated metabelian group G, finite subsets defining nearly normal subgroups H and K, and an element g of G, decides whether g belongs to the subset HK.*

Our motivation for this theorem is the desire to prove.

Theorem 7.2 (Generalized conjugacy problem). *There is an algorithm which, when given a finitely generated metabelian group G, and two sequences of elements $x_1, \dots, x_n$ and $y_1, \dots, y_n$, decides if there is an element g of G such that $x_i^g = y_i$ for $i = 1, 2, \dots, n$.*

Proof. By Theorem 2.3 we may assume that $m > 1$, and argue by induction on m. We can suppose that there are elements g_1, g_2 in G such that $x_i^{g_1} = y_i$ for $i = 1, \dots, m-1$, and $x_m^{g_2} = y_m$; of course such elements can be found by enumeration. Clearly there is a g in G such that $x_i^g = y_i$ for $i = 1, \dots, m$ if and only if the subset

$$\left(\bigcap_{i=1}^{m-1} C_G(x_i)\right) g_1 \cap C_G(x_m) g_2$$

is not empty, or, equivalently, if $g_1 g_2^{-1} \in C_G(\{x_1, \dots, x_{m-1}\}) C_G(x_m)$. By Theorem 6.1 we can find $C_G(\{x_1, \dots, x_{m-1}\})$ and $C_G(x_m)$. Since these subgroups are nearly normal, membership in their product is decidable by 7.1.

Corollary 7.3. *If G is a finitely generated metabelian group, the word problem for the outer automorphism group* $\mathrm{Out}(G)$ *is soluble.*

Proof. Let $G = \langle x_1, \dots, x_n \rangle$. An automorphism α of G is specified by an n-tuple $(w_1, \dots, w_n)$ of words in $\mathbf{x}$ where $x_i^\alpha = w_i$. By Theorem 7.2 we can decide if α is induced by an element of G.

The proof of Theorem 7.1 depends ultimately on our ability to decide membership in the image of a derivation.

Proposition 7.4. *There is an algorithm which, when given a finitely generated abelian group Q, a finitely generated $\mathbf{Z}Q$-module M, a derivation $\delta: Q \to M$, and an element a of M, decides whether a belongs to* $\mathrm{Im}(\delta)$.

The problem described in Proposition 7.4 will be referred to as the membership problem for the triple (Q, M, δ). Before proving the proposition we shall establish a technical result.

Lemma 7.5. *Let there be given a finitely generated abelian group Q, a finitely generated $\mathbf{Z}Q$-module M, and a derivation $\delta: Q \to M$. Assume in addition that a series of submodules $0 = M_0 \leq M_1 \leq \cdots \leq M_r = M$ is given, and that the membership problem is soluble for each triple $(Q_i, M_i/M_{i-1}, \delta_i)$ where $Q_i = \{q \in Q | q^\delta \in M_i\}$ and $\delta_i: Q_i \to M_i/M_{i-1}$ is induced by δ. Then the membership problem is soluble for (Q, M, δ).*

Proof. In the first place Q_i is the kernel of the derivation $\delta_i': Q \to M/M_i$ defined by $q^{\delta_i'} = q^\delta + M_i$. Thus Q_i is a subgroup of Q, which can be found by Lemma 5.5.

Suppose that the membership problem is soluble for $(Q, M/M_i, \delta_i')$; we shall show how to solve the problem for $(Q, M/M_{i-1}, \delta_{i-1}')$. Let $a \in M$ be given. Then we can assume that $a + M_i \in \mathrm{Im}(\delta_i')$, and by enumeration we can find elements $q \in Q$, $b \in M_i$ such that $a = q^\delta + b$. Now $a + M_{i-1} \in \mathrm{Im}(\delta_{i-1}')$ if and only if there exists $q_1 \in Q$ such that $q_1^\delta - q^\delta \equiv b \pmod{M_{i-1}}$, i.e., $(q_1 q^{-1})^\delta \equiv bq^{-1} \pmod{M_{i-1}}$. Hence $a + M_{i-1} \in \mathrm{Im}(\delta_{i-1}')$ if and only if $bq^{-1} + M_{i-1} \in \mathrm{Im}(\delta_i)$. (Notice that $q_1 q^{-1} \in Q_i$ since $bq^{-1} \in M_i$.) This is decidable by solubility of the membership problem for $(Q_i, M_i/M_{i-1}, \delta_i)$. It follows by induction on $r - i$ that the membership problem is soluble for (Q, M, δ) since it is known to be soluble for $(Q, M/M_{r-1}, \delta_{r-1}')$.

