Central Extensions of Polycyclic Groups

Werner Nickel

Originally submitted July 1993
Consolidated version prepared November 1993

A thesis submitted for the degree of Doctor of Philosophy
of the Australian National University
Declaration

The work in this thesis is my own unless otherwise stated.

Werner Nickel
Abstract

There are two main results contained in this dissertation. The first result is a description of an algorithm for the computation of polycyclic presentations for nilpotent factor groups of a given finitely presented group. This algorithm is a generalization of the methods employed in the $p$-quotient algorithm (Havas & Newman, 1980) to possibly infinite nilpotent groups. The second is a method for the computation of the Schur multiplicator of a group given by a polycyclic presentation and a method for the classification of the isomorphism types of Schur covering groups for finite soluble groups. Both algorithms can be treated in a similar context, namely forming central downward extensions of polycyclic groups.
Acknowledgements

It is with great pleasure that I take this opportunity to thank all the people and organizations whose support and influence has made it possible for me to carry out the work for this dissertation.

My sincerest thanks go to my supervisor, Dr M.F. Newman. I cannot overestimate his guidance during the course of my studies at the Australian National University. He provided a level of supervision that I cannot imagine could have been any better. I am very grateful for all he has taught me during many hours of discussion and for his considered and careful advice and encouragement. My thanks also go to my adviser Dr L.G. Kovács for sharing his knowledge and insight with me in numerous long discussions. Many times he led me back to the right mathematical path when I had lost my way in the maze of mathematical considerations. My adviser Dr E.A. O'Brien has been invaluable during my work for this dissertation both as a friend and an academic adviser.

Alice Niemeyer has always provided cordial support and encouragement. She was often a critical partner for discussions and helped me on many occasions to clarify my own thoughts. I am very grateful for this and her constant interest in my work. Without her positive influence I would not have decided to continue my mathematical studies at the Australian National University and my life would undoubtedly have taken a different course. She has made my life richer and for this I owe her a great debt.

Philippa Harvey has been a great adviser and friend in matters of administration and daily life. She and Annette Hughes were a great help in those little things that can make life so difficult.
With gratitude I acknowledge the help I received from Alice Niemeyer, Dr M.F. Newman and Michael Smith in proof reading of parts of this thesis. Michael Smith has also been a great help in technical matters of type setting and word processing. My thanks goes to all the people in the School of Mathematical Sciences, in particular in the former Mathematics Research Section, for creating a friendly and encouraging academic environment that I will certainly miss in the future.

I thank my Diplom supervisor, Prof. J. Neubüser for his continued support and interest in my work.

With deep gratitude I thank Cecilia Shlegel for her affection and support in the difficult times of the last 11 months.

I am indebted to Dr Charles C. Sims for making available to me a draft of Chapters 8 to 11 of his book “Computation with Finitely Presented Groups”.

I wish to express my thank to various organizations for their support;

- to the Australian Department for Education, Employment and Training for an Overseas Postgraduate Research Scholarship;
- to the Australian National University for a PhD-scholarship;
- to the Internet community, in particular to the Australian Academic Research Network, for providing a world wide computer network that makes communication so much easier;
- to the Lehrstuhl D für Mathematik at the RWTH Aachen for making available their facilities to me in the final two weeks of writing up this dissertation.

At last, I would like to give my warmest thanks to my family in Germany which has been, in spite of the vast distances, a constant source of love and understanding.
List of Some Symbols

\( \mathcal{R}, \mathcal{S}, \mathcal{I} \) sets of relations

\((X, \mathcal{R})\) a finite presentation

\(\Phi(G)\) the Frattini subgroup of a group \(G\) (p. 8)

\((A, \mathcal{S})\) a polycyclic presentation (p. 24)

\(I\) the indices of generators of a polycyclic presentation that have a power relation (p. 25)

\((A, \mathcal{S}, w)\) a weighted nilpotent presentation (p. 51)

\(\mathcal{A}, ((X, \mathcal{R}), (A, \mathcal{S}), \sigma)\) quotient systems (p. 39)

\(((X, \mathcal{R}), (A, \mathcal{S}, w), \sigma)\) a weighted nilpotent quotient system (p. 56)

\(w(u)\) the weight of an element \(u\) of a nilpotent group or the weight of a word \(u\) of a weighted nilpotent presentation (p. 17, p. 51)

\(M(G)\) the Schur multiplicator of a group \(G\) (p. 79)
Introduction

This dissertation is written in the area of computational group theory. Computational group theory is concerned with the design and application of computational methods for the study and construction of groups. In this dissertation the main objects of study are polycyclic groups. A polycyclic group is characterized by the existence of a subnormal series of subgroups with cyclic factor groups. Such a subnormal series is called a **polycyclic series**. Finitely generated nilpotent groups and finite soluble groups are polycyclic. While many problems regarding groups are known to be algorithmically unsolvable, polycyclic groups form a class of groups in which many of the generally unsolvable problems have an algorithmic solution (Segal, 1990). Many algorithms have been designed for the study of finite soluble group and their practical implementations have been developed (see, for example, Schönert et al. 1993) but the number of practical implementations of algorithms for infinite polycyclic groups is still very small.

A polycyclic series of a polycyclic group gives rise to a special finite presentation called a **polycyclic presentation**. Such a presentation defines a normal form on the words in the generating set of the presentation which can be determined algorithmically for any word in the generating set. For polycyclic groups this solves one of the basic problems in group theory, the word problem, namely to decide whether two words in a generating set are the same element of the group. It also makes it possible to multiply two words in normal form by concatenating the two words and computing the normal form of the concatenation.
Classes of groups in which it is possible to solve the word problem and in which elements can be multiplied in an efficient way are naturally an attractive object of study in computational group theory. Such classes are, among others, finite permutation groups and matrix groups. The class of groups which can be defined by a finite presentation does not allow an algorithmic solution to the word problem. It is well known that there exists a finite presentation for a group for which no algorithm exists that can decide whether a given word is the identity element of the group. However, this can serve only as an indication that finite presentations pose difficult computational problems. There are well developed and widely used tools for the study of finitely presented groups, for instance coset enumeration.

This motivates that part of computational group theory concerned with the design of methods for the computation of those factor groups of finitely presented groups which can be described in a way that allows practical computations. These methods include algorithms for the computation of the isomorphism type of the largest abelian factor group, the computation of quotient $p$-groups (Havas&Newman, 1980) and the computation of metabelian groups with finitely generated derived group (Sims, 1990). Factor groups of finitely generated groups are often computed in order to gain insight into the structure of the finitely presented group. Therefore, algorithms which compute quotients of finitely presented groups tend to be used as an analytic tool. Computational group theory, however, also designs methods for the construction of groups or lists of groups that have a given set of properties. Two examples of this are the computer aided construction of many of the sporadic finite simple groups and the $p$-group generation algorithm (O'Brien, 1990). The importance of the computational methods becomes clear from the fact that for many sporadic simple groups the first constructions and uniqueness proofs relied on computer calculations. The $p$-group generation algorithm has been used for the listing of all groups of order 128 (James, Newman, O'Brien, 1990) and the listing of all groups of order 256 (O'Brien, 1990). These two aspects, here called the analytic and the synthetic aspect, of computational group theory are closely related. It should not be surprising that construction methods for groups facilitate representations of groups that are well suited for practical computations.
This dissertation is written on "Central Extensions of Polycyclic Groups". The title encompasses both aspects of computational group theory. The first part of this dissertation is concerned with the analytic aspect. Here, we describe an algorithm for the computation of polycyclic presentations for nilpotent quotient groups of finitely presented groups. The second part describes a method for the construction of polycyclic presentations of representatives of the different isomorphism classes of Schur covering groups of a finite soluble group. For this it is assumed that the soluble group is given in terms of a polycyclic presentation. Both algorithms take a polycyclic presentation for a group $G$ and construct a polycyclic presentation for a preimage $H$ of $G$ such that the kernel of the projection $H \rightarrow G$ is central in $H$. Informally, the polycyclic presentation "is extended by a central part". This step is applied repeatedly in order to construct polycyclic presentations for nilpotent factor groups of finitely presented groups. The classification of Schur covers of $G$ is achieved by describing the action of a group of automorphisms on a suitable preimage of $G$ such that certain orbits under this action correspond to the isomorphism classes of Schur covers of $G$.

Chapter 1 sets up some notation and cites basic results that are used in the rest of the dissertation. In Chapter 2 the basic theory of polycyclic groups is described. The material in this chapter is well known and mostly contained in Hirsch (1938a, 1938b) and Sims (1993). Chapter 3 discusses polycyclic presentations and addresses the problem of testing the consistency of a polycyclic presentation. Chapter 4 introduces the notion of quotient systems. This is an attempt to describe a standard situation in the computation of factor groups of finitely presented groups by a mathematical object, the quotient system. In this chapter central extensions of quotient systems are discussed. From this a first approach to the computation of nilpotent factor groups of finitely presented groups follows. The next chapter, Chapter 5, refines this to a practical "nilpotent quotient algorithm". It also discusses special kinds of polycyclic presentations and quotient systems for nilpotent groups. This concludes the "analytic" part of the dissertation.

In the relatively short Chapter 6 we make some general observations that reduce the problem of determining downward extensions of groups up to isomorphism to the problem of calculating certain orbits of a group of automorphisms on
a suitably chosen quotient of some free group. Here we have to restrict our considerations to Hopfian groups. Chapter 7 describes the basic theory of the Schur multiplicator of a group and a method for the computation of the Schur multiplicator of a polycyclic group. Again it is assumed that the polycyclic group is given by a polycyclic presentation. We then proceed to use the results of Chapter 6 to describe a method for the classification of the isomorphism classes of Schur covers of finite soluble groups. The chapter finishes with an extended example to demonstrate the algorithm.

The computational theory of polycyclic presentations can be treated in the very general context of rewriting systems. This is done, for example, in Sims (1987, 1993). We have treated the subject "purely group theoretically" and avoided all references to rewriting systems. There is, however, one issue that should be addressed. Polycyclic presentations that define a normal form on the set of words in the generating set are traditionally called consistent and one talks of the consistency check as the algorithm that checks this property. In the context of rewriting systems the same property is called confluence. In recent years it has been discussed, as far as I know without a definitive conclusion, which of the two terms should be used in the future. One argument against the use of 'consistent' is that it has a specific meaning in mathematical logic in the context of consistency of axiomatic systems. However, I felt that I should use the traditional term 'consistent' in this dissertation because it has been the term most widely used in the group theoretic literature. Without mentioning rewriting systems it would have been difficult to justify the use of confluent. The proof of the Consistency Theorem in Chapter 3 shows that a polycyclic presentation is consistent if the action of each polycyclic generator as defined by the polycyclic presentation on the group defined by the later generators and the relevant relations is consistent with the structure of that group. Perhaps this might serve as a (admittedly weak) justification of the term 'consistent'.

During the work on this thesis I had access to a draft of August 1991 of Chapters 8 to 11 of Sims (1993). The material in these chapters was very helpful to me and has undoubtedly had a great influence on this thesis, in particular on Chapters 2 and 3 of this dissertation.
Chapter 9 of this draft of Sims (1993) describes an algorithm for the computation of polycyclic presentations of nilpotent groups. This algorithm and the algorithm described in Chapter 5 of this dissertation are very similar. The algorithm described here has the additional feature of a tails routine (Section 5.4). The performance of an implementation using a tails routine is compared to the performance of an implementation without a tails routine in Section 5.5. The first implementation of a nilpotent quotient algorithm has been done by C.C. Sims in Mathematica. A tails routine is used in the ANU PQ program (former Canberra Nilpotent Quotient Program).

Two computer implementations arose out of the work for this dissertation. The first is a program for the computation of nilpotent factor groups of finitely presented groups. It takes a finite presentation and an optional positive integer $c$ as input and computes a weighted polycyclic presentation (see Chapter 5) for the nilpotency class-$c$ quotient of the finitely presented group. If the parameter $c$ is not specified, the program attempts to compute the largest nilpotent factor group. If a largest nilpotent factor does not exist, it only stops if it runs out of resources. It also has facilities that can be used to enforce various Engel laws on the computed nilpotent group. The program is in demand and is available via anonymous ftp from the Internet host pell.anu.edu.au. It is also available as shared package in the system GAP (Schönert et. al., 1993) and is used as part of the system quotpic (Holt & Rees, to appear). There are plans to make the program available as part of the system Magma which is under development at the University of Sydney. The options for enforcing Engel conditions on nilpotent groups have initiated and have been very useful in Newman and Nickel (1993). However, this program is still under development and an improved version is planned for the near future. The second program takes a polycyclic presentation for a finite soluble group and computes the isomorphism type of the Schur multiplicator for this group. This program is still a prototype version but it is planned to make it publicly available soon.
Chapter 1:
Preliminaries and Notation

This chapter defines some basic notation and lists some basic theorems.

1.1 Presentations

Let $X$ be a set. A \textit{word} $w$ in $X$ is an element of the free monoid generated by the union of $X$ and the set $X^{-1} = \{ x^{-1} \mid x \in X \}$. A generator $x \in X$ occurs in a word $w$ in $X$ if $w$ can be written as $uxv$ or $ux^{-1}v$ where $u$ and $v$ are words in $X$. If it is necessary to make explicit which elements of $X$ occur in $w$, we will write $w(x; x \in X)$ or $w(x_1, \ldots, x_n)$ if $X = \{x_1, \ldots, x_n\}$.

A group presentation is a pair $(X, \mathcal{R})$ in which $X$ is a set and $\mathcal{R}$ is either a set of relators, i.e., a set of words in $X$, or a set of relations, i.e., the elements of $\mathcal{R}$ are of the form $u = v$ where $u$ and $v$ are words in $X$. If $u = v$ is a relation, the \textit{corresponding relator} is the word $v^{-1}u$. Let $F$ be the free group on $X$. The set $\mathcal{R}$ defines a unique normal subgroup $N$ of $F$; if $\mathcal{R}$ is a set of relators, then $N$ is the normal closure of $\mathcal{R}$ in $F$; if $\mathcal{R}$ is a set of relations, then $N$ is the normal closure of the set of relators corresponding to relations in $\mathcal{R}$. In both cases we refer to $N$ as the normal closure of $\mathcal{R}$ in $F$. The group defined by $(X, \mathcal{R})$ is the group $F/N$.

It will often be necessary to equip the generating set $X$ of a finite presentation $(X, \mathcal{R})$ with a linear order. Since only finite presentations are used in this dissertation, we will use the terms 'finite set with a linear order' and 'sequence'
interchangeably and often talk about generating sequences. As a general rule, if elements of a generating sequence carry indices, then the lexicographic order of the indices of two given elements indicate which element is the smaller one. For example, if two elements $a_i$ and $a_j$ of a generating sequence are given, then $a_i$ would be the smaller of the two elements.

A presentation $(X, R)$ can be interpreted as a presentation for an abelian group. Let $F$ be the free abelian group on $X$ and $N$ the subgroup generated by $R$ in $F$. The abelian group defined by the group presentation $(X, R)$ is the factor group $F/N$. Let $X = \{x_1, \ldots, x_n\}$ be equipped with a linear order. An element $w$ of $F$ can be written uniquely in the form $w = x_1^{e_1} \cdots x_n^{e_n}$ where the exponents are integers. The exponent vector $(e_1, \ldots, e_n)$ describes the element $w$ uniquely with respect to the free generating sequence $X$. The set $R$ can be written as an integer matrix $M$ in which the rows of the matrix are the exponent vectors of the elements of $R$. This matrix $M$ is called the relation matrix of $(X, R)$. A relation matrix is a convenient way to represent an abelian group.

Let $M$ be an integer matrix with $m$ rows and $n$ columns. The element in row $i$ and column $j$ is denoted by $M_{ij}$. We say that $M$ is in row Hermite normal form if the following conditions are satisfied, compare Sims (1993), Chapter 8.

- All rows of $M$ are non-zero.
- For $1 \leq i \leq m$ let $M_{ij(i)}$ be the first non-zero entry of row $i$ of $M$. Then $j(1) < \ldots < j(m)$.
- The first non-zero entries in each row are positive.
- For $1 \leq k < i \leq m$ we have that $0 \leq M_{kj(i)} < M_{ij(i)}$.

It is well known that any integer matrix can be transformed to a unique matrix in row Hermite normal form by row reduction, see for example Sims (1993), Chapter 8.

1.1.1 Theorem Let $(X, R)$ be a presentation for an abelian group and let $X$ be equipped with a linear order. Let $N$ be the subgroup of the free abelian group $F$ on $X$ generated by $R$.

There is a generating sequence $R'$ for $N$ for which the corresponding relation matrix is in row Hermite normal form.
The set of all elements of an abelian group $G$ that have finite order is a subgroup of $G$ called the torsion subgroup $\text{Tor}(G)$. The torsion subgroup of a finitely generated abelian group is always complemented and every complement is a free abelian group.

1.2 Groups

Let $G$ be a group and $g$ and $h$ elements of this group. The identity of $G$ is denoted by $1$. The element $g$ acts on $G$ via conjugation by mapping $h$ to $g^{-1}hg$. The commutator of $g$ and $h$ is the term $[g,h] = g^{-1}h^{-1}gh$. For subgroups $U$ and $V$ of $G$ the subgroup of $G$ generated by the set of all commutators $\{ [u,v] \mid u \in U, v \in V \}$ is denoted by $[U,V]$. If $U = V = G$, then $[G,G]$ is called the derived group. The center of $G$ is denoted by $Z(G)$. The Frattini subgroup $\Phi(G)$ of $G$ is the intersection of all maximal subgroups of $G$ if $G$ has maximal subgroups and $G$ itself if $G$ does not have maximal subgroups. The element $g$ is called a non-generator if, whenever $G$ is generated by $S \cup \{g\}$, then it is already generated by $S$ for any subset $S$ of $G$.

1.2.1 Theorem The Frattini subgroup is the set of non-generators of a group $G$.

Proof: See Hall (1959), Section 10.4

1.2.2 Theorem The intersection of the center and the derived group of a group is contained in the Frattini group.

Proof: The proof in Huppert (1967), Kapitel III.3 for Satz 3.12 works for groups in general.

The exponent of $G$ is the smallest positive integer $e$ such that $x^e$ is the identity of $G$ for all $x \in G$ if such an integer $n$ exists; otherwise it is $\infty$.  

8
Chapter 2:
Polycyclic Groups

The systematic study of polycyclic groups was started by Hirsch in two publications (1938a,b) and continued in three further papers (1946, 1952, 1954). In recent years polycyclic groups have attracted attention because they form a large class of groups for which many problems can be solved algorithmically (Segal 1990). This class of groups includes the class of finite soluble groups and the class of finitely generated nilpotent groups. In this chapter we summarize the basic theory for polycyclic groups with focus on computational applications. Material on polycyclic groups can be found in, apart from the publications by Hirsch mentioned above, Sims (1993) and Segal (1983).

2.1 Basic Properties

A group $G$ is called \textit{polycyclic} if it has a finite chain

$$G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n \supseteq G_{n+1} = 1$$

of subgroups such that $G_{i+1}$ is normal in $G_i$ and $G_i/G_{i+1}$ is cyclic for all $1 \leq i \leq n$. Such a chain of subgroups is called a \textit{polycyclic series of G}.

The next theorem summarizes some basic properties of polycyclic groups.

2.1.1 Theorem

a) Subgroups and factor groups of polycyclic groups are polycyclic.
b) Polycyclic groups are finitely generated.
c) Polycyclic groups are soluble.

Proof: Let $G$ be a polycyclic group and $G = G_1 \supseteq \ldots \supseteq G_{n+1} = 1$ a polycyclic series of $G$.

a) For a subgroup $U$ of $G$ define $U_1 = U$, $U_{i+1} = U_i \cap G_{i+1}$. The fact that $G_{i+1}$ is normal in $G_i$ implies that $U_{i+1}$ is normal in $U_i$. The isomorphism $U_iG_{i+1}/G_{i+1} \cong U_i/G_{i+1} \cap U_i = U_i/U_{i+1}$ shows that $U_i/U_{i+1}$ is cyclic because $U_iG_{i+1}/G_{i+1}$ is a subgroup of $G_i/G_{i+1}$.

For a normal subgroup $N \leq G$ define $N_i = G_iN/N$. It is easy to see that $N_{i+1}$ is normal in $N_i$. The factor group $N_i/N_{i+1}$ is isomorphic to $G_iG_{i+1}N/G_{i+1}N$ which in turn is isomorphic to $G_i/G_i \cap G_{i+1}N$. The latter is a factor group of $G_i/G_{i+1}$ and therefore cyclic.

b) Assume that $G_2$ has a finite generating set $\{g_2, \ldots, g_l\}$. Because $G/G_2$ is cyclic, there is an element $g_1 \in G$ such that $G = \langle g_1, G_2 \rangle$. Then $\{g_1, \ldots, g_l\}$ is a generating set for $G$ and the claim follows by induction.

c) Assume that $G_2$ is soluble. The factor group $G/G_2$ is, as it is cyclic, soluble. Therefore, $G$ is soluble because it has a soluble normal subgroup with soluble quotient. The claim follows by induction.

From part b) and c) of the theorem above the question arises whether finitely generated soluble groups are polycyclic. Since polycyclic groups are finitely generated, only finitely generated soluble groups can be polycyclic. But the following example shows that a finitely generated soluble group need not be polycyclic. The reason for this is that finitely generated soluble groups can have subgroups which are not finitely generated.

