JOURNAL OF ALGEBRA **142**, 118–149 (1991)

The Algorithmic Theory of Polycyclic-by-Finite Groups*

GILBERT BAUMSLAG

Department of Mathematics, City College, The City University of New York, New York, New York 10021

FRANK B. CANNONITO

Department of Mathematics, University of California, Irvine, California 92664

DEREK J. S. ROBINSON

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801

AND

DAN SEGAL

All Souls College, Oxford, England

Communicated by Marshall Hall, Jr.

Received October 1989

1. INTRODUCTION

A group is said to be *polycyclic-by-finite*, or a *PF-group* for short, if it has a polycyclic normal subgroup of finite index. Equivalently, PF-groups are exactly the groups which have a series of finite length whose infinite factors are cyclic. By a well-known theorem of P. Hall every PF-group is finitely presented—and in fact PF-groups form the largest known section-closed class of finitely presented groups. It is this fact that makes PF-groups natural objects of study from the algorithmic standpoint.

The general aim of the algorithmic theory of PF-groups can be described as the collection of information about a PF-group which can, in principle

* During the final stage of work on this article the authors were visitors at the Mathematical Sciences Research Institute in Berkeley.

0021-8693/91 $3.00

at least, be obtained by machine computation. Somewhat more precisely, the information sought should be capable of being coded by partial recursive functions or, equivalently, be obtainable from the output of a Turing machine.

Polycyclic groups were introduced by K. A. Hirsch in [14]–[17], and their central position in infinite group theory has long been recognized. Under these circumstances it seems remarkable that there has been no systematic study of their algorithmic properties. In fact the literature seems to contain only the solutions of the generalized word problem (Mal'cev [24]) and conjugacy problems (Formanek [10], Remeslennikov [25], Grunewald and Segal [13]), and some results about polycyclic presentations due to Baumslag, Cannonito, and Miller [3];[1] we mention also a fragmentary unpublished dissertation of N. Maxwell which gives algorithms to construct certain subgroups of PF-groups, for example, the Fitting subgroup. In addition Baumslag, Cannonito, and Miller [5] have given an algorithm to construct the homology of a PF-group with coefficients in a finitely generated module.

The present work is an attempt to remedy the situation by giving a systematic account of the algorithmic theory of PF-groups. It should be pointed out that our algorithms are algorithms in the classical sense, and so will rarely satisfy the strict constructivist. Nor have we made any attempt to produce practical algorithms that might lead to computer implementation. We feel however that this is an important topic which merits investigation.

Finally, the reader is reminded that no satisfactory algorithmic theory exists for finitely presented soluble groups; for Kharlampovič [19]—see also Baumslag, Gildenhuys, and Strebel [6]—has shown that even the word problem is in general insoluble for such groups.

Terminological Note. For economy of expression we shall frequently say that "we can find X" if there is an algorithm or recursive procedure which produces X. If X is a subgroup of a PF-group with a given presentation, it is understood that the algorithm furnishes a finite set of generators for X. The phrase "given a PF-group G" will always mean that G is given by means of a specific finite presentation.

Results

As is to be expected, the algorithms which we describe lie at various depths. Those in Section 2 are mainly elementary and most depend only on solubility of the generalized word problem for PF-groups, itself an

[1] To this list should be added the solution of the isomorphism problem for finitely generated nilpotent groups due to Grunewald and Segal, *Ann. of Math.* **112** (1980), 585–617.

elementary result. Under this category are algorithms to find the terms of the lower central series and derived series, and to find the soluble radical.

In Section 3 we prove a fundamental theorem which is the key to obtaining information about subgroups of PF-groups.

THEOREM (3.4). *There is an algorithm which, on being given a PF-group G and a finite subset X of G, produces a finite presentation of the subgroup $\langle X \rangle$ in the generators X.*

Almost all subsequent results rest ultimately on this. The proof is accomplished by constructing a so-called consistent polycyclic presentation in a polycyclic group. Consequences of (3.4) are algorithms to find the Hirsch number and the maximum finite normal subgroup of a PF-group, and to find a normal poly-infinite cyclic subgroup of finite index.

The algorithms developed in Section 4 and later sections depend on some constructive commutative algebra, namely an algorithm which produces a finite presentation of the unit group of an algebraic number field; this is essentially the work of Borevič and Šafarevič [8]. The first main result obtained on this basis is

THEOREM (4.1). *There is an algorithm which, on being given a finite subset X of $GL(n, \mathbb{Z})$, decides if $\langle X \rangle$ is a PF-group, and if so, finds a finite presentation of it.*

In view of the well-known theorem of Auslander [1] and Swan [34] that every PF-group is isomorphic with a subgroup of some $GL(n, \mathbb{Z})$, a PF-group can always be given by specifying finitely many elements of $GL(n, \mathbb{Z})$ as generators. Then (4.1) makes it possible to apply to a PF-group given in this manner any of the algorithms developed for PF-groups defined by a finite presentation. Other consequences of the constructive commutative algebra are algorithms to find the Fitting subgroup, the centre, and the FC-centre of a PF-group (Theorems 5.1, 5.2, and 5.5).

Derivations from a PF-group G to a $\mathbb{Z}G$-module which is finitely generated as an abelian group play a prominent role in Section 6, being instrumental in the production of algorithms that perform some standard group theoretic constructions. In the following results it is assumed that a PF-group G is given, together with two finite subsets X and Y. Write $H = \langle X \rangle$ and $K = \langle Y \rangle$.

THEOREM (6.3). *We can find $H \cap K$.*

THEOREM (6.5). *We can find the centralizer $C_K(H)$.*

THEOREM (6.8). *We can find the normalizer* $N_K(H)$.

Among applications of these results are: (i) an algorithm to find the normal core of a subgroup (6.4); (ii) the solution of a generalized conjugacy problem applicable to finite sets of elements and subgroups (6.9).

Finite subgroups of PF-groups are featured in Section 7. Recall that Mal'cev [23] showed that the finite subgroups of a polycyclic group fall into finitely many conjugacy classes. The same is true of PF-groups. This opens up the possibility of obtaining information about the finite subgroups of a PF-group, even although they may be infinite in number.

THEOREM (7.1). *There is an algorithm which, when given a PF-group G, produces finite subsets* $X_1, X_2, ..., X_k$ *such that the* $\langle X_i \rangle$ *are finite non-conjugate subgroups whose conjugates account for all the finite subgroups of G.*

It is apparent that from this we can tell if a PF-group is torsion-free. Another application of (7.1) is

THEOREM (7.7). *There is an algorithm which, when given a PF-group G and a finite subset X of G, decides if* $\langle X \rangle$ *is permutable in G.*

Here $H = \langle X \rangle$ is said to be *permutable* in G if and only if $HK = KH$ for all subgroups K. The final section is entirely devoted to proving

THEOREM (8.1). *There is an algorithm which, on being given a PF-group G, finds the Frattini subgroup* $\varphi(G)$ *of G.*

Perhaps because of the highly non-constructive form of the definition of the Frattini subgroup this has proved to be the most difficult algorithm to produce. The proof of (8.1) calls for the construction of the Frattini submodule of a module over a PF-group which is finitely generated as an abelian group. We have not been able to find results of this character in the literature of constructive commutative algebra.

It is tempting to conclude from these results that there is an algorithm to solve any well-posed problem about PF-groups. However, this is by no means the case. Indeed some years ago Remeslennikov [26] observed that there is no algorithm to decide of a finitely generated nilpotent group G whether G/P can be mapped epimorphically onto G/Q where P, Q are given subgroups of the centre of G. This rests on the insolubility of Hilbert's Tenth Problem. For more insolubility results of this kind see the forthcoming paper of Segal [31].

In conclusion we mention that the paper of Segal just referred to contains a solution of the isomorphism problem for PF-groups, as well as

a variety of algorithms relating to automorphisms of a PF-group. Segal's paper may be regarded as a continuation of the present work.

Some Open Questions. Are the algorithms to decide if a PF-group is residually nilpotent or residually finite-p? Is there an algorithm to find the minimum number of generators of a PF-group?

2. Basic Algorithms

We begin by recalling the positive solutions of the word problem and generalized word problem for PF-groups.

Proposition (2.1). *There is an algorithm which, when given a PF-group G and an element g of G (as a word in the generators), decides if g equals the identity.*

Proposition (2.2). *There is an algorithm which, when given a PF-group G and elements $g, g_1, ..., g_n$ of G, decides if $g \in \langle g_1, ..., g_n \rangle$.*

The usual way to prove these results is by means of what may be called the *local-global principle.* Take the case of (2.1), and keep in mind that G is residually finite [16]. Two recursive procedures are set in motion. The first constructs all finite groups in increasing orders—say by means of their group tables—and finds the finitely many homomorphisms θ_i from G into each finite group, using the finite presentation of G. It tests to see if g^{θ_i} equals the identity and stops if this ever fails to hold. The second procedure simply enumerates all consequences of the defining relators and looks for the word g; it stops if g appears. Either the first procedure stops and $g \neq 1$ or the second stops and $g = 1$.

Proposition (2.2) can be proved in the same way, using the fact that the subgroup $\langle g_1, ..., g_n \rangle$ is closed in the profinite topology (Mal'cev [24]; for a simple proof see [30, Chap. 1, Exercise 11]). Thus if $g \notin \langle g_1, ..., g_n \rangle$, this can be detected modulo a normal subgroup of finite index.

Proposition (2.3) [10, 25]. *There is an algorithm which, when given a PF-group G and elements x, y of G, decides if x and y are conjugate in G.*

Proposition (2.4) [13]. *There is an algorithm which, when given a PF-group G and finite subsets X and Y of G, decides if $\langle X \rangle$ and $\langle Y \rangle$ are conjugate in G.*

Both results follow quickly by the local-global method once it is shown that two elements (subgroups) which are not conjugate in a PF-group G

have non-conjugate images in some finite image of G. For the latter see [10, 25, 13] or [30, Chap. 4]; the proofs involve non-trivial algebraic number theory.

We come now to an extremely simple result that is used constantly.

LEMMA (2.5) (The Normal Closure Lemma). *There is an algorithm which, when given a PF-group G and finite subsets X, Y of G, finds the normal closure of X in $\langle X, Y\rangle$.*

Proof. Let $Y=\{y_1, ..., y_n\}$, and define subsets X_i recursively by

$$X_0 = X \qquad \text{and} \qquad X_{i+1} = X_i \cup \bigcup_{j=1}^{n} (X_i^{y_j} \cup X_i^{y_j^{-1}}).$$

If $H_i = \langle X_i\rangle$, then $H_1 \leqslant H_2 \leqslant \cdots$, and by the maximal condition there is an i for which $H_i = H_{i+1}$. Clearly H_i is the normal closure of X in $\langle X, Y\rangle$. Now $H_i = H_{i+1}$ if and only if $X_{i+1} \subseteq H_i$. For $i = 0, 1, 2, ...$ use (2.2) to decide if this inclusion holds; eventually such an i will appear.

COROLLARY (2.6). *There are algorithms which, when given a PF-group G and a finite subset X of G, find the terms of the derived series and the lower central series of $\langle X\rangle$.*

If $X=\{x_1, ..., x_m\}$ and $\gamma_i(\langle X\rangle) = \langle y_1, ..., y_n\rangle$, then $\gamma_{i+1}(\langle X\rangle)$ is the normal closure of the set of all $[x_j, y_k]$ in $\langle X\rangle$. By (2.5) we can find this. Thus the result for the lower central series follows by induction on i. The assertion for the derived series is an immediate consequence.