Proof of Proposition 7.4.

(i) *Case*: *Q contains an element x such that $C_M(x) = 0$.*

Define $b = x^\delta \in M$. Let $a \in M$ be given. If y is any element of Q, then $x^\delta(y-1) = y^\delta(x-1)$ because $xy = yx$. Thus $a = y^\delta$ if and only if $a(x-1) = b(y-1)$ since $C_M(x) = 0$. Therefore $a \in \mathrm{Im}(\delta)$ if and only if b and $b + a(x-1)$ are Q-conjugate. This is decidable by Lemma 3.7.

(ii) *The general case.*

We argue by induction on the Hirsch number $h(Q)$. Of course, should this be zero, Q and $\mathrm{Im}(\delta)$ will be finite, and the assertion of the proposition is obvious. Let $h(Q) > 0$. Then we can find an element x of Q with infinite order.

Let M_i denote the kernel of the $\mathbf{Z}Q$-endomorphism $a \mapsto a(x-1)^i$ of M. Notice that $M_k = M_{k+1}$ for some k since M is a noetherian module. We can find the M_i and k, so we have explicit knowledge of the series $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k \subseteq M$. Since $C_{M/M_k}(x) = 0$, it follows from (i) that the membership problem for $(Q, M/M_k, \bar{\delta})$ is soluble; here $\bar{\delta}: Q \to M/M_k$ is induced by δ. Lemma 7.5 shows that it is enough to prove that the membership problem is soluble for each triple $(Q_i, M_i/M_{i-1}, \delta_i)$ where $Q_i = \{q \in Q | q^\delta \in M_i\}$, and $\delta_i: Q_i \to M_i/M_{i-1}$ is induced by δ.

For each i find Q_i, using Lemma 5.5, and compute $h(Q/Q_i)$. If this is positive, then $h(Q_i) < h(Q)$ and the desired conclusion is true by induction. Suppose that $h(Q/Q_i) = 0$, so that Q/Q_i is finite. Find a positive integer m such that $q = x^m \in Q_i$. Thus $q^{\delta_i} \in M_i/M_{i-1}$. It follows that it is sufficient to solve the membership problem for a triple (Q, M, δ) where Q contains an element q of infinite order such that $M(q-1) = 0$.

Consider the subgroup $N = \langle q^\delta \rangle$ of M. Then N is a trivial $\mathbf{Z}Q$-submodule since $q^\delta(y-1) = y^\delta(q-1) = 0$ for y in Q. A function $\bar{\delta}: Q/\langle q \rangle \to M/N$ is defined by the rule $(y\langle q \rangle)^{\bar{\delta}} = y^\delta + N$. This is a well-defined derivation. Let $a \in M$; then $a \in \mathrm{Im}(\delta)$ if and only if $a + N \in \mathrm{Im}(\bar{\delta})$. For, if $a = y^\delta + z$ with $y \in Q$ and $z \in N$, then $z = (q^\delta)i = (q^i)^\delta$ for some i, and hence $a = (yq^i)^\delta$. Consequently, it suffices to solve the membership problem for the triple $(Q/\langle q \rangle, M/N, \bar{\delta})$. But this is soluble since $h(Q/\langle q \rangle) < h(Q)$ and the induction hypothesis on $h(Q)$ is applicable.

Proof of Theorem 7.1. As usual write $A = G'$. A few reductions must first be made.