2.1.2 Example The subgroup $T = \{2^i m \mid i, m \in \mathbb{Z}\}$ of the additive group of the rational numbers is clearly not finitely generatable. A generating set for $T$ is the set $\{2^{-i} \mid i \in \mathbb{N}\}$. It is easy to see that the map $2^{-i} \mapsto 2^{-i-1}$ defines an automorphism $\alpha$ of $T$ of infinite order. The orbit of $2^{-1}$ under $\alpha$ generates $T$. Therefore, the semidirect product $S$ of $T$ and the cyclic group generated by $\alpha$ can be generated by two elements. $S$ is clearly soluble but not polycyclic because $T$ cannot be generated by a finite number of elements. Compare Segal (1983, p.4) and Sims (1987).
However, the following theorem shows that a soluble group all of whose subgroups are finitely generated is polycyclic. It is sufficient to impose this condition on the subgroups of the derived series.

2.1.3 Theorem

a) A group is polycyclic if it has a polycyclic normal subgroup with polycyclic factor group.

b) Finitely generated abelian groups are polycyclic.

c) A soluble group is polycyclic if all the subgroups in its derived series are finitely generated.

Proof:

a) Let $N$ be a normal subgroup of a group $G$ such that $N$ and $H = G/N$ are polycyclic. Let $N = N_0 \supseteq \ldots \supseteq N_{l+1} = 1$ be a polycyclic series for $N$ and $H = H_0 \supseteq \ldots \supseteq H_{k+1} = 1$ a polycyclic series for $H$. Define $G_i$ to be the complete preimage of $H_i$ in $G$. Then $G_0 \supseteq \ldots \supseteq G_k \supseteq G_{k+1} = N_0 \supseteq \ldots \supseteq N_{l+1}$ is a polycyclic series for $G$.

b) If $G$ is a finitely generated abelian group and $\{g_1, \ldots, g_n\}$ a generating set for $G$, then the groups $G_i = \langle g_i, \ldots, g_n \rangle$ form a polycyclic series.

c) Let $G$ be a soluble group and let $G^{(i)}$ be the $i$-the term in the derived series of $G$. Assume that $G/G^{(i)}$ is polycyclic. The factor group $G^{(i)}/G^{(i+1)}$ is a finitely generated abelian group because $G^{(i)}$ is finitely generated. By parts a) and b) of this theorem, it follows that $G/G^{(i+1)}$ is polycyclic and the claim follows by induction.

The following theorem is useful in deciding whether a given endomorphism of a polycyclic group is an automorphism. It will be used in Section 3.3. The proof is really an argument from universal algebra. A group $G$ satisfies the ascending chain condition on subgroups if there is no infinite ascending sequence $U_1 < U_2 < \ldots$ of subgroups of $G$.

2.1.4 Theorem

a) A polycyclic group satisfies the ascending chain condition on subgroups.

b) Every surjective endomorphism of a polycyclic group is an automorphism.

Proof:
a) The claim follows from the fact that subgroups of polycyclic groups are finitely

generatable. For, if \( U_1 \leq U_2 \ldots \) is an ascending sequence of subgroups of a
polycyclic group \( G \), then \( U = \bigcup_{i=1}^{\infty} U_i \) is a subgroup of \( G \) and has a finite
generating set \( S \). Because \( S \) is finite, there is a \( k \) such that \( S \subseteq U_k \) and
\( U = U_k \).

b) Let \( \sigma \) be a surjective endomorphism of a polycyclic group \( G \). Define \( \sigma^0 \) to be
the identity on \( G \) and \( \sigma^{i+1} = \sigma^i \sigma \) for \( i > 0 \). Clearly, \( \sigma^i \) is surjective. Therefore,
for \( h \in \ker \sigma \) there is a \( g \in G \) such that \( g \sigma^i = h \). Obviously, \( g \in \ker \sigma^{i+1} \).
This shows that \( (\ker \sigma^{i+1}) \sigma^i = \ker \sigma \) and the homomorphism theorem yields
\( \ker \sigma^{i+1} / \ker \sigma^i \cong \ker \sigma \). If \( \ker \sigma \neq 1 \), then \( 1 < \ker \sigma < \ker \sigma^2 < \ldots \) is
a strictly ascending chain of subgroups. Therefore \( \ker \sigma \) must be trivial.

A group is called hopfian if every surjective endomorphism of the group is an
automorphism. A hopfian group cannot be isomorphic to a proper factor group
of itself. Part b) of the theorem above says that polycyclic groups are hopfian.
In Section 3.3 and Chapter 6 we will consider hopfian groups and the statements
made there are directly applicable to polycyclic groups.

2.2 Polycyclic Generating Sequences

We are now going to use the existence of a polycyclic series in polycyclic
groups to define a normal form for the elements of polycyclic groups. For this, let
\( G \) be a polycyclic group with a polycyclic series \( G = G_1 \geq \ldots \geq G_{n+1} = 1 \). The
proof of Theorem 2.1.1 b) shows that there are elements \( \{g_1, \ldots, g_n\} \) of \( G \) such
that \( G_i = \langle g_1, \ldots, g_n \rangle \) and \( g_i G_{i+1} \) is a generator of \( G_i / G_{i+1} \).

2.2.1 Definition A sequence \( \langle g_1, \ldots, g_n \rangle \) of elements of \( G \) is called a polycyclic
generating sequence of \( G \) if the groups \( G_i = \langle g_i, \ldots, g_n \rangle \) form a polycyclic series
of \( G \).

A polycyclic generating sequence can be used to express each element of \( G \)
in a unique form as follows. An element \( g \in G_i \) can be written as a product \( g_i^{e_i} g' \)
with \( g' \in G_{i+1} \). This product is unique if \( G_i / G_{i+1} \) is infinite or if \( G_i / G_{i+1} \) is
finite of order \( m_i \) and \( 0 \leq e_i < m_i \). By induction, every \( g \in G \) can be expressed
uniquely as a product $g_1^{e_1} \ldots g_n^{e_n}$ where $0 \leq e_j < m_j$ if $G_j/G_{j+1}$ is finite of order $m_j$. The word $g_1^{e_1} \ldots g_n^{e_n}$ is called the normal form of $g$ with respect to the polycyclic generating sequence $(g_1, \ldots, g_n)$. If it is clear from the context which polycyclic generating sequence is meant, it will be called the normal form of $g$.

A word $w$ in the generators of a polycyclic generating sequence $(g_1, \ldots, g_n)$ is in normal form if and only if $w = g_1^{e_1} g_2^{e_2} \ldots g_n^{e_n}$ with $0 \leq e_i < m_i$ if $G_i/G_{i+1}$ is finite of order $m_i$.

Now let $G$ be a polycyclic group with a polycyclic generating sequence $(g_1, \ldots, g_n)$ and $G = G_1 \geq \ldots \geq G_{n+1} = 1$ the corresponding polycyclic series. If $G_i/G_{i+1}$ is finite of order $m_i$ then $g_i^{m_i}$ is an element of $G_{i+1}$ and its normal form is a product $w_{ii}$ of powers of $g_{i+1}, \ldots, g_n$. In this case the normal form of $g_i^{-1}$ is $g_i^{-m_i-1} w_{ii}$ where $w_{ii}$ is a word in $g_{i+1}, \ldots, g_n$. The subgroup $G_{i+1}$ is normal in $G_i$ and therefore the conjugates $g_i^{-1} g_j g_i$ for $i + 1 \leq j \leq n$ are elements of $G_{i+1}$ and their normal forms are products $w_{ij}^{\pm}$ of powers of $g_{i+1}, \ldots, g_n$. Similarly, the normal forms of the conjugates $g_i g_j g_i^{-1}$, $g_i^{-1} g_j^{-1} g_i$ and $g_i g_j^{-1} g_i^{-1}$, are products $w_{ij}^{\pm}$, $w_{ij}^{-\pm}$, $w_{ij}^{-\pm}$ of powers of $g_{i+1}, \ldots, g_n$, respectively. We summarize this in the following list of equations:

$$
g_i^{m_i} = w_{ii} \quad \text{if } G_i/G_{i+1} \text{ is finite of order } m_i
$$
$$
g_i^{-1} = g_i^{m_i-1} w_{ii}^{-} \quad \text{if } G_i/G_{i+1} \text{ is finite of order } m_i
$$

$$
g_i^{-1} g_j g_i = w_{ij}^{\pm}
$$
$$
g_i g_j g_i^{-1} = w_{ij}^{-\pm}
$$
$$
g_i^{-1} g_j^{-1} g_i = w_{ij}^{+\pm}
$$
$$
g_i g_j^{-1} g_i^{-1} = w_{ij}^{-\pm}.
$$

The words on the right hand side of the relations carry superscripts that indicate which generators on the left hand side of the relation are inverted.

If a word $w$ in the generators of the polycyclic generating sequence is not in normal form, then there are subwords of $w$ which are minimal with respect to not being in normal form. The definition of the normal form yields the following four cases:

- the factor $G_k/G_{k+1}$ is finite and $g_k^{-1}$ is a subword of $w$;
- the factor $G_k/G_{k+1}$ is finite of order $m_k$ and the power $g_k^{m_k}$ is a subword of $w$;
- the word $g_l^{\varepsilon_l} g_k^{\varepsilon_k}$ with $l > k$ and $\varepsilon_k, \varepsilon_l \in \{1, -1\}$ is a subword of $w$;
- the word $g_k^{-1} g_k^l$ or the word $g_k^{-1} g_k^l$ is a subword of $w$.

In each of these cases a minimal subword of $w$ violating the normality conditions can be replaced by a word in normal form as follows
- replace $g_k^{-1}$ by $g_k^{-1} w_{kk}$;
- replace $g_k^{m_k}$ by $w_{kk}$;
- replace $g_l^{\varepsilon_l} g_k^{\varepsilon_k}$ by $g_k^{\varepsilon_k} w_{k l}^{\varepsilon_l}$;
- replace $g_l g_l^{-1}$ or $g_l^{-1} g_l$ by the empty word.

Each of these steps is called an elementary collection step. Note that a word in the generators $g_1, \ldots, g_n$ can be transformed to a word in normal form by only using relations that involve these generators.

2.2.2 Lemma Each word in the polycyclic generating sequence can be transformed into normal form by a sequence of elementary collection steps.

Proof: The subgroup $G_n$ consists only of powers of $g_n$. A word in $\{g_n\}$ can be transformed to the word $g_n^{\varepsilon_n}$ with $\varepsilon_n \in \mathbb{Z}$ by a sequence of free reduction steps, i.e., replacing $g^{-1} g$ or $gg^{-1}$ by the empty word. If $G_n$ is infinite, then this word is already in normal form. If $G_n$ is finite of order $m_n$, then the equation $g^{-1} = g^{m_n-1}$ can be used to make the exponent positive and the equation $g_n^{m_n} = 1$ to make it smaller than $m_n$.

For $i < n$ assume that every word in the generators $\{g_{i+1}, \ldots, g_n\}$ can be transformed into normal form. Consider a word $u$ in $\{g_i, \ldots, g_n\}$. All occurrences of the generator $g_i$ and its inverse in $u$ can be moved to the left using a sequence of elementary collection steps. The result is a product $u' u''$ where $u'$ is a word in $g_i$ and $u''$ a word in $\{g_{i+1}, \ldots, g_n\}$. Applying a sequence of free reduction steps to $u'$ gives the word $g_i^{\varepsilon_i} u''$ with $\varepsilon_i \in \mathbb{Z}$. If $G_i/G_{i+1}$ is infinite, then the word $g_i^{\varepsilon_i}$ is in normal form. If $G_i/G_{i+1}$ is finite of order $m_i$, then $g_i^{\varepsilon_i}$ can be transformed to a word $g_i^{\varepsilon_i} v$, where $v$ is a word in $\{g_{i+1}, \ldots, g_n\}$ and $0 \leq \varepsilon_i < m_i$, by a series of elementary collection steps. By the inductive assumption, the remaining words $u''$ and $vu''$, respectively, can be transformed into a word $u'''$ in normal form. The word $g_i^{\varepsilon_i} u'''$ is in normal form.
Some remarks about this proof are in order. The process of transforming a given word in the polycyclic generating sequence of a group into normal form is called collection. The above proof uses the fact that applying an elementary collection step to a subword in the generators $g_k, \ldots, g_n$ for all $1 \leq k \leq n$ cannot introduce any of the generators $g_1, \ldots, g_{k-1}$. This fact will be called the fundamental principle of collection. It could not be guaranteed that the procedure in the proof for computing the normal form of a word would ever terminate if moving occurrences of $g_i$ to the left or collecting the words $u''$ and $vu''$ could introduce generators $g_1, \ldots, g_i$.

While collecting all occurrences of the generator $g_i$ and its inverse in $u$ to the left, it is possible to apply a sequence of elementary collection steps to subwords consisting of the generators $\{g_{i+1}, \ldots, g_n\}$. This cannot introduce new occurrences of $g_i$ because of the fundamental principle of collection. Therefore, as long as all occurrences of $g_i$ or its inverse are collected to the left after a finite number of steps, the collection process will stop. There are a variety of different collection strategies; see for example Leedham-Green & Soicher (1990) and Vaughan-Lee (1990) and the references in those papers.

2.2.3 Theorem The relations (*) define $G$ as a group.
Proof: All that has to be shown is that any relation that holds in $G$ is a consequence of the relations (*). But a relation in $G$ is an equation $u = v$, which is equivalent to $v^{-1}u = 1$. The normal form of $v^{-1}u$ is the empty word. By the previous lemma, the word $v^{-1}u$ can be reduced to the empty word by the relations (*) and therefore is a consequence of those relations. ■

2.2.4 Corollary The relations involving only the generators $\{g_i, \ldots, g_n\}$ define $G_i$ as a group.

2.2.5 Theorem The relations

$$g_i^{m_i} = w_{ii} \quad \text{if } G_i/G_{i+1} \text{ is finite}$$

$$g_i^{-1} g_j g_i = w_{ij}^{++}$$

are already sufficient to define $G$ as a group.
Proof: It has to be proved that the following relations

\[ g_i^{-1} = g_i^{m_i} w_{ii}^{-1} \]
\[ g_i g_j g_i^{-1} = w_{ij}^{-+} \]
\[ g_i^{-1} g_j^{-1} g_i = w_{ij}^{+-} \]
\[ g_i g_j^{-1} g_i^{-1} = w_{ij}^{-+} \]

are consequences of the relations in the claim. The proof works by induction along the polycyclic series of \( G \). For the subgroup generated by \( g_n \) nothing has to be proved. Assume that the relations involving only the generators \( g_{i+1}, \ldots, g_n \) define the subgroup \( G_{i+1} \) as a group and that therefore the relations above for \( G_{i+1} \) are a consequence of the relations in the claim and known.

The word \( w_{ij}^{-+} \) can be computed as follows. Conjugation by \( g_i \) is an automorphism of \( G_{i+1} \) because \( G_{i+1} \) is normal in \( G_i \). Therefore, \( G_{i+1} \) is generated by the conjugates \( g_i^{-1} g_{i+1} g_i, \ldots, g_i^{-1} g_n g_i \) and there exist words \( u_{i+1}, \ldots, u_n \) in these conjugates such that \( u_k = g_k \) as elements of \( G_{i+1} \). With this we get

\[ w_{ik}^{-+} = g_i g_k g_i^{-1} = g_i u_k(g_i^{-1} g_{i+1} g_i, \ldots, g_i^{-1} g_n g_i) g_i^{-1} = u_k(g_{i+1}, \ldots, g_n) \]

as elements of \( G \). The word \( u_k(g_{i+1}, \ldots, g_n) \) can be collected to normal form using the complete set of relations for \( G_{i+1} \) which are known by the inductive assumption. The words \( w_{ii}^{-}, w_{ij}^{+-} \) and \( w_{ij}^{-+} \) can be computed in \( G_{i+1} \) as the inverses of \( w_{ii}^{-}, w_{ij}^{+-} \) and \( w_{ij}^{-+} \), respectively.

The above proof can be turned into an algorithm based on an algorithm known as the noncommutative Gauss-algorithm. For finite polycyclic groups it has been described in Laue et al. (1984). A description for the general case of polycyclic groups appears in Sims (1993). The non-commutative Gauss algorithm takes a generating set for a subgroup of a polycyclic group and computes a polycyclic generating sequence for the subgroup. Define a subgroup \( U \) of the direct product \( G_{i+1} \times G_{i+1} \) as generated by the \( \{(w_{ij}^{+-}, g_j) \mid i + 1 \leq j \leq n\} \). The elements of \( U \) are of the form \( (g_i^{-1} gg_i, g) \) or, equivalently, \( (g, g_i gg_i^{-1}) \) with \( g \in G_{i+1} \). The noncommutative Gauss-algorithm applied to this generating set of \( U \) will
terminate with the generating sequence \(((g_{i+1}, g_i g_{i+1}^{-1}), \ldots, (g_n, g_i g_n g_i^{-1}))\) for \(U\) with the second components being words in normal form. From this the action of \(g_i^{-1}\) on the generators \(g_{i+1}, \ldots, g_n\) can be read off. The computation requires only the complete set of relations for \(G_{i+1}\) which can be assumed to be known by induction. For similar techniques compare Leedham-Green et al. (1991).

2.3 Polycyclic Nilpotent Groups

We now turn attention to nilpotent groups. The lower central series of a group \(G\) is defined as

\[ \gamma_1(G) = G, \quad \gamma_{i+1}(G) = [\gamma_i(G), G] \quad \text{for} \quad i \in \mathbb{N}. \]

The group \(G\) is called nilpotent if \(\gamma_{c+1}(G) = 1\) for some \(c \in \mathbb{N}\). The smallest number \(c\) such that \(\gamma_{c+1}(G) = 1\) is called the nilpotency class of \(G\). The weight \(w(g)\) of an element \(g\) of \(G\) is the smallest positive integer \(i\) such that \(g\) is not an element of \(\gamma_i(G)\). If \(g\) is contained in \(\gamma_i(G)\) for all \(i \in \mathbb{N}\), the weight of \(g\) is defined to be \(\infty\). We adopt the convention that \(\infty + i = \infty\) for all \(i \in \mathbb{N}\).

Of central importance in nilpotent groups is the commutator calculus and we are going to prove some basic identities in the following lemma.

2.3.1 Lemma Let \(a, b, c\) be elements of a group.

a) \([ab, c] = [a, c][a, c, b][b, c]\).

b) \([a, bc] = [a, c][a, b][a, b, c]\).

c) \([b, a, c^b][c, b, a^c][a, c, b^a] = 1\).

d) \([a, b^{-1}, c]^b[c, b^{-1}, a]^c[c, a^{-1}, b]^a = 1\) (Witt-identity).

Proof: Any of these identities could be proved by expanding the left and the right hand sides and comparing the results. A more elegant approach is to derive each identity by collecting a suitable word and thereby introducing the required commutators.

a) \((ab)c = cab[ab, c]\)

\[ a(bc) = ca[a, c][b, c] = cab[a, c][a, c, b][b, c]. \]
b) \[ a(bc) = bca[a, bc] \]
\[ (ab)c = ba[a, b]c = bca[a, c][a, b][a, b, c]. \]

c) \[ acb^a = ca[a, c]b^a \]
\[ = cab^a[a, c][a, c, b^a] \]
\[ = cba^c[a, c, b^a]. \]

Applying the permutation \((a, c, b)\) to the equation above gives \(cba^c = bac^b[c, b, a^c]\) and applying it again gives \(bac^b = acb^a[b, a, c^b]\). Now substituting backwards into the right hand side of the first equation proves the identity.

d) This identity follows from c) and the fact \([a, b^{-1}]^b = [b, a]\). 

A consequence of the Witt-identity is the Three Subgroup Lemma.

2.3.2 Lemma  
Let \(K, L\) and \(M\) be subgroups of a group and let \(N\) be a normal subgroup of the same group. If two of the subgroups \([K, L, M]\), \([L, M, K]\), and \([M, K, L]\) are contained in \(N\), then the third is also contained in \(N\).

Proof: We show that \([K, L, M]\), \([L, M, K]\) \(\subseteq N\) implies \([M, K, L] \in N\). The normal closure of the set \(\{[m, k, l] \mid m \in M, k \in K, l \in L\}\) contains \([M, K, L]\) and is contained in \(N\) as the Witt-identity shows: \([m, k^{-1}, l]^k = [l, m^{-1}, k]^{-m[k, l^{-1}, m]}\). The right hand side is contained in \(N\) and therefore the left hand side is contained in \(N\).

The next lemma proves a basic fact about the subgroups in the lower central series. A consequence is that the weight is a subadditive function on the set of commutators.

2.3.3 Lemma  

a) \([\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)\) for all \(i, j \in \mathbb{N}\).

b) \(w(g) + w(h) \leq w([g, h])\) for all \(g, h \in G\).

Proof:

a) The proof is done by induction on \(j\). For all \(i \in \mathbb{N}\) and \(j = 1\) the claim is true by the definition of the lower central series. Let the induction hypothesis
be that \([\gamma_i(G), \gamma_j(G)]\) is a subgroup of \(\gamma_{i+j}(G)\) for some fixed \(j \in \mathbb{N}\) and for all \(i \in \mathbb{N}\). Now

\[
[\gamma_i(G), \gamma_{j+1}(G)] = [\gamma_i(G), [\gamma_j(G), G]] = [\gamma_j(G), \gamma_i(G)].
\]

It suffices to show that \(\gamma_{i+j+1}(G)\) contains the subgroups \([G, \gamma_i(G), \gamma_j(G)]\) and \([\gamma_i(G), \gamma_j(G), G]\) because then, by the Three Subgroup Lemma, it follows that \(\gamma_{i+j+1}(G)\) contains \([\gamma_j(G), G, \gamma_i(G)]\) and therefore \([\gamma_i(G), \gamma_{j+1}(G)]\) and the claim follows by induction on \(j\). The subgroup \([G, \gamma_i(G), \gamma_j(G)]\) is equal to \([\gamma_{i+1}(G), \gamma_j(G)]\) which is contained in \(\gamma_{i+j+1}(G)\) by the induction hypothesis. The subgroup \([\gamma_i(G), \gamma_j(G), G]\) is, again by the induction hypothesis, contained in \([\gamma_i+1(G), G]\) which is equal to \(\gamma_{i+j+1}(G)\).

b) The elements \(g\) and \(h\) are contained in \(\gamma_{w(g)}(G)\) and \(\gamma_{w(h)}(G)\), respectively. Their commutator \([g, h]\) is contained in \([\gamma_{w(g)}(G), \gamma_{w(h)}(G)]\) and the claim follows by a).