COROLLARY (2.7). *There is an algorithm which, when given a PF-group G, produces a recursive enumeration of the normal subgroups of finite index in G.*

Proof. Enumerate homomorphisms θ_i from G into all the finite groups, and find a finite presentation of each $\operatorname{Im}\theta_i$. Then $\operatorname{Ker}\theta_i$ is the normal closure in G of the defining relators as words in the generators of G. By (2.5) we can find a finite set of generators for $\operatorname{Ker}\theta_i$. All normal subgroups of finite index are found by this procedure.

PROPOSITION (2.8). *There is an algorithm which finds the soluble radical of a given PF-group G.*

Proof. Using (2.7), enumerate pairs (N, i) where N is a normal subgroup with finite index in G and i is a natural number. For each pair find $N^{(i)}$, the ith term of the derived series, using (2.6), and decide if $N^{(i)}=1$ using (2.1). Eventually we shall discover a pair (N, i) such that $N^{(i)}=1$.

Find a finite presentation of the finite group G/N by adding the generators of N to the relators of G. Find the soluble radical of G/N by enumeration, say S/N. Then S is the soluble radical of G.

COROLLARY (2.9). *There are algorithms which decide if a given PF-group G is soluble, supersoluble, or nilpotent.*

Proof. Find the soluble radical S and decide if $S = G$ (using (2.2)). Thus we can decide if G is soluble and hence polycyclic. As for the other properties, we can invoke theorems of Baer [2] and Hirsch [15] which assert that if a polycyclic group is not supersoluble (nilpotent), then some finite quotient is not supersoluble (nilpotent): the local-global method can then be used. Alternatively we could appeal to algorithms of Baumslag, Cannonito, and Miller [4] which apply to finitely presented soluble groups.

PROPOSITION (2.10). *There is an algorithm which, when given a PF-group G and a natural number m, finds the mth power $G^m = \langle g^m \mid g \in G \rangle$.*

Proof. Using (2.8), find the soluble radical S of G. By enumerating finite subsets and using (2.2) find a set of generators $\{x_1, ..., x_n\}$ of S such that $x_i^{x_j} \in \langle x_1, ..., x_{j-1} \rangle$ for $i < j$, $i, j = 1, ..., n$. Such a subset exists since S is polycyclic. Find $|G : S|$. Then $|G : G^m| \leqslant m^n |G : S| = l$, say. Enumerate the finitely many normal subgroups of index at most l, as in (2.7). Pick out from these the subgroups N such that G/N has exponent dividing m. The smallest such subgroup is G^m.

PROPOSITION (2.11). *There is an algorithm which, when given a PF-group G and a finite subset X of G, decides whether $\langle X \rangle$ is subnormal in G.*

Proof. Let $H = \langle X \rangle$. Recall the theorem of Kegel [18] that H is subnormal in G if and only if HN/N is subnormal in G/N for all normal subgroups N of finite index in G. Also recall the series of successive normal closures of H in G; this is the descending series $\{H_i \mid i = 0, 1, ...\}$ with $H_0 = G$ and $H_{i+1} = \langle H^{H_i} \rangle$, the normal closure of H in H_i. The subgroup H is subnormal in G if and only if some H_i equals H.

Two procedures are set in motion. The first constructs homomorphisms from G to all finite groups and checks to see if the image of H is subnormal: if not, it stops. The second procedure finds successively $H_1, H_2, ...$ using (2.5), and tests to see if $H = H_i$, using (2.2). If this happens, the procedure stops. If the first procedure stops, H is not subnormal: if the second procedure stops, H is subnormal.

3. Polycyclic Presentations

By a *polycyclic presentation* π we mean a finite presentation of a group in generators $x_1, x_2, ..., x_n$ with defining relations of the following forms:

(i) $x_i^{x_j} = v_{ij}(x_1, ..., x_{j-1})$ and $x_i^{x_j^{-1}} = v'_{ij}(x_1, ..., x_{j-1})$ where $1 \leqslant i < j \leqslant n$;

(ii) $x_i^{e_i} = u_i(x_1, ..., x_{i-1})$ where $1 < e_i \leqslant \infty$, and $1 \leqslant i \leqslant n$. (If $e_i = \infty$, the relation is vacuous.)

Here, of course, v_{ij}, v'_{ij}, u_i are words. This is a slight adaptation of the definition in [3]. Clearly a group has a polycyclic presentation if and only if it is a polycyclic group.

For $i = 1, 2, ..., n-1$, let π_i be the sub-presentation obtained from π by omitting generators $x_{i+1}, ..., x_n$ and deleting all relations involving these elements. Then π_i is also a polycyclic presentation. Let G and H_i be the groups presented by π and π_i, respectively. Also let $G_i = \langle x_1, ..., x_i \rangle$. Thus $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$ is a series in G with cyclic factors. There are obvious homomorphisms $H_i \to H_{i+1}$ and epimorphisms $H_i \to G_i$ which make the following diagram commute:

$$\begin{array}{ccccccccc} 1 = H_0 & \to & H_1 & \to & \cdots & \to & H_{n-1} & \to & H_n = G \\ \downarrow & & \downarrow & & & & \downarrow & & \downarrow \\ 1 = G_0 & \subsetneq & G_1 & \subsetneq & \cdots & \subsetneq & G_{n-1} & \subsetneq & G_n = G. \end{array}$$

Lemma (3.1). *With the above notation, the following statements about the presentation π are equivalent:*

(i) *the maps $H_i \to H_{i+1}$ are monomorphisms;*

(ii) *H_i and G_i are isomorphic for all i;*

(iii) *the maps $H_i \to G_i$ are isomorphisms.*

Proof. Easy diagram chases show that (i) implies (ii) and (iii) implies (i). The hopfian property of polycyclic groups shows that (ii) implies (iii).

A polycyclic presentation will be called *consistent* if it has the properties of (3.1)—the term "honest" is used in [3]. Evidently every polycyclic group has a consistent polycyclic presentation.

Proposition (3.2). *There is an algorithm which can decide if a given polycyclic presentation π is consistent.*

This is part of Theorem 4.3 of [3]. We briefly review the proof, taking the opportunity to correct a slight omission.

Proof. We use the notation introduced above. By induction on $n > 1$ it

can be assumed that the presentation π_{n-1} is consistent. Then π will be consistent if and only if the assignments $x_i \mapsto v_{in}(x_1, ..., x_{n-1})$ and $x_i \mapsto v'_{in}(x_1, ..., x_{n-1})$ determine automorphisms of H_{n-1} the first of which fixes $u_n(x_1, ..., x_{n-1})$, its e_nth power being just conjugation in H_{n-1} by $u_n(x_1, ..., x_{n-1})$, in case $e_n \neq \infty$. The solution of the word problem allows us to decide if these conditions hold.

The next result is concerned with the construction of a consistent polycyclic presentation from an arbitrary finite presentation of a polycyclic group.

THEOREM (3.3). *There is an algorithm which, when a polycyclic group G is given, finds a consistent polycyclic presentation of G.*

Proof. Recall that, given two finite presentations of a group, there is a finite sequence of elementary Tietze transformations which, when applied to the first presentation, produces the second one [22, 1.5]. Observe also that the set of all finite sequences of elementary Tietze transformations is recursively enumerable. Starting with the given finite presentation of G, apply finite sequences of Tietze transformations, and, when a polycyclic presentation appears, use (3.2) to test it for consistency. Eventually a consistent presentation will be found by this procedure.

One would expect a consistent polycyclic presentation to be the most appropriate vehicle for the production of practical algorithms for a polycyclic group. For example, such algorithms exist to solve the word problem and the generalized word problem [3, Sect. 4].

Finite Presentations of Subgroups of PF-Groups

The next theorem is fundamental in the algorithmic study of subgroups of PF-groups. A version of it appears in [3, Theorem 4.3]; it has also been found by N. Maxwell.

THEOREM (3.4). *There is an algorithm which, when given a PF-group G and a finite subset X, finds a finite presentation for $\langle X \rangle$ in the generators X.*

Proof. Let $H = \langle X \rangle$. By (2.8) we can find the soluble radical S of G. Since $|G : S|$ is finite, the Reidemeister–Schreier procedure can be used to produce a finite presentation of S. Use (3.3) to produce a consistent polycyclic presentation of S, with generators $s_1, ..., s_n$, say. Let $S_i = \langle s_1, ..., s_i \rangle$; we suppose the s_i to be labelled so that $1 = S_0 \lhd S_1 \lhd \cdots \lhd S_n = S$.

Find a finite presentation of HS/S in the xS, $x \in X$; if the relators are

$r_1, ..., r_l$, then $H \cap S$ is the normal closure in H of $r_1(\mathbf{x}), ..., r_l(\mathbf{x})$. Use the Normal Closure Lemma to find a finite set of generators for $H \cap S = H_0$.

A finite presentation of the cyclic group S/S_{n-1} is at hand, so we can use it to find a finite presentation of $H_0/H_0 \cap S_{n-1}$. Just as above, we find a finite set of generators for $H_0 \cap S_{n-1}$. Induction on $n > 0$ yields a finite presentation for $H_0 \cap S_{n-1}$. Combining the presentations for $H_0 \cap S_{n-1}$, $H_0/H_0 \cap S_{n-1}$, and H/H_0 in the standard manner (see [30, Chap. 8, Lemma 10], we obtain a finite presentation of H. This may now be transformed in the usual way into a finite presentation in the generators X.

There are numerous applications of (3.4); one of the most frequently used is

PROPOSITION (3.5). *There is an algorithm which, when a PF-group G and a finite subset X of G are given, finds $h(\langle X \rangle)$, the Hirsch number of $\langle X \rangle$.*

Proof. Find a finite presentation of $\langle X \rangle$ using (3.4), and then find a consistent polycyclic presentation of the soluble radical of $\langle X \rangle$ by (2.8) and (3.3). Then $h(\langle X \rangle)$ equals the number of infinite exponents in the latter presentation.

COROLLARY (3.6). *There are algorithms which, when a PF-group G and a finite subset X of G are given, decide if $\langle X \rangle$ is finite and if $|G : \langle X \rangle|$ is finite.*

For $\langle X \rangle$ is finite if and only if $h(\langle X \rangle) = 0$, and $|G : \langle X \rangle|$ is finite if and only if $h(\langle X \rangle) = h(G)$.

LEMMA (3.7). *There is an algorithm which, when given a PF-group G, decides if G is infinite and, if so, finds a non-trivial free abelian normal subgroup of G.*

Proof. The first part follows from (3.6). Assume G infinite. Enumerate finite subsets of G, form the subgroup generated by each one, and test for commutativity, and normality (using (2.1) and (2.2)). If both hold, determine if the Hirsch number of the subgroup is positive. Eventually the procedure will produce an infinite abelian normal subgroup A. Find a presentation of A using (3.4), and use it to compute the order t of its torsion subgroup. (Here we are invoking a standard procedure for finitely generated abelian groups.) Then A^t is a subgroup of the type sought.

LEMMA (3.8). *There is an algorithm which, when given PF-groups G and H and a homomorphism $\theta: G \to H$ (by means of its effect on the generators of G), finds* Ker θ.

Proof. Find a finite presentation of Im θ by (3.4), and hence of $G/\text{Ker}\,\theta$. The Normal Closure Lemma produces a finite set of generators for Ker θ.

COROLLARY (3.9). *There is an algorithm which, when given a PF-group G and finite subsets X and Y such that $\langle Y\rangle \lhd \langle X, Y\rangle$, finds $\langle X\rangle \cap \langle Y\rangle$.*

Proof. Let $H = \langle X\rangle$ and $K = \langle Y\rangle$. Define $\theta: H \to HK/K$ by $h^\theta = hK$. Thus Ker $\theta = H \cap K$. The result follows from (3.4) and (3.8).