(i) *It is enough to decide membership of elements of A in $(HK) \cap A$.*

We have a finite set of generators for the subgroup HAK/A of G_{ab}, and we can certainly decide membership in it. Assuming that $g \in HAK$, we find elements $h \in H$, $k \in K$, $a \in A$, such that $g = hak$. Then $g \in HK$ if and only if $a \in (HK) \cap A$.

(ii) *We may assume that $HA = KA$.*

Put $\overline{H} = H \cap (KA)$ and $\overline{K} = (HA) \cap K$. By Theorem 5.4 we can find $\overline{H}$ and $\overline{K}$. Clearly $(\overline{H}\,\overline{K}) \cap A = (HK) \cap A$ and also $\overline{H}A = (HA) \cap (KA) = \overline{K}A$. Replace H, K by $\overline{H}, \overline{K}$.

(iii) *We may assume that $H \cap A = 1 = K \cap A$.*

For we can find the G_{ab}-module $D = (H \cap A)(K \cap A)$, and pass to the group G/D since $(HD)(KD) = HK$.

(iv) *Final step.*

We now have $HA = KA$ and $H \cap A = 1 = K \cap A$. Notice that we have finitely many generators for the abelian group H, say $h_1, \dots, h_m$. Let $\delta: H \to A$ be the derivation defined by $K = \{hh^\delta | h \in H\}$. Of course we can find the h_i^δ.

Let $a \in A$; then $a \in HK$ if and only if a can be written in the form $a = h^{-1}(h'h'^\delta)$ for some $h, h' \in H$. This is equivalent to $h = h'$ and $a = h^\delta$. Therefore $(HK) \cap A = \operatorname{Im}(\delta)$. Let A_0 be the $\mathbf{Z}H$-submodule generated by $\operatorname{Im}(\delta)$. Then A_0 is generated by the elements h_i^δ. A finite $\mathbf{Z}H$-presentation of A_0 can be found by Theorem 2.6. Finally, Proposition 7.4 may be applied to give the result.

8. The associated set of primes of a module

Let R be a finitely generated commutative ring, and M a finitely generated R-module. The associated set of primes of M, $\operatorname{Ass}(M)$, is the set of prime annihilators of elements of M. Since M is noetherian, this is a finite set, which is nonempty if $M \neq 0$. It is important for us to be able to construct $\operatorname{Ass}(M)$ because results of §§9 and 10 depend on this.

Theorem 8.1. *There is an algorithm which, when given a finitely generated commutative ring R and a finitely generated R-module M, finds the set* $\operatorname{Ass}(M)$.

During the proof we shall make use of the following technical lemma.

Lemma 8.2. *Let M be a finitely generated module over a finitely generated commutative ring R. Let M_0 be a submodule such that* $\operatorname{Ass}(M_0) = \{P\}$, $\operatorname{Ass}(M/M_0) = \{Q\}$, $Q \not\subseteq P$. *Denote by N the submodule of all elements of M that are annihilated by a power of Q. Then either* $\operatorname{Ass}(M) = \{P\}$ *or else* $\operatorname{Ass}(M) = \{P, Q\}$, $\operatorname{Ass}(M/N) = \{P\}$, *and* $\operatorname{Ass}(N) = \{Q\}$. *Moreover, if P, Q, M_0 are given, it is possible to decide which of these alternatives occurs.*

Proof. If I is an ideal of R, let ${}^*I = \{a \in M | aI = 0\}$. Then $N = {}^*Q^i$ for some i since M is noetherian. Now $\operatorname{Ass}(M) = \{P\}$ or $\{P, Q\}$, (see [6, IV 1.1]). If ${}^*Q = 0$, then $Q \notin \operatorname{Ass}(M)$ and $\operatorname{Ass}(M) = \{P\}$.

Suppose that ${}^*Q \neq 0$, so that $N \neq 0$. Thus $\varnothing \neq \operatorname{Ass}(N) \subseteq \{P, Q\}$. If $P \in \operatorname{Ass}(N)$, then $Q^i \subseteq P$ and $Q \subseteq P$. By this contradiction $\operatorname{Ass}(N) = \{Q\}$, and so $\operatorname{Ass}(M) = \{P, Q\}$.

