RECOGNIZING FREE METABELIAN GROUPS

BY

J.R.J. GROVES AND CHARLES F. MILLER III

Dedicated to the memory of W.W. Boone

1. Introduction

For groups in general many algorithmic problems are known to be recursively unsolvable. But for some special classes of groups one can give algorithms for solving certain decision problems—for example, there is a well-known algorithm to solve the isomorphism problem for finitely presented abelian groups. This paper is concerned with finitely generated metabelian groups. The isomorphism problem for this class is as yet unresolved, but we show there is an algorithm to determine whether or not a suitably given finitely generated metabelian group is free metabelian. A useful algebraic characterization of free metabelian groups is also obtained.

2. Some presentations, algorithms and observations

Let G be a finitely generated metabelian group and A = [G, G] = G' its commutator subgroup. Because finitely generated metabelian groups satisfy max-n, the maximum condition for normal subgroups, G can be defined by finitely many generators subject to the relations which are consequences of the metabelian law plus finitely many additional relations. So G can be presented in the form

(1)
$$G = \langle x_1, \dots, x_n; r_1 = 1, \dots, r_m = 1, G'' = 1 \rangle$$

where the r_j 's are certain words in the x_i and G'' = 1 represents the infinitely many relations corresponding to the metabelian law. We call this a *finite metabelian presentation of G*. Of course such a presentation is a finite description of G even though G may not be finitely presented in the usual sense.

Again because G satisfies max-n, its commutator subgroup A = [G, G] is a finitely generated ZG-module where G acts on A by conjugation. Putting

Received April 8, 1985.

^{© 1986} by the Board of Trustees of the University of Illinois Manufactured in the United States of America

Q = G/A it follows that A is also a finitely generated ZQ-module. Since Q is a finitely generated abelian group the ring ZQ is a finitely generated commutative ring and so, in the terminology of [1], ZQ is submodule computable. We recall briefly that this means the ring operations in the Noetherian ring ZQ are computable and given a finite presentation of a ZQ-module we can effectively present submodules and determine membership in submodules. See [1] for a discussion of algorithms for such rings.

Associated with the short exact sequence

(2)
$$0 \to A \to G \stackrel{\sigma}{\to} Q \to 0$$

where σ is the quotient map from G onto Q, there is a well-known exact sequence of **Z**Q-modules (see [4])

(3)
$$0 \to A \xrightarrow{\rho} \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG \xrightarrow{\tau} IQ \to 0$$

where *IG* and *IQ* are the augmentation ideals of ZG and ZQ respectively. Here the maps are defined by $\rho(a) = 1 \otimes (a - 1)$ and $\tau(q \otimes (y - 1)) = q(\sigma(y) - 1)$. We also have the corresponding augmented exact sequence

(4)
$$0 \to A \xrightarrow{\rho} \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG \xrightarrow{\tau} \mathbb{Z}Q \xrightarrow{\varepsilon} Z \to 0$$

where ε is the augmentation map with kernel Q. Indeed the sequence (2) determines a cohomology class in $H^2(Q, A)$ and the sequences (3) and (4) are the extensions corresponding to (2) under the usual isomorphisms

$$H^2(Q, A) \cong \operatorname{Ext}^2_{\mathbf{Z}O}(\mathbf{Z}, A) \cong \operatorname{Ext}^1_{\mathbf{Z}O}(IQ, A).$$

See [3, Chapter XIV] or [7, Chapter IV, Section 6] concerning these correspondences.

Because of its importance for our considerations we write $M = \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$. In the augmentation ideal *IG* we have the identity $y_1y_2 - 1 = y_1(y_2 - 1) + (y_1 - 1)$ and so in *M* we have $1 \otimes (y_1y_2 - 1) = \sigma(y_1) \otimes (y_2 - 1) + 1 \otimes (y_1 - 1)$. Consequently, if x_1, \ldots, x_n generate *G* as a group then $1 \otimes (x_1 - 1), \ldots, 1 \otimes (x_n - 1)$ generate $M = \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$ as a $\mathbb{Z}Q$ -module.