PROPOSITION (3.10). *There are algorithms which, when given a PF-group G, can* (i) *decide if G is a poly-infinite cyclic group, and* (ii) *construct a poly-infinite cyclic normal subgroup of finite index.*

Proof. A finite presentation of G/G' is at hand, so we can find the torsion-subgroup T/G'. Decide if $T = G$ using (2.2). If so, then G is not poly-infinite cyclic unless $G = 1$. If $T \neq G$, find a finite presentation of T. Now $h(T) < h(G)$, and G is poly-infinite cyclic if and only if T is. But this can be decided by induction on $h(G)$.

For the second part, enumerate normal subgroups of finite index in G and test each one to see if it is poly-infinite cyclic. A well-known theorem of Hirsch [15] guarantees that such a subgroup will appear eventually.

The next algorithm finds the maximum finite normal subgroup; this frequently used result was found by Maxwell.

THEOREM (3.11). *There is an algorithm which, when given a PF-group G, finds its maximum finite normal subgroup.*

Proof. Let T denote the maximum finite normal subgroup of G. If $h(G) = 0$, then $T = G$. Otherwise use (3.7) to find a non-trivial torsion-free abelian normal subgroup A of G. We have a finite presentation of G/A and $h(G/A) < h(G)$, so by induction on $h(G)$ we can find the maximum finite normal subgroup of G/A, say T_0/A. Clearly $T \leqslant C_{T_0}(A) = C$, say. By (3.4) we can find a finite presentation of the finite group T_0/A, and, by determining which of its elements centralize every generator of A, we are able to find C/A, and hence C. Now $C/Z(C)$ is finite, so by Schur's Theorem C' is finite, and this can be found by (2.6). Clearly T/C' is exactly the torsion-subgroup of C/C', and this can be found from a finite presentation of C. Consequently we can find T.

4. POLYCYCLIC-BY-FINITE SUBGROUPS OF $GL(n, \mathbb{Z})$

We begin by quoting a result from constructive algebraic number theory upon which most subsequent theorems depend.

PROPOSITION (4.1). *There is an algorithm which, when an algebraic number field K is given, finds a finite presentation of the group of units of the ring of algebraic integers in K.*

Here K is regarded as *given* if an irreducible polynomial f in $\mathbb{Q}[t]$ such that $K \simeq \mathbb{Q}[t]/(f)$ is specificd. Proposition (4.1) is essentially due to Borevič and Šafarevič [8]; see also [12].

The main result to be established in this section is

THEOREM (4.2). *There is an algorithm which, when a finite subset X of $GL(n, \mathbb{Z})$ is specified, decides if $G = \langle X \rangle$ is a PF-group, and if so, finds a finite presentation of it.*

Two preliminary results will be proved first.

LEMMA (4.3). *There is an algorithm which, when given a finite subset X of $GL(n, \mathbb{Z})$ such that $G = \langle X \rangle$ is a PF-group, finds the following:*

(i) *a triangularizable normal subgroup T with finite index in G;*

(ii) *a finite presentation of T/U where U is the unipotent part of T;*

(iii) *a finite presentation of U.*

Proof. The first step is to enumerate the normal subgroups of G with finite index. To do this enumerate finite subsets S of G and positive integers m. Test to see if $T = \langle S \rangle$ is normal in G, using the solution of the membership problem in PF-subgroups of $GL(n, \mathbb{Z})$—this depends on the fact that such subgroups are closed in the congruence topology (see [30, Chap. 4, Theorem 5]). Then enumerate up to m cosets of T in G and check to see if their union V satisfies $Vx = V$ for all x in X. This is possible by the solution of the membership problem. When this occurs $G = V$.

At the same time enumerate algebraic number fields K and non-singular $n \times n$ matrices α over K, and test to see if $\alpha^{-1} t \alpha$ is (upper) triangular for each generator t of T. The Lie–Kolchin–Mal'cev Theorem on soluble linear groups [30, Chap. 2(c)] guarantees that a (T, K, α) will appear such that $\alpha^{-1} T \alpha$ is triangular over K.

Next use (4.1) to find a finite presentation for the group of units D of K. Let $\pi: T \to D \times \cdots_n \times D$ be the map associating with x in T the diagonal of $\alpha^{-1} x \alpha$. Then π is a homomorphism whose kernel equals U. We know the images under π of the generators of T, so we can find a finite presentation of $\operatorname{Im} \pi$, and hence of T/U. From the latter find a finite set of generators for U, using the argument of the Normal Closure Lemma (2.5), and solubility of the membership problem in PF-subgroups.

Finally, $\alpha^{-1} U \alpha$ is a subgroup of $U(n, \mathbb{Z})$, the group of all $n \times n$ upper unitriangular matrices over $\mathbb{Z}$. But it is easy to write down a finite presenta-

tion of $U(n, \mathbb{Z})$; then (3.4) allows us to find a finite presentation of $\alpha^{-1}U\alpha$, and hence of U.

The following elementary result is also needed in the proof of (4.2); it is related to a theorem of Jordan and Schur on periodic subgroups of linear groups of characteristic 0 (see [9, Theorem 36.14]).

LEMMA (4.4). *Let G be a PF-subgroup of $GL(n, \mathbb{Z})$ with soluble radical S. Then $|G : S| \leqslant f(n)$ where $f: \mathbb{P} \to \mathbb{P}$ is a computable increasing function, $\mathbb{P}$ being the set of positive integers.*

Proof. Let G act on a free abelian group M of rank n in the natural way. If $n = 1$, the result is obvious with $f(1) = 1$. Let $n > 1$ and argue by induction on n. If M is $\mathbb{Z}G$-rationally reducible, there is a $\mathbb{Z}G$-submodule B of M with M/B torsion-free, $h(B) = n_1$, $h(M/B) = n_2$, and $0 < n_i < n$. By induction on n, if $S_1/C_G(B)$ and $S_2/C_G(M/B)$ are the soluble radicals of $G/C_G(B)$ and $G/C_G(M/B)$, respectively, then $|G : S_i| \leqslant f(n_i)$. Let $N = S_1 \cap S_2$; then $|G : N| \leqslant f(n_1) f(n_2)$, and it is easy to see that N is soluble. Let $b_1 = \max\{f(n_1) f(n_2) \mid 0 < n_i < n,\ n_1 + n_2 = n\}$; then $|G : N| \leqslant b_1$.

Suppose now that M is rationally irreducible, so G is abelian-by-finite. Let A be a maximal abelian normal subgroup of G with finite index. We show that $|G : A| \leqslant b_2$ where b_2 is computable from n. Recall that finite subgroups of $GL(n, \mathbb{Z})$ have order at most $d(n)$, where d is an increasing function of n that can be written down explicitly (see [9, 36.14]). Let $C = C_G(A)$. Then C' is finite, by Schur's Theorem; hence the elements of finite order in C form a normal subgroup U of G with order at most $d(n)$. Let $D = C_C(U)$; then $|C : D| \leqslant d(n)!$.

Denote by T the torsion-subgroup of A. Then $|T| \leqslant d(n)$ and $|G : C_G(T)| \leqslant d(n)!$. Now it is also true that $h(A) \leqslant n - 1$; this is because A is essentially a completely reducible subgroup of $GL(n, \mathbb{Q})$ and the Hirsch number of the unit group of an algebraic number field of degree m is at most $m - 1$. A routine argument yields $|G : C| \leqslant d(n)!\, d(n-1)(d(n))^{n-1} = e(n)$, say. Hence $|G : D| \leqslant e(n)\, d(n)!$. Now $D/Z(D)$ embeds in $\mathrm{Hom}(D/Z(U), Z(U))$ in an obvious way, and $Z(D) = A$ by maximality of A. Therefore $|G : A| \leqslant e(n)\, d(n)!\, d(n)^{n-1+d(n)} = b_2$, say. (Since D is nilpotent, it is in fact enough to bound $|G : D|$.)

Finally put $f(n) = \max\{b_1, b_2\}$.

Proof of Theorem (4.2). We show first how to decide if G is a PF-group. If p is a prime, the mapping $x \mapsto x \pmod p$ is a homomorphism from G to $GL(n, p)$, with image $G(p)$ and kernel $K(p)$ say. If G is a PF-group, then (4.4) shows that each $G(p)$ is soluble-by-finite of order $\leqslant f(n)$. Conversely, assume that each $G(p)$ has this property. Note that G is finitely generated and $\bigcap_p K(p) = 1$; in addition recall that a soluble

linear group of degree n has derived length at most some $e(n)$. Consequently G is soluble-by-finite, and hence it is a PF-group by a theorem of Mal'cev [23].

Two procedures are now set in motion. The first finds a finite presentation for each $G(p)$ and uses it to determine if $G(p)$ is soluble-by-finite of order $\leqslant f(n)$. The procedure stops if this fails to be true.

The second procedure attempts to construct a polycyclic subgroup of finite index in G. Enumerate finite subsets $\{x_1, ..., x_n\}$ of G and positive integers l, and check to see if $x_i^{x_j^{\pm 1}} \in \langle x_1, ..., x_{j-1} \rangle$ for $j = 2, ..., m$, $i = 1, ..., j-1$. This is possible by the solution of the membership problem for PF-subgroups. If the subset $\{x_1, ..., x_n\}$ passes this test, enumerate up to l cosets of $\langle x_1, ..., x_n \rangle$ and determine if the union of these cosets equals G. The procedure stops if such a subset appears.

If the first procedure stops, G is not a PF-group; if the second stops, G is a PF-group. Assuming that G is a PF-group, we find subgroups U and T of G, as in (4.3), and finite presentations of T/U and U. Since G/T is finite, we can construct a transversal to T in G, and hence a finite presentation of G/T. By a standard method we obtain a finite presentation of G.

COROLLARY (4.5). *There is an algorithm which, when given a PF-group G, a finitely generated abelian group M, and an explicit $\mathbb{Z}G$-module structure for M (by means of the action of the generators of G on those of M), finds $C_G(M)$.*

Proof. Find the order t of the torsion-subgroup of M, and note that $M_0 = tM$ is torsion-free. Find a basis for M_0, and use this to associate with each generator of G a matrix in $GL(n, \mathbb{Z})$. These matrices generate a subgroup of $GL(n, \mathbb{Z})$ that is isomorphic with $G/C_G(M_0)$. By (4.2) we can find a finite presentation of $G/C_G(M_0)$; then, in the usual way, we go on to obtain a finite set of generators for $C_G(M_0)$. In addition we can find $C_G(M/M_0)$ by enumerating normal subgroups with finite index in G. Finally $C_G(M) = C_G(M_0) \cap C_G(M/M_0)$ can be found by (3.9).

5. THE FITTING SUBGROUP, THE CENTRE, AND THE FC-CENTRE

As a further application of (4.3) we establish

THEOREM (5.1). *There is an algorithm which, on being given a PF-group G, finds its Fitting subgroup* Fitt(G).

Proof. The first step is to find a normal nilpotent subgroup N such that G/N is abelian-by-finite. To do this enumerate normal subgroups H of

finite index in G; in each case find H', using (2.6), and test it for nilpotence (using (3.4) and (2.9)). Since PF-groups are nilpotent-by-abelian-by-finite (Mal'cev [23]; see also [30, Sect. 2, Theorem 4]), such an H will eventually appear. Put $N = H'$.