Next let $U \in \operatorname{Ass}(M/N)$. Then $Q \not\subseteq U$ since Q annihilates no nonzero elements of M/N. On the other hand, some P^rQ^s annihilates M and so is contained in U ([6], IV, 1.4 Proposition 9). Therefore $P \subseteq U$. If $U = \operatorname{Ann}_R(x + N)$, then $xQ^iU = 0$. By the Artin-Rees property $MQ^r \cap {}^*Q = 0$ for some $r \geq i$; thus $Q \notin \operatorname{Ass}(xQ^r)$. Since $\varnothing \neq \operatorname{Ass}(xQ^r) \subseteq \{P, Q\}$, it follows that $\operatorname{Ass}(xQ^r) = \{P\}$. But $(xQ^r)U = 0$, so $U \subseteq P$ and hence $U = P$. Therefore $\operatorname{Ass}(M/N) = \{P\}$, as required.

Finally, to decide which of the two possibilities occurs, enumerate the nonzero elements of M and find their annihilators; then test each annihilator for primeness (using [17, Theorem 5]). This procedure will detect if $\operatorname{Ass}(M) \neq \{P\}$. Similarly we can tell if $\operatorname{Ass}(N) \neq \{Q\}$. Therefore we can tell which of the two situations occurs.

Proof of Theorem 8.1. We can assume that M is nonzero. By Lemma 4.2 we can construct a series of submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_l = M$ and prime ideals $P_1, \dots, P_l$ such that $\mathrm{Ass}(M_{i+1}/M_i) = \{P_i\}$. Now $\mathrm{Ass}(M)$ is a subset of $\{P_1, \dots, P_l\}$, and in addition these sets have the same minimal elements [6, IV, 1.4]. Thus we can find the minimal associated primes of M. Let P be one of these.

Applying Lemma 8.2 to each R-module M_{i+2}/M_i such that $P = P_i$ and $P \neq P_{i+1}$, we conclude that either $\mathrm{Ass}(M_{i+2}/M_i) = \{P\}$ or else we can find a submodule $\overline{M}_{i+1}$ such that $\mathrm{Ass}(\overline{M}_{i+1}/M_i) = \{P_{i+1}\}$ and $\mathrm{Ass}(M_{i+2}/\overline{M}_{i+1}) = \{P\}$. By repeated application of this procedure we shall find a submodule M_P such that $\mathrm{Ass}(M/M_P) = \{P\}$ and $\mathrm{Ass}(M_P) \subseteq \mathrm{Ass}(M)\backslash\{P\}$. In fact it is easy to see that $\mathrm{Ass}(M) = \mathrm{Ass}(M_P) \cup \{P\}$. The same procedure can now be applied to M_P, which has one fewer associated prime. After a finite number of such steps we shall have found $\mathrm{Ass}(M)$.

Corollary 8.3. *There is an algorithm which, when a finitely generated commutative ring R and a finitely generated R-module M are given, constructs a primary decomposition of the zero submodule of M.*

Proof. First find $\mathrm{Ass}(M) = \{P_1, \dots, P_k\}$. For each i find by enumeration a submodule M_i such that $\mathrm{Ass}(M/M_i) = \{P_i\}$ and $P_i \notin \mathrm{Ass}(M_i)$. Then $M_1 \cap \dots \cap M_k = 0$.

We conclude the section with an application of Theorem 8.1. Since a finitely generated metabelian group satisfies $\max -n$, it has a *finite radical*, i.e. a maximum finite normal subgroup.