Assume that G is presented as in (1) and let F be the (absolutely) free group freely generated by x_1, \ldots, x_n . Denote by θ the surjective homomorphism from F to G defined by $\theta(x_i) = x_i$, $i = 1, \ldots, n$ and let

$$\phi = \sigma \circ \theta \colon F \twoheadrightarrow Q.$$

The extensions of these maps to $\mathbb{Z}F$, $\mathbb{Z}G$ and $\mathbb{Z}Q$ are likewise denoted by ϕ , θ and σ .

Now *IF* is a free **Z***F*-module with basis $(x_1 - 1), \ldots, (x_n - 1)$ and the fundamental formula of Fox's free differential calculus asserts that for any $f \in F$ we have

$$(f-1) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} (x_i - 1)$$

where the elements $\partial f / \partial x_i \in \mathbb{Z}F$ are easily computed (see [2, pp. 103–106]). Moreover a theorem of Blanchfield ([2] p. 107) asserts that $f \in [\ker \phi, \ker \phi]$ if and only if

$$\phi\left(\frac{\partial f}{\partial x_i}\right) = 0 \quad \text{for } i = 1, \dots, n.$$

Observe that $\mathbb{Z}Q \otimes_{\mathbb{Z}F} IF$ is the free $\mathbb{Z}Q$ -module with basis

$$1 \otimes (x_1 - 1), \dots, 1 \otimes (x_n - 1).$$

Consequently $1 \otimes (f-1) = 0$ in $\mathbb{Z}Q \otimes_{\mathbb{Z}F} IF$ if and only if $f \in [\ker \phi, \ker \phi]$ because of the fundamental formula and Blanchfield's theorem. Now the induced map $IF \to IG$ has as kernel the abelian group generated by all (f-1) such that $f \in \ker \theta$. So a presentation for $M = \mathbb{Z}Q \otimes_{\mathbb{Z}F} IG \cong$ $\mathbb{Z}Q \otimes_{\mathbb{Z}F} IG$ can be obtained from the free presentation for $\mathbb{Z}Q \otimes_{\mathbb{Z}F} IF$ by adding the relations

$$1\otimes (r_j-1)=0$$

for j = 1, ..., m expressed in the given basis. Explicitly the added relations are

$$\sum_{i=1}^{n} \phi\left(\frac{\partial r_{j}}{\partial x_{i}}\right) \otimes (x_{i} - 1) = 0$$

for j = 1, ..., m. Note that the relations in (1) corresponding to the metabelian law G'' = 1 are unnecessary because of Blanchfield's theorem. Also observe that if G is a free metabelian group on n generators and the relations $r_j = 1$ are absent from (1), then Q is a free abelian group of rank n and $M = \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$ is a free $\mathbb{Z}Q$ -module of rank n. The converse is also true and will be proved in the next section.

Turning to algorithmic aspects we observe that given a finite metabelian presentation for G as in (1), we can effectively find a finite presentation of the ZQ-module $M = ZQ \otimes_{ZG} IG$. Now A is generated as ZQ-module by the commutators

$$x_i x_j x_i^{-1} x_j^{-1} = [x_i, x_j]$$

and ρ embeds A in M. So A is isomorphic to the submodule of M generated by the finite set of elements $1 \otimes ([x_i, x_j] - 1)$ say with $1 \le i, j \le n$. Because ZQ is submodule computable (see [1]) and we have a presentation for M we can effectively find a presentation for A. This is summarized as follows:

THEOREM 1. There is a recursive procedure which when applied to a finite metabelian presentation (1) of a metabelian group G yields finite presentations for the ZQ-modules A = [G, G] and $M = ZQ \otimes_{ZG} IG$ where Q = G/A is the abelianization of G. Moreover if G is free metabelian of rank n then Q is free abelian of rank n and M is a free ZQ-module of rank n.