Next $\mathrm{Fitt}(G/N') = \mathrm{Fitt}(G)/N'$ by a well-known result of P. Hall. Since we can find a finite presentation of G/N', we may asume that N is abelian. Apply (3.10) to find a poly-infinite cyclic normal subgroup K of finite index in H. Let $A = K'$, a free abelian group, and find $h(A) = n$, say. Choose a basis for A. Then $K/C_K(A)$ is isomorphic with an abelian subgroup of $GL(n, \mathbb{Z})$ with an explicit finite set of generators. Let $F = \mathrm{Fitt}(K)$. Now $F/C_K(A)$ is exactly the unipotent subgroup of $K/C_K(A)$. By (4.3) we can find a finite set of generators for $F/C_K(A)$; thus by (4.5) we can find a finite set of generators for $C_K(A)$ and so for F.

Finally we show how to find $\mathrm{Fitt}(G)$. Use (3.11) to find the maximum finite normal subgroup of G/F, say T/F. Now $\mathrm{Fitt}(G) \cap K = F$, so $F \leqslant \mathrm{Fitt}(G) \leqslant T$. Thus all we need do is list the finitely many subgroups L satisfying $F \leqslant L \leqslant T$, test each such L to see if it is normal in G, and then test for nilpotency. The largest such subgroup will be $\mathrm{Fitt}(G)$.

On the basis of this result we show how to find the centre.

THEOREM (5.2). *There is an algorithm which, on being given a PF-group G, finds its centre $Z(G)$.*

Proof. Consider first the case where G is nilpotent. We can clearly assume that G is infinite. Use (3.7) to find an infinite abelian normal subgroup A_1. Find $C_1 = C_G(A_1)$ using (4.5), and decide if $A_1 = C_1$. If not, then $I = C_1/A_1 \cap Z(G/A_1) \neq 1$. By induction on the Hirsch number we can find $Z(G/A_1)$, and then I. Find a non-trivial element $a_1 A_1$ of I, and put $A_2 = \langle a_1, A_1 \rangle$, an abelian normal subgroup of G. Find $C_2 = C_G(A_2)$ and decide if $A_2 = C_2$; if not, repeat the procedure. This process produces an ascending chain of abelian normal subgroups which must terminate, say at $A = A_r$; then $A = C_G(A)$, so $Z(G) \leqslant A$.

Let $x_1, x_2, \ldots, x_n$ be the generators of G, and write $B_i = C_A(x_i)$. Then $Z(G) = B_1 \cap \cdots \cap B_n$. Find a basis for A using (3.4), and then find $Z(G)$ by solving a finite set of linear equations over $\mathbb{Z}$.

The general case is now easy. Use (5.1) to find the Fitting subgroup F; then find a finite presentation of F, and find $B = Z(F)$ by the procedure described in the first paragraph. But $Z(G) = C_B(G)$, which can be found by once again solving linear equations over $\mathbb{Z}$.

COROLLARY (5.3). *There is an algorithm which, when given a PF-group G, finds the successive terms of the upper central series of G, and hence the hypercentre.*

The FC-centre is approached through the following lemma. If M is a $\mathbb{Z}G$-module, define the *FC-submodule* $\mathrm{FC}(M)$ of M to be the set of all a in M such that $|G : C_G(a)|$ is finite. Evidently this is a submodule of M.

LEMMA (5.4). *There is an algorithm which, when given finitely generated abelian groups G and M, the latter being torsion-free, and an explicit $\mathbb{Z}G$-module structure for M, finds* $\mathrm{FC}(M)$.

Proof. Let $x_1, ..., x_n$ be the generators of G in the presentation, and put $F = \mathrm{FC}(M)$. If $a \in F$, then $a(x_i^{r_i} - 1) = 0$ for some least $r_i > 0$. Now $a\mathbb{Z}\langle x_i \rangle$ is a $\mathbb{Z}\langle x_i \rangle$-submodule with $\mathbb{Z}$-rank at most $r = h(M)$; also x_i induces an automorphism in the submodule with order r_i. Hence $r_i \leqslant d(r)$ for some function d. Put $e = (d(r))!$. Then $F \leqslant \bigcap_{i=1}^{n} C_M(x_i^e)$. The converse inclusion holds too, so $F = \bigcap_{i=1}^{n} C_M(x_i^e)$. This can be found in the usual way by finding a basis for M.

THEOREM (5.5). *There is an algorithm which, when given a PF-group G, finds the FC-centre* $\mathrm{FC}(G)$.

Proof. Find the maximum finite normal subgroup T using (3.11). Then $T \leqslant F = \mathrm{FC}(G)$ and clearly $\mathrm{FC}(G/T) = F/T$. A finite presentation of G/T is at hand, so we can pass to G/T, i.e., assume that $T = 1$. Now F is centre-by-finite, being a finitely generated FC-group, so F' is finite and therefore F is abelian. Thus $F \leqslant \mathrm{Fitt}(G)$.

Let $x \in F$ and let y belong to the second centre of $\mathrm{Fitt}(G)$. Then $[x, y^m] = 1$ for some $m > 0$; hence $1 = [x, y]^m$ and $[x, y] = 1$. Consequently $F \leqslant Z(\mathrm{Fitt}(G))$.

Now $G/\mathrm{Fitt}(G)$ has an abelian normal subgroup $H/\mathrm{Fitt}(G)$ with finite index. Moreover we can find $\mathrm{Fitt}(G)$ by (5.1), and hence H. Without loss we can suppose that $H = G$, i.e., $G/\mathrm{Fitt}(G)$ is abelian. Finally F equals the FC-submodule of the $\mathbb{Z}(G/\mathrm{Fitt}\, G)$-module $Z(\mathrm{Fitt}(G))$. Find finite presentations for $G/\mathrm{Fitt}(G)$ and $Z(\mathrm{Fitt}(G))$; then apply (5.4) to find F.

6. CENTRALIZERS, INTERSECTIONS, AND NORMALIZERS

The section begins with an algorithm to find centralizers of elements in modules over group rings.

PROPOSITION (6.1). *There is an algorithm which, when given a PF-group G, a finitely generated abelian group M, an explicit $\mathbb{Z}G$-module structure for M, and an element a of M, finds $C_G(a)$.*

Proof. Consider first the case where G is abelian-by-finite. Find an

abelian normal subgroup N with finite index in G. Find finite presentations for N, and for the group $(a)\,\mathbb{Z}N$. Then use (4.5) to find $C_N((a)\,\mathbb{Z}N) = C_N(a)$. Find a transversal to N in G by coset enumeration, say $\{t_1, ..., t_k\}$. Now $C_G(a) \cap Nt_i$ is non-empty if and only if $at_i^{-1} = ax$ for some x in N: this is decidable by the solution of the conjugacy problem for the semi-direct product $N \ltimes M$. For each such i find by enumeration x_i in N such that $ax_it_i = a$. Then $C_G(a) \cap Nt_i = C_N(a)\,x_it_i$. Consequently $C_G(a)$ is generated by $C_N(a)$ and these x_it_i.

We return to the general case, arguing by induction on $h(M)$. If $h(M) = 0$ and M is finite, we can find $C_G(M)$ and hence a finite presentation of the finite group $G/C_G(M)$. This case has already been dealt with, so let $h(M) > 0$. Use (5.1) to find $\mathrm{Fitt}(G \ltimes M)$, and then find its projection N on G. Thus N is the largest nilpotent normal subgroup of G that acts nilpotently on M. Find a finite presentation of N and then find $B = C_M(N)$ by exploiting the equation $B = M \cap Z(N \ltimes M)$ and applying (5.2). If B is finite, then so is M. Assume that B is infinite; by induction hypothesis we can find $C_G(a + B) = H$, say.

Next write $A = B + \langle a \rangle$, noting that A is a $\mathbb{Z}H$-submodule of M. Also we can find $K = C_H(B)$ by (4.5). There is an obvious homomorphism $\theta: K \to \mathrm{Hom}(A/B, B)$ given by $(a + B)\,k^\theta = a(k - 1)$; the kernel of θ is exactly $C_K(a)$. Since we are able to find finite presentations of K and $\mathrm{Hom}(A/B, B)$, as well as an explicit description of θ, it is possible to find $\mathrm{Ker}\,\theta = C_K(a)$ by using (3.8).

Let $P = [a, K]$. Suppose first that P is finite. Then K induces a finite group of automorphisms in A, so that $K/C_H(A)$ is finite. Also G/N is abelian-by-finite, whence so is H/K since $H \cap N \leqslant K$. Therefore $H/C_H(A)$ is finite-by-abelian-by-finite, which is easily seen to imply that it is abelian-by-finite. Since a finite presentation of $H/C_H(A)$ can be found, we are in the situation of the first part of the proof, so $C_H(a) = C_G(a)$ can be found.

Finally assume that P is infinite. Then by induction we can find $C_H(a + P) = R$, say. Now $R = C_H(a)K$; for if $h \in H$, then $h \in C_H(a)K$ if and only if $ah = ak$ for some k in K, i.e., $a(h - 1) = a(k - 1)$, which is a typical element of P.

We now know that $C_H(a)$ satisfies $C_H(a)K = R$ and $C_H(a) \cap K = C_K(a)$; moreover both R and $C_K(a)$ are known. To find $C_H(a)$ enumerate finite subsets S of H such that $as = a$ for all $s \in S$; then check if $\langle S \rangle K = R$ and $\langle S \rangle \cap K = C_K(a)$ (here we use (2.1), (2.2), and (3.9)). When such an S appears, the subgroup it generates will equal $C_H(a) = C_G(a)$.

COROLLARY (6.2). *There is an algorithm which, when given a PF-group G, a finitely generated abelian group M with an explicit $\mathbb{Z}G$-module structure, and a derivation $\delta: G \to M$ (by means of its effect on the generators of G), finds the kernel of δ.*

Proof. Define a new $\mathbb{Z}G$-module $L = M \oplus \langle a \rangle$ where a has infinite order and the module structure is given by

$$(x, an) \cdot g = (xg + g^{\delta} n, an);$$

here $x \in M$, $n \in \mathbb{Z}$, and $g \in G$. Thus the $\mathbb{Z}G$-module structure of L is explicitly describable. Obviously $\operatorname{Ker} \delta = C_G((0, a))$, which can be found by (6.1).

The corollary can be applied with advantage to the intersection of an arbitrary pair of subgroups.

THEOREM (6.3). *There is an algorithm which, when given a PF-group G and finite subsets X and Y of G, finds $\langle X \rangle \cap \langle Y \rangle$.*

Proof. Let $H = \langle X \rangle$ and $K = \langle Y \rangle$. The proof is by induction on $h(G)$, which can be assumed positive. Find a non-trivial free abelian normal subgroup A of G. By (2.2) we can decide if $A \leqslant H$. If this is the case, then we can find $H \cap KA = (H \cap K)A$, by the induction hypothesis. We can also find $K \cap A$ by (3.9). Enumerate finite subsets U of G such that $A \cap K \leqslant \langle U \rangle \leqslant H \cap K$ and check to see if $\langle U \rangle A = (H \cap K)A$, all of which is possible by (2.2). When such a U appears, it will generate $H \cap K$.

Assume now that $A \not\leqslant H$. Apply the method of the first paragraph to the pairs (HA, K) and (H, KA). In this way we can find

$$P = HA \cap K \qquad \text{and} \qquad Q = H \cap KA.$$

Then $P \cap Q = H \cap K$; also, if G^* denotes $HA \cap KA$, then $G^* = PA = QA$, so that $P \cap A \lhd G^*$ and $Q \cap A \lhd G^*$. If either $P \cap A$ or $Q \cap A$ is non-trivial, we can substitute it for A and use the argument of the first paragraph to find $P \cap Q$ (it will be necessary to find a finite presentation for G^*).