Theorem 8.4. *There is an algorithm which finds the finite radical of a finitely generated metabelian group G.*

Proof. Let Q be a finitely generated abelian group with generators $x_1, \dots, x_m$. Write $R = \mathbf{Z}Q$, and let M be a finitely generated R-module: the first step is to find the finite radical (i.e. maximum finite submodule) of M. To start off, find $\mathrm{Ass}(M) = \{P_1, \dots, P_k\}$, using Theorem 8.1. Now make the elementary observation that the finite radical of M is nontrivial if and only if some R/P_i is finite. We can decide if R/P_i is finite; first find the order of the additive subgroup $\langle 1 + P_i \rangle$, using Theorem 2.6, and hence the characteristic of the domain R/P_i. If this is positive, find the (multiplicative) order of $x_j + P_i$ for each j, by Noskov's Lemma. R/P_i is finite if and only if all of these orders are finite. Thus we can decide if the finite radical of M is nontrivial. If it is, find a finite submodule $M_0 \neq 0$. If $M_0 \neq M$, pass to M/M_0 and repeat the procedure. When the process terminates—as it must since M is noetherian—we shall have constructed the finite radical of M.

Now put $Q = G_{ab}$, and take M to be a maximal abelian subgroup containing G'. This can be found by Proposition 3.4. The finite radical of M is constructible by the first part of the proof. Factor it out and repeat the procedure. Eventally we shall reach a quotient group $\overline{G}$ which has a torsion-free maximal abelian normal subgroup $\overline{M}$ (by $\max -n$). If $\overline{F}$ is a finite normal subgroup of $\overline{G}$, then $\overline{F} \leq C_{\overline{G}}(\overline{M}) = \overline{M}$, and $\overline{F} = 1$. It follows that our procedure will determine the finite radical of G.

9. The limit of the lower central series

Let G be a finitely generated metabelian group, and let $\gamma_\alpha(G)$ denote the αth term of the transfinite lower central series of G. Then it is well known that the series terminates at ω,

$$\gamma_\omega(G) = \gamma_{\omega+1}(G) = \cdots .$$

This follows quickly on applying the Artin-Rees property to the $\mathbf{Z}G_{ab}$-module G', using the augmentation ideal (see [13, §15, p. 450]).

The finite terms of the lower central series have already been constructed—see Corollary 3.2—but $\gamma_\omega(G)$ is more elusive.

Theorem 9.1. *There is an algorithm which, when given a finitely generated metabelian group G, finds $\gamma_\omega(G)$.*

Corollary 9.2. *There is an algorithm which can decide if a finitely generated metabelian group is residually nilpotent.*

Theorem 9.1 will follow quickly from a result about modules.

Proposition 9.3. *Let R be a finitely generated commutative ring and I an ideal of R. Let M be a finitely generated R-module with a primary decomposition of the zero submodule $M_1 \cap M_2 \cap \cdots \cap M_k = 0$. Then*

$$\bigcap_{r=1,2,\ldots} MI^r = M_{l+1} \cap \cdots \cap M_k$$

where $M = MI + M_i$ holds if and only if $1 \leq i \leq l$.

Proof. Consider first the case where $k = 1$ and $\operatorname{Ass}(M) = \{P\}$. Denote by M_0 the submodule of all elements of M which are annihilated by some power of P. Suppose that $M_0' = \bigcap_{i=1,2,\ldots} M_0 I^i \neq 0$, and let $0 \neq a \in M_0'$ be an element with maximal (proper) annihilator. Then $\operatorname{Ann}_R(a) = \{P\}$. By the Krull Intersection Theorem $a = au$ for some $u \in I$. Thus $1 - u \in P$ and therefore $R = I + P$. Since $MP^m = 0$ for some $m > 0$, it follows that $M = MI$ in this case.

Next assume that $M_0' = 0$, and put $M' = \bigcap_{j=1,2,\ldots} MI^j$. By the Artin-Rees property $M' \cap M_0 = M_0' = 0$. Since $\operatorname{Ass}(M') \subseteq \{P\}$, it follows that $M' = 0$. Thus we have proved that either $M = MI$ or $M' = 0$, which is exactly the assertion of the proposition when $k = 1$.