2.3.4 Lemma Let \(a, b\) and \(c\) be elements of a group and let \(v = 2w(a) + w(c)\) and \(w = w(a) + w(b) + w(c)\).

a) \([ab, c] = [a, c][b, c]\) modulo \(\gamma_w(G)\).

b) \([a, bc] = [a, b][a, c]\) modulo \(\gamma_w(G)\).

c) \([a^{-1}, c] = [a, c]^{-1}\) modulo \(\gamma_v(G)\).

Proof: The commutators \([a, b, c]\), \([a, c, b]\) and \([a, c, [a, b]]\) are elements of \(\gamma_w(G)\). The first two claims now follow from the first lemma in this section. The third claim follows from a) by setting \(b = a^{-1}\).

2.3.5 Lemma Let \(a_1, \ldots, a_n\) and \(c\) be elements of a group, let \(v\) be the minimum of the weights of \(a_i\), \(1 \leq i \leq n\), and let \(w = 2v + w(c)\). Then

a) \([a_1 \ldots a_n, c] = [a_1, c] \ldots [a_n, c]\) modulo \(\gamma_w(G)\).

b) \([c, a_1 \ldots a_n] = [c, a_1] \ldots [c, a_n]\) modulo \(\gamma_w(G)\).

Proof: By induction on \(n\). For \(n = 2\) the claims are part of the previous lemma. For \(n > 2\) the elements \(a_1 \ldots a_{n-1}\) and \(a_n\) both have weight at least \(v\) and therefore \([a_1 \ldots a_n, c] = [a_1 \ldots a_{n-1}, c][a_n, c]\) modulo \(\gamma_w(G)\) by the previous lemma. Now a) follows by induction. Part b) is proved similarly.
2.3.6 Theorem The Frattini group of a nilpotent group contains the derived group.

Proof: For a proof see Hall (1959), Section 10.4.

2.3.7 Theorem Let \( \{a_1, \ldots, a_d\} \) be a generating set for a group \( G \) modulo \( \gamma_2(G) \) and let \( \{b_1, \ldots, b_e\} \) be a generating set for \( \gamma_i(G) \) modulo \( \gamma_{i+1}(G) \).

Then \( \{[b_j, a_i] \mid 1 \leq i \leq d, 1 \leq j \leq e\} \) generates \( \gamma_{i+1}(G) \) modulo \( \gamma_{i+2}(G) \).

Proof: Let \( b \) be an element of \( \gamma_i(G) \). Then \( b \) is a product \( b_{i_1} \ldots b_{i_m} c \) for some \( m \in \mathbb{N} \) and \( c \in \gamma_{i+1}(G) \). Each element \( b_{i_j} \) has at least weight \( i \) and \( c \) is central modulo \( \gamma_{i+2}(G) \). Therefore, the commutator \( [b, a] \) for any element \( a \in G \) is equal to \( [b_{i_1}, a] \ldots [b_{i_m}, a] \) modulo \( \gamma_{2i+1}(G) \subseteq \gamma_{i+2}(G) \).

Any element \( a \in \gamma_1(G) = G \) is a product \( a_{i_1} \ldots a_{i_l} \) for some \( l \in \mathbb{N} \) because \( \Phi(G) \geq \gamma_2(G) \). Each \( a_{i_j} \) has weight at least 1. Therefore, the commutator \( [b, a] \) for any \( b \in \gamma_i(G) \) is equal to \( [b, a_{i_1}] \ldots [b, a_{i_l}] \) modulo \( \gamma_{i+2}(G) \).

By definition, \( \gamma_{i+1}(G) \) is generated by \( \{[b, a] \mid b \in \gamma_i(G), a \in G\} \). Each element of this set can be expressed, by the considerations above, as a product of commutators \( [b_j, a_i] \) modulo \( \gamma_{i+2}(G) \). This proves the claim.

2.3.8 Theorem Finitely generated nilpotent groups are polycyclic.

Proof: Let \( G \) be a finitely generated nilpotent group. The quotient group \( \gamma_i(G)/\gamma_{i+1}(G) \) is an abelian group and, by the previous theorem, finitely generated. If \( G/\gamma_i(G) \) is polycyclic, then \( G/\gamma_{i+1}(G) \) is polycyclic by Theorem 2.1.3. The claim follows by induction.

2.3.9 Definition A polycyclic series \( G = G_1 \geq \ldots \geq G_{n+1} = 1 \) is called a central polycyclic series if \( G_i \) is normal in \( G \) and \( G_i/G_{i+1} \) is a subgroup of the centre of \( G/G_{i+1} \). A polycyclic generating sequence for \( G \) that defines a central series is called a central polycyclic generating sequence.

2.3.10 Definition A polycyclic series refining the lower central series of a nilpotent group \( G \) is called a nilpotent series for \( G \). It is clear that a nilpotent series is
a central series. A polycyclic generating sequence for $G$ that defines a nilpotent series is called a nilpotent generating sequence.

Let $G$ be a polycyclic group given by a central polycyclic generating sequence $(a_1, \ldots, a_n)$ and let $G = G_1 \geq \ldots \geq G_{n+1} = 1$ be the corresponding polycyclic series. Because this is a central series for $G$, we have $[a_j, a_i] \in G_{j+1}$ and, therefore, the normal form of $a_j^{-1}a_i^{-1}a_ja_i$ is a word in the generators $a_{j+1}, \ldots, a_{n+1}$ and their inverses. This leads to the following set of defining relations for $G$:

$$a_i^{m_i} = w_{ii} \quad \text{if } G_i/G_{i+1} \text{ is finite of order } m_i$$

$$a_i^{-1} = a_i^{m_i}w_{ii}^{-1} \quad \text{if } G_i/G_{i+1} \text{ is finite of order } m_i$$

$$a_i^{-1}a_ja_i = a_jw_{ij}^{++}$$

$$a_ia_ja_i^{-1} = a_jw_{ij}^{+}$$

$$a_i^{-1}a_j^{-1}a_i = a_jw_{ij}^{-+}$$

$$a_i^{-1}a_j^{-1} = a_jw_{ij}^{-},$$

where $w_{ij}^{e_i e_i}$ is a word in the generators $a_{j+1}, \ldots, a_n$ and $1 \leq i < j \leq n$. If one of the subgroups in the central polycyclic series is the Frattini subgroup of $G$, then $G$ is, as the following theorem shows, defined by a set of relations smaller than the set in Theorem 2.2.5. Note that the generator $a_i$ in the set of conjugate relations in the claim of the following theorem only runs through a set of generators modulo $\Phi(G)$.

2.3.11 Theorem Let $G$ be a nilpotent group with a central polycyclic generating sequence $(a_1, \ldots, a_n)$ and let $G = G_1 \geq \ldots \geq G_{n+1} = 1$ be the corresponding central series. Furthermore, let $G_{d+1}$ be contained in the Frattini subgroup $\Phi(G)$ of $G$ for some $1 \leq d \leq n$. Then $G$ is defined as a group by the relations

$$a_i^{m_i} = w_{ii} \quad \text{if } G_i/G_{i+1} \text{ is finite of order } m_i \text{ for } 1 \leq i \leq n$$

$$a_i^{-1}a_ia_i = a_iw_{il}^{++} \quad \text{for } 1 \leq i \leq d \text{ and } 1 \leq i < l \leq n.$$
The proof proceeds by induction along the polycyclic series. Assume that for
\( G_{j+1} \) a complete set of defining relations is given, i.e.,

\[
\begin{align*}
    a_k^{m_k} &= w_{kk} & \text{if } G_k/G_{k+1} \text{ is finite of order } m_k \\
    a_k^{-1} &= a_k^{m_k-1}w_k^{-1} & \text{if } G_k/G_{k+1} \text{ is finite of order } m_k \\
    a_k^{-1}a_i a_k &= a_i w_{kl}^{++} \\
    a_k a_i a_k^{-1} &= a_i w_{kl}^{-1} \\
    a_k^{-1} a_i^{-1} a_k &= a_i w_{kl}^{+-} \\
    a_k a_i^{-1} a_k^{-1} &= a_i w_{kl}^{-+},
\end{align*}
\]

where \( j + 1 \leq k < l \leq n \), as well as the relations

\[
\begin{align*}
    a_i^{-1} a_i a_i &= a_i w_{il}^{++} \\
    a_i a_i a_i^{-1} &= a_i w_{il}^{-+} \\
    a_i^{-1} a_i^{-1} a_i &= a_i w_{il}^{+-} \\
    a_i a_i^{-1} a_i^{-1} &= a_i w_{il}^{-+},
\end{align*}
\]

where \( 1 \leq i \leq d \) and \( j + 1 \leq l \leq n \).

It has to be shown that a complete set of defining relations for \( G_j \) can be derived. The right hand side of the relation \( a_j^{-1} a_l a_j = a_l w_{jl}^{++} \) can be computed for \( j + 1 \leq l \leq n \) using the word \( u_j(a_1, \ldots, a_d) \):

\[
a_j^{-1} a_l a_j = u_j(a_1, \ldots, a_d)^{-1} a_l u_j(a_1, \ldots, a_d).
\]

The generators to the right of \( a_l \) can be moved, one by one, to the left by using the relations \((*)\). Each generator in \( u_j(a_1, \ldots, a_d) \) cancels out with the corresponding inverse of that generator in \( u_j(a_1, \ldots, a_d)^{-1} \). After all generators have been moved to the left of \( a_l \), the right hand side of the above equation has become a product \( a_l v \) where \( v \) is a word in the generators \( a_{l+1}, \ldots, a_n \). This word can be transformed to normal form by the relations for \( G_{j+1} \).
The relations

\[
\begin{align*}
    a_j a_l a_j^{-1} &= a_l w_{jl}^- \\
    a_j^{-1} a_i^{-1} a_j &= a_l w_{jl}^+ \\
    a_j a_l^{-1} a_j^{-1} &= a_l w_{jl}^- & \text{for } j + 1 \leq l \leq n
\end{align*}
\]

can now be obtained as in the proof of Theorem 2.2.5.

It remains to compute the right hand sides \( w_{ij}^- \) for \( 1 \leq i \leq d \). Each can be computed as follows:

\[
    a_j = a_j a_i^{-1} a_j^{-1} = a_j a_i a_j^{-1} a_i w_{ij}^+ a_i^{-1}
\]

The word \( w_{ij}^+ \) is a word in \( \{a_{j+1}, \ldots, a_n\} \) and the conjugate \( a_i w_{ij}^+ a_i^{-1} \) can be calculated by moving \( a_i^{-1} \) to the left using the relations (*) \( \text{(*)} \). The result is again a word in \( \{a_{j+1}, \ldots, a_n\} \) and can be transformed to normal form in a series of collection steps using the relations for \( G_{j+1} \). The equation above shows that this is the normal form for \( (w_{ij}^-)^{-1} \). The elements \( w_{ij}^+ \) and \( w_{ij}^- \) can now be computed as the inverses of \( w_{ij}^+ \) and \( w_{ij}^- \), respectively. This completes the induction step.  

\[ \blacksquare \]
Chapter 3:  
Polycyclic Presentations

In the previous chapter we used an important property of polycyclic and nilpotent polycyclic groups, namely the existence of a polycyclic generating set, to explore computational aspects of these groups. In particular, we saw that a special type of presentation could be derived from a polycyclic generating sequence which allowed the solution of the word problem for polycyclic groups. In this chapter we will give these presentations the name polycyclic presentations. The focus in this chapter will be that a polycyclic presentation does not in general define a normal form in the sense of the previous section. This might first seem to be a disadvantage but it will turn out that this is an important aspect in the construction of polycyclic presentations for larger quotients of a given finitely presented group.

3.1 Polycyclic Presentations

3.1.1 Definition  
A presentation $(A, S)$ is called a **polycyclic presentation** if the following conditions are satisfied:

1) The generating set $A$ of the presentation is a finite linearly ordered, possibly empty, set. If $A$ is not empty, the elements are denoted by $\{a_1, \ldots, a_n\}$.

2) There is a subset $I$ of $\{1, \ldots, n\}$ such that $i \in I$ if and only if there is a
positive number $m_i$ and two relations

$$a_i^{m_i} = w_{ii} \quad (*)$$

and

$$a_i^{-1} a_i = a_i^{-1} w_{ii}^- \quad (**)$$

The right hand sides $w_{ii}$ and $w_{ii}^-$ are words in \{a_{i+1}, \ldots, a_n\}. A relation of the form (*) is called a power relation and a relation of the form (*) an inversion relation. The elements of $I$ correspond to the generators for which there exists a power relation in $S$.

3) For each pair $i, j \in \{1, \ldots, n\}$, $j > i$, there are the four relations

$$a_i^{-1} a_j a_i = w_{ij}^{++}, \quad (*)$$

$$a_i a_j a_i^{-1} = w_{ij}^{-+}, \quad i \not\in I, \quad (**)$$

$$a_i^{-1} a_j^{-1} a_i = w_{ij}^{+-}, \quad j \not\in I, \quad (***)$$

$$a_i a_j^{-1} a_i^{-1} = w_{ij}^{--}, \quad i, j \not\in I, \quad (****)$$

in $S$. The right hand sides $w_{ij}^{++}$, $w_{ij}^{-+}$, $w_{ij}^{+-}$, and $w_{ij}^{--}$ are words in \{a_{i+1}, \ldots, a_n\}. These relations are called conjugate relations. A relation of the form (*) is called a positive conjugate relation and a relation of the form (**) is called an inverse conjugate relation. Relations of the form (****) are called inverted conjugate relations.

4) There are no other relations in $S$.

A presentation in which the set of generators and the set of relations is empty is a polycyclic presentation for the trivial group.

The set of relations we obtained for a polycyclic group in the previous chapter together with the polycyclic generating sequence form a polycyclic presentation.

In dealing with polycyclic presentations and elements of groups defined by polycyclic presentations, it is useful to define a simplifying convention. Let $(A, S)$ be a polycyclic presentation. The group $G$ defined by $(A, S)$ is the quotient group $F/N$ of the free group $F$ on $A$ by the normal closure $N$ of $S$ in $F$. A word $w$ in $A$ belongs, as an element of $F$, to a unique coset $wN$. We are going to use 'the
coset $wN'$ and 'the element $w$ of $G$' as synonyms. This makes it possible to write
down calculations with elements of $G$ without having to carry along the symbol
$N$. In order to avoid confusion, we will always make clear when we are referring
to the word $w$ and when we are referring to $w$ as an element of $G$.

3.1.2 Lemma The group given by a polycyclic presentation is polycyclic.
Proof: Let $(A, S)$ be a polycyclic presentation and let $G$ be the group defined
by it. Let $G_i$ be the group generated by the set $\{a_i, \ldots, a_n\}$ of elements of $G$.
Obviously, $G_n$ is polycyclic. Assume that $G_{i+1}$ is polycyclic. If we can show
that $G_{i+1}$ is normal in $G_i$, it follows that $G_i/G_{i+1}$ is cyclic and, by Theorem
2.1.3, that $G_i$ is polycyclic. It suffices to show that $a_i^{-1}G_{i+1}a_i \subseteq G_{i+1}$ and
$a_iG_{i+1}a_i^{-1} \subseteq G_{i+1}$. But this is the case because the conjugates $a_i^{-1}a_ia_i$ and
$a_ia_ja_i^{-1}$ are words in $a_{i+1}, \ldots, a_n$ for $i + 1 \leq j \leq n$. This means that $a_i^{-1}a_ia_i$
and $a_ia_ja_i^{-1}$, as elements of $G$, are elements of $G_{i+1}$. Now the claim follows by
induction.

The proof of the previous lemma shows that $(a_1, \ldots, a_n)$ is a polycyclic gen­
erating sequence and that $G = G_1 \supseteq \ldots \supseteq G_n = 1$ is a polycyclic series. If $i \in I$,
then the order of $G_i/G_{i+1}$ is at most $m_i$. However, the order of $G_i/G_{i+1}$ can be
smaller than $m_i$. Likewise, if $i \notin I$, the order of $G_i/G_{i+1}$ can be finite. This is
related to the question whether a polycyclic presentation defines a normal form.
For this we need the following definition.

3.1.3 Definition Let $(A, S)$ be a polycyclic presentation. A word $w$ in $A$ is
in reduced form with respect to $(A, S)$ if there are integers $e_i$ for $1 \leq i \leq n$, with
$0 \leq e_i < m_i$ if $i \in I$, such that $w$ is equal to the word $a_1^{e_1} \ldots a_n^{e_n}$.

Let $a_1^{e_1} \ldots a_n^{e_n}$ and $a_1^{f_1} \ldots a_n^{f_n}$ be two reduced words in $A$ and let $G$
be the group defined by $(A, S)$. The polycyclic presentation $(A, S)$ defines a normal
form on the set of words in $A$ if $a_1^{e_1} \ldots a_n^{e_n} = a_1^{f_1} \ldots a_n^{f_n}$, as elements of $G$, implies
$e_i = f_i$ for $1 \leq i \leq n$.

Similarly to the previous chapter, the following operations are sufficient to
transform any word in $A$ to a reduced form:

- replace $a_k^{-1}$ by $a_k^{-m_k}w_k^{-1}$.
- replace $a_i^{\wedge m_k}$ by $w_{kk}$;
- replace $a_i^{e_i}a_k^{e_k}$ by $a_k^{e_k}w_{kl}^{e_k e_l}$;
- replace $a_i a_i^{-1}$ or $a_i^{-1} a_i$ by the empty word.

Extending the terminology of the previous chapter, each of these steps is called an elementary collection step. The fundamental principle of collection also applies in this context; transforming a word in the generators $\{a_i, \ldots, a_n\}$ to normal form does not introduce any of the generators $\{a_1, \ldots, a_{i-1}\}$.

Not every polycyclic presentation defines a normal form as illustrated by the following example.

3.1.4 Example

Let $G$ be the group defined by the polycyclic presentation

$$(a, b \mid b^a = b^2, \quad b^{(a^{-1})} = b^{-2}, \quad (b^{-1})^a = b^{-2}, \quad (b^{-1})^{(a^{-1})} = b^2).$$

Then $b = baa^{-1} = ab^2a^{-1} = b^{-4}$ and $b$ is of order dividing 5. But the word $b^5$ is reduced because there is no power relation for $b$. This shows that $b^5$ and the empty word represent the same element of $G$ and therefore the above polycyclic presentation does not define a normal form. In fact, the group $G$ is the semidirect product of an infinite cyclic group and a group of order 5 on which the infinite cycle acts by mapping each element to its square. A polycyclic series for $G$ is $G \geq (b) \geq 1$. The order of the subgroup generated by $b$ is 5 and not infinite as one might expect from the fact that $b$ has no power relation. We also note that the word $baa^{-1}$ can be collected in two different ways resulting in the two reduced words $b$ and $b^{-4}$.

The previous example showed that the result of collecting a word to reduced form can depend on the sequence of elementary collection steps that is applied to the word. Occasionally, it will be useful to indicate that a particular elementary collection step is to be applied first. We will use a pair of double square brackets for this. For example, collecting $b[aa^{-1}]$ in the example above results in the word $b$ while collecting $[ba]a^{-1}$ results in the word $b^{-4}$.

Let $uav$ be a word such that $u$ is reduced, $a$ is a generator and $v$ is a word in generators larger than $a$. Moving $a$ to the left does not interfere with collection steps applied to $v$. Let $(s_1, \ldots, s_{l-1})$ be a sequence of elementary collection steps...
applied to \( v \) and let \( s' \) be an elementary collection step that moves \( a \) past the generator to the left of \( a \). Clearly, the sequence \( (s_1, \ldots, s_{i-1}, s') \) applied to \( uav \) produces the same word as the sequence \( (s', s_1, \ldots, s_{i-1}) \) applied to \( uav \). A repeated application of this argument shows that in a given sequence of elementary collection steps applied to \( uav \) all the collection steps that move \( a \) to the left can be applied first postponing the other collection steps. We call this the \textit{first postponing principle}.

The following theorem shows that the power relations of a polycyclic presentation give an accurate picture of the orders of the factors of the polycyclic series if and only if the polycyclic presentation defines a normal form.

3.1.5 Theorem A polycyclic presentation defines a normal form, if and only if the order of \( G_i/G_{i+1} \) is \( m_i \) if \( i \in I \) and infinite otherwise.

Proof: Let \( (A, S) \) be a polycyclic presentation that defines a normal form and suppose that \( G_i/G_{i+1} \) has order \( m > 0 \) with \( m < m_i \) if \( i \in I \). Then \( a_i^{m_i} \) is in reduced form. But \( a_i^{m_i} \in G_{i+1} \) and therefore there is a reduced word \( a_i^{e_i} \ldots a_n^{e_n} \) such that \( a_i^{m_i} = a_i^{e_i} \ldots a_n^{e_n} \) as elements of \( G \) contradicting the fact that \( (A, S) \) defines a normal form.