We now make a few additional observations concerning the sequence (4) and presentations of M and A. Since $\tau: M \twoheadrightarrow IQ \subseteq \mathbb{Z}Q$ is $\mathbb{Z}Q$ -linear, it follows that τ extends uniquely to an anti-derivation d of degree -1 of the exterior algebra $\Lambda(M)$ defined by the formula

(5)
$$d_{k}(m_{1} \wedge \cdots \wedge m_{k}) = \sum_{i=1}^{k} (-1)^{i-1} \tau(m_{i}) m_{1} \wedge \cdots \wedge m_{i-1} \wedge m_{i+1} \wedge \cdots \wedge m_{k}$$

with $d_1 = \tau$. Now $d_{i-1} \circ d_i = 0$ and in particular image $d_2 \subset \ker \tau$ so we have a complex

(6)
$$\rightarrow \Lambda^3 M \xrightarrow{d_3} \Lambda^2 M \xrightarrow{d_2} M \xrightarrow{\tau} \mathbb{Z} Q \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0.$$

This sequence is not exact at each term although we know it is exact at $\mathbb{Z}Q$ and \mathbb{Z} . Moreover we claim image $d_2 = \ker \tau$ so the sequence (6) is always exact

at *M*.

To see this observe that for any $y_1, y_2 \in G$,

(7)
$$1 \otimes (y_1 y_2 y_1^{-1} y_2^{-1} - 1) = (\sigma(y_1) - 1) \otimes (y_2 - 1) - (\sigma(y_2) - 1) \otimes (y_1 - 1) = d_2 (1 \otimes (y_1 - 1) \land 1 \otimes (y_2 - 1)).$$

Now A is generated as a ZQ-module by the commutators $x_i x_j x_i^{-1} x_j^{-1} = [x_i, x_j]$, with say i < j, so image $\rho = \ker \tau$ is generated by elements of the form of (7). From this it follows that $\ker \tau = \text{image } d_2$ as claimed. Moreover it follows that if $h_1, \ldots, h_i \in G$ are such that $1 \otimes (h_1 - 1), \ldots, 1 \otimes (h_k - 1)$ generate M as ZQ-module, then the elements $[h_i, h_j]$ generate A as ZQ-module.

In the special case that G is free metabelian and so Q is free abelian and M is a free module of rank the same as Q the sequence (6) is actually exact and is the familiar Koszul resolution for Z as ZQ-module [3, p. 193]. In this case all of the $\Lambda^k M$ are finitely generated free ZQ-modules and exactness implies

$$A \cong \Lambda^2 M / d_3(\Lambda^3 M).$$

If we write $e_i = 1 \otimes (x_i - 1)$ the the module $\Lambda^2 M$ is free with basis $e_i \wedge e_j$, $1 \leq i < j \leq n$. From (7) we recall that the image of $e_i \wedge e_j$ under d_2 corresponds to the element $[x_i, x_j] \in A$. Now $\Lambda^3 M$ has as free basis $e_i \wedge e_j \wedge e_k$, $1 \leq i < j < k \leq n$. So if we observe that $\tau(e_i) = (\sigma(x_i) - 1)$ the formula (5) for d_3 gives explicitly a presentation for the module A in the form $\Lambda^2 M/d_3(\Lambda^3 M)$. Moreover, using the identity for $y \in G$, $a \in A$,

$$(\sigma(y) - 1) \otimes (a - 1) = 1 \otimes ([y, a] - 1)$$

one calculates that the image of $d_3(e_i \wedge e_j \wedge e_k)$ under d_2 corresponds to the instance of the Jacobi identity

$$\left[x_i, \left[x_j, x_k\right]\right] \left[x_j, \left[x_k, x_i\right]\right] \left[x_k, \left[x_i, x_j\right]\right] = 1$$

in A. It is known (and easily shown by calculation) that metabelian groups satisfy this version of the Jacobi identity. But we conclude that in case G is free metabelian A = [G, G] can be presented as **Z**Q-module as having generators the elements $[x_i, x_j]$ (i < j) subject to defining relations the above finite set of instances of this Jacobi identity.