Now for $k > 1$. By the case $k = 1$ we have $\bigcap_{j=1,2,\ldots} (M/M_i)I^j = 0$ for $i = l+1, \ldots, k$. Therefore

$$M' = \bigcap_{j=1,2,\ldots} MI^j \subseteq M_{l+1} \cap \cdots \cap M_k = L,$$

say. Let $\operatorname{Ass}(M/M_i) = \{P_i\}$, so $\operatorname{Ass}(M) = \{P_1, \ldots, P_k\}$. Now $MP_i^{e_i} \subseteq M_i$ for some $e_i > 0$; hence $LP_1^{e_1} \cdots P_l^{e_l} \subseteq M_1 \cap \cdots \cap M_k = 0$. If $1 \leq i \leq l$, the argument of the first two paragraphs of the proof, when applied to the module M/M_i, yields $R = I + P_i$. Consequently $R = I + P_1^{e_1} \cdots P_l^{e_l}$, and so $L = LI \subseteq M'$. The conclusion is that $L = M'$.

Corollary 9.4. *There is an algorithm which, when a finitely generated commutative ring R, a finitely generated R-module M, and an ideal I of R are given, finds the submodule $\bigcap_{i=1,2,\ldots} MI^i$.*

Proof. By Corollary 8.3 we can find a primary decomposition $M_1 \cap \cdots \cap M_k = 0$. Now determine those i for which $(M/M_i)I \neq M/M_i$. The required submodule is the intersection of all these M_i.

Proof of Theorem 9.1. We apply Corollary 9.4 with $R = \mathbf{Z}G_{ab}$, $M = G'$ and I the augmentation ideal of R. The conclusion is that we can find $\bigcap_{i=1,2,\dots} MI^i = \gamma_\omega(G)$.

10. The Frattini subgroup

Our last main theorem is

Theorem 10.1. *There is an algorithm which, when a finitely generated metabelian group G is given, finds the Frattini subgroup $\varphi(G)$.*

As might be expected, most of the proof is devoted to establishing a corresponding result for modules. If M is a module over a ring R, the *Frattini submodule* $\varphi_R(M)$ or $\varphi(M)$ is defined to be the intersection of all the maximal submodules of M, (or M itself should there be no such submodules). The critical result which we need is

Proposition 10.2. *There is an algorithm which, when given a finitely generated commutative ring R and a finitely generated R-module M, finds $\varphi_R(M)$.*

Proof. Certainly we can assume that $M \neq 0$, so $\text{Ass}(M) \neq \varnothing$. The first step is to construct the set $\text{Ass}(M)$, using Theorem 8.1. We can then decide whether M is (R-) torsion-free since this is true if and only if $\text{Ass}(M) = \{0\}$.

(i) *If M is torsion-free, then* $\varphi(M) = 0$.

Of course R is a domain in this case. Now there is a free submodule F such that M/F is a torsion module. Because M is finitely generated, there is an $r \neq 0$ in R such that $Mr \subseteq F$. But $M \overset{R}{\simeq} Mr$ since M is torsion-free; thus $\varphi(M) \overset{R}{\simeq} \varphi(Mr)$ and it is easy to see that $\varphi(Mr) \subseteq \varphi(F)$. Also $\varphi(R) =$ the Jacobson radical of R, which is 0 since R is a finitely generated domain. Therefore $\varphi(F) = 0$ and $\varphi(M) = 0$. So $\varphi(M)$ is known in this case. We can therefore assume that M is not torsion-free, and $\text{Ass}(M)$ contains a nonzero prime.

(ii) *Case*: $0 \in \text{Ass}(M)$.

Here R is a domain since 0 is a prime ideal, so the torsion-elements form a submodule T. Let J denote the product of the nonzero primes in $\text{Ass}(M)$; then $TJ^e = 0$ for some $e > 0$, and clearly, $T = \{a \in M \mid aJ^e = 0\}$. Since e can be computed, we can find T.

Next M/T is torsion-free, so (1) shows that $\varphi(M) \subseteq T$. Suppose that L is a maximal submodule of M not containing T; then $M = L + T$ and therefore $MJ^e = LJ^e \leq L$. It follows that $\varphi(M) = T \cap \varphi_0$ where $\varphi_0/MJ^e = \varphi(M/MJ^e)$. But $J^e \neq 0$, so M/MJ^e is a torsion module, and it is clearly enough to find φ_0. Consequently we have reduced to the situation where $0 \notin \text{Ass}(M)$.