Now assume that $P \cap A = 1 = Q \cap A$. If $x \in P$, then $xx^{\delta} \in Q$ for some $x^{\delta} \in A$; here $\delta: P \to A$ is a derivation. Clearly $x \in P \cap Q$ if and only if $x \in \operatorname{Ker} \delta$, so $H \cap K = P \cap Q = \operatorname{Ker} \delta$, which can be found by (6.2).

COROLLARY (6.4). *There is an algorithm which, when given a PF-group G and finite subsets X and Y of G, finds $H_K = \bigcap_{k \in K} H^k$ where $H = \langle X \rangle$ and $K = \langle Y \rangle$. In particular the algorithm can find the normal core H_G of H in G.*

Proof. The point to note here is that by a theorem of Rhemtulla [27], H_K is the intersection of *finitely* many conjugates of H in K. To find H_K enumerate finite subsets S of K and form H_S using (6.3). Now $H_S = H_K$ if and only if $(H_S)^y = H_S$ for each y in Y. We can decide if this is true by using (2.2). Therefore we can find H_K.

As a consequence of (6.3) we are now in a position to construct arbitrary centralizers.

THEOREM (6.5). *There is an algorithm which, when given a PF-group G and finite subsets X and Y of G, finds $C_{\langle Y\rangle}(\langle X\rangle)$.*

Proof. In view of (6.3) it suffices to find $C_G(x)$ for a given x in G. Argue by induction on $h(G)>0$. Find a non-trivial free abelian normal subgroup A of G. If $x\in A$, then we can find $C_G(x)$ by (6.1). Suppose that $x\notin A$. By induction hypothesis we can find $C_G(xA)=D$, say. A derivation $\delta: D\to A$ is defined by the rule $d^\delta=[d,x]$, $(d\in D)$. Then $C_G(x)=C_D(x)=\operatorname{Ker}\delta$, which can be found by (6.2).

We turn now to the problem of finding normalizers, beginning with a result on modules.

LEMMA (6.6). *There is an algorithm which, when given a PF-group G, a finitely generated free abelian group M with an explicit $\mathbb{Z}G$-module structure, and a subgroup M_0 of M, finds $N_G(M_0)$.*

Proof. Find the order t of the torsion-subgroup of M/M_0. Then $Mt+M_0/M_0$ is $\mathbb{Z}$-torsion-free. Replace M by $Mt+M_0$, i.e., assume that M/M_0 is $\mathbb{Z}$-torsion-free. Now find a $\mathbb{Z}$-basis $\{a_1,\ldots,a_r\}$ for M_0 and extend it to one for M, say $\{a_1,\ldots,a_r,\ldots,a_n\}$. Let $E=\bigwedge M^r$, the rth exterior power of M, regarded as a $\mathbb{Z}G$-module via diagonal action. Note that this module structure can be described explicitly. Then $E_0=\bigwedge M_0^r$ is the infinite cyclic group generated by $b=a_1\wedge a_2\wedge\cdots\wedge a_r$. We can find $H=C_G(b)$ by (6.1). It is a routine exercise in linear algebra to show that $H\leqslant N_G(M_0)$. Thus if $g\in N_G(M_0)$, then either $g\in H$ or else $bg=-b$. Now solubility of the conjugacy problem allows us to decide if b and $-b$ are conjugate in $G\ltimes M$. If not, then $N_G(M_0)=H$. Otherwise find g such that $bg=-b$; then again it is routine to show that $b\in N_G(M_0)$, so that $N_G(M_0)=\langle g,H\rangle$.

The next result shows how to find a basis for the derivation group $\operatorname{Der}(G,M)$ when G is a finitely presented group and M a finitely generated free abelian group.

PROPOSITION (6.7). *There is an algorithm which, when given a finitely presented group G, a finitely generated free abelian group M, and an explicit $\mathbb{Z}G$-module structure for M, finds a basis for the finitely generated free abelian group* $\operatorname{Der}(G,M)$.

Proof. Let $G=\langle x_1,\ldots,x_n\,|\,r_1,\ldots,r_m\rangle$ be the given finite presentation of G. Let F be the free group on $\{f_1,\ldots,f_n\}$ and R the kernel of the homomorphism $\theta: F\to G$ in which $f_i^\theta=x_i$. Thus $\operatorname{Im}\theta=G$ and R is the

normal closure in F of $\{r_1, ..., r_m\}$, where the r_i are now words in **f**. Find a $\mathbb{Z}$-basis $\{a_j\}$ for M, and note that M becomes a $\mathbb{Z}F$-module via θ. Certainly $\mathrm{Der}(F, M) \simeq M \oplus \cdots \oplus M$, ($n$ summands), via the map $\delta \mapsto (f_1^\delta, ..., f_n^\delta)$. Thus we can find a basis of $\mathrm{Der}(F, M)$.

Now $\theta: F \to G$ induces a monomorphism

$$\theta^*: \mathrm{Der}(G, M) \to \mathrm{Der}(F, M);$$

moreover δ in $\mathrm{Der}(F, M)$ belongs to $\mathrm{Im}\,\theta^*$ if and only if $r^\delta = 0$ for all r in R. This condition is equivalent to $r_1^\delta = \cdots = r_n^\delta = 0$ since R acts trivially on M.

Let $f_i^\delta = \sum_j a_j d_{ij}$ where $d_{ij} \in \mathbb{Z}$. The conditions $r_i^\delta = 0$, $i = 1, 2, ..., n$, are equivalent to the d_{ij} forming a solution vector of a finite set of homogeneous linear equations over $\mathbb{Z}$. Using standard procedures, we find a $\mathbb{Z}$-basis for the solution space of this system, which will then provide a $\mathbb{Z}$-basis for $\mathrm{Im}\,\theta^*$. Thus we obtain a $\mathbb{Z}$-basis of $\mathrm{Der}(G, M)$.

THEOREM (6.8). *There is an algorithm which, when given a PF-group G and finite subsets X and Y of G, finds $N_{\langle Y\rangle}(\langle X\rangle)$.*

Proof. Let $H = \langle X\rangle$. By (6.3) it suffices to show how to find $N_G(H)$. Argue by induction on $h(G)$ and let $h(G) > 0$. Find a non-trivial free abelian normal subgroup A of G, and then find $H \cap A$. By induction hypothesis we can find $N_G(HA/A) = G_1$. Now find finite presentations for G_1 and A, and use (6.6) to find $N_{G_1}(H \cap A) = G_2$, say.

Suppose first that $H \cap A \neq 1$. Then we can find $N_{G_2}(H/H \cap A)$. But this is just $N_G(H)/H \cap A$, so we can find $N_G(H)$ in this case.

Assume now that $H \cap A = 1$, so that $G_1 = G_2 = N_G(HA)$. If $g \in G_1$, then H^g is also a complement of A in HA. Therefore it determines a derivation g^Δ from HA/A to A, and there is a function $\Delta: G_1 \to \mathrm{Der}(HA/A, A) = D$. A routine computation reveals that Δ is a derivation; here the $\mathbb{Z}G_1$-module structure of D is given by $(x)^{\delta g} = ((x^{g^{-1}})^\delta)^g$ where $x \in HA/A$, $g \in G_1$, $\delta \in D$. By (6.7) we can find a $\mathbb{Z}$-basis for D once finite presentations of HA/A and A have been found. Finally $\mathrm{Ker}\,\Delta = N_{G_1}(H) = N_G(H)$, and this can be found by (6.2).

We conclude with an application of the main results of this section which generalizes (2.3) and (2.4).

THEOREM (6.9) (The Generalized Conjugacy Theorem). *There is an algorithm which, when given a PF-group G, together with finite subsets X, $X_1, ..., X_m$, $Y_1, ..., Y_m$, and elements $a_1, ..., a_n$, $b_1, ..., b_n$ of G, decides if there is an element h of $\langle X\rangle$ such that $\langle X_i\rangle^h = \langle Y_i\rangle$ and $a_j^h = b_j$ for all $i = 1, ..., m$, $j = 1, ..., n$.*

Proof. Let $H = \langle X \rangle$, $A_i = \langle X_i \rangle$, $B_j = \langle Y_j \rangle$. We argue by induction on $m+n$. If $m+n=0$, there is nothing to decide, so assume $m+n>0$. Suppose that in fact $m>0$; if $n>0$, the argument is similar. By induction hypothesis we can assume that we have found an element h of H such that $A_i^h = B_i$ and $a_j^h = b_j$ where $i = 1, ..., m-1$, $j = 1, ..., n$. Put

$$D = \bigcap_{i=1}^{m-1} N_H(A_i) \cap \bigcap_{j=1}^{n} C_H(a_j),$$

which is taken to be H if $m=1$ and $n=0$. This can be found by (6.3), (6.5), and (6.8). Then the set of all elements H that conjugate A_i to B_i, $i = 1, ..., m-1$, and a_j to b_j, $j = 1, ..., n$, is exactly Dh. Next we can also assume that A_m and B_m are conjugate in G by (2.4), and find x in G such that $A_m^x = B_m$. The set of all elements in G that conjugate A_m to B_m is then Ex where $E = N_G(A_m)$.

The problem is now to decide if $Dh \cap Ex$ is non-empty, i.e., if $hx^{-1} \in DE$. This decidable in view of the profinite closure of DE in G (Lennox and Wilson [21]).

Remark. Theorem (6.9) can also be proved by a local-global argument: see [31, Theorem B].

7. Finite Subgroups of PF-Groups

Our initial aim in this section is to prove

Theorem (7.1). *There is an algorithm which, when given a PF-group G, produces finite subsets $X_1, X_2, ..., X_k$ such that the $\langle X_i \rangle$ are finite non-conjugate subgroups whose conjugates account for all the finite subgroups of G. Hence this algorithm can decide if G is torsion-free.*

The main tool used in the proof is an algorithm to decide if certain group extensions split.

Proposition (7.2). *There is an algorithm which, when given a finite presentation of a group E and a finite subset that forms a basis of a free abelian normal subgroup M of E, decides if E splits over M.*

Proof. Let $x_1, ..., x_n$ be the given generators of E. By adding the basis elements of M to the relators in the presentation of E we obtain a finite presentation of $G = E/M$ in generators $x_1 M, ..., x_n M$; let $r_1, ..., r_l$ be the defining relators of this presentation. Thus $r_i(\mathbf{x}) \in M$. Suppose that F is the free group on a set $\{f_1, ..., f_n\}$ and let $\theta: F \to E$ be the epimorphism such that $f_i^\theta = x_i$. Then, if R is the preimage of M under θ, we have $F/R \simeq G$ and

$R = \langle r_1, ..., r_l \rangle^F$. Note that $R_{ab} = R/R'$ is a $\mathbb{Z}G$-module by conjugation, and M becomes a $\mathbb{Z}F$-module via θ. Clearly θ induces a $\mathbb{Z}G$-homomorphism $\varphi: R_{ab} \to M$ in which $(rR')^\varphi = r(\mathbf{x})$.