3. A criterion for freeness

As in the previous section let G denote a finitely generated metabelian group, A = [G, G] = G' and Q = G/A. Again for $M = \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$ we have the exact sequence (3). We will show that if Q is free abelian of rank k and $M = \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$ is a free $\mathbb{Z}Q$ -module of rank k then G is a free metabelian group of rank k.

Henceforth we assume Q is free abelian of rank k with basis $\{z_1, \ldots, z_k\}$. For any *m*-tuple $(a_1, \ldots, a_m) \in (\mathbb{Z}Q)^m$, if

$$\psi\{(a_1,\ldots,a_m)\}=(a'_1,\ldots,a'_m)$$

for ψ a **Z***Q*-automorphism of $(\mathbb{Z}Q)^m$ we will say that (a_1, \ldots, a_m) and (a'_1, \ldots, a'_m) are unimodularly equivalent (u.e.). Also (a_1, \ldots, a_m) will be called unimodular if (a_1, \ldots, a_m) is u.e. to $(1, 0, 0, \ldots, 0)$.

From the work of Quillen, Suslin and Swan on the solution of Serre's problem (see [5, Corollary 4.12, p. 147] and [6, Theorem 4.51, p. 139]) we know

that (a_1, \ldots, a_m) is unimodular if and only if there exist $(b_1, \ldots, b_m) \in (\mathbb{Z}Q)^m$ with $\sum_{i=1}^m a_i b_i = 1$. Hence (a_1, \ldots, a_m) is unimodular if and only if the ideal of $\mathbb{Z}Q$ generated by $\{a_1, \ldots, a_m\}$ is $\mathbb{Z}Q$ itself.

THEOREM 2. Let $\{\alpha_1, \ldots, \alpha_m\} \subseteq IQ$ generate IQ as a ZQ-module. Then

$$(\alpha_1,\ldots,\alpha_m)$$

is u.e. to

$$(z_1 - 1, \ldots, z_k - 1, 0, \ldots, 0)$$

Proof. By induction on k, the rank of Q. For k = 0 there is nothing to prove.

Let

$$\alpha_i = \overline{\alpha}_i(z_k - 1) + \alpha'_i(z_1, \dots, z_{k-1}).$$

Then it is clear that $\{\alpha'_1, \ldots, \alpha'_m\}$ generate the augmentation ideal of the subgroup generated by z_1, \ldots, z_{k-1} . Thus by the induction hypothesis

 $(\alpha'_1,\ldots,\alpha'_m)$

is u.e. to

 $(z_1 - 1, \ldots, z_{k-1} - 1, 0, \ldots, 0)$

and so $(\alpha_1, \ldots, \alpha_m)$ is u.e. to $(\beta_1, \ldots, \beta_m)$

$$\boldsymbol{\beta}_i \equiv \begin{cases} z_i - 1, & 1 \le i \le k - 1\\ 0, & i \ge k \end{cases} \mod \mathbb{Z}Q(z_k - 1).$$

The β_i still generate IQ as $\mathbb{Z}Q$ -module and so $\sum_{i=1}^{m} c_i \beta_i = z_k - 1$ for some $c_i \in \mathbb{Z}Q$. Observe that there is considerable freedom in the choice of the c_i 's. In fact, for any $\lambda \in \mathbb{Z}Q$ and any $i \neq j \in \{1, \ldots, m\}$ we can replace c_i, c_j by $c_i - \lambda \beta_i, c_j + \lambda \beta_i$ respectively. Now using the fact that

$$\beta_i \equiv z_i - 1 \mod \mathbb{Z}Q(z_k - 1)$$
 for $1 \le i \le k - 1$

we can assume, firstly, that for $i \ge k$, $c_i \equiv b_i \mod \mathbb{Z}Q(z_k - 1)$ for suitable $b_i \in \mathbb{Z}$ and, secondly, by successive reduction that for i < k,

$$c_i = c'_i(z_1, \dots, z_i) \mod \mathbb{Z}Q(z_k - 1)$$

where $c'_i(z_1, \ldots, z_i)$ lies in the group ring of the subgroup generated by z_1, \ldots, z_i .