Now let \( G_i/G_{i+1} \) be of order \( m_i \) if \( i \in I \) and infinite otherwise. Assume that \( (A, S) \) defines a normal form for words in \( \{a_{i+1}, \ldots, a_n\} \). The group \( G_i/G_{i+1} \) is generated by the coset \( a_i G_{i+1} \). Therefore, for \( a \in G_i \) there is a unique \( e_i \in \mathbb{Z} \), with \( 0 \leq e_i < m_i \) if \( i \in I \), such that \( aG_i = a_i^{e_i} G_i \). Then \( a_i^{-e_i} a \) has, as an element of \( G_{i+1} \), a normal form \( a_i^{e_{i+1}} \ldots a_n^{e_n} \). This means that \( a_i^{e_i} \ldots a_n^{e_n} \) is a word in normal form equal to \( a \) as element of \( G \). Induction completes the proof.

This behaviour of polycyclic presentations leads to the following definition.

3.1.6 Definition A polycyclic presentation as given in the above definition is called \textit{consistent} if \( G_i/G_{i+1} \) is of order \( m_i \) if \( i \in I \) and is infinite if \( i \not\in I \).

A consistent polycyclic presentation defines a normal form for words in the generating set of the presentation. In order to decide whether a given polycyclic presentation is consistent, we will need some theory about groups with cyclic factor groups which will be presented in the next section. A polycyclic presentation that
is derived from a polycyclic group as explained in the previous chapter is always consistent. Theorem 2.2.5 can be rephrased in this context as follows.

3.1.7 Theorem A group given by a consistent polycyclic presentation is already defined by the set of power relations and the set of positive conjugate relations.

This is not true for inconsistent polycyclic presentations. A presentation containing only the positive conjugate relations does not even have to be polycyclic. This is illustrated again by Example 3.1.4.

3.1.8 Example The group $G$ defined by the presentation $\langle a, b \mid b^a = b^2 \rangle$ is isomorphic to the group in Example 2.1.2 via the isomorphism $a \mapsto a^{-1}$ and $b \mapsto 2^{-1}$. Therefore, $G$ is not polycyclic. The generator $b$ has infinite order in $G$. One reason for $G$ failing to be polycyclic is that $(aba^{-1})^2 = ab^2a^{-1} = b$ and hence $aba^{-1}$ cannot be expressed as a power of $b$. However, the proof of Lemma 3.1.2 shows that a group given by power relations, positive and inverse conjugate relations is polycyclic.

Consider as an example the group given by the presentation

$$\langle a, b \mid b^a = b^2, \ b^{(a^{-1})} = b^{-2} \rangle.$$ 

The missing conjugate relations can be computed by inverting the given relations: $(b^{-1})^a = b^{-2}$ and $(b^{-1})^{(a^{-1})} = b^{-2}$. If we add the relation $b^5 = 1$ to the presentation, the presentation becomes consistent and the inversion relation for $b$ is clearly $b^{-1} = b^4$.

3.1.9 Lemma A group given by a presentation consisting of generators and power relations, positive conjugate relations and inverse conjugate relations in the sense of Definition 3.1.1 is polycyclic.

Proof: The proof is the same as the proof of Lemma 3.1.2. □

Let $(A, T)$ be a finite presentation in which the set of generators is a finite linearly ordered set $A = \{a_1, \ldots, a_n\}$. Let the relation set $T$ consist of power relations, positive conjugate relations and inverse conjugate relations in the sense
of Definition 3.1.1. The following procedure can be used to complete the presentation to a polycyclic presentation. Assume that a complete set of polycyclic relations is given for the generators \(a_{i+1}, \ldots, a_n\). Now \(a_i^{-1}a_j^{-1}a_i = w_{ij}^{\pm 1}\) for which a reduced form can be computed because we assume a complete polycyclic presentation on the generators \(a_{i+1}, \ldots, a_n\). Similarly, if the generator \(a_i\) does not have a power relation in \(T\), the right hand side of the relation \(a_i a_j^{-1} a_i^{-1}\) can be computed as the inverse of \(w_{ij}^{-1}\). If the generator \(a_i\) has a power relation \(a_i^{m_i} = w_{ii}\) in \(T\), then the word \(w_{ii}^{-1}\) in the inversion relation \(a_i^{-1} = a_i^{m_i-1} w_{ii}^{-1}\) can be computed as the inverse of the word \(w_{ii}\). By induction, the presentation \((A, T)\) can be completed to a polycyclic presentation. From now on we will assume that the inverted conjugate relations are consequences of the power relations and the positive and inverse conjugate relations.

An inconsistent polycyclic presentation is characterized by the fact that different reduced words represent the same element of the group defined by the presentation. This is unsatisfactory because it means that one cannot easily decide whether two words represent the same element of the group. Therefore, it is important to be able to change an inconsistent polycyclic presentation into a consistent one.

We close this section with summarizing the different properties of polycyclic presentations in the following theorem.

3.1.10 Theorem Let \(G\) be a group given by a polycyclic presentation \((A, S)\) and let \(G = G_1 \geq \ldots \geq G_{n+1} = 1\) be the corresponding polycyclic sequence of \(G\). Then the following statements are equivalent.

- \((A, S)\) is consistent.
- \((A, S)\) defines a normal form.
- The result of collecting a word in \(A\) to reduced form is independent of the sequence of elementary collection steps.
- \(G_i/G_{i+1} \cong C_{m_i}\) if \(i \in I\) and \(G_i/G_{i+1} \cong C_{\infty}\) if \(i \not\in I\) for \(1 \leq i \leq n\).

3.2 Groups with Cyclic Factor Groups

This section is motivated by the fact that each polycyclic group has a normal subgroup such that the corresponding quotient group is cyclic. The intention of
this section is to derive conditions under which a group $G$ can be built from a group $N$ and a cyclic group $C$ such that $G$ has a normal subgroup isomorphic to $N$ and the quotient group is isomorphic to $C$. Later, this will be used in order to test a given polycyclic presentation for consistency. For different accounts of the theory in this section see Zassenhaus (1958, III.7), Scott (1964, 9.7) and Sims (1993).

In the following let $C_{\infty}$ be the infinite cyclic group and let $z$ be a generator of $C_{\infty}$.

3.2.1 Lemma Let $G$ be a group with a normal subgroup $N$ such that $G/N$ is cyclic. Then $G$ is a homomorphic image of a semidirect product $C_{\infty} \ltimes N$.

Proof: Let $x \in G$ such that $G = \langle x, N \rangle$ and let $\alpha$ be the automorphism of $N$ induced by $x$ via conjugation. Define a homomorphism $\varphi$ from $C_{\infty}$ into the automorphism group of $N$ by mapping $z$ to $\alpha$. Now the semidirect product $H = C_{\infty} \ltimes N$ with respect to this action of $C_{\infty}$ on $N$ can be formed. The map

$$\psi : H \rightarrow G$$

$$(z^i, u) \mapsto x^i u$$

is a homomorphism, which is obviously surjective, as the following calculation for $i, j \in \mathbb{Z}$ and $u_1, u_2 \in N$ shows.

$$((z^i, u_1)(z^j, u_2))\psi = (z^{i+j}, (u_1 \alpha^j)u_2)\psi$$

$$= z^{i+j}(u_1 \alpha^j)u_2$$

$$= z^{i+j}x^{-j}u_1x^j u_2$$

$$= z^i u_1 x^j u_2$$

$$= (z^i, u_1)\psi(z^j, u_2)\psi.$$  

The element $(z^i, u)$ of $H$ is mapped by $\psi$ to the identity in $G$ if and only if $x^i = u^{-1}$. If some positive power of $x$ lies in $N$, let $k$ be the smallest positive integer such that $x^k \in N$ and let $u = x^k$. Then the kernel of $\psi$ is generated by $(z^k, u^{-1})$. The group $G$ is a semidirect product of $\langle x \rangle$ and $N$ if and only if
\( u = 1 \). If \( x^i \not\in N \) for all \( i \in \mathbb{Z} \), then \( \psi \) is an isomorphism and \( G \) is isomorphic to a semidirect product of \( \langle x \rangle \) and \( N \).

Let \( N \) be a group and let \( z \mapsto \alpha \) be a homomorphism from \( C_\infty \) into the automorphism group of \( N \). Furthermore, let \( H \) be the semidirect product of \( C_\infty \) and \( N \) with respect to this homomorphism. If \( G \) is a group with \( N \) as a normal subgroup such that \( G/N \) is cyclic and if \( G \) has an element \( x \) generating a supplement to \( N \) and acting on \( N \) via conjugation as \( \alpha \), then \( G \) is a homomorphic image of \( H \). The kernel of any such homomorphism has been determined in the previous paragraph. Therefore, in order to determine all such groups \( G \), it is sufficient to determine all possible normal subgroups of \( H \) that are generated by an element of the form \((z^k, u^{-1})\) where \( k \) is a positive integer and \( u \) an element of \( N \).

Let \( Z \) be the cyclic group generated by \((z^k, u^{-1})\). Then \( Z \) is normal in \( H \) if and only if \((z^i, v)^{-1}(z^k, u^{-1})(z^i, v) \in Z \) for all \( i \in \mathbb{Z} \) and \( v \in N \). Consider

\[
(z^i, v)^{-1}(z^k, u^{-1})(z^i, v) = (z^{-i}, v^{-1}\alpha^{-i})(z^k, u^{-1})(z^i, v) \\
= (z^{-i}, v^{-1}\alpha^{-i})(z^{i+k}, (u^{-1}\alpha^i)v) \\
= (z^k, (v^{-1}\alpha^k)(u^{-1}\alpha^i)v).
\]

Because \( z \) has infinite order, the last term in this chain of equalities is an element of \( Z \) if and only if

\[
(v^{-1}\alpha^k)(u^{-1}\alpha^i)v = u^{-1} \quad \text{for } i \in \mathbb{Z} \text{ and } v \in N. \quad (*)
\]

Setting \( v \) to the identity of \( H \) and \( i \) to 1 shows that \( u\alpha = u \). From this and specializing \( i \) to 0 in the equation above it follows that \( v\alpha^k = u^{-1}vu \) for all \( v \in N \).

On the other hand, if \( u\alpha = u \) and \( v\alpha^k = u^{-1}vu \) for all \( v \in N \), then \( v\alpha^k = (u^{-1}\alpha^i)vu \) for all \( v \in N \) and all \( i \in \mathbb{Z} \). This shows that these two conditions are equivalent to \((*)\).

The previous discussion is summarized in the following lemma.
3.2.2 Lemma  

The subgroup of the semidirect product $C_\infty \rtimes N$ generated by $(z^k, u^{-1})$ is normal if and only if the conditions

\[
u\alpha = u \\
va^k = u^{-1}vu \quad \text{for all } v \in N
\]

are met.

If $(z^k, u^{-1})$ generates a normal subgroup $U$, the factor group $(C_\infty \rtimes N)/U$ has a normal subgroup of index $k$ isomorphic to $N$.

Let $N$ be given by a finite presentation $(X, R)$. For each element $x \in X$ there is a word $w_x$ in $X$ such that $x\alpha = w_x$ as elements of $N$. The following is a presentation for $H$:

\[
\left( X \cup \{z\}, R \cup \{z^{-1}xz = w_x \mid x \in X\} \right).
\]

Let $k$ be a positive integer and $u$ a word in $X$ such that $u\alpha = u$ as elements of $N$ and $va^k = u^{-1}vu$ as elements of $N$ for all words $v$ in $X$, then

\[
\left( X \cup \{z\}, R \cup \{z^{-1}xz = w_x \mid x \in X\} \cup \{z^k = u\} \right)
\]

is a finite presentation for $H/\langle (z^k, u^{-1}) \rangle$. Compare Johnson (1990, Chapter 10.2.).

As a first application of the above theory we prove the following theorem.

3.2.3 Theorem  

Let $(A, S)$ be a polycyclic presentation in which all conjugate relations are trivial. Then $(A, S)$ is consistent.

Proof: Let $G$ be the group defined by $(A, S)$ and let $A' = A \setminus \{a_1\}$ and $S'$ be the set of relations of $S$ that do not involve $a_1$.

Assume that $(A', S')$ is consistent. Let $a_1$ act trivially on the group $G'$ defined by $(A', S')$. If $a_1$ has no power relation in $S$ then $(A, S)$ is a consistent polycyclic presentation by the previous lemma because $G/G' \cong C_\infty$. If $a_1$ has a power relation then the two conditions of the previous lemma are trivially satisfied and $(A, S)$ is a consistent polycyclic presentation because $G/G' \cong C_k$. Now the claim follows by induction. 

\[\square\]
3.3 Factor Groups of Free Groups

In the previous section we studied a semidirect product of a group $N$ and an infinite cyclic group. The action of the cyclic group on $N$ was given by an automorphism $\alpha$ of $N$. Let $F$ be the free group on $\{a_1, \ldots, a_n\}$ and $R$ a normal subgroup of $F$ such $N \cong F/R$. Now one can consider a map $\{a_1, \ldots, a_n\} \to F$ mapping $a_i$ to an element $w_i$ and ask if this map induces an automorphism of $N$. This situation arises, for instance, in checking consistency of polycyclic presentations. Such a map extends uniquely to an endomorphism $\varphi$ of $F$, but can fail in two ways to induce an automorphism of $N$. First, the normal subgroup $R$ need not be invariant under $\varphi$. Second, if $R$ is invariant under $\varphi$, the endomorphism of $N$ induced by $\varphi$ need not be an automorphism of $N$. We are interested in finding a normal subgroup of $F$, containing $R$, such that $\varphi$ induces an automorphism on the corresponding factor group.

For a normal subgroup $R$ of $F$ we define the $\varphi$-closure $S$ of $R$ to be the normal closure of the subgroup generated by $\prod_{i=0}^{\infty} (R^i \varphi^j)$. Clearly, $S \varphi \subseteq S$ and $\varphi$ induces an endomorphism on $F/S$ via $a_iS \mapsto (a_i\varphi)S$ (compare Chapter 6). Moreover, $S$ is the smallest normal subgroup of $F$ containing $R$ such that $\varphi$ induces an endomorphism on the factor group $F/S$. If $R$ is given by a finite set $\{r_1, \ldots, r_l\}$ of normal subgroup generators, then $S$ is the normal closure of $\{r_i\varphi^j | 1 \leq i \leq l, j \in \mathbb{N}\}$.

In view of the last section and Lemma 3.2.2, we distinguish two cases for the question whether $\varphi$ induces an automorphism on $F/S$. For the first case we require that a map $\{a_1, \ldots, a_n\} \to F$ defining an endomorphism $\psi$ is given and describe the smallest normal subgroup $T$ of $F$ containing $S$ such that $\varphi$ and $\psi$ induce automorphisms on $F/T$ that are inverses of each other. In the second case we require a positive integer $k$ and an element $w \in F$ to be given and ask for the smallest normal subgroup $T$ of $F$ containing $S$ such that $\varphi$ fixes $w$ and $\varphi^k$ acts on $F/T$ as conjugation by $w$.

In the first case, let $T$ be the $\varphi$-closure of the normal closure in $F$ of $R \cup \{(a_1\psi\varphi)a_1^{-1}, \ldots, (a_n\psi\varphi)a_n^{-1}\}$. Then $\varphi$ is surjective modulo $T$ because $a_i\psi$ is a preimage of $a_i$ for the endomorphism induced by $\varphi$ on $F/T$. If the surjectivity implies that $\varphi$ induces an automorphism on $F/T$, we get that $a_i\psi = a_i\varphi^{-1}$ modulo $T$. This is the case if $F/T$ is hopfian. If $F/S$ is polycyclic then $F/T$
is also polycyclic and therefore hopfian. Since we will apply this to polycyclic groups, the above definition of \( T \) is sufficient for our purposes. Note that in this case the construction of \( T \) does not require that \( T \) is invariant under \( \psi \). It is a consequence of the fact that \( \varphi \) induces an automorphism on \( F/T \).

In the second case, define \( T \) to be the \( \varphi \)-closure of the normal closure in \( F \) of \( R \cup \{(a_1\varphi^k)(a_w)^{-1}, \ldots, (a_n\varphi^k)(a_w)^{-1}\} \cup \{(w\varphi)w^{-1}\} \). Then \( \varphi \) induces an endomorphism on \( F/T \) that fixes \( w \) and whose \( k \)-th power acts as conjugation by \( w \). The latter implies that the endomorphism induced by \( \varphi \) is an automorphism of \( F/T \).

3.4 Checking and Enforcing Consistency

We assume the notation of the previous section. In order to apply the considerations of the previous section to checking the consistency of a polycyclic presentation, let \( G \) be given by a polycyclic presentation on the generators \( \{a_1, \ldots, a_n\} \) with relations

\[
\begin{align*}
a_i^{m_i} &= w_{ii} \quad \text{for } i \in I \\
a_i^{-1}a_ja_i &= w_{ij}^{++} \quad \text{for } 1 \leq i < j \leq n \\
a_i^{-1}a_ja_i^{-1} &= w_{ij}^{-+} \quad \text{for } 1 \leq i < j \leq n, i \in I.
\end{align*}
\]

We assume that the right hand side of each relation is a reduced word. Let \( N \) be the group defined by the presentation on the set \( \{a_2, \ldots, a_n\} \) of generators and the relations

\[
\begin{align*}
a_i^{m_i} &= w_{ii} \quad \text{for } i \in I \setminus \{1\} \\
a_i^{-1}a_ja_i &= w_{ij}^{++} \quad \text{for } 2 \leq i < j \leq n \\
a_i^{-1}a_ja_i^{-1} &= w_{ij}^{-+} \quad \text{for } 2 \leq i < j \leq n, i \notin I.
\end{align*}
\]

Assume that this presentation for \( N \) is consistent. The subgroup of \( G \) generated by \( \{a_2, \ldots, a_n\} \) is a homomorphic image of \( N \). Define a map \( \varphi : \{a_2, \ldots, a_n\} \to N \) as mapping \( a_i \) to \( w_{1i}^{++} \). If \( 1 \notin I \), also define \( \psi : \{a_2, \ldots, a_n\} \to N \) mapping \( a_i \) to \( w_{1i}^{-+} \).

For \( i \in I \setminus \{1\} \) let \( q_{ii} \) be the term

\[w_{ii}(a_{i+1}\varphi, \ldots, a_n\varphi)^{-1}(a_i\varphi)^{m_i},\]

for \( 2 \leq i < j \leq n \) let \( q_{ij} \) be the term

\[w_{ij}(a_{i+1}\varphi, \ldots, a_n\varphi)^{-1}(a_i\varphi)^{-1}(a_j\varphi)(a_i\varphi)\]
and, extending the notion of $\varphi$-closure from free groups to factor groups of free groups, let $S$ be the $\varphi$-closure of the normal closure of

$$\{ q_{ii} \mid i \in I \setminus \{1\} \} \cup \{ q_{ij} \mid 2 \leq i < j \leq n \}.$$ 

By the considerations of the previous section, $\varphi$ induces a map $a_iS \mapsto (a_i \varphi)S$ on $N/S$ which defines an endomorphism of $N/S$. Since $N$ is given by a consistent polycyclic presentation, the normal forms of the $q_{ij}$ can be computed. Note that there is a positive integer $L$ such that $\prod_{i=0}^{\infty} (R\varphi^i) = \prod_{i=0}^{L} (R\varphi^i)$ because there are no infinitely ascending chains in the polycyclic group $N$.

If $1 \not\in I$, then for $2 \leq i \leq n$ let $r_i$ be $(a_i \psi) \varphi a_i^{-1}$. The $\varphi$-closure $T$ of the normal closure of $S \cup \{ r_i \mid 2 \leq i \leq n \}$ is the smallest normal subgroup of $N$ such that $\varphi$ induces an automorphism on $N/T$ with inverse $\psi$.

If $1 \in I$, then there is a relation $a_1^{m_1} = w_{11}$. For $2 \leq i \leq n$ let $r_i$ be $(a_i \varphi^{m_1}) w_{11}^{-1} a_i^{-1} w_{11}$. Then the $\varphi$-closure $T$ of the normal closure of the set $S \cup \{ r_i \mid 2 \leq i \leq n \} \cup \{ (w_{11} \varphi) w_{11}^{-1} \}$ is the smallest normal subgroup of $N$ such that $\varphi$ induces an automorphism on $N/T$ such that its $m_1$-th power is the inner automorphism of $N$ defined via conjugation by $w_{11}$.

The map $\varphi$ defines an automorphism (that, if $1 \in I$, also satisfies the conditions of Lemma 3.2.2) on $N$ in both cases if and only if the subgroup $T$ is trivial in both cases.

For $2 \leq j \leq n$ we have that $a_j \varphi = w_{1j}^{++}$ and, if $1 \not\in I$, $a_j \psi = w_{1j}^{-+}$. By the first postponing principle and the fact that $w(a_2, \ldots, a_n)$ is a reduced word, the word $w(a_2, \ldots, a_n) a_1$ collects to the same normal form as the word $a_1 w(a_2 \varphi, \ldots, a_n \varphi)$. Now $T$ is trivial if and only if the following equations are satisfied as equations in $N$

$$a_j^{m_j} a_1 = a_j^{m_j-1} [a_j a_1]$$

for $2 \leq j \leq n$, $j \in I$,

$$a_k [a_j a_1] = [a_k a_j] a_1$$

for $2 \leq j < k \leq n$,

$$a_j a_1^{m_1} = [a_j a_1] a_1^{m_1-1}$$

for $2 \leq j \leq n$, $1 \in I$,

$$a_1 a_1^{m_1} = a_1^{m_1} a_1$$

if $1 \in I$,

$$a_j = [a_j a_1^{-1}] a_1$$

for $2 \leq j \leq n$, $1 \not\in I$.