We recall a standard result from the cohomology of groups—for this and other facts cited see [11, Sect. 3]. There is an exact sequence of groups

$$\mathrm{Hom}_{\mathbb{Z}G}(I_F/I_F\bar{I}_R, M) \xrightarrow{\rho} \mathrm{Hom}_{\mathbb{Z}G}(\bar{I}_R/I_F\bar{I}_R, M) \longrightarrow H^2(G, M) \longrightarrow 0,$$

where I_F is the augmentation ideal of $\mathbb{Z}F$, $\bar{I}_R$ is the kernel of the canonical homomorphism $\mathbb{Z}F \to \mathbb{Z}G$, and ρ is restriction. Now $\bar{I}_R/I_F\bar{I}_R \simeq^{\mathbb{Z}G} R_{ab}$ via $(r-1) + I_F\bar{I}_R \to rR'$, $r \in R$. Thus φ can be regarded as an element of the middle term of the exact sequence, and E splits over M if and only if $\varphi \in \mathrm{Im}\ \rho$.

Next $I_F/I_F\bar{I}_R$ is the free $\mathbb{Z}G$-module on the $(x_i - 1) + I_F\bar{I}_R$. Therefore $\mathrm{Hom}_{\mathbb{Z}G}(I_F/I_F\bar{I}_R, M)$ is free abelian of finite rank with an explicit basis. Also $\bar{I}_R/I_F\bar{I}_R$ is generated as a $\mathbb{Z}G$-module by the $(r_j - 1) + I_F\bar{I}_R$, so that $\mathrm{Hom}_{\mathbb{Z}G}(\bar{I}_R/I_F\bar{I}_R, M)$ can be identified with a subgroup of $D = M \oplus \cdots \oplus M$, ($l$ summands), via the map $\theta \mapsto ((r_j - 1 + I_F\bar{I}_R)\theta)$. The situation now is that we have a specific element φ and a specific subgroup $\mathrm{Im}\ \rho$ of D, both expressible in terms of the natural finite basis of D. Consequently we can decide if $\varphi \in \mathrm{Im}\ \rho$.

Proof of (7.1). Argue by induction on $h(G)$. If $h(G) = 0$, then G is finite and we simply choose a representative of each conjugacy class of subgroups of G. Let $h(G) > 0$.

By (3.7) we can find a non-trivial free abelian normal subgroup A of G. By induction on $h(G)$ we can find finite subgroups $U_1/A, ..., U_r/A$ whose conjugates account for all the finite subgroups of G/A. If F is a finite subgroup of G, then $U_i = F^g A$ and $F^g \cap A = 1$ for some $g \in G$ and $1 \leqslant i \leqslant r$.

The first step is to find a finite presentation of each U_i; then one decides if U_i splits over A, using (7.2). For each U_i that splits over A we can find a complement X_i of A by enumeration. Next it is easy to see that $H^1(X_i, A)$ is finite, i.e., D/I is finite, where $D = \mathrm{Der}(X_i, A)$ and $I = \mathrm{Inn}(X_i, A)$. A finite basis can be found for D in view of (6.7). Also $I \simeq A/C_A(X_i)$, and it is evident that we can furnish a finite set of generators for I and express them in terms of the basis of D. A finite transversal to I in D is then obtained by coset enumeration, let us say $\{\delta_{ij} \mid j = 1, ..., k(i)\}$.

Define $H_{ij} = \{xx^{\delta_{ij}} \mid x \in X_i\}$. Then H_{ij} is a complement of A in U_i and each complement of A in U_i is conjugate to some H_{ij}. It is clear that the conjugates of the finite subgroups H_{ij}, $j = 1, ..., k(i)$, $i = 1, ..., r$, account for all finite subgroups of G. To complete the proof examine the H_{ij} for conjugacy and discard any conjugates found.

A number of rather immediate consequences follow.

COROLLARY (7.3). *There is an algorithm which, when given a PF-group G, produces finite subsets $X_1, ..., X_l$ such that $\langle X_1 \rangle, ..., \langle X_l \rangle$ are non-conjugate finite subgroups whose conjugates exhaust all maximal finite subgroups of G.*

Indeed, if the finite subgroups found in (7.1) are $G_1, ..., G_k$, we simply discard any G_i which is conjugate to a proper subgroup of a G_j, $j \neq i$. The conjugates of the remaining G_i's are the maximal finite subgroups of G.

COROLLARY (7.4). *There is an algorithm which, when given a PF-group G, finds its cohomological dimension $cd(G)$.*

For if G is torsion-free, $cd(G) = h(G)$, and otherwise $cd(G) = \infty$ (see [7, Sects. 4 and 7]). The result now follows from (7.1) and (3.5).

If G is a PF-group, we can find the subgroup generated by all the elements of finite order by using (7.1) together with the Normal Closure Lemma. A more difficult problem is to find the subgroup

$$G_\infty$$

generated by all the elements of infinite order. Note that $|G : G_\infty|$ is finite since G has a torsion-free normal subgroup of finite index.

THEOREM (7.5). *There is an algorithm which, when given a PF-group G, finds the subgroup G_∞.*

Proof. If G is finite, then $G_\infty = 1$. So let $h(G) > 0$ and find a non-trivial free abelian normal subgroup A of G.

(a) Consider first of all the special case where G/A is a finite cyclic group of order d. We can assume $d > 1$ and proceed by induction on d. By (3.11) we can find the maximum finite normal subgroup F of G. Obviously $(G/F)_\infty = G_\infty F/F$, so G/F may be substituted for G; assume from now on that $F = 1$. By (4.5) we can find $C = C_G(A)$; now C/A is finite, so C' is finite and therefore C is abelian. If $A \neq C$, the result will follow by induction on d. Assume that $A = C$. Find by enumeration an x such that $G = \langle x, A \rangle$.

Suppose $G_\infty \neq G$. Then xa has finite order for all a in A, and so $1 = (xa)^d = x^d a^\nu$ where ν is the endomorphism of A mapping a to $a^{1+x+\cdots+x^{d-1}}$. Hence $x^d = 1$ and $\nu = 0$.

Conversely, suppose that $\nu = 0$. Since $x^d \in A$, we have $1 = (x^d)^\nu = (x^d)^d$, and thus $x^d = 1$. If i is any integer that is prime to d, then $1 + x^i + x^{2i} + \cdots + x^{(d-1)i} = \nu = 0$ in End A. Therefore $(x^i a)^d = 1$ for all a in A. It follows that if $\nu = 0$, an element of G with infinite order must have the form $x^i a$ where $a \in A$ and there is a prime p dividing i and d; thus an element of

G with infinite order must belong to $\langle x^p, A\rangle_\infty$ for some prime p dividing d.

The following procedures are to be set in motion. Find the action of v on a basis of A and decide if v is zero. If $v \neq 0$, then $G_\infty = G$. If $v = 0$, then for each prime p dividing d find $G(p) = \langle x^p, A\rangle_\infty$, which is possible by induction on d. Thus we can find $G_\infty = \langle G(p) \mid p \text{ divides } d\rangle$.

(b) In the general case argue by induction on $h(G) > 0$. Certainly $A \leqslant G_\infty$, and by induction hypothesis we can find $(G/A)_\infty = L/A$, say, and hence L. It remains to deal with elements g of infinite order such that gA has finite order. By (7.1) we can find up to conjugacy the finite cyclic subgroups of G/A, say $\langle g_i, A\rangle/A$, $i = 1, ..., k$. Thus g is conjugate modulo A to an element of some $\langle g_i, A\rangle$. By (a) we can find $\langle g_i, A\rangle_\infty = K_i$, say. Put $K = \langle K_1, ..., K_r\rangle^G$, and find K by the Normal Closure Lemma. Finally $G_\infty = \langle L, K\rangle$.

We shall now use (7.5) to give an algorithm to decide if a subgroup of a PF-group is permutable. First we cite two known properties of permutable subgroups.

PROPOSITION (7.6). *Let H be a permutable subgroup of a group G. Then the following hold*:

(i) *if G is finitely generated, then $|H^G : H|$ is finite* [20];

(ii) *if G satisfies the maximal condition, then H is subnormal in G* [33].

THEOREM (7.7). *There is an algorithm which, when given a PF-group G and a finite subset X of G, decides if $\langle X\rangle$ is permutable in G.*

Proof. Let $H = \langle X\rangle$. Note that if H is permutable, then by (7.6), $|H^G : H^g|$ is finite for all $g \in G$, and by Rhemtulla's theorem [27], it follows that $|H^G : H_G|$ is finite, where H_G is the core of H in G.

The first step is to find H_G, using (6.4). Now H is permutable in G if and only if H/H_G is permutable in G/H_G. We can therefore assume that $H_G = 1$. Next, if H is permutable, then by (7.6), H is finite and subnormal, so H is contained in the maximum finite normal subgroup F. Find F, using (3.11), and decide if $H \leqslant F$. If not, then H is not permutable. So assume that $H \leqslant F$.

We show next that if H is permutable, then G_∞ normalizes H. Suppose that g in G has infinite order; then $\langle g, H\rangle = \langle g\rangle H = \langle g\rangle H^{\langle g\rangle}$, and since $H^{\langle g\rangle} \leqslant F$, it follows that $H^{\langle g\rangle} = H$. Find G_∞ using (7.5), and decide if it normalizes H. We can assume this is so, otherwise H is not permutable.

It remains to decide if H permutes with every finite subgroup of G. By (7.1) we can find a finite set of representatives of the conjugacy classes of

finite subgroups of G, say $C_1, ..., C_k$. Then we find the finitely many conjugates of H in G, by enumerating the subgroups of F and testing each for conjugacy to H; let these be $H_1, ..., H_l$. Then H is permutable in G if and only if $H_iC_j = C_jH_i$ for $i = 1, ..., l$, $j = 1, ..., k$. This can certainly be decided since the H_iC_j and C_jH_i are finite subsets.

8. The Frattini Subgroup

This entire section is taken up with the proof of

THEOREM (8.1). *There is an algorithm which, when given a PF-group G, finds the Frattini subgroup $\varphi(G)$.*

A number of preliminary results are needed, some of which are of independent interest.

PROPOSITION (8.2). *There is an algorithm which, when given a PF-group G, a finitely generated abelian group M, and an explicit $\mathbb{Z}G$-module structure for M, finds a finite presentation of M as a $\mathbb{Z}G$-module.*

Proof. (a) Let $R = \mathbb{Z}G$ and let $a_1, a_2, ..., a_m$ be the given group generators of M. Then we can find finite group presentations for $(a_1)R$ and $M/(a_1)R$. Now it is sufficient to find finite R-presentations of $(a_1)R$ and $M/(a_1)R$. Therefore, using induction on m, we reduce to the case where $M = (a)R$.

(b) *Case: M is $\mathbb{Z}$-torsion-free.* Let J be the annihilator of a in R, so that $M \simeq^R R/J$. We show how to find a finite set of generators for the right ideal J. First find a basis for M, and hence for R/J. Enumerate finite subsets X of R, test each to see if $ax = 0$ for all x in X, and then decide if $R/(X)R$ is a finitely generated abelian group. The last step is possible by [4, Lemma 2.1]. Eventually we shall find such a subset X. Let $\bar{J}_0 = (X)R$; thus $\bar{J}_0 \leqslant J$.

We have a finite R-module presentation for $R/\bar{J}_0$. By the argument of [5, Theorem 2.14] (see also [29, Proposition 2]), we can find a finite group presentation of $R/\bar{J}_0$; then we can use this to find the torsion-subgroup $J_0/\bar{J}_0$. Evidently J_0 is a right ideal of R and $J_0 \leqslant J$ because R/J is $\mathbb{Z}$-torsion-free. Find $h(R/J_0)$; if it equals $r = h(M)$, then $J = J_0$. Otherwise find u_1 in $J \setminus J_0$ by enumerating elements u_1 of R, testing to see if $au_1 = 0$, and then to see if $u_1 \notin J_0$. Put $\bar{J}_1 = J_1 + u_1R$. Find a finite group presentation of $R/\bar{J}_1$, and then find its torsion-subgroup $J_1/\bar{J}_1$. Thus $J_0 < J_1 \leqslant J$. If $h(R/J_1) = r$ then $J_1 = J$. Otherwise find u_2 in $J \setminus J_1$, and repeat the argument. Since $h(R/J_0) > h(R/J_1) > \cdots$, we shall, by repetition of this procedure, find a J_k that coincides with J.