But now, putting $z_j = \cdots = z_i = 1$ in the equation $\sum_{i=1}^{m} c_i \beta_i = z_i - 1$ we obtain the congruences

$$\sum_{i=1}^{j-1} c'_i(z_i - 1) \equiv 0 \mod \mathbb{Z}Q(z_k - 1) \quad (j = 2, \dots, k)$$

For j = 2 this yields $c'_1 \equiv 0$. For j = 3 it yields $c'_1(z_1 - 1) + c'_2(z_2 - 1) \equiv 0$ and so $c'_2 \equiv 0$. Thus clearly $c'_i \equiv 0$ for i = 1, ..., k - 1.

Now, if J is the ideal of ZQ generated by $\{c_1, \ldots, c_m\}$ we clearly have $z_k - 1 \in J$. But then as,

$$(z_k - 1)|c_i$$
 for $i = 1, ..., k - 1$

and

$$c_i \equiv b_i \mod \mathbb{Z}Q(z_k - 1) \quad \text{for } i \ge k$$

J is generated by $\{z_k - 1, b_k, \dots, b_m\}$. Since the $b_k, \dots, b_m \in \mathbb{Z}$ we may put

$$t = \gcd(b_k, \dots, b_m)$$

and observe that J is also generated by $\{z_k - 1, t\}$. But, as

$$z_k - 1 = \sum_{i=1}^m c_i \beta_i,$$

we have

$$z_k - 1 \in JIQ \le (IQ + t\mathbf{Z}Q)IQ \le (IQ)^2 + tIQ.$$

Thus $t = \pm 1$ and so $J = \mathbb{Z}Q$. Hence (c_1, \ldots, c_m) is a unimodular sequence and so, as $\sum_{i=1}^{m} c_i \beta_i = z_k - 1$, the sequence $(\beta_1, \ldots, \beta_m)$ is equivalent to a sequence $(\gamma_1, \ldots, \gamma_m)$ with $\gamma_k = z_k - 1$. Clearly by further unimodular (in fact, elementary) operations, we can assume that $\gamma_i = \gamma_i(z_1, \ldots, z_{k-1})$ for $i \neq k$.

Now by the inductive hypothesis on k,

$$(\gamma_1,\ldots,\gamma_{k-1},\gamma_{k+1},\ldots,\gamma_m)$$

is u.e. to

$$(z_1 - 1, \ldots, z_{k-1} - 1, 0, \ldots, 0)$$

and so

 $(\gamma_1,\ldots,\gamma_m)$

is u .e. to

$$(z_1 - 1, \ldots, z_k - 1, 0, \ldots, 0)$$

as required. This completes the proof of Theorem 2.

COROLLARY 1. If $M = \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$ can be generated as a $\mathbb{Z}Q$ -module by m generators, then G can be generated by m generators.

Proof. Suppose $\{\alpha_1, \ldots, \alpha_m\}$ generates *M*. Then $\{\tau(\alpha_1), \ldots, \tau(\alpha_m)\}$ generates *IQ* and so, by Theorem 2, the sequence

$$(\tau(\alpha_1),\ldots,\tau(\alpha_m))$$

is u.e. to

$$(z_1 - 1, \ldots, z_k - 1, 0, \ldots, 0).$$

Hence we can find β_1, \ldots, β_m generating M such that $\tau(\beta_i) = z_i - 1$ for $i \le k$ and $\tau(\beta_i) = 0$ for i > k. Choose $g_i \in G$ with $\sigma(g_i) = z_i$.

If
$$\tau(\beta_i) = z_i - 1$$
 then $\tau(\beta_i - 1 \otimes (g_i - 1)) = 0$. Hence
 $\beta_i - 1 \otimes (g_i - 1) = 1 \otimes (a - 1)$ for some $a \in A$

and so $\beta_i = 1 \otimes (g_i - 1) + 1 \otimes (a - 1) = 1 \otimes (ag_i - 1)$. Thus for each *i* we can write $\beta_i = 1 \otimes (h_i - 1)$ for $h_i \in G$. We claim $\{h_1, \ldots, h_m\}$ generates G.