This can be checked by collecting both sides of the equation to normal form because $N$ is defined by a consistent polycyclic presentation. By induction we get the following theorem.
3.4.1 Theorem  (Consistency Check)

A polycyclic presentation on the generating set \{a_1, \ldots, a_n\} is consistent if and only if the following words collect to the empty word

\[
([a_j^m a_i]^{-1} a_j^{m_j} [a_j a_i])^{-1} \quad \text{for } 1 \leq j < i \leq n, \ j \in I,
\]
\[
(a_k [a_j a_i])^{-1} \quad \text{for } 1 \leq i < j < k \leq n,
\]
\[
(a_j [a_i^m])^{-1} [a_j a_i] a_i^{m_j} \quad \text{for } 1 \leq j < i \leq n, \ i \in I,
\]
\[
(a_i [a_i^m])^{-1} \quad \text{for } i \in I,
\]
\[
a_j^{-1} [a_j a_i^{-1}] a_i \quad \text{for } 1 \leq i < j \leq n, \ j \notin I.
\]

Note that, if we do not assume that the inverted conjugate relations are consequences of the power relations and the positive and inverse conjugate relation, the following words have also to be taken into account

\[
a_i^{-1} a_j^{-1} [a_j a_i] \quad \text{for } 1 \leq i < k \leq n, \ j \notin I,
\]
\[
a_i a_j^{-1} [a_j a_i^{-1}] \quad \text{for } 1 \leq i < j \leq n, \ j \notin I.
\]

For practical purposes it is desirable to turn an inconsistent polycyclic presentation into a consistent one. We will sketch a procedure that does this. Using the non-commutative Gauss algorithm a polycyclic generating sequence for \(T\) can be computed. This generating sequence can be extended to a polycyclic generating sequence \(B = (b_1, \ldots, b_k)\) of \(N\). It is then possible to calculate a consistent polycyclic presentation \((B, Q)\) for \(N\) and to calculate the relations \(a_1^{-1} b_j a_1 = v_1^{i_j} \), \(a_1 b_j a_1^{-1} = v_1^{i_j} \) if \(1 \notin I\) and \(a_i^{m_i} = v_{ii} \) if \(1 \in I\). A consistent polycyclic presentation \((B', Q')\) for the factor group \(N/T\) is obtained from \((B, Q)\) by replacing all occurrences of the generators of the polycyclic generating sequence for \(T\) in \((B, Q)\) by the empty word. The action of \(a_1\) on \(N/T\) can be obtained from the relations above by deleting all occurrences of the polycyclic generators of \(T\) from the right hand side of these relations. The union of \(Q'\) and this set of relations together with \(\{a_1\} \cup B\) form a consistent presentation for \(G\).

For a different approach of converting an inconsistent polycyclic presentation into a consistent polycyclic presentation, see Sims (1987).
Chapter 4: Quotient Systems

In this chapter we will define a mathematical object, the quotient system, in order to describe the following typical situation in computing quotient groups of finitely generated groups. We have a finite presentation for a group $G$, a polycyclic presentation for a quotient group $Q$ of $G$ and a map that maps each generator of the finite presentation into $Q$ and thereby defines a surjective homomorphism from $G$ to $Q$. Usually the generating set for $Q$ is larger than the generating set of the finite presentation for $G$. Therefore, some of the generators in the polycyclic presentation for $Q$ might be redundant. Those generators can be expressed in terms of some other generators of the polycyclic presentation. Ideally, the number of in this sense non-redundant generators should not be bigger than the number of generators in the generating set for $G$. Quotient systems are an attempt to bring together all this information in one mathematical object.

Let $X$ be a partially ordered set and $\mathcal{R}$ a set of words in $X$. The element $x \in X$ is said to have a definition in $\mathcal{R}$, if $\mathcal{R}$ contains a word of the form $wx$ and $w$ is a word in generators smaller than $x$. The word $wx$ is a definition of $x$. In the presentation $(X, \mathcal{R})$, such a generator $x$ can be eliminated from $(X, \mathcal{R})$ by a sequence of Tietze transformations replacing $x$ by the word $w^{-1}$ in all other relators. The resulting presentation defines the same group as $(X, \mathcal{R})$. In this way, all generators with a definition in $\mathcal{R}$ can be eliminated from the presentation. Beginning with the elimination of a largest generator via a definition, this process
can be repeated until all defined generators are removed from the presentation. If \( R \) is given as a set of relations rather than words, then \( x \in X \) is said to have a definition in \( R \) if there is a relation \( v = wx \) where \( v \) and \( w \) are words in generators smaller than \( x \). Then \( x \) can be replaced by \( w^{-1}v \) in all words in \( R \).

4.1 Definition A quotient system is a triple \( ((X,R),(A,S),\sigma) \) where
- \( (X,R) \) is a finite presentation with a generating set \( X \) and a relator set \( R \),
- \( (A,S) \) is a polycyclic presentation with a finite linearly ordered set \( A \) of generators and a set \( S \) of relations and
- \( \sigma \) is a map from \( X \) into the set of words in \( A \)
such that each generator \( a \in A \) is defined either by a relation of the polycyclic presentation or by the image \( x \sigma \) for some \( x \in X \), i.e., there is a word \( u \) in generators smaller than \( a \) such that \( x \sigma = ua \). For each generator \( a \in A \) one such definition is fixed and called the definition of \( a \). We say that the quotient system \( A \) is based on \( (X,R) \).

A quotient system is called consistent if the map \( \sigma \) defines a homomorphism from the group defined by \( (X,R) \) onto the group defined by the polycyclic presentation and if the polycyclic presentation is consistent. If this is the case, we will not distinguish between \( \sigma \) and the homomorphism. It is always the case that \( \sigma \) defines a (unique) homomorphism from the free group on \( X \) to the group defined by \( (A,S) \) and we also will not distinguish between \( \sigma \) and this homorphism.

The trivial quotient system based on \( (X,R) \) is the triple \( ((X,R),(\emptyset,\emptyset),\sigma) \) where \( \sigma \) maps each element of \( X \) to the empty word.

Let \( A = ((X,R),(A,S),\sigma) \) be a quotient system and let \( G \) be the group defined by \( (X,R) \). The quotient system \( A \) describes a polycyclic quotient, \( Q \), of the finitely presented group, \( G \), together with a projection of \( G \) onto \( Q \). A presentation of \( Q \) is

\[
(X \cup A, R \cup S \cup \{x = x \sigma; x \in X\}).
\]

We say that \( A \) represents \( Q \). Note that, using the relations \( x = x \sigma \) for \( x \in X \), the relators in \( R \) can be written as words in the generators \( A \). If \( \sigma \) defines a homomorphism, those relators are consequences of the relations in \( S \) and can be
omitted from the presentation. This shows that \((A, S)\) is a presentation for \(Q\), if \(\sigma\) defines a homomorphism. Note also that each generator \(a \in A\) can be eliminated from this presentation using its definition. This means that the above presentation can be transformed into a presentation on the generating set \(X\) by a sequence of Tietze transformations. This shows that \(\sigma\) defines a surjective homomorphism onto \(Q\).

4.2 Definition

Let \(A = ((X, \mathcal{R}), (A, S), \sigma)\) and \(A' = ((X, \mathcal{R}), (A', S'), \sigma')\) be quotient systems. Then \(A'\) is called an extension of \(A\) if the following conditions are satisfied:

- \(A \subseteq A'\) and the elements in \(A' \setminus A\) are later in \(A'\) than the elements of \(A\);
- the subgroup generated by the elements \(A' \setminus A\) is normal in the group defined by \((A', S')\);
- eliminating the elements \(A' \setminus A\) from the presentation \((A', S')\) by replacing every occurrence by the empty word results in the presentation \((A, S)\) after removing trivial relations;
- deleting the generators in \(A' \setminus A\) from the image of \(x\) under \(\sigma'\) for \(x \in X\) gives \(x\sigma\).

An extension of a quotient system is called central if the generators \(A' \setminus A\) are central in the group defined by \((A', S')\).

Let \(Q\) and \(Q'\) be the groups represented by \(A\) and \(A'\), respectively. Eliminating the generators \(A' \setminus A\) from the presentation \((A', S')\) is equivalent to taking the factor group \(Q'/N'\) where \(N'\) is the (normal) subgroup generated by the elements \(A' \setminus A\). The third condition of the definition implies that \(Q'/N'\) is isomorphic to \(Q\). The fourth condition implies that \(\sigma'\) induces \(\sigma\) on \(Q'/N'\) and is therefore a lifting of \(\sigma\) to \(Q'\) (compare Chapter 6).

4.3 Example

Let \(X = \{x_1, x_2\}\) and \(\mathcal{R}\) be the empty set. Then \((X, \mathcal{R})\) is a presentation for the free group of rank 2. Let \(A = \{a_1, a_2\}\) and let \(S\) be the set \(\{a_1^2, a_1^{-1}a_2a_1 = a_2^2, a_2^3\}\) of relations. The presentation \((A, S)\) is a consistent polycyclic presentation for the symmetric group on three letters. Define \(\sigma\) by \(x_1 \mapsto a_1\) and \(x_2 \mapsto a_2\). Obviously, \(\sigma\) defines a surjective homomorphism from the free group \(F\) on \(X\) to the group defined by \((A, S)\). Therefore, the triple \(((X, \mathcal{R}), (A, S), \sigma)\) is
a consistent quotient system based on \((X, \mathcal{R})\). The two generators of the polycyclic presentation are defined as images of the generators in \(X\).

Set \(A' = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\}\) and let \(S'\) be the set of the following relations together with the relations \(a_i^{-1}a_ja_i = a_j\) for \(3 \leq i < j \leq 9\):

\[
\begin{align*}
  a_1^2 &=: a_3, \\
  a_1^{-1}a_2a_1 &=: a_2^2a_4, \\
  a_1^{-1}a_3a_1 &= a_3, \\
  a_1^{-1}a_4a_1 &=: a_6, \\
  a_1^{-1}a_5a_1 &= a_4a_2^2a_7a_8, \\
  a_1^{-1}a_6a_1 &= a_4, \\
  a_1^{-1}a_7a_1 &=: a_3^{-1}a_5^{-1}a_7^{-1}a_8^{-1}a_9, \\
  a_1^{-1}a_8a_1 &= a_3a_4^{-2}a_5^{-2}a_6^{-1}a_7^{-1}a_8^{-1}a_9^{-1}, \\
  a_1^{-1}a_9a_1 &= a_3a_4^{-1}a_5^{-1}a_6^{-1}a_8^{-1},
\end{align*}
\]

\[
\begin{align*}
  a_2^2 &=: a_5, \\
  a_2^{-1}a_3a_2 &= a_3a_4^{-1}a_5^{-1}a_6^{-1}a_8^{-1}, \\
  a_2^{-1}a_4a_2 &=: a_7, \\
  a_2^{-1}a_5a_2 &= a_5, \\
  a_2^{-1}a_6a_2 &= a_3a_4^{-2}a_5^{-2}a_6^{-1}a_7^{-1}a_8^{-1}a_9^{-1}, \\
  a_2^{-1}a_7a_2 &=: a_8, \\
  a_2^{-1}a_8a_2 &= a_4, \\
  a_2^{-1}a_9a_2 &= a_3.
\end{align*}
\]

The map \(\sigma'\) is defined by \(x_1 \mapsto a_1\) and \(x_2 \mapsto a_2\) and extends to a surjective homomorphism onto the group defined by \((A', S')\). Each generator \(a_3, \ldots, a_9\) is defined by a word in earlier generators, for instance, the generator \(a_9\) is defined as

\[
a_9 := a_3^{-1}a_5^{-1}a_7^{-1}a_8^{-1}a_1^{-1}a_7a_1 = a_8a_7a_5a_3a_1^{-1}a_7a_1.
\]

Relations defining a generator are marked with a colon on the same side of the equal sign as the defined generator. The defined generator is always the last generator of the word on this side of the relation. It is clear that it is possible to use the definitions of the generators \(a_3, \ldots, a_9\) to transform the above polycyclic presentation into a finite presentation on two generators by a series of Tietze transformations. We remark without proof that, if \(N\) is the kernel of \(\sigma\), then \((A', S')\) is a polycyclic presentation for \(F/[N, N]\).
The following is a consistent central extension of \(((X, \mathcal{R}), (A, S), \sigma)\)

\[ A'' = \{a_1, a_2, a_3, a_4\} \]
\[ S'' = \{ a_1^2 = a_3, a_1^{-1}a_2a_1 = a_2^2a_4, a_2^3 = a_4^{-3}, a_1^{-1}a_3a_1 = a_3, a_2^{-1}a_3a_2 = a_3, a_1^{-1}a_4a_1 = a_4, a_2^{-1}a_4a_2 = a_4, a_3^{-1}a_4a_3 = a_4\} \]
\[ \sigma'': \begin{align*} x_1 & \mapsto a_1 \\ x_2 & \mapsto a_2. \end{align*} \]

It represents the group \(F/[F, N]\) and can be obtained from the previous quotient system by making the new generators central.

Now let \(A = ((X, \mathcal{R}), (A, S), \sigma)\) be a consistent quotient system. Let \(F_X\) be the free group on \(X\). Denote by \(K\) the kernel of \(\sigma\) and let \(L\) be the smallest normal subgroup of \(F_X\) contained in \(K\) and containing \(\mathcal{R}\) such that \(K/L\) is central in \(F_X/L\). Then \(L\) is the normal closure of \(\mathcal{R}[K, F_X]\). In the following we describe a central extension \(A'\) of \(A\) that represents the group \(F_X/L\).

The first step is to define a new generator \(a_x\) for each generator \(x \in X\) whose image \(x\sigma\) is not a definition of a generator of \(A\). Define \(\sigma'\) on \(X\) by

\[ \sigma': x \mapsto x\sigma \quad \text{if } x\sigma \text{ is a definition} \]
\[ x \mapsto x\sigma a_x \quad \text{if } x\sigma \text{ is not a definition.} \]

Note that all images of \(\sigma'\) are definitions.

The second step defines a generator for each power relation, positive conjugate relation and inverse conjugate relation in \(S\) that is not a definition of a generator in \(A\). For this, denote the elements of \(A\) by \(a_1, \ldots, a_n\) ordered in this sequence. Define new generators \(t_{ij}^{++}\), for \(1 \leq i < j \leq n\), \(t_{ij}^{-+}\), for \(1 \leq i < j \leq n\) and \(i \notin I\), and \(t_{ii}\), for \(i \in I\), corresponding to those of the following relations that are not already a definition of a generator in \(A\):

\[ a_i^{-1}a_ja_i = w_{ij}^{++} \quad \text{for } 1 \leq i < j \leq n, \]
\[ a_i a_j a_i^{-1} = w_{ij}^{-+} \quad \text{for } 1 \leq i < j \leq n, \quad i \notin I, \]

and

\[ a_i^{m_i} = w_{ii}, \quad \text{for } i \in I. \]

The generating set \( A' \) for a new polycyclic presentation is the union of \( A \) and the set of newly defined generators. The linear order on \( A \) is extended to \( A' \) such that the elements in \( A' \setminus A \) are larger than the generators in \( A \) and the generators in \( A' \setminus A \) are linearly ordered such that generators defined by images of \( \sigma \) are smaller than generators defined by relations. The set \( S' \) of relations is the set of all definitions in \( S \) together with the relations

\[
\begin{align*}
    a_i^{-1} a_j a_i &= w_{ij}^{++} t_{ij}^{++} & \text{for } 1 \leq i < j \leq n, \\
a_i a_j a_i^{-1} &= w_{ij}^{+-} t_{ij}^{+-} & \text{for } 1 \leq i < j \leq n, \quad i \notin I, \\
a_i^{m_i} &= w_{ii} t_{ii} & \text{for } i \in I, \\
bcb^{-1} &= c & \text{for } b \in A', \quad c \in A' \setminus A \text{ and } b < c, \\
b^{-1} cb &= c & \text{for } b \in A', \quad c \in A' \setminus A \text{ and } b < c.
\end{align*}
\]

The presentation can be completed to a polycyclic presentation as explained in Chapter 3. The quotient system \( \mathcal{A}' = ((X, \mathcal{R}), (A', S'), \sigma') \) is clearly a central extension of the quotient system \( \mathcal{A} \). We will now prove that the group represented by \( \mathcal{A}' \) is isomorphic to \( F_X / L \). This follows directly from the following theorem which will be proved in a series of lemmas.

**4.4 Theorem** The group \( F_X / L \) is a homomorphic image of the group defined by \( (A', S') \). The kernel of this homomorphism is generated as a subgroup by the set \( \{ r(x) \in X \mid r \in \mathcal{R} \} \).

For the proof of the theorem let \( F_{A'} \) be the free group on \( A' \) and define

\[
\varphi : F_{A'} \to F_X
\]

\[ a \mapsto (t^{-1} \varphi)a \quad \text{if } a \text{ is defined by } x \sigma' = ta \]

\[ a \mapsto (v^{-1} u) \varphi \quad \text{if } a \text{ is defined by the relation } u = va. \]

This definition of \( \varphi \) is recursive but \( \varphi \) is well defined since all generators occurring in \( t \) and \( v^{-1} u \), respectively, are smaller than \( a \) and it can be assumed by induction.
that \( \varphi \) is already defined on those generators. Since \( F_{A'} \) is free, \( \varphi \) defines a homomorphism.

**4.5 Lemma**  The homomorphism \( \varphi \), defined as above, is surjective.

**Proof:** Let \( x \in X \) and \( a \in A \) be the generator defined by \( x \sigma' \), i.e., \( x \sigma' = ta \) for some word \( t \) in \( A \). Then \( (ta)\varphi = (t\varphi)(t^{-1}\varphi)x = x \) shows that \( x \sigma' \) is a preimage of \( x \) under \( \varphi \) and, therefore, \( \varphi \) is surjective. ■

Let \( N \) be the normal subgroup of \( F_{A'} \) defined by the relations in \( S' \) together with the relations \( \{ \sigma = 1 \mid \sigma \notin A' \setminus A \} \). Recall that \( \sigma \) defines a homomorphism from the group \( F_X \) onto the group defined by \( (A, S) \). The quotient group \( F_{A'}/N \) is clearly isomorphic to the group defined by \( (A, S) \) and this gives rise to a homomorphism \( \tau \) from \( F_X \) onto \( F_{A'}/N \) mapping \( x \) to \( (x\sigma)N \). Clearly, \( \ker \sigma = \ker \tau = K \).

The following two lemmas show that \( \varphi \) induces a homomorphism from \( F_{A'}/N \) to \( F_X/K \). The inverse of this homomorphism is \( \tau \).

**4.6 Lemma**

\[
a \varphi \tau = \begin{cases} aN & \text{if } a \in A \\ N & \text{if } a \in A' \setminus A \end{cases}
\]

**Proof:** By induction on \( A' \).

If \( a = x \sigma' \), then \( a \varphi \tau = (x \sigma')\varphi \tau = x \tau \) because \( x \sigma' \) is a preimage for \( x \) under \( \varphi \). Now \( x \tau = N \) if \( a \in A' \setminus A \) and \( x \tau = aN \) if \( a \in A \).

Assume that the claim is true for all generators smaller than \( a \). If \( a \) is defined by \( x \sigma' = ta \), then

\[
a \varphi \tau = ((t^{-1}\varphi)x)\tau = (t^{-1}N)(x\tau) = \begin{cases} t^{-1}taN & \text{if } a \in A \\ t^{-1}tN & \text{if } a \in A' \setminus A. \end{cases}
\]

Note that the induction hypothesis is used in the second equality and that \( t^{-1} \) involves only generators smaller than \( a \).

If \( a \) is defined as \( u = va \), then we get

\[
a \varphi \tau = (v^{-1}u)\varphi \tau = v^{-1}uN = aN,
\]

44
which is equal to \( N \) if \( a \in A' \setminus A \). The second equality holds because of the induction hypothesis and the third equality because of the induction hypothesis and the fact that all generators in \( v^{-1}u \) are elements of \( A \).

4.7 Lemma \( N\varphi = K \).

Proof: Let \( s \) be a relator corresponding to a relation in \( S \). Then \( s \) is a word in the generating set \( A \) and, by the previous lemma, \( s\varphi \tau = sN = N \). This shows that \( s\varphi \) is an element of \( K = \ker \tau \) and \( N\varphi \subseteq K \).

If \( w(x; x \in X) \) is an element of \( \ker \tau \), then \( w(x\sigma'; x \in X) \) is a preimage of \( w(x; x \in X) \) under \( \varphi \) because \( x\sigma' \) is a preimage for \( x \) under \( \varphi \) for all \( x \in X \). It remains to show that \( w(x\sigma'; x \in X) \) is an element of \( N \). This follows from \( N = w(x; x \in X)\tau = (w(x; x \in X)\sigma)N \) and the fact that \( x\sigma \) and \( x\sigma' \) differ by a word in \( A' \setminus A \subseteq N \). This proves that \( N\varphi = \ker \tau = K \).

Define \( N' \) to be the normal subgroup of \( F_{A'} \) defined by the relations in \( S' \). This means that \( F_{A'}/N' \) is the group defined by the polycyclic presentation \((A', S')\). Now we have the following lemmas.

4.8 Lemma \( N'\varphi \subseteq [F_X, K] \).

Proof: It is sufficient to prove that \( \varphi \) maps all relators corresponding to relations in \( S' \) into \([F_X, K]\). There are two kinds of relations in \( S' \) that have to be considered; definitions of the form \( u = va \) and conjugate relations of the form \( c^b = c \) for \( c \in A' \setminus A, b \in A' \) and \( c > b \). All other relations are consequences of these ones.

Let \( u = va \) be the definition of the generator \( a \in A' \). The image of the corresponding relator \( a^{-1}v^{-1}u \) under \( \varphi \) is \((a\varphi)^{-1}(v^{-1}u)\varphi \) which, by the definition of \( \varphi \), is equal to \(((v^{-1}u)\varphi)^{-1}(v^{-1}u)\varphi = 1 \).