(c) *The general case.* Find the torsion-subgroup T of M, and then find $C_G(T)$ by enumerating normal subgroups of index $\leqslant |T|!$ in G. Then find finite presentations of T and $G/C_G(T)$. It is easy to obtain a finite R-module presentation of T, while (b) allows us to find such a presentation of M/T. The result now follows easily.

If M is a module over a ring R, define the *Frattini submodule*

$$\varphi_R(M) \qquad \text{or} \qquad \varphi(M)$$

to be the intersection of all the maximal submodules of M (with the usual stipulation that $\varphi_R(M) = M$ if no maximal submodules exist).

LEMMA (8.3). *Let there be given a finitely presented group G, a finitely generated abelian group M and an explicit $\mathbb{Z}G$-module structure for M. Also let there be given a subgroup M_0 with finite index in M, and assume that M_0 is a $\mathbb{Z}G$-submodule. If a finite set of group generators for $\varphi_{\mathbb{Z}G}(M_0)$ is known, then there is a uniform recursive procedure which finds a finite set of group generators for $\varphi_{\mathbb{Z}G}(M)$.*

Proof. Using the presentation of M, we first find $m = |M : M_0|$. Define

$$\varphi^{(m)}(M)$$

to be the intersection of all the maximal $\mathbb{Z}G$-submodules of M which have index prime to m (of course, if N is a maximal submodule of M, then M/N is a finite elementary abelian p-group for some prime p). Clearly $\varphi^{(m)}(M_0)/\varphi(M_0)$ is exactly the set of all elements of $M_0/\varphi(M_0)$ with order dividing m. Find a finite presentation of $M_0/\varphi(M_0)$, and hence find $\varphi^{(m)}(M_0)$.

Suppose that N is a maximal submodule of M with index prime to m. Then $M = N + M_0$ and $M/N \simeq^{\mathbb{Z}G} M_0/M_0 \cap N$. Hence $N_* = M_0 \cap N$ is a maximal submodule of M_0. Conversely, if L is a maximal submodule of M_0 with index prime to m, then $M/L = M_0/L \oplus L^*/L$ where $L^* = \{a \in M \mid am \in L\}$, a maximal submodule of M with index prime to m. The mappings $N \to N_*$ and $L \to L^*$ are mutually inverse; therefore $\varphi^{(m)}(M) \cap M_0 = \varphi^{(m)}(M_0)$, and hence $\varphi^{(m)}(M)/\varphi^{(m)}(M_0)$ is the subgroup of all elements of $M/\varphi^{(m)}(M_0)$ of order dividing m. This can be found. Finally, find the maximal submodules of the finite module M/Mm, say $M_1/Mm, \ldots, M_r/Mm$; then $\varphi(M) = M_1 \cap \cdots \cap M_r \cap \varphi^{(m)}(M)$, which can certainly be found.

The principal module theoretic tool needed in the proof of (8.1) is

PROPOSITION (8.4). *There is an algorithm which, when given finitely*

generated abelian groups G and M, together with an explicit $\mathbb{Z}G$-module structure for M, finds a finite set of group generators for $\varphi_{\mathbb{Z}G}(M)$.

Proof. (1) The proof is by induction on $h(M)$, which can be assumed positive. It suffices to deal with the case where M is $\mathbb{Z}$-torsion-free. For we can certainly find the order t of the torsion-subgroup of M; then Mt is $\mathbb{Z}$-torsion-free and M/Mt is finite. By (8.3) it is enough to find $\varphi(Mt)$. From now on we assume that M is torsion-free.

Use the given presentation to express G as a direct product of n cyclic groups. From this we obtain an explicit surjective ring homomorphism from $R = \mathbb{Z}[t_1, ..., t_{2n}]$ to $\mathbb{Z}G$ where n is the number of generators of G. Thus we can make M into an R-module in an explicit fashion, and $\varphi_{\mathbb{Z}G}(M) = \varphi_R(M)$.

(2) *We can find the associated set of prime ideals $\mathrm{Ass}_R(M)$ of M. Moreover, if $P \in \mathrm{Ass}_R(M)$, then P is a maximal ideal of infinite index in R.* Let M_1 be a cyclic $\mathbb{Z}G$-submodule which is rationally irreducible. If M/M_1 is infinite, it contains a cyclic rationally irreducible $\mathbb{Z}G$-submodule M_2/M_1. Repetition of this procedure leads to a chain of $\mathbb{Z}G$-submodules $0 = M_0 < M_1 < \cdots < M_m$ where M/M_m is finite and each M_{i+1}/M_i is a cyclic rationally irreducible $\mathbb{Z}G$-module. Thus $M_{i+1}/M_i \simeq^R R/P_i$ where the ideal P_i is maximal of infinite index in R, and so is prime.

Suppose now that $Q \in \mathrm{Ass}_R(M)$, so $Q = \mathrm{Ann}_R(a)$ is prime for some $a \neq 0$ in M. Now $al \in M_m$ for some $l > 0$, and $Q = \mathrm{Ann}_R(al)$. If $al \in M_{i+1} \setminus M_i$, then $aP_0P_1 \cdots P_i = 0$, whence $P_0P_1 \cdots P_i \subseteq Q$ and $P_j \subseteq Q$ for some j. Since R/Q cannot be finite, $Q = P_j$. Thus Q is maximal of infinite index in R.

Let $a_1, ..., a_s$ be group generators of M. Enumerate the elements of M, say $b_1, b_2, ...$, and for each i use (8.2) to find a finite $\mathbb{Z}G$-presentation of $(b_i)\mathbb{Z}G = (b_i)R$, and hence a finite R-module presentation of $(b_i)R$. Thus we have a finite set of generators for the ideal $\mathrm{Ann}_R(b_i)$. By Seidenberg [32, Theorem 5], we can find (finite sets of generators for) the associated primes of $\mathrm{Ann}_R(b_i)$, and hence the primes in $\mathrm{Ass}_R(b_iR)$. Let

$$\mathbf{S}_i = \bigcup_{j=1}^{i} \mathrm{Ass}_R(b_jR).$$

Let R_i be the product of all the primes in $\mathbf{S}_i$. We now test to see if $a_jR_i = 0$ for each $j = 1, 2, ..., s$. If so, then $MR_i = 0$ and, if $Q \in \mathrm{Ass}_R(M)$, then $R_i \leqslant Q$, whence Q equals some element of $\mathbf{S}_i$. Hence $\mathrm{Ass}_R(M) = \mathbf{S}_i$. Note that it is guaranteed that such an i will appear.

(3) *We can find finite sets of group generators for the primary components M_P of M where $P \in \mathrm{Ass}_R(M)$.* Here M_P is the set of all elements of M that are annihilated by a power of P: this is an R-submodule. Let $u_1, ..., u_t$ be the generators found for the ideal P. Define

$M[P] = \{a \in M \mid aP = 0\}$. Then $M[P]$ is the set of elements of M that are annihilated by each u_i. Pick a basis of M and represent the endomorphism of M induced by each u_i by an integral matrix. The conditions $au_i = 0$ are equivalent to a finite set of linear homogeneous equations over $\mathbb{Z}$. By solving this system we find $M[P]$. Notice that $M/M[P]$ is $\mathbb{Z}$-torsion-free. Thus we can find the successive terms of the chain of submodules $0 = M_0 \leqslant M_1 \leqslant \cdots$ where $M_{j+1}/M_j = (M/M_j)[P]$. We can also determine the smallest j such that $M_j = M_{j+i}$; then $M_P = M_j$.

(4) *We may assume that* $M = M_{P_1} \oplus \cdots \oplus M_{P_k}$ *where* $\mathrm{Ass}_R(M) = \{P_1, ..., P_k\}$. If $M_{P_i} \cap \sum_{j \neq i} M_{P_j} \neq 0$, there is an $a \neq 0$ in M such that $aP_i = 0 = aQ$ where $Q = \prod_{j \neq i} P_j^{e_j}$ for some $e_j > 0$. Now $R/P_i + Q$ is finite since $Q \not\leqslant P_i$; thus aR is finite and $a = 0$. Therefore the sum S of the M_{P_i} is direct. We argue now that M/S is finite. For there are positive integers d_i such that $MP_1^{d_1} \cdots P_k^{d_k} = 0$. Let Q_i be the product of the $P_j^{d_j}$, $j \neq i$. Then $R/P_i + Q_i$ is finite, so $P_i + Q_i$ contains a positive integer l_i, and $l_i^{d_i} \in P_i^{d_i} + Q_i$. Then $l = l_1^{d_1} \cdots l_k^{d_k} \in Q_1 + \cdots + Q_k + P_1^{d_1} \cdots P_k^{d_k}$, so that

$$Ml \subseteq \sum_{i=1}^{k} MQ_i \subseteq \sum_{i=1}^{k} M_{P_i} = S$$

since $MP_1^{d_1} \cdots P_m^{d_m} = 0$. But M/Ml is finite, so M/S is finite. In view of (8.3) we can replace M by S.

(5) *The final step.* Since $\varphi(M) = \bigoplus_{i=1}^{k} \varphi(M_{P_i})$ and we have found M_{P_i}, we can suppose that $\mathrm{Ass}_R(M) = \{P\}$. Let B be a maximal submodule of M. Then P annihilates M/B, so $MP \subseteq B$ and $MP \leqslant \varphi(M)$. Note that $\varphi(M/MP) = \varphi(M)/MP$, and that we have a finite set of generators for the ideal P, so we can find a finite set of group generators for MP. Therefore we can assume that $MP = 0$, or else the result is obtained by induction on $h(M)$. We shall now argue that $\varphi(M) = 0$.

Write $\bar{R} = R/P$, a domain. Then M is a noetherian $\bar{R}$-module, and M is also $\bar{R}$-torsion-free. Let F be the field of fractions of $\bar{R}$, and put $V = M \otimes_{\bar{R}} F$, a finite dimensional F-space. Let V_0 be a subspace of codimension 1, and put $M_0 = V_0 \cap M$. Then

$$L = M/M_0 \simeq^{\bar{R}} M + V_0/V_0 \leqslant V/V_0 \simeq^{\bar{R}} F.$$

It follows that L is isomorphic with an ideal J of R. But $\varphi(J) \leqslant \varphi(\bar{R})$ and $\varphi(\bar{R}) = 0$ since it is the Jacobson radical of the noetherian domain $\bar{R}$. Therefore $\varphi(J) = 0$ and $\varphi(M) \leqslant \varphi_F(V) = 0$.

Proof of (8.1). Let G be a PF-group. We can assume that G is infinite and argue by induction on $h(G)$.

(1) *We may assume that if we are in possession of a finite set of generators of a normal subgroup N of G and $N \leqslant \varphi(G)$, then N is finite.* For, if N is infinite, then $h(G/N) < h(G)$, and we have a finite presentation of G/N, so a finite set of generators can be found for $\varphi(G/N) = \varphi(G)/N$, and hence for $\varphi(G)$.

(2) *We may assume that G has no non-trivial finite normal subgroups.* Use (3.11) to find the maximum finite normal subgroup T of G; thus a finite presentation of G/T is at hand. Suppose that we have found $\varphi(G/T) = F/T$, say, and write $t = |T|$.