(iii) *Case*: $0 \notin \text{Ass}(M)$.

Let $\text{Ass}(M) = \{P_1, \dots, P_k\}$; here each P_i is a nonzero prime. Suppose that L is a maximal submodule of M. Now some positive power of $P_1 \cdots P_k$ annihilates M, so L must contain some MP_i. Now it suffices to find the submodules $\varphi_{R/P_i}(M/MP_i)$; for we need only intersect the preimages of these modules under the natural maps $M \to M/MP_i$ to obtain $\varphi(M)$. If M/MP_i is torsion-free as an R/P_i-module, then $\varphi(M/MP_i) = 0$ by (1). Otherwise the reductions of (2) and (3) are applied to M/MP_i.

Repeated application of this procedure produces chains of prime ideals of R, typically $P_{i_1} \subset P_{i_1 i_2} \subset P_{i_1 i_2 i_3} \subset \cdots$. The procedure will terminate at $P_{i_1 i_2 \cdots i_s}$ if and only if $M/MP_{i_1 i_2 \cdots i_s}$ is torsion-free as an $R/P_{i_1 i_2 \cdots i_s}$-module. Thus $\varphi(M)$ is the intersection of all such $MP_{i_1 i_2 \cdots i_s}$.

The primes $P_{i_1 i_2 \cdots i_s}$ are constructible by Theorem 8.1. They may be visualized as the nodes of a finitary tree T, the nodes at level s of the tree being the $P_{i_1 i_2 \cdots i_s}$. To complete the proof of the constructibility of $\varphi(M)$, we show that T is a finite tree. If T is infinite, it must have infinitely many levels, and hence infinitely many finite paths. Since T is finitary, it follows that there must exist an infinite path. But this is impossible since R is noetherian.

Proof of Theorem 10.1. Let $Q = G_{ab}$, $R = \mathbf{Z}Q$, and $A = G'$. By Proposition 10.2 we can construct $\varphi_R(A)$. We show how to find $\varphi(G)$ via three reductions.

(i) *It is enough to find* $\varphi(G/Z(G))$.

Let L be a maximal subgroup of G. If $Z(G) \not\leq L$, then $G = LZ(G)$ and $A = G' = L' \leq L$. Hence L contains $Z(G)$ or A. We can certainly find $\varphi(G_{ab}) = \varphi_1/A$. Since $Z(G)$ can be found by Theorem 3.5, a finite presentation of $G/Z(G)$ is at hand. If $\varphi(G/Z(G)) = \varphi_2/A$ has been found, we can surely find $\varphi(G) = \varphi_1 \cap \varphi_2$.

(ii) *It is enough to find* $\varphi(G/\varphi_R(A))$.

Let L be a maximal subgroup of G not containing A. Then $G = LA$ and $L \cap A$ is a maximal R-submodule of A. Hence $\varphi_R(A) \leq L$, and it follows that $\varphi_R(A) \leq \varphi(G)$. Thus $\varphi(G/\varphi_R(A)) = \varphi(G)/\varphi_R(A)$, and it suffices to find this subgroup.

(iii) *It can be assumed that* $\varphi_R(A) = 1 = Z(G)$.

An ascending chain of normal subgroups of G

$$1 = M_0 = N_0 \leq M_1 \leq N_1 \leq \ldots$$

is defined by the rules $M_{i+1}/N_i = Z(G/N_i)$ and $N_{i+1}/M_{i+1} = \varphi_{R_i}((G/M_{i+1})')$ where $R_i = Z(G/M_{i+1})_{ab}$. Assume that M_i and N_i have been constructed (as the normal closures of finite subsets). Then a finite presentation of G/N_i is at hand, so we can find $Z(G/N_i) = M_{i+1}/N_i$, and hence M_{i+1}. Now we use a finite presentation of G/M_{i+1}, to find $(G/M_{i+1})'$, and hence $\varphi_{R_i}((G/M_{i+1})') = N_{i+1}/M_{i+1}$, by Proposition 10.2. Therefore the subgroups in the chain can be constructed.