Let \([c, b]\) be the relator corresponding to one of the conjugate relations. Since \( c \in A' \setminus A \), its image under \( \varphi \) is an element of \( K \) by the previous lemma. The subgroup \( K/[F_X, K] \) of \( F_X/[F_X, K] \) is central. Therefore, \([c, b]\varphi = [c\varphi, b\varphi] \in [F_X, K] \).

4.9 Lemma \([F_X, K] \subseteq N'\varphi \).
Proof: It is sufficient to show that \([x, y]\), for \(x \in F_X\) and \(y \in K\), is an image of an element of \(N'\) under \(\varphi\). As in the proof of Lemma 4.5, \(x\sigma'\) and \(y\sigma'\) are preimages of \(x\) and \(y\), respectively, and \(y\sigma' \in N\). Since \(N/N'\) is a central subgroup of \(F_{A'}/N'\), it follows that \([x\sigma', y\sigma'] \in [F_{A'}, N] \subseteq N'\). ■

Let \(D' \leq F_{A'}\) be the normal subgroup defined by all defining relations in \(S'\).

4.10 Lemma \(F_X \cong F_{A'}/D'\).
Proof: First we show that \(D'\) is a subgroup of \(\ker \varphi\). Let \(u = va\) be a defining relation for \(a \in A'\). Then the corresponding relator \(a^{-1}v^{-1}u\) is mapped to \((a\varphi)^{-1}(v^{-1}u)\varphi = ((v^{-1}u)\varphi)^{-1}(v^{-1}u)\varphi = 1\). This shows that \(\varphi\) induces a homomorphism \(\tilde{\varphi} : F_{A'}/D' \to F_X\) mapping \(D'b\) to \(b\varphi\). Define a homomorphism \(\psi : F_X \to F_{A'}/D'\) by mapping \(x\) to \(D'(x\sigma')\). We will show that \(\tilde{\varphi}\) is the inverse of \(\psi\).

Let the generator \(a\) be defined by \(x\sigma' = ta\). Then

\[x\psi \tilde{\varphi} = (D'ta)\tilde{\varphi} = (ta)\varphi = (t\varphi)(a\varphi) = (t\varphi)(t\varphi)^{-1}x = x.\]

By induction on the generators defined by images of \(\sigma'\) we show that \(\psi\) is a right inverse for \(\tilde{\varphi}\). Assume that \((D'b)\tilde{\varphi}\psi = D'b\) for \(b < a\). This implies

\[D'b = (D'b)\tilde{\varphi}\psi = b\varphi\psi = D'(b\varphi\sigma').\]

From this and the fact that \(t\) involves only generators smaller than \(a\) we get

\[(D'a)\tilde{\varphi}\psi = a\varphi\psi = ((t\varphi)^{-1}x)\psi = (D'(t\varphi\sigma'))^{-1}D'x\sigma' = (D't)^{-1}D'ta = D'a.\]

This completes the proof. ■

Lemma 4.8 shows that \(\varphi\) induces a surjective homomorphism \(\varphi'\) from \(F_{A'}/N'\) to \(F_X/L\) because \(L \supseteq [F_X, K]\).

4.11 Lemma The kernel of \(\varphi'\) is generated by \(\{ r(x\sigma'; x \in X)N' \mid r \in R \}\) as a subgroup.
Proof: By Lemma 4.8 and Lemma 4.9 we have \( N' \varphi = [F_X, K] \). Now the proof of Lemma 4.10 shows that \( \sigma' \) induces an isomorphism from \( F_X/[F_X, K] \) to \( F_{A'}/N' \) and that the inverse \( \psi \) is induced by \( \varphi \).

The kernel of \( \varphi' \) is the preimage of \( L \) under \( \psi \). The preimage is equal to the image of the isomorphism above induced by \( \sigma' \) and therefore generated by \( \{ r(x\sigma'; x \in X)N' \mid r \in R \} \) as a normal subgroup. Since \( L/[F_X, K] \) is central, \( L/[F_X, K] \) is generated as a subgroup by \( \{ r[F_X, K] \mid r \in R \} \). From this the claim follows.

The last lemma completes the proof of Theorem 4.4.

It remains to make the quotient system \( A' \) consistent. This involves two parts; making the presentation \( (A', S') \) consistent and enforcing the relations \( R \) on the group defined by \( (A', S') \), i.e., forming the quotient group over the kernel of \( \varphi' \).

In order to make \( (A', S') \) consistent we apply the theory in section 3.4. Let \( T \) be the free abelian group on the generating set \( A' \setminus A \). If all occurrences in \( (A', S') \) of generators in \( A' \setminus A \) are replaced by the empty word, we get the consistent polycyclic presentation \( (A, S) \). Therefore, computing the reduced form of each of the words in Theorem 3.4.1 results in a set of words in \( A' \setminus A \).

In order to compute the kernel of \( \varphi' \) we have to collect the set of words \( \{ r(x\sigma'; x \in X)N' \mid r \in R \} \). Since the kernel of \( \varphi' \) is contained in the subgroup of \( F_{A'}/N' \) generated by \( A' \setminus A \), the collected words are words in \( A' \setminus A \).

Let \( U \) be the subgroup of \( T \) generated by the union of the set of reduced words obtained from checking consistency and the set of words obtained from evaluating the relations in \( R \). Furthermore, let \( u_1 = v_1, \ldots, u_r = v_r \) be a set of relations for \( T/U \) such that the corresponding relation matrix is in row Hermite reduced form in the sense of Theorem 1.1.1. Adding these relations to \( S' \) makes the polycyclic presentation \( (A', S') \) consistent.

Let \( u_i = v_i \) be one of the above relations for \( T/U \) such that \( u_i \) is a generator in \( A' \setminus A \). Then this relation can be used to eliminate \( u_i \) from the presentation \( (A', S') \) and the images of \( X \) under \( \sigma' \). This means that all generators in \( A' \setminus A \) that occur on a left hand side of one the relations for \( T/U \) with exponent 1 can be eliminated from the quotient system \( A \). The resulting quotient system is a consistent quotient system \( B \) representing \( F_X/L \).
4.12 Definition

The quotient system $B$ is called the *central covering* (*quotient*) system of $A$. 
Chapter 5: Computing Nilpotent Quotients

This chapter describes an algorithm that computes quotient systems for certain nilpotent factor groups of a group given by a finite presentation. The basic algorithm is a repeated application of the methods in Chapter 4. The main part of the chapter is concerned with defining special polycyclic presentations for nilpotent groups and describing an improved version of the basic algorithm. The methods used for this algorithm are a generalization of the methods employed by Havas and Newman (1980) for the computation of what they call weighted power-commutator presentations for factor $p$-groups of finitely presented groups. The first implementation of a nilpotent quotient algorithm has been done by C.C. Sims in Mathematica.

5.1 The basic algorithm

Throughout this chapter let $(X, \mathcal{R})$ be a finite presentation for a group $G$. Let $F_X$ be the free group on $X$ and $N$ the normal closure of $\mathcal{R}$ in $F_X$. Furthermore, define $K = N\gamma_{c+1}(F_X)$ and $L = N[K, F_X]$. Then $G/\gamma_{c+1}(G) \cong F_X/K$. From this we get $L = N[N\gamma_{c+1}(F_X), F_X] = N[N, F_X]\gamma_{c+1}(F_X) = N\gamma_{c+2}(F_X)$. The second equality follows from Hilfsatz III.1.10a) in Huppert (1967). This shows that $F_X/L \cong G/\gamma_{c+2}(G)$. If $\mathcal{A}_c$ is a consistent quotient system representing $G/\gamma_{c+1}(G)$, then the central covering system $\mathcal{A}_{c+1}$ of $\mathcal{A}_c$ represents $F_X/L$ by the remarks before Theorem 4.4 and therefore $G/\gamma_{c+2}(G)$ by the above argument.
Let $C$ be a positive integer. The aim is to compute a consistent quotient system based on $(X, \mathcal{R})$ representing $G/\gamma_{C+1}(G)$. This can be done by starting with the trivial quotient system $\mathcal{A}_0$ based on $(X, \mathcal{R})$. If the consistent quotient system $\mathcal{A}_c$ represents $G/\gamma_{C+1}(G)$, then its central covering system $\mathcal{A}_{c+1}$ represents $G/\gamma_{C+2}$. A consistent quotient system for $G/\gamma_{C+1}(G)$ can be computed by successively computing $\mathcal{A}_{c+1}$ from $\mathcal{A}_c$ until $c + 1 = C$.

The main drawback of this approach is that in computing $\mathcal{A}_c$ the number of new generators quickly becomes too large for practical purposes. Let $n_c$ be the number of generators of the polycyclic presentation in $\mathcal{A}_c$. Each of the generators of the polycyclic presentation of $\mathcal{A}_c$ is defined either by an image of an element in $X$ or by a polycyclic relation. Let $I_c$ be the set of indices of generators with a power relation in the polycyclic presentation of $\mathcal{A}_c$. There are $|X|$ images of generators in $X$, the number of power relations is $|I_c|$ and the number of positive and inverse conjugate relations is at most $n_c(n_c - 1)$. The number of new generators that have to be defined is the sum of these three values minus the number of generators because each generator has a definition. Therefore the number of new generators is at most $|X| + |I_c| + n_c(n_c - 2)$. In other words, the number of new generators is a quadratic function of the number of generators in the polycyclic presentation. However, by Theorem 2.3.7 we know that $\gamma_c(G)/\gamma_{C+1}(G)$ can be generated by $n_1 e$ generators, where $n_1$ is the number of generators for $G/\gamma_1(G)$ and $e$ the number of generators for $\gamma_{c-1}(G)/\gamma_c G$. So it is desirable to reduce the number of newly defined generators. We will describe an algorithm that defines

$$|X| + |I_c| + \binom{n_1}{2} + n_1(n_c - n_1) - n_c$$

new generators.

5.2 Polycyclic Presentations for Nilpotent Groups

In Section 2.3 we saw that nilpotent polycyclic groups can be defined by a special type of polycyclic presentation. The structure of those presentations makes it possible to carry out computations with nilpotent groups more efficiently than with general polycyclic presentations.
5.2.1 Definition A polycyclic presentation is called a nilpotent (polycyclic) presentation if the conjugate relations take the following form.

For each pair $i, j \in \{1, \ldots, n\}$, $i < j$, there are the relations

\[
\begin{align*}
    a_i^{-1} a_j a_i &= a_j w_{ij}^{++}, \\
    a_i a_j a_i^{-1} &= a_j w_{ij}^{-+}, \quad i \notin I, \\
    a_i^{-1} a_j^{-1} a_i &= a_j^{-1} w_{ij}^{+-}, \quad j \notin I, \\
    a_i a_j^{-1} a_i^{-1} &= a_j^{-1} w_{ij}^{--}, \quad i, j \notin I.
\end{align*}
\]

The right hand sides $w_{ij}^{++}$, $w_{ij}^{-+}$, $w_{ij}^{+-}$, and $w_{ij}^{--}$ are words in $\{a_{j+1}, \ldots, a_n\}$.

5.2.2 Theorem A group given by a nilpotent polycyclic presentation is nilpotent.

Proof: Let $(A, S)$ be a nilpotent polycyclic presentation and define $G_i$ to be the group generated by the elements $\{a_i, \ldots, a_n\}$. Similarly to the proof of Lemma 3.1.2 we see that $G_i$ is normal in $G = G_1$. From the presentation it is clear that $a_i G_i$ is central in $G/G_{i+1}$. Therefore, $G = G_1 \geq \ldots G_{n+1} = 1$ is a central series of $G$ and $G$ is nilpotent.

In Section 2.3 we defined a weight function in terms of the lower central series of a group and showed that the weight of a commutator is at least the sum of the weights of the two components of the commutator. This motivates the following definition.

5.2.3 Definition A weighted nilpotent presentation is a triple $(A, S, w)$ such that $(A, S)$ is a nilpotent polycyclic presentation in which the right hand sides of all relations are reduced words and $w : \{a_1, \ldots, a_n\} \rightarrow \mathbb{N}$ is a function such that the relations satisfy the following conditions

\[
\begin{align*}
    w(a) &\geq w(a_i) \quad \text{for each generator } a \text{ occurring in } w_{ii} \text{ and } w_{ii}^{-}, \\
    w(a) &\geq w(a_i) + w(a_j) \quad \text{for each generator } a \text{ occurring in } w_{ij}^{++}, w_{ij}^{-+}, w_{ij}^{+-} \text{ and } w_{ij}^{--}.
\end{align*}
\]
The value \( w(a) \) for a generator \( a \) is called the weight of \( a \). The weight of the inverse of a generator is defined to be the same as the weight of the generator. The weight \( w(u) \) of a non-empty word \( u \) in the generators \( a_1, \ldots, a_n \) is defined as the minimum of the weights of the generators occurring in \( u \). The empty word is assigned the weight \( \infty \).

By Lemma 2.3.3, the weight function for nilpotent groups defined in Section 2.3 is a weight function in the sense of the previous definition. The weight function defined here does not indicate in which term of the lower central series a group element lies but rather which conjugate relations are involved in collecting a word to normal form. Let \((A, S, w)\) be a weighted polycyclic presentation and \(c\) the highest weight assigned to a generator by the weight function \(w\). Then two generators evidently commute if the sum of their weights is bigger than \(c\). Consequently, two words in the generating set commute if the sum of their weights is larger than \(c\).

5.2.4 Example The following is a consistent weighted nilpotent presentation,

\[
\langle a_1, a_2, a_3, a_4 \mid a_1^{-1}a_2a_1 =: a_2a_3, \\
a_1^{-1}a_3a_1 =: a_3a_4, \quad a_2^{-1}a_3a_2 = a_3a_4, \\
a_1^{-1}a_4a_1 = a_4, \quad a_2^{-1}a_4a_2 = a_4, \quad a_3^{-1}a_4a_3 = a_4, \\
a_1a_2a_1^{-1} = a_2a_3^{-1}a_4, \\
a_1a_3a_1^{-1} = a_3a_4^{-1}, \quad a_2a_3a_2^{-1} = a_3a_4^{-1}, \\
a_3a_4a_3^{-1} = a_4 \rangle
\]

The weight of \(a_1\) and \(a_2\) is 1, the weight \(a_3\) is 2 and the weight of \(a_4\) is 3. The word \(a_4a_3a_1a_1^{-1}\) has weight 1. It can be collected in two different ways. If \(a_1a_1^{-1}\) is replaced by the empty word, we get \(a_4a_3\). Because \(w(a_3) + w(a_4) > 3\), these two generators commute and we get \(a_3a_4\). Therefore, the group element corresponding to \(a_3a_4\), and \(a_4a_3a_1a_1^{-1}\), has weight 2. However, it is possible that in collecting the word \(a_4a_3a_1a_1^{-1}\) to normal form conjugate relations are used that involve generators of weight smaller than 2. If the first elementary collection step applied to \(a_4a_3a_1a_1^{-1}\) is to move \(a_1\) past \(a_3\), the conjugate relation \(a_1^{-1}a_3a_1 =: a_3a_4\) is used. Since the presentation above is consistent, this will lead to the same reduced
word. This example shows that the weight of a word indicates which conjugate relations might be used in collecting a word. If a word has weight \( c \), then conjugate relations in which the conjugating generator has weight \( c \) might have to be used to collect the word to normal form. On the other hand, conjugate relations in which the conjugating generator has weight smaller than \( c \) will not be used in collecting the word to reduced form.

5.2.5 Lemma

Let \( (A, S, w) \) be a weighted polycyclic presentations with generating sequence \( (a_1, \ldots, a_n) \) and let \( c \) be the highest weight of a generator in \( A \). Let \( i \) be an integer such that \( 1 \leq i \leq n \) and \( w(a_j) + w(a_k) > c \) for \( i \leq j, k \leq n \). If we define \( A' \) to be the sequence \( (a_1, \ldots, a_n) \), \( S' \) to be the set of relations in \( S \) that only involve the generators in \( A' \) and \( w' \) to be the restriction of \( w \) to \( A' \), then \( (A', S', w') \) is consistent.

Proof: The weight condition on the generating set \( A' \) implies that all conjugate relations are trivial. The claim follows from Theorem 3.2.3. \( \blacksquare \)

Let \( (A, S, w) \) be a weighted nilpotent presentation, \( u \) a word in \( A \) and \( a \in A \) such that \( w(a) < w(u) \) and \( w(a) + w(u) > c \) where \( c \) is the highest weight of a generator in \( A \). Then \( a \) commutes with \( u \) and with all words which are created from \( u \) by applying a sequence of elementary collection steps to \( u \). This means that in a given sequence of elementary collection steps applied to \( u a \) those steps that move \( a \) to the left can be carried out at any time. In particular, \( a \) can be moved to the left of \( u \) postponing any collection steps applied to \( u \). We call this the second postponing principle.

5.2.6 Theorem

(Consistency test for weighted nilpotent presentations)

Let \( (A, S, w) \) be a nilpotent weighted presentation with generating sequence \( (a_1, \ldots, a_n) \) and let \( c \) be the highest weight of a generator in \( A \). Then \( (A, S, w) \) is consistent if the following conditions are satisfied:

\[
\begin{align*}
  a_k [a_j a_i] &= [a_k a_j] a_i & \text{for } 1 \leq i < j < k \leq n \\
  \text{and } w(a_k) + w(a_j) + w(a_i) &\leq c \\
  [a_k^{m_k}] a_i &= a_k^{m_k-1} [a_k a_i] & \text{for } 1 \leq k < i \leq n, \ k \in I \\
  \text{and } w(a_k) + w(a_i) &\leq c
\end{align*}
\]
\[
\begin{align*}
  a_k[a_j^{mj}] &= \llbracket a_k a_j \rrbracket a_j^{mj - 1} & \text{for } 1 \leq k < j \leq n, j \in I \\
  \text{and } w(a_k) + w(a_j) \leq c \\
  a_j[a_j^{mj}] &= \llbracket a_j^{mj} \rrbracket a_j & \text{for } j \in I \\
  \text{and } 2w(a_j) \leq c \\
  a_k &= \llbracket a_k a_j^{-1} \rrbracket a_j & \text{for } 1 \leq i < k \leq n, k \notin I \\
  \text{and } w(a_k) + w(a_j) \leq c
\end{align*}
\]

If it is not assumed that the inverted conjugate relations are consequences of the other relations, the following conditions have also to be satisfied.

\[
\begin{align*}
  a_j &= a_k^{-1}[a_k a_j] & \text{for } 1 \leq i < k \leq n, k \notin I \\
  \text{and } w(a_k) + w(a_j) \leq c \\
  a_j^{-1} &= a_k^{-1}[a_k a_j^{-1}] & \text{for } 1 \leq i < k \leq n, k \notin I \\
  \text{and } w(a_k) + w(a_j) \leq c
\end{align*}
\]

Proof: In view of Theorem 3.4.1 we need to prove that both sides of those conditions for which the sum of the weights of the relevant generators is larger than \(c\) collect to the same reduced form. We will only present the first case because it is the most complicated one and the arguments for the other cases are similar.

Let \(a_k > a_j > a_i\) be generators such that \(w(a_k) + w(a_j) + w(a_i) > c\). We show that collecting \(a_k[a_j a_i]\) and \([a_k a_j]a_i\) results in the same reduced word.

First we collect \(a_k[a_j a_i]\) to reduced form. The first two elementary collection steps are uniquely determined resulting in the words

\[
a_k a_j a_i w_{ij}^{++}
\]

and

\[
a_i a_k w_{ik}^{++} a_j w_{ij}^{++}.
\]

The generator \(a_j\) commutes with \(w_{ik}^{++}\) because \(w(a_j) + w(w_{ik}^{++}) > c\). Applying the second postponing principle to \(a_j\) we get the word

\[
a_i a_j a_k w_{jk}^{++} w_{ik}^{++} w_{ij}^{++}.
\]

Write \(w_{ij}^{++}\) as a product of \(u_1 a_k u_2 u_3\) where \(u_1\), \(u_2\) and \(u_3\) are chosen such that all generators in \(u_1\) are smaller than \(a_k\), all generators occurring in \(u_2\) are larger
than $a_k$, $w(u_2) < w(w_{ik}^{++})$ and $w(u_3) \geq w(w_{ik}^{++})$. With this the word above is equal to

$$a_ia_ja_kw_{jk}^{++}w_{ik}^{++}u_1a_k^{e_k}u_2u_3.$$ 

By the second postponing principle, $u_1$ and $a_k^{e_k}u_2$ can be moved to the left to get the word

$$a_ia_ju_1a_k^{e_k+1}u_2w_{jk}^{++}w_{ik}^{++}u_3.$$ 

Now we collect $[a_k a_j]a_i$. The first collection step results in the word

$$a_ja_kw_{jk}^{++}a_i.$$ 

Because of weight considerations, $a_i$ commutes with $w_{jk}^{++}$ and can be moved past it giving

$$a_ja_k a_i w_{jk}^{++}.$$ 

By the first postponing principle we get

$$a_ia_jw_{ij}^{++}a_kw_{ik}^{++}w_{jk}^{++}.$$ 

Replacing $w_{ij}^{++}$ by $u_1a_k^{e_k}u_2u_3$ gives

$$a_ia_ju_1a_k^{e_k}u_2u_3a_kw_{ik}^{++}w_{jk}^{++}.$$ 

The sum of the weights of $u_2u_3$ and $a_k$ is larger than $c$, therefore, by the second postponing principle, $a_k$ can be moved to the left producing the word

$$a_ia_ju_1a_k^{e_k+1}u_2u_3w_{ik}^{++}w_{jk}^{++}.$$ 

Each generator in the word $u_3w_{ik}^{++}w_{jk}^{++}$ has weight at least $w(a_i) + w(a_k)$. Therefore, all conjugate relations used in collecting this word to normal form are trivial because $2w(a_i) + 2w(a_k) \leq 2w(a_i) + w(a_k) + w(a_j) > c$. This means that collecting this word takes place in an abelian subgroup for which the relevant relations form a consistent polycyclic presentation. Since $w_{jk}^{++}w_{ik}^{++}u_3$ and $u_3w_{ik}^{++}w_{jk}^{++}$ clearly represent the same element of the group, they collect to the same (unique) normal
form. This shows that collecting $a_k[a_ja_i]$ and $[a_k a_j]a_i$ leads to the same reduced form.