Since $\sigma(h_i) = z_i$ it is clear that $\langle h_1, \ldots, h_m \rangle A = G$. But as $A = \operatorname{im} \tau = \operatorname{im} d_2$ from (6) and (7) it follows that ker $\tau \cong A$ is generated as $\mathbb{Z}Q$ -module by $1 \otimes ([h_i, h_j] - 1)$. So if $a \in A$ for some $\gamma_{ij} \in \mathbb{Z}Q$,

$$1 \otimes (a-1) = \sum \gamma_{ij} \otimes ([h_i, h_j] - 1) = 1 \otimes (\prod [h_i, h_j]^{\gamma_{ij}} - 1).$$

Since ρ is injective, $a = \prod [h_i, h_j]^{\gamma_{ij}} \in \langle h_1, \dots, h_m \rangle$. Whence $\{h_1, \dots, h_m\}$ generates G. This completes the proof.

COROLLARY 2. If Q is free abelian of finite rank k and $M = \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$ is a free $\mathbb{Z}Q$ -module of rank k then G is free metabelian of rank k.

Proof. By Corollary 1, G is k-generator and so there is an epimorphism ψ from a free metabelian group H of rank k onto G and we can identify Q with H/[H, H]. But this induces an epimorphism $\psi^*: \mathbb{Z}Q \otimes_{\mathbb{Z}H} IH \to \mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$ of isomorphic Noetherian modules which must therefore be an isomorphism. But $\psi^*|_{H'}$ is then also an isomorphism, so ψ was an isomorphism and G is free as claimed. This proves Corollary 2.

The solution to Serre's problem [5, p. 147] gives that for a finitely generated free abelian group Q, finitely generated projective $\mathbb{Z}Q$ -modules are free. From [1] we know there is an algorithm to determine whether or not a finitely presented $\mathbb{Z}Q$ -module is projective, hence free and if so determine its rank. Combining this with Theorem 1 and Corollary 2 we obtain the following:

COROLLARY 3. There is a recursive procedure which when applied to a finite metabelian presentation (1) of a metabelian group G determines whether or not G is free metabelian. Indeed, G is free metabelian of rank k if and only if Q is free abelian of rank k and $\mathbb{Z}Q \otimes_{\mathbb{Z}G} IG$ is a free $\mathbb{Z}Q$ -module of rank k and the latter property is recursively recognizable.

Note added July 1985. Since this paper was submitted Karl Gruenberg has drawn our attention to the paper of Linnell, McIsaac and Webb [8] where more general versions of our Theorem 2 and Corollary 1 are obtained for the case Q an arbitrary finitely generated abelian group. While a reference to their work would suffice, our proofs given above seem more elementary and constructive.

REFERENCES

- 1. G. BAUMSLAG, F.B. CANNONITO and C.F. MILLER III, Computable algebra and group embeddings, J. Algebra, vol. 69 (1981), 186-212.
- 2. J. BIRMAN, Braids, links, and mapping class groups, Ann. of Math. Study 82, Princeton University Press, Princeton, N.J., 1975.
- 3. H. CARTAN and S. EILENBERT, Homological algebra, Princeton University Press, Princeton, N.J., 1956.
- 4. P.J. HILTON and U. STAMMBACH, A course in homological algebra, Graduate Texts in Mathematics, no. 4, Springer-Verlag, New York, 1071.
- 5. T.Y. LAM, Serre's conjecture, Lecture Notes in Mathematics, no. 635, Springer-Verlag, Berlin, 1978.
- 6. J.J. ROTMAN, An introduction to homological algebra, Academic Press, New York, 1979.
- 7. S. MACLANE, Homology, Springer-Verlag, New York, 1963.
- 8. P.A. LINNELL, A.J. MCISAAC and P.J. WEBB, Bounding the number of generators of a metabelian group, Archiv Math., vol. 38, (1982), pp. 501-505.

UNIVERSITY OF MELBOURNE Parkville, Victoria, Australia

254