Since G satisfies $\max -n$, there is an integer r such that $M_r = N_r = M_{r+1} = N_{r+1} =$ etc. Clearly this r can be computed. The reductions of (i) and (ii) tell us that it is sufficient to find $\varphi(G/M_r)$. Therefore we may replace G by G/M_r, which allows us to assume that $Z(G) = 1 = \varphi_R(A)$. With these hypotheses, we complete the proof by showing that

(iv) $\varphi(G) = 1$.

Let L be a maximal R-submodule of A not containing $[A, G]$. Then A/L is a noncentral minimal normal subgroup of G/L. A theorem of Newman ([10]; see also [12]) shows that there is a subgroup X satisfying $G = XA$ and $X \cap A = L$. Plainly X is maximal in G, so $\varphi(G) \leq X$. It follows that

$$\varphi(G) \cap [A, G] \leq \varphi_R(A) = 1$$

and therefore $[\varphi(G), G, G] = 1$. Finally $\varphi(G) = 1$ since $Z(G) = 1$.

REFERENCES

1. G. Baumslag, F. B. Cannonito, and C. F. Miller III, *Infinitely generated subgroups of finitely presented groups*. II, Math. Z. **172** (1980), 97–105.
2. ——, *Computable algebra and group embeddings*, J. Algebra **69** (1981), 186–212.
3. G. Baumslag, F. B. Cannonito, D. J. S. Robinson, and D. Segal, *The algorithmic theory of polycyclic-by-finite groups*, J. Algebra **141** (1991), 118–149.
4. G. Baumslag, D. Gildenhuys, and R. Strebel, *Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras*. I, II, J. Pure Appl. Algebra **39** (1986), 53–94; J. Algebra **97** (1985), 278–285.
5. G. Baumslag, U. Stammbach, and R. Strebel, *The free metabelian group of rank* 2 *contains continuously many non-isomorphic subgroups*, Proc. Amer. Math. Soc. **104** (1988), 702.
6. N. Bourbaki, *Commutative algebra*, Springer, Berlin, 1989.
7. P. Gianni, B. Trager, and G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Comput. **6** (1988), 149–167.
8. P. Hall, *Finiteness conditions for soluble groups*, Proc. London Math. Soc. (3) **4** (1954), 419–436.
9. O. G. Harlampovič, *A finitely presented soluble group with insoluble word problem*, Izv. Akad. Nauk Ser. Math. **45** (1981), 852–873.
10. M. F. Newman, *On a class of metabelian groups*, Proc. London Math. Soc. (3) **10** (1960), 354–364.
11. G. A. Noskov, *On conjugacy in metabelian groups*, Mat. Zametki **31** (1982), 495–507.
12. D. J. S. Robinson, *Splitting theorems for infinite groups*, Symposia Math. **17** (1976), 441–470.
13. ——, *A course in the theory of groups*, Springer, New York, 1982.
14. N. S. Romanovskiĭ, *The occurrence problem for extensions of abelian groups by nilpotent groups*, Sibirsk. Mat. Ž. **21** (1980), 170–174.
15. D. Segal, *Decidable properties of polycyclic groups*, Proc. London Math. Soc. (3) **61** (1990), 497–528.
16. A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.
17. ——, *Constructions in a polynomial ring over the ring of integers*, Amer. J. Math. **100** (1978), 685–703.

DEPARTMENT OF MATHEMATICS, CITY COLLEGE, NEW YORK, NEW YORK 10031
E-mail address: gilbert@groups.sci.ccny.cuny.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, IRVINE, CALIFORNIA 92717
E-mail address: fcannoni@math.uci.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS IN URBANA-CHAMPAIGN, URBANA, ILLINOIS 61801
E-mail address: robinson@math.uiuc.edu