If M is a maximal subgroup of G not containing T, then $G = MT$ and $|G : M| = |T : M \cap T| \leqslant t$. Now we can find the finitely many maximal subgroups of this type by enumerating the subgroups of index $\leqslant t$ and picking out the maximal ones. If these are $M_1, ..., M_l$, then $\varphi(G) = F \cap M_1 \cap \cdots \cap M_l$, which can be found by (6.3).

(3) *We may assume that we have found two finite subsets generating free abelian subgroups H and A such that $A \lhd G$, $HA \lhd G$, $|G : HA|$ is finite, and $H \cap A = 1$.* Since G is nilpotent-by-abelian-by-finite, we can find a normal subgroup M of finite index in G such that $B = M'$ is nilpotent. Find finite presentations of B and B', and then find $\varphi(B/B') = \varphi(B)/B'$; this is certainly possible once the structure of B/B' is known. But it is easy to see that $\varphi(B) \leqslant \varphi(G)$. Thus, on the basis of (1) and (2), we can assume that $\varphi(B) = 1$, which implies that B is free abelian.

The next step calls for the computation of the Hirsch numbers of $[B, {}_iM]$, $i = 1, 2, ...$, and the determination of the first i such that the quotient $[B, {}_iM]/[B, {}_{i+1}M]$ is finite. Write

$$A = [B, {}_iM].$$

Then A is free abelian, $A \lhd G$, and $A/[A, M]$ is finite. Since M/A is nilpotent, we can apply [28, Theorem 5] to deduce that there is a nilpotent subgroup K satisfying $|M : KA| < \infty$ and $K \cap A = 1$. Moreover we can actually find such a subgroup by enumerating subgroups K of M, computing $h(KA)$, checking to see if $h(KA) = h(M)$, and then finding $K \cap A$ and deciding if it is trivial.

Having found K, we obtain a finite presentation of it, and then a finite set of generators for a torsion-free subgroup H_0 of finite index in K (apply 3.10). Then $|G : H_0A|$ is finite and $H_0 \cap A = 1$. Now define N to be the normal core of H_0A in G. Then, if $H = N \cap H_0$, we have $|G : N|$ finite, $N = HA \lhd G$, and $H \cap A = 1$. It remains to explain why we can assume that H is free abelian.

Suppose that $H' \not\leqslant \varphi(N)$. Then there is a maximal subgroup L of N such that $H' \not\leqslant L$. Now $[A, H'] \leqslant B' = 1$, so that $H' \lhd HA = N$. Therefore

$N = LH'$ and $H = H \cap (LH') = (H \cap L)\, H'$; however, H is nilpotent, so this leads to $H = H \cap L$, a contradiction.

Put $U = \langle (H')^G \rangle$. By the Normal Closure Lemma we can find a finite set of generators for U. But $U \leqslant \varphi(N) \leqslant \varphi(G)$, so by (1) and (2) we may suppose that $U = 1$, and H is free abelian.

(4) *We can assume that* $\varphi(N) = \varphi_{\mathbb{Z}H}(A) = 1$. Since N/A is free abelian, $\varphi(N) \leqslant A$. If L is a maximal subgroup of N which does not contain A, then $L \cap A$ is a maximal $\mathbb{Z}H$-submodule of A. Hence $\varphi(N) = \varphi(N) \cap A \geqslant \varphi_{\mathbb{Z}H}(A)$. Also, if B is a maximal $\mathbb{Z}H$-submodule of A, then HB is a maximal subgroup of N; thus $\varphi(N) \leqslant A \cap HB = B$ and so $\varphi(N) = \varphi_{\mathbb{Z}H}(A)$. By (8.4) we can find $\varphi(N)$. But $\varphi(N) \leqslant \varphi(G)$, so we may assume that $\varphi(N) = 1$ by (1) and (2).

(5) *If* $m = |G : N|$, *then* $\varphi^{(m)}_{\mathbb{Z}G}(A) = 1$. Recall that $\varphi^{(m)}_{\mathbb{Z}G}(A)$ denotes the intersection of all the maximal submodules of the $\mathbb{Z}G$-module A whose index in A is prime to m. In the first place we observe that $\varphi^{(m)}_{\mathbb{Z}H}(A)/\varphi_{\mathbb{Z}H}(A)$ is finite, so $\varphi^{(m)}_{\mathbb{Z}H}(A) = 1$ by (2) and (4).

Let M be a maximal $\mathbb{Z}H$-submodule of A, and assume that A/M is a p-group where p does not divide m. Denote the normal core of M in G by M_1. Then A/M_1 is a finite elementary p-group. The subgroup H induces a finite abelian group of automorphisms $\bar{H}$ in A/M_1; here $\bar{H} \lhd \bar{G} = G/C_G(A/M_1)$ since $N = HA \lhd G$. Furthermore $\bar{H}_p$, the p-component of $\bar{H}$, acts nilpotently, and hence trivially, on A/M_1. It follows that $\bar{H}$ is a p'-group and H induces a p'-group of automorphisms in A/M_1. Also $|G : N|$ is prime to p, so G induces a finite p'-group of automorphisms in A/M_1. By Maschke's Theorem $\varphi^{(m)}_{\mathbb{Z}G}(A) \leqslant M_1 \leqslant M$, and in consequence $\varphi^{(m)}_{\mathbb{Z}G}(A) \leqslant \varphi^{(m)}_{\mathbb{Z}H}(A) = 1$.

(6) $\varphi(G) = 1$. By Schur's Theorem G/H^pA splits over N/H^pA. Also N/H^pA is a completely reducible $\mathbb{Z}G$-module. Therefore $\varphi(G) \cap N$ is contained in H^pA for all p not dividing n, which means that $\varphi(G) \cap N \leqslant A$. Hence

$$\varphi(G) \cap N = \varphi(G) \cap A.$$

We claim next that G/A^p splits over A/A^p if p does not divide m. The reason is that G/N is a finite p'-group and N/A^p visibly splits over A/A^p, so a well-known extension of Schur's Theorem applies. Let $K(p)/A^p$ denote a complement to A/A^p in G/A^p.

Suppose that M is a maximal $\mathbb{Z}G$-submodule of A and that A/M is a p-group with m prime to p. Then $K(p)\, M$ is maximal in G, and therefore $\varphi(G) \cap A \leqslant (K(p)M) \cap A = A^pM = M$. It follows that $\varphi(G) \cap A \leqslant \varphi^{(m)}_{\mathbb{Z}G}(A) = 1$, by (5). Hence $\varphi(G) \cap N = 1$ by the equation above, so $\varphi(G)$ is finite. By (2) we obtain finally that $\varphi(G) = 1$.

REFERENCES

1. L. AUSLANDER, On a problem of Philip Hall, *Ann. of Math. (2)* **86** (1967), 112–116.
2. R. BAER, Überauflösbare Gruppen, *Abh. Math. Sem. Univ. Hamburg* **23** (1957), 11–28.
3. G. BAUMSLAG, F. B. CANNONITO, AND C. F. MILLER III, Infinitely generated subgroups of finitely presented groups, I, *Math. Z.* **153** (1977), 117–134.
4. G. BAUMSLAG, F. B. CANNONITO, AND C. F. MILLER III, Some recognizable properties of solvable groups, *Math. Z.* **178** (1981), 289–295.
5. G. BAUMSLAG, F. B. CANNONITO, AND C. F. MILLER III, Computable algebra and group embeddings, *J. Algebra* **69** (1981), 186–212.
6. G. BAUMSLAG, D. GILDENHUYS, AND R. STREBEL, Algorithmically insoluble problems about finitely presented solvable groups, Lie and associative algebras, I, *J. Pure Appl. Algebra* **39** (1986), 53–94.
7. R. BIERI, "Homological Dimension of Discrete Groups," Queen Mary College Math. Notes, London, 1976.
8. Z. I. BOREVIČ AND I. R. ŠAFAREVIČ, "Number Theory," Academic Press, New York, 1966.
9. C. W. CURTIS AND I. REINER, "Representation Theory of Finite Groups and Associative Algebras," Interscience, New York, 1966.
10. E. FORMANEK, Conjugacy separability of polycyclic groups, *J. Algebra* **42** (1976), 1–10.
11. K. W. GRUENBERG, Cohomological topics in group theory, "Lecture Notes in Math.," Vol. 143, Springer, Berlin, 1970.
12. F. GRUNEWALD, Solution of the conjugacy problem in certain arithmetic groups, *in* "Word Problems, II," pp. 101–139, North-Holland, Amsterdam, 1980.
13. F. GRUNEWALD AND D. SEGAL, Conjugacy in polycyclic groups, *Comm. Algebra* **6** (1978), 775–798.
14. K. A. HIRSCH, On infinite soluble groups, I, *Proc. London Math. Soc. (2)* **44** (1938), 53–60.
15. K. A. HIRSCH, On infinite soluble groups, III, *Proc. London Math. Soc. (2)* **49** (1946), 184–194.
16. K. A. HIRSCH, On infinite soluble groups, IV, *J. London Math. Soc.* **27** (1952), 81–85.
17. K. A. HIRSCH, On infinite soluble groups, V, *J. London Math. Soc.* **29** (1954), 250–251.
18. O. H. KEGEL, Über den Normalisator von subnormalen und erreichbaren Untergruppen, *Math. Ann.* **163** (1966), 248–258.
19. O. G. KHARLAMPOVIČ, A finitely presented soluble group with insoluble word problem, *Izv. Akad. Nauk. Ser. Mat.* **45** (1981), 852–873.
20. J. C. LENNOX, A note on quasinormal subgroups of finitely generated groups, *J. London Math. Soc. (2)* **24** (1981), 127–128.
21. J. C. LENNOX AND J. S. WILSON, On products of subgroups in polycyclic groups, *Arch. Math. (Basel)* **33** (1979), 305–309.
22. W. MAGNUS, A. KARRASS, AND D. SOLITAR, "Combinatorial Group Theory," Interscience, New York, 1966.
23. A. J. MAL'CEV, On certain classes of infinite soluble groups, *Mat. Sb.* **28** (1951), 567–588.
24. A. J. MAL'CEV, Homomorphisms onto finite groups, *Ivanov. Gos. Ped. Inst. Učen. Zap.* **18** (1958), 49–60.
25. V. N. REMESLENNIKOV, Conjugacy in polycyclic groups, *Algebra i Logika* **8** (1969), 712–725.
26. V. N. REMESLENNIKOV, An algorithmic problem for nilpotent groups and rings, *Sibirsk. Mat. Žh.* **20** (1979), 1077–1081.
27. A. RHEMTULLA, A minimality property of polycyclic groups, *J. London Math. Soc.* **42** (1967), 456–462.
28. D. J. S. ROBINSON, Splitting theorems for infinite groups, *Sympos. Math.* **17** (1976), 441–470.

29. D. J. S. ROBINSON, Algorithmic problems for automorphisms and endomorphisms of infinite soluble groups, preprint.
30. D. SEGAL, "Polycyclic Groups," Cambridge, 1983.
31. D. SEGAL, Decidable properties of polycyclic groups, *Proc. London Math. Soc. (3)* **61** (1990), 497–528.
32. A. SEIDENBERG, Constructions in a polynomial ring over the ring of integers, *Amer. J. Math.* **100** (1978), 685–703.
33. S. E. STONEHEWER, Permutable subgroups of infinite groups, *Math. Z.* **125** (1972), 1–16.
34. R. G. SWAN, Representations of polycyclic groups, *Proc. Amer. Math. Soc.* **18** (1967), 573–574.