5.3 Quotient systems for nilpotent groups

5.3.1 Definition A quotient system $\mathcal{A} = ((X, R), (A, S, w), \sigma)$ is called a weighted nilpotent quotient system if $(A, S, w)$ is a weighted polycyclic presentation such that the following conditions hold.

- For each generator $a \in A$ there is either
  - an element $x \in X$ such that $x \sigma = a$ is the definition of $a$ in which case $w(a) = 1$ or
  - a pair $x, y \in A$ with $w(x) = 1$ such that $x^{-1}yx = ya$ is the definition of $a$ in which case $w(a) = w(y) + 1$.

- If $\mathcal{A}$ is consistent, the weight function $w$ coincides on $A$ with the weight function defined by the lower central series of the group defined by $(A, S)$.

We will now describe an algorithm that constructs a consistent weighted nilpotent quotient system for $G/\gamma_C(G)$.

We start with $\mathcal{A}_0 = ((X, R), (\emptyset, \emptyset), \sigma_0)$, the trivial quotient system based on $(X, R)$. Let $X$ be the set $\{x_1, \ldots, x_m\}$. Then the central covering system $\mathcal{A}_0'$ of $\mathcal{A}_0$ has the form $((X, R), (A'_0, S'_0, w'_0), \sigma'_0)$ where

\[
\begin{align*}
A'_0 &= \{a_1, \ldots, a_m\} \\
S'_0 &= \{ a_i^{-1} a_j a_i = a_j \mid 1 \leq i < j \leq m \} \\
w'_0 : a_i &\longrightarrow 1 \quad \text{for } 1 \leq i \leq m \\
\sigma'_0 : x_i &\longrightarrow a_i \quad \text{for } 1 \leq i \leq m.
\end{align*}
\]

The polycyclic presentation is consistent by Theorem 3.2.3. In order to make $\mathcal{A}_0'$ consistent the relations in $\mathcal{R}$ have to be enforced. By Theorem 4.4 this gives a generating set $\{ r(a_1, \ldots, a_n) \mid r \in \mathcal{R} \}$ for a subgroup $V$ of the free abelian group $U$ defined by $(A'_0, S'_0, w'_0)$. Let $I'_0 \subseteq \{1, \ldots, n\}$ and $\{ a_i^{m_i} = w_{ii} \mid i \in I'_0 \}$ be a set of relations for $U/V$ with a relation matrix in row Hermite normal form.

56
Now let $I_1 \subseteq I_0'$ be the indices of generators for which $m_i > 1$ and define $J = \{1, \ldots, n\} \setminus I_0' \cup I_1$. Then we get the following consistent weighted nilpotent quotient system $A_1 = ((X, \mathcal{R}), (A_1, S_1, w_1), \sigma_1)$ representing the largest abelian quotient of $G$ with

$$A_1 = \{ a_i \mid i \in J \},$$
$$S_1 = \{ a_i^{-1}a_ja_i = a_j \mid i, j \in J, i < j \} \cup \{ a_i^{m_i} = w_{ii} \mid i \in I_1 \},$$
$$w_1 : a_i \mapsto 1 \quad \text{for} \quad i \in J,$$
$$\sigma_1 : x_i \mapsto a_i \quad \text{for} \quad i \in J,$$
$$x_i \mapsto w_{ii} \quad \text{for} \quad i \in I_0' \setminus I_1.$$

Let $A_c = ((X, \mathcal{R}), (A_c, S_c, w_c), \sigma_c)$ be a consistent weighted nilpotent quotient system representing $G/\gamma_{c+1}(G)$. We form the central covering system $A'_c$ defined by $((X, \mathcal{R}), (A'_c, S'_c), \sigma'_c)$ as in Chapter 4 representing $G/\gamma_{c+2}(G)$. Let $T = A'_c \setminus A_c$ be the set of newly defined generators. The weight function $w_c$ is extended to a weight function $w'_c$ on $A'_c$ by defining $w'_c(a) = w_c(a)$ if $a \in A_c$ and $w'_c(a) = c + 1$ if $a \in T$. Then $(A'_c, S'_c, w'_c)$ is a weighted nilpotent presentation. We define the following subsets of $T$. Let

- $T_{c+1} \subseteq T$ be the set of newly defined generators that are defined by a conjugate relation with left hand side $a_i^{-1}a_ja_i$ such that $w(a_i) = 1$ and $w(a_j) = c$;
- $T_{pc} \subseteq T$ be the set of generators defined by a power relation or a conjugate relation with left hand side $a_i^{-1}a_ja_i$ such that $w(a_i) = 1$;
- $T_{\sigma} \subseteq T$ be the set of generators defined by an image of $\sigma'_c$;
- $T_{\text{conj}} \subseteq T$ be the set of generators that are defined by a conjugate relation but are not elements of $T_{pc}$.

Note that $T_{c+1} \subseteq T_{pc}$. We define the linear order on the generators in $T$ such that all generators in $T_{c+1}$ are larger than the generators in $T_{pc} \setminus T_{c+1}$, the generators in $T_{pc}$ are larger than the generators in $T_{\sigma}$ and the generators in $T_{\sigma}$ are larger than the generators in $T_{\text{conj}}$.

By Theorem 2.3.7 the set $\{ [y, x] \mid x, y \in A_c, w(y) = c, w(x) = 1 \}$ generates the group $\gamma_{c+1}(G)/\gamma_{c+2}(G)$. This means that in making $A'_c$ consistent, we will find a set of relations that expresses each generator in $T \setminus T_{c+1}$ as a word in $T_{c+1}$. It
is possible to describe an algorithm, often called the tails routine, that expresses each generator in $T_{\text{conj}}$ as a word in $T_{\text{pc}}$. The name comes from the following definition.

5.3.2 Definition Let $(A, S, w)$ be a weighted nilpotent presentation and let $c$ be the highest weight of a generator in $A$. If $y$ is a reduced word in $A$, write $y$ as a product $y_1y_2$ with $w(y_1) < c$ and $w(y_2) \geq c$. Then $y_2$ is called the tail of the word $y$. If $y$ is the right hand side of a relation $x = y$ in $S$, then $y_2$ is called the tail of the relation $x = y$.

The tails routine is described in the next section. We assume for now that all generators in $T_{\text{conj}}$ have been replaced by words in $T_{\text{pc}}$.

Let $U$ be the free abelian group on the generating set $T_{\sigma} \cup T_{\text{pc}}$. Rename the generators in this linearly ordered set as $a_{n_c+1}, \ldots, a_{n_c+1}$, where $n_c$ is the number of generators in $A_c$. Applying Theorem 5.2.6 to the weighted nilpotent presentation results in a set of reduced words in $T_{\sigma} \cup T_{\text{pc}}$. The union of this set and the set $\{ r(x_1\sigma, \ldots, x_n\sigma) \mid r \in R \}$ generates a subgroup $V$ of $U$. Let $I'_c \subseteq \{n_c + 1, \ldots, n_c+1\}$ and $\{ a_i^{m_i} = w_{ii} \mid i \in I'_c \}$ be a set of relations for $U/V$ with a relation matrix in row Hermite normal form.

Now let $I_{c+1} \subseteq I'_c$ be the indices of generators for which $m_i > 1$ and define $J_{c+1} = \{n_c + 1, \ldots, n_c+1\} \setminus I'_c \cup I_{c+1}$. All generators in $T_{\sigma}$ and $T_{\text{pc}} \setminus T_{c+1}$ can be expressed as words in $T_{c+1}$ by Theorem 2.3.7. The linear ordering on $T_{\text{pc}} \cup T_{\sigma}$ guarantees that each of these generators appears with exponent 1 on the left hand side of a relation for $U/V$. This means that the set of generators corresponding to $J_{c+1}$ is a subset of $T_{c+1}$. Eliminating all other generators from the quotient system $A'_c$ we get a consistent weighted nilpotent quotient system $A_{c+1} = (\langle X, R \rangle, (A_{c+1}, S_{c+1}, w_{c+1}), \sigma_{c+1})$ representing the quotient $G/\gamma_{c+2}(G)$.

5.4 The Tails Routine

For practical purposes it is desirable to keep the number of new generators small. This is what the tails routine achieves by precomputing a word in $T_{\text{pc}}$ for each generator $t \in T_{\text{conj}}$ using certain checks of the consistency theorem.

The tails routine as described here is a generalisation of the tails routine used in the ANU PQ program (formerly Canberra Nilpotent Quotient Program). It
differs from the tails routine as used in that program in two respects: The first difference is that the tails routine in a nilpotent quotient algorithm has to be able to handle conjugate relations that involve inverses of generators, a condition that does not appear in the ANU PQ. The second difference is that the weight function in a nilpotent quotient algorithm is slightly different from the weight function used in the ANU PQ. All generators in the nilpotent quotient algorithm we are describing are defined as commutators of earlier generators. This assumption cannot be made in the ANU PQ since here generators can also be defined as $p$-th powers. If all generators are defined as commutators, the tails routine is easier to describe because there are fewer subcases to deal with. The details of the tails routine implemented in the ANU PQ have not been published but will become available in the near future as a joint research report (Celler, Newman, Nickel, Niemeyer, 1993).

We fix two generators $a_l$ and $a_k$ with $w(a_l) \geq w(a_k) > 1$. If $b$ is the sum of the weights of $a_k$ and $a_l$, then $b \geq 4$. We want to compute the tails of the relations

$$a_k^{-1}a_la_k = a_l^{w_{kl}^{-1}+t_{kl}^{-1}}$$
$$a_k^{-1}a_la_k^{-1} = a_l^{w_{kl}^{-1}+t_{kl}^{-1}}, \text{ if } k \not\in I,$$
$$a_k^{-1}a_la_k^{-1} = a_l^{w_{kl}^{-1}+t_{kl}^{-1}}, \text{ if } l \not\in I,$$
$$a_k^{-1}a_la_k^{-1} = a_l^{w_{kl}^{-1}+t_{kl}^{-1}}, \text{ if } k, l \not\in I.$$

For this we assume that the tails of the following conjugate relations are words in $T_{pc}$:

$$a_i^{-1}a_ja_i = a_j^{w_{ij}^{+}+t_{ij}^{+}}$$
$$a_i^{-1}a_ja_i^{-1} = a_j^{w_{ij}^{-}+t_{ij}^{-}}$$

for $i < j$ and $w(a_i) + w(a_j) > b$ and

$$a_i^{-1}a_j^{-1}a_i = a_j^{w_{ij}^{+}+t_{ij}^{-}}$$
$$a_i^{-1}a_j^{-1}a_i^{-1} = a_j^{w_{ij}^{-}+t_{ij}^{-}}$$

for $i < j$, $w(a_i) + w(a_j) = b$ and $w(a_j) > w(a_l)$.

Note that by the definition of $T_{pc}$ the tails of all positive conjugate relations where the conjugating generator has weight 1 and the tails of all power relations are words (of length 1) in $T_{pc}$. If $w$ is a word of weight at least $\lfloor b/2 \rfloor + 1$, then collecting $w$ to normal form only involves relations whose tails are words in $T_{pc}$. Let $a_i^{-1}a_ja_i = a_ja_k$ be the definition of $a_k$. This means that $a_i$ has weight 1 and
$a_j$ has weight $w(a_k) - 1$. The weight of $a_l$ is bigger than or equal to the weight of $a_k$; hence $w(a_l) \geq b/2$.

We will collect the word $a_l a_j a_i$ in two different ways. In each case we have to go through the collection carefully and see which relations are used. The quotient for the two results will be a reduced word for the identity. This reduced word will be a word in $T_{pc} \cup \{t_{kl}^{++}\}$ in which $t_{kl}^{++}$ will have exponent $-1$ and can therefore be used to express $t_{kl}^{++}$ as a word in $T_{pc}$.

First, we collect $a_l(a_j a_i)$ and obtain, by applying two elementary collection steps,

$$a_l(a_j a_i) = a_l a_ia_j a_k = a_l a_i w_{il}^{++} t_{il}^{++} a_j a_k.$$  

Here, the generator $a_j$ has to be moved to the left. The word $w_{il}^{++} t_{il}^{++}$ has weight $w(a_l) + 1$. In moving $a_j$ across, only conjugate relations with left hand side $a_j^{-1} x a_j$ are used with $w(x) + w(a_j) \geq w(a_l) + 1 + w(a_j) = b$. The tail of each of these conjugate relations is a word in $T_{pc}$ by assumption because either $w(x) + w(a_j) > b$ or, if $w(x) + w(a_j) = b$, $w(x) > w(a_l)$. After a series of elementary collection steps we get the word

$$a_i a_l w_1 a_j w_2 a_k w_3$$

where $w_1$ is an initial segment of $w_{il}$ and the words $w_2$ and $w_3$ are words of weight at least $w(a_l) + 1 \geq \lceil b/2 \rceil + 1$. Therefore, applying elementary collection steps to the word $w_2 a_k w_3$ involves only relations whose tails are words in $T_{pc}$. Continuing collection we get the following situation just before $a_l$ is going to be moved past $a_i$

$$a_l a_i a_j w_4 a_k w_5$$

where $w_4$ and $w_5$ are words of weight at least $w(a_l) + 1$. In moving $a_j$ past $a_l$ the relation $a_j^{-1} a_l a_j = a_l w_{jl}^{++} t_{jl}^{++}$ is used. The sum of the weights $w(a_j)$ and $w(a_l)$ is $b - 1$. Therefore, using this relation introduces a tail which is not a word in $T_{pc}$. From here collection of the word

$$a_l a_j a_l w_{jl}^{++} t_{jl}^{++} w_4 a_k w_5$$

proceeds by applying relations whose tails are words in $T_{pc}$ until the following situation occurs

$$a_l a_j a_l a_k w_6 t_{jl}^{++} w_7$$
with $w_6$ and $w_7$ being words of weight at least $w(a_l) + 1$. Now applying the relation $a_k^{-1}a_l a_k = a_l w_k t t_{kl}^{++}$ gives the following word

$$a_i a_j a_k a_l w_k t t_{kl}^{++} w_6 t_{ji}^{++} w_7.$$

The word $w_k t t_{kl}^{++} w_6 t_{ji}^{++} w_7$ can be collected to normal form because its weight is at least $\lceil b/2 \rceil + 1$ resulting in the reduced form

$$a_i a_j a_k a_l w_8 t t_{kl}^{++} w_9 t_{ji}^{++} w_{10}.$$

Now we will collect the word $(a_i a_j) a_i$. We have that $w(a_l) + w(a_j) = b - 1$, so we get

$$(a_i a_j) a_i = a_j a_l w_j t_{ij}^{++} t_{kl}^{++} a_i.$$ Moving $a_i$ to the left uses only conjugate relations whose tails are words in $T_{pc}$. The word $w_{ji}^{++} t_{kl}^{++}$ has weight $b - 1$. After $a_i$ has been moved next to $a_i$ we have the following situation

$$a_j a_l a_i v_1 t_{ji}^{++} v_2$$

where $v_1 t_{ji}^{++} v_2$ is a word of weight at least $b$. Now we get

$$a_j a_l a_i w_{it}^{++} t_{il}^{++} v_1 t_{ji}^{++} v_2.$$ The word $w_{it}^{++} t_{il}^{++} v_1 t_{ji}^{++} v_2$ has weight $b - 1$ and therefore collecting this word to reduced form only involves relations whose tails are words in $T_{pc}$. Finally $a_i$ moves past $a_j$ resulting in the reduced word

$$a_i a_j a_k a_l v_3 t_{ji}^{++} v_4$$

where $v_3$ and $v_4$ are reduced words.

Multiplying the inverse of the first result with the second result from the right gives the following

$$w_{10}^{-1}(t_{ji}^{++})^{-1} w_{9}^{-1}(t_{kl}^{++})^{-1} w_{8}^{-1} a_l^{-1} a_k^{-1} a_l^{-1} a_i^{-1} a_i a_j a_k a_l v_3 t_{ji}^{++} v_4.$$
After cancelling the middle part of this expression we are left with a word of weight at least \( b - 1 \). Collecting this word involves only relations whose tails are a word in \( T_{pc} \). The generator \( t_{jl}^{++} \) does not occur in the reduced form because it cancels with its inverse. The result of collecting the word above is the following reduced word which is, as an element of the group, the identity:

\[
v_5(t_{kl}^{++})^{-1}v_6.
\]

From this we get the relation

\[
t_{kl}^{++} = v_5v_6.
\]

For the next calculation assume that \( k \notin I \). We want to calculate the tail of \( a_k a_l a_k^{-1} = a_l w_{kl}^{-t} t_{kl}^{-+} \). This is done by collecting the word \((a_l a_k^{-1}) a_k\). Swapping \( a_l \) and \( a_k^{-1} \) results in the word

\[
a_k^{-1} a_l w_{kl}^{-+} t_{kl}^{-+} a_k.
\]

Now in moving \( a_k \) to the left only relations are used with tails that are words in \( T_{pc} \). After a sequence of elementary collection steps the following situation arises

\[
a_k^{-1} a_l a_k v_1 t_{kl}^{-+} v_2.
\]

The word \( v_1 t_{kl}^{-+} v_2 \) comes from partly collecting the word that was produced by moving \( a_k \) to the left. Now swapping \( a_l \) and \( a_k \) and deleting \( a_k^{-1} a_k \) gives the word

\[
a_l w_{kl} v_1 t_{kl}^{-+} v_2.
\]

The weight of the word \( w_{kl} v_1 t_{kl}^{-+} v_2 \) is clearly larger than the weight of \( a_l \). Collecting it involves only relations whose tails are words in \( T_{pc} \) and results in a reduced word

\[
a_l v_3 t_{kl}^{-+} v_4.
\]

This word is, as an element of the group, equal to \( a_l \). This produces the relation

\[
t_{kl}^{-+} = (v_4v_3)^{-1}.
\]
For the next calculation assume that \( l \notin I \). We want to calculate the tail of the relation \( a_k^{-1}a_l^{-1}a_k = a_lw_{kl}^+t_{kl}^- \) as a word in \( T_{pc} \). This is done by collecting \( a_l^{-1}(a_la_k) \). This results in the word

\[
a_l^{-1}a_ka_lw_{kl}^+
\]

and then in the word

\[
a_ka_l^{-1}w_{kl}^+t_{kl}^-a_lw_{kl}^+t_{kl}^+
\]

Collecting this word only involves relations whose tails are words in \( T_{pc} \). If the reduced form of the word above is

\[
a_kv_1t_{kl}^-v_2,
\]

then we get the relation

\[
t_{kl}^+ = (v_1v_2)^{-1}.
\]

The last calculation to be performed is the computation of the tail of the relation \( a_k^{-1}a_l^{-1}a_k = a_lw_{kl}^+t_{kl}^- \) if \( l \notin I \). For this the word \( a_l^{-1}(a_la_k^{-1}) \) has to be collected. Mutatis mutandis, the argument is the same as in the previous case.

### 5.5 Remarks on an Implementation

This section outlines an implementation of the nilpotent quotient algorithm described in this chapter. The program described here is Version 1.1c of the Australian National University Nilpotent Quotient Program (ANU NQ).

The program takes as input a finite presentation \((X, \mathcal{R})\) for a group \( G \) and an optional positive integer \( c \). It then computes a consistent weighted nilpotent quotient system \(((X, \mathcal{R}), (A, S, w), \sigma)\) representing \( G/\gamma_{c+1}(G) \). If the integer \( c \) is not given, the program attempts to compute a consistent weighted nilpotent quotient system representing the largest nilpotent quotient of \( G \). If \( G \) does not have a largest nilpotent quotient, the program only terminates if it exceeds its resources. The program also has the option of enforcing certain commutator laws on \( G \). Details of this will be given in the next section.
The three basic data structures of the ANU NQ are the data structures \texttt{word}, \texttt{expvec} and \texttt{lvector}.

The first represents elements of a group given by a polycyclic presentation as generator exponent lists. The list \((i_1, e_1, \ldots, i_l, e_l)\) represents the word \(a_{|i_1|}^{\text{sign}(i_1)e_1} \cdots a_{|i_l|}^{\text{sign}(i_l)e_l}\). The elements \(e_1, \ldots, e_n\) in a generator exponent list are always positive; inverses of generators are represented by the negative of the generator number. For example, the word \(a_1^5a_2^{-2}a_5^{-1}\) would be represented by the list \((1, 5, -2, 2, -5, 1)\). As will be explained later, this convention is convenient in accessing the right hand side of a conjugate relation in the data structure for polycyclic presentations.

The second data structure \texttt{expvec} is an array of integers representing the exponent vector \((e_1, \ldots, e_n)\) of a reduced word \(a_1^{e_1} \cdots a_n^{e_n}\), where \(n\) is the number of generators in the polycyclic presentation. The exponent vector corresponding to the word \(a_1^5a_2^{-2}a_5^{-1}\) is \((5, -2, 0, 0, -1, 0)\) assuming that the polycyclic presentation has 6 generators.

In both data structures the exponents are implemented by the C-data type \texttt{long}. On a DECstation 5000/120, the computer type the examples below were computed on, 32 bits are used to represent this data type.

The basic routine that uses these two data structures is the collection routine implementing "collection from the left". It is based on the description by Leedham-Green and Soicher (1990). The collection routine accepts an exponent vector for a reduced word \(v\), a word \(w\) and a positive integer \(k\) and returns an exponent vector for the reduced word of \(vw^k\). It is the basis for the arithmetic operations for polycyclic groups in the ANU NQ. Other routines such as the consistency check, the tails routine and the computation of inverses, powers and commutators of elements are based on the collection routine. The computation of inverses is adapted to polycyclic presentations from the inversion routine in Leedham-Green and Soicher (1990). In a future version of the ANU NQ this collection routine will be replaced by an implementation of "combinatorial collection from the left" as described by Vaughan-Lee (1990).

The exponents that arise during collection are checked for overflow and need to be. Overflow was encountered in some computations. For example, overflow occurs in the computation of the class-19 quotient of the group \(G_9\) below. The
overflow check used in the collection routine works on the assumption that the
C-operator >> performs an arithmetic right shift on long integers.

A weighted nilpotent presentation is stored in several parts. We assume the
notation of definitions 5.2.1 and 5.2.3. An integer variable stores the number \( n \)
of generators in the presentation, an integer array \( \text{Exponent} \) stores the exponents
\( m_i, i \in I \), another integer array \( \text{Weight} \) stores the weights of the generators,
an array \( \text{Power} \) stores the right hand sides of the power relations as words and
a two-dimensional array \( \text{Conjugate} \) stores the right hand sides of the conjugate
relations;

\[
\begin{align*}
\text{Exponent}[i] & = m_i & i \in I, \\
\text{Power}[i] & = w_{ii} & i \in I, \\
\text{Weight}[i] & = w(a_i) & 1 \leq i \leq n, \\
\text{Conjugate}[j][i] & = a_j w_{ij}^{++} & 1 \leq i < j \leq n, \\
\text{Conjugate}[j][-i] & = a_j w_{ij}^{-+} & 1 \leq i < j \leq n, i \not\in I, \\
\text{Conjugate}[-j][i] & = a_j^{-1} w_{ij}^{+-} & 1 \leq i < j \leq n, j \not\in I, \\
\text{Conjugate}[-j][-i] & = a_j^{-1} w_{ij}^{--} & 1 \leq i < j \leq n, i, j \not\in I.
\end{align*}
\]

Now it becomes apparent why the inverse of a generator in an element of
type \text{word} is stored by the negative generator number. The right hand sides of
the conjugate relations can be stored in one data structure and when the collector
encounters a pair \( j, i \) of generator numbers with \( |j| > |i| \) the conjugate relation
necessary to swap the generators is \( \text{Conjugate}[j][i] \).

The consistency check implemented in the ANU NQ uses the test words of
Theorem 5.2.6 where only those of the words \( a_k a_j a_i \) and \( a_k^{m_k} a_i \) are used in which
\( a_i \) has weight 1. This reduction of the set of test words was proved by Vaughan-Lee

The third basic data structure used by the ANU NQ is called \text{lvector} and
stores integer vectors as an array of arbitrary precision integers. The GNU MP
package written by Torbjörn Granlund is used to perform arithmetic operations
with arbitrary precision integers. The ANU NQ has a collection of basic routines to
perform vector operations and, based on those, an implementation of the Kannan-
Bachem algorithm (Sims, 1993) for the computation of the row Hermite normal
form of integer matrices. An integer matrix is stored as a list of integer vectors of
type \text{lvector}.
The ANU NQ uses expression trees to store the relations of the presentation \((X, \mathcal{R})\). The input presentation is read in from file by a recursive descent parser and the relations are translated into a list of expression trees. In order to illustrate this we give an example. Let \((X, \mathcal{R})\) be the presentation \(<a,b| [b,a,a]^{-2}[b,a,b*a]^{-1}>\) as written on the input file. This presentation is read by the parser and the only relation is translated into the following tree.

This tree can be evaluated recursively on specific elements for \(a\) and \(b\) from a polycyclicly presented group. A widely used way of storing relations is a generator list in which a relation is stored as a string of generators and their inverses. The main drawback of generator lists is that compact expressions, like the example above, have to be expanded. Our example expands to the following product with 28 factors and 14 inverted generators:

\[
a^{-1}b^{-1}aba^{-1}b^{-1}a^{-1}bab^{-1}aba^{-1}b^{-1}a^{-1}bab^{-1}a^{-1}b^{-1}aba^{-1}b^{-1}aba^{-1}b^{-1}a^{-1}ba.
\]

Consequently, it is more expensive to evaluate the generator list on specific values for \(a\) and \(b\) than to evaluate the expression tree. However, it is possible that a complicated relation can be freely reduced to a short expression and it may be better to use the equivalent generator list. It seems that in practice the reverse happens more frequently, namely that a relation when expanded to a generator list becomes a long product. A clear advantage of storing relations as expression trees is that the parser preserves the structure of the relation. This allows the user of the ANU NQ to specify relations such that their evaluation is efficient.
While running the ANU NQ prints out a message for each factor of the lower central series that it computes. When the program terminates normally, i.e., before it runs out of resources, it outputs the polycyclic presentation for the quotient group of the input group that it has computed. Inverted conjugate relations and trivial conjugate relations are not printed. Here is a typical output. The group $G$ is given by the input presentation $\langle a,b | [b,a,a]^2*[b,a,b]^3 \rangle$. The program computes a consistent weighted polycyclic presentation for $G/\gamma_4(G)$.

# The ANU Nilpotent Quotient Program
# (Version 1.1c, 12 Aug, 14 Oct 1993)
# Calculating a nilpotent quotient
# Input: comm2.3
# Nilpotency class: 3
# Program: /usd/werner/PC/bin/nq.ds Machine: ernie
# Calculating the abelian quotient ...
# The abelian quotient has 2 generators
# with the following exponents: 0 0
# Calculating the class 2 quotient ...
# Layer 2 of the lower central series has 1 generators
# with the following exponents: 0
# Calculating the class 3 quotient ...
# Layer 3 of the lower central series has 2 generators
# with the following exponents: 2 0

# The epimorphism :
# a|---|-> A
# b|---|-> B

# The nilpotent quotient :
$\langle A,B,C,D,E \mid D^2 = E^{-3},$  
$B^{-A} = B*C,$  
$B^{-}(A^{-1}) = B*C^{-1}D,$  
$C^{-A} = C*D,$  
$C^{-}(A^{-1}) = C*D*E^{-3},$  
$C^{-B} = C*E,$  
$C^{-}(B^{-1}) = C*E^{-1} >$

# Class : 3
# Nr of generators of each class : 2 1 2
# total runtime : 27 msec
# total size : 42732 byte

For each factor of the lower central series of $G$ the program prints the number of generators in the final polycyclic presentation for this factor. However, this
is not the minimal number of generators for this factor. The reason for this is that the ANU NQ computes the row Hermite normal form for the integer matrix that arises in the calculation of each factor of the lower central series (compare Section 5.3). For instance, the integer matrix computed by the ANU NQ for $\gamma_3(G)/\gamma_4(G)$ is $[2, 3]$. It stems from evaluating the relation $[y, x, z]^2[y, x, y]^3$. This matrix is already in row Hermite normal form. From this matrix the program introduces the relation $D^2 = E^{-3}$ into the polycyclic presentation for $G/\gamma_4(G)$. The subgroup $\gamma_3(G)/\gamma_4(G)$ can be generated by the element $DE$ because $(DE)^3 = D^3E^3 = D^3D^{-2} = D$ and $(DE)^{-2} = D^{-2}E^{-2} = E^3E^{-2} = E$. Setting $a = A, b = B, c = C, z = DE$ one gets the following consistent polycyclic presentation on 4 generators for $G/\gamma_4(G)$ (trivial and inverted conjugate relations are left out)

\[
(a, b, c, z | a^{-1}ba =: bc, \quad aba^{-1} = bc^{-1}z^3 \\
\quad a^{-1}ca = cz^3, \quad ac^{-1} = cz^{-3} \\
\quad b^{-1}cb = cz^{-2}, \quad bcb^{-1} = cz^2).
\]

We see that the generator $z$ in this presentation is not defined as a commutator of earlier generators. In fact, we have that $z = [c, a][c, b]$. The tails routine (Section 5.4) assumes generators to be defined as single commutators. Therefore, the implementation of the ANU NQ is such that it chooses the redundant generating set $\{D, E\}$ for $\gamma_3(G)/\gamma_4(G)$ instead of the minimal generating set $\{DE\}$. The worst case encountered so far is the example $G_4$ below where 62 generators are used for $\gamma_{11}(G_4)/\gamma_{12}(G_4)$ instead of a minimal set of 42 generators. Sims (1993), Chapter 11, discusses a routine ADJUST which computes a minimal generating set for each factor of the lower central series during the computation of a nilpotent quotient. We have not followed such an approach but have favoured a tails routine which we will see has a great influence on the performance of the ANU NQ.

For each generator $a_i$ of a factor of the lower central series the program also prints the exponent $m_i$ if the generator has a power relation and zero otherwise. The number of zeroes is the free rank of the central factor.

In the following the runtimes for the ANU NQ (Version 1.1c) on some selected examples are listed. All timings are taken on a DECstation 5000/120 with a CPU time limit of two hours and a data size limit of 16 megabyte.
For each of the following groups we list the nilpotency class of the quotient computed, the Hirsch length (i.e., the number of infinite cyclic factors in a polycyclic series), the number of generators in the polycyclic presentation, the runtime in seconds for the whole computation, the maximal amount of memory in kilobytes the run used and the time in seconds that was spent in computing the row Hermite normal form for the integer matrices that arise for each central factor. The total space used by the ANU NQ was determined using the UNIX system call sbrk(). This system call returns the first illegal address in the virtual linear address space of the calling program. The figures shown here are the differences of the values returned by sbrk() at the end and beginning of each run. The timings are given for the following groups:

\( G_1 \) is the free group on 2 generators.

\( G_2 \) is the free group on 3 generators.

\( G_3 \) is the free group on 4 generators.

\( G_4 = \langle a, b \mid [b, a, a, a], [b, a, b, b, b], b, ab, ab, ab, [b, ab^2, ab^2, ab^2] \rangle. \)

\( G_5 = \langle a, b \mid [a, [a, b]], [b, [a, b]] \rangle. \)

\( G_6 = \langle a, b \mid [a, [a, b]], [b, [a, b]], [b, a, b, a, b] \rangle. \)

\( G_7 = \langle a, b \mid [b, a, a, a], [b, a, b, b, b], [b, a, ab, ab, ab], [b, a, ab^2, ab^2, ab^2], \)

\[ [b, a, b, a, a, a], [b, a, b, a, b, b] \rangle. \)

\( G_8 = \langle g_1, g_2, g_3, g_4, g_5 \mid [g_2, g_1], [g_3, g_1, g_4, g_1] = [g_3, g_2], [g_5, g_1] = [g_4, g_2], \)

\[ [g_5, g_2] = [g_4, g_3], [g_4, g_3], [g_5, g_4] \rangle. \)

\( G_9 = \langle x, y \mid [y, x, y], [y, x, x, x, x] \rangle. \)

The groups \( G_6, G_7 \) and \( G_8 \) have a largest nilpotent quotient. This nilpotent quotient was computed in each case. For all other groups the ANU NQ was run with the parameter \( c \) specified.
The following table shows timings for a variation of the ANU NQ that uses only part of the tail computation as explained in Section 5.4. At each class this program defines new generators for all positive conjugate relations that are not definitions. It then uses the relevant part of the tails routine to compute the tails for the inverse and inverted conjugate relations. The table shows that this has two main effects. The first effect is that each run needs more memory than the corresponding run with the standard ANU NQ. The reason for this is that the integer matrices that arise at each class have more columns because the number of newly defined generators is larger. The second effect is an increase in the overall runtime which is mainly due to an increase of the time spent in computing the row Hermite normal form at each class. Those computations from the table above that are not listed in the table below could not be completed within the available memory.

<table>
<thead>
<tr>
<th>group</th>
<th>class</th>
<th>Hirsch</th>
<th>gens</th>
<th>time</th>
<th>space</th>
<th>Hermite</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_1$</td>
<td>12</td>
<td>747</td>
<td>747</td>
<td>177</td>
<td>6380</td>
<td>37.3</td>
</tr>
<tr>
<td>$G_1$</td>
<td>10</td>
<td>226</td>
<td>226</td>
<td>6.5</td>
<td>600</td>
<td>0.7</td>
</tr>
<tr>
<td>$G_2$</td>
<td>6</td>
<td>196</td>
<td>196</td>
<td>2.5</td>
<td>432</td>
<td>0.4</td>
</tr>
<tr>
<td>$G_2$</td>
<td>8</td>
<td>1318</td>
<td>1318</td>
<td>222</td>
<td>10905</td>
<td>117</td>
</tr>
<tr>
<td>$G_3$</td>
<td>5</td>
<td>294</td>
<td>294</td>
<td>4.5</td>
<td>915</td>
<td>0.9</td>
</tr>
<tr>
<td>$G_3$</td>
<td>6</td>
<td>964</td>
<td>964</td>
<td>83.1</td>
<td>8952</td>
<td>41.3</td>
</tr>
<tr>
<td>$G_4$</td>
<td>10</td>
<td>23</td>
<td>111</td>
<td>134</td>
<td>1075</td>
<td>106</td>
</tr>
<tr>
<td>$G_4$</td>
<td>11</td>
<td>24</td>
<td>173</td>
<td>1353</td>
<td>3750</td>
<td>623</td>
</tr>
<tr>
<td>$G_5$</td>
<td>12</td>
<td>17</td>
<td>76</td>
<td>50.0</td>
<td>678</td>
<td>42.1</td>
</tr>
<tr>
<td>$G_6$</td>
<td>9</td>
<td>8</td>
<td>14</td>
<td>0.6</td>
<td>80</td>
<td>0.2</td>
</tr>
<tr>
<td>$G_7$</td>
<td>10</td>
<td>11</td>
<td>36</td>
<td>9.0</td>
<td>313</td>
<td>8.0</td>
</tr>
<tr>
<td>$G_8$</td>
<td>6</td>
<td>21</td>
<td>31</td>
<td>30.9</td>
<td>674</td>
<td>27.7</td>
</tr>
<tr>
<td>$G_9$</td>
<td>18</td>
<td>22</td>
<td>178</td>
<td>5523</td>
<td>7473</td>
<td>2878</td>
</tr>
</tbody>
</table>

We conclude this section by listing the times for the computation of the class-10 quotient of $G_4$ with expanded relations in order to demonstrate the usefulness of using expression trees for storing the input relations.
Comparing this with the corresponding line in the first table we see that the overall runtime has drastically gone up while the amount of memory used and the time used on computing the row Hermite normal form has stayed the same. The increase in the overall runtime is due to the time that is spent in evaluating the expanded relations.

5.6 Some Applications

In this section we describe some problems to which the ANU NQ has been applied. In Newman and Nickel (1992) the ANU NQ is applied to the question whether a power of a right $n$-Engel element is a left $n$-Engel element.

5.6.1 Definition

Let $G$ be a group and $n$ be a positive integer. For elements $g, h \in G$ we define $[h, 1g] = [h, g]$ and $[h, (n+1)g] = [[h, ng], g]$. An element $g \in G$ satisfying $[g, nh] = 1$ for all $h \in G$ is called a right $n$-Engel element. The element $g \in G$ is called a left $n$-Engel element if $[h, ng] = 1$ for all $h \in G$.

The group $G$ is called an $n$-Engel group if for all $g, h \in G$ the commutator $[g, nh]$ is trivial.

The ANU NQ, Version 1.1c, allows a user to specify a positive integer $n$, in addition to a finite presentation for a group $G$ and an optional integer $c$. From this data it computes the largest $n$-Engel quotient group of $G$ of nilpotency class at most $c$. For this the following lemma is used.

5.6.2 Lemma

Let $H$ be a group of nilpotency class $c$ generated by elements $b_1, \ldots, b_d$, $d \in \mathbb{N}$. Then $G$ is an $n$-Engel group if and only if $[x, ny] = 1$ for all $x, y \in G$ such that $x$ and $y$ are words in $\{b_1, b_1^{-1}, \ldots, b_d, b_d^{-1}\}$ and the sum of their lengths is smaller than or equal to $c$.

Proof: This follows immediately from Lemma 3.5 in Higman (1959).

The ANU NQ has a subroutine that generates the set of words at each class that is needed to enforce the $n$-Engel condition and adds those words to the set of relations for $G$.  

<table>
<thead>
<tr>
<th>group</th>
<th>class</th>
<th>Hirsch</th>
<th>gens</th>
<th>time</th>
<th>space</th>
<th>Hermite</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_4$</td>
<td>10</td>
<td>23</td>
<td>111</td>
<td>4062</td>
<td>1087</td>
<td>108</td>
</tr>
</tbody>
</table>
The ANU NQ has been applied to the free 4-Engel group $E(2,4)$ generated by 2 elements and the free 5-Engel group $E(2,5)$ generated by two elements. It turned out that both groups have a largest nilpotent quotient $\tilde{E}(2,4)$ and $\tilde{E}(2,5)$, respectively.

The group $\tilde{E}(2,4)$ has nilpotency class 6 and Hirsch length 11. The factors of the lower central series are in descending order

$$C_2^2 \times C_\infty, C_\infty, C_\infty^2, C_\infty^3, C_2 \times C_\infty^2, C_\infty.$$

The following is a consistent weighted polycyclic presentation of $\tilde{E}(2,4)$. Trivial conjugate relations are left out and only positive conjugate relations are listed.

$$\langle A, B, C, D, E, F, G, H, I, J, K, L, M \mid J^4 = K^{-2}LM^{-1}, L^2 = M^{-1},$$

$$B^A = BC,$$

$$C^A = CD,$$

$$C^B = CE, F^B = FI^{-2}J^2KM^3,$$

$$D^A = DF,$$

$$D^B = DGI^{-3}J^3M^3, G^B = GJ,$$

$$D^C = DI^3J^2KM^{-3}, H^A = HK,$$

$$E^A = EG,$$

$$E^B = EH,$$

$$E^C = EJ^3K^3LM^2, K^A = KM,$$

$$E^D = ELM^2 \rangle$$

The computation took 35.6 seconds on a DECstation 5000/120 and needed 67 kilobytes of memory for storing the data.

For the group $\tilde{E}(2,5)$ only a preimage $G$ has been computed by only using (semigroup) words from Lemma 5.6.2 in the generators. The group $G$ has nilpotency class 9 and Hirsch length 23. The factors of the lower central series are

$$C_\infty^2, C_\infty, C_\infty^2, C_\infty^3, C_\infty^6, C_6 \times C_6 \times C_\infty, C_6^2 \times C_\infty^2 \times C_\infty^4, C_2 \times C_\infty^2 \times C_\infty, C_5^4 \times C_\infty^2.$$
This computation took 6 hours and 45 minutes on a DECstation 5000/120 and used 555 kilobytes of memory for storing the data. It has been verified that \( G/\gamma_8(G) \cong \overline{E}(2,5)/\gamma_8(\overline{E}(2,5)) \). Computing the class-7 quotient of \( \overline{E}(2,5) \) took 4 hours and 46 minutes on a DECstation 5000/120. It is estimated that the computation of \( \overline{E}(2,5) \) with the current version of the ANU NQ will take 120 hours of CPU time. The reason for the difficulty of this computation lies in the exponentially growing number of instances of the Engel condition that have to be enforced and the fact that collection becomes more time consuming as the class increases.

The following is a presentation for a subgroup \( U \) of index 24 of the group \( D_2 \) in Felsch et al. (1993)

\[
\langle a, b, c, d, e, f \mid ab^{-1}a^{-1}b^{-1}, \quad ada^{-1}d^{-1}, \quad bcb^{-1}c^{-1},
   \quad cdc^{-1}d^{-1}, \quad cfc^{-1}f^{-1}, \quad efe^{-1}f^{-1},
   \quad aea^{-1}be^{-1}b^{-1}, \quad ae^{-1}f^{-1}a^{-1}f e, \quad bf^{-1}df^{-1}b^{-1}d^{-1},
   \quad cec^{-1}de^{-1}d^{-1}, \quad aedf^{-1}a^{-1}f^{-1}d^{-1}e^{-1},
   \quad af^{-1}d^{-1}bf^{-1}b^{-1}d, \quad bdf c^{-1}e^{-1}f^{-1}d^{-1} \rangle.
\]

In Felsch et al. (1993) it is proved that \( U \) is a subgroup of the direct product \( H \) of four free groups of rank 2 such that \( U \) contains the derived subgroup of \( H \) and \( H/U \) is free abelian of rank two. Using the ANU NQ to compute the nilpotency class-7 quotient of \( U \) yields the following factors for the lower central series

\[
C_6^\infty, \quad C_4^4, \quad C_8^8, \quad C_\infty^{12}, \quad C_\infty^{24}, \quad C_\infty^{36}, \quad C_\infty^{72}
\]
in accordance with the theoretical result. The computation takes 308 seconds on a DECstation 5000/120 and uses 6 megabytes of memory to store the data.
In this chapter we are going to study the following situation. Let $F$ be a free group and $R$ and $S$ normal subgroups of $F$ such that $S$ is contained in $R$. Furthermore, let $\mathcal{N}$ be a set of normal subgroups of $F$ all of which contain $S$ and are contained in $R$. The problem here is the determination of the different isomorphism types of factor groups $F/N$ for $N \in \mathcal{N}$. Partly inspired by the ideas of the $p$-group generation algorithm (O'Brien, 1990) we will describe conditions that admit an action on $\mathcal{N}$ by a certain group of automorphisms. The orbits under this action correspond to the isomorphism types of factor groups $F/N$ for $N \in \mathcal{N}$.

6.1 Definition Let $G$ be a group with normal subgroups $M$ and $N$ and let $\varepsilon$ be an endomorphism of $G$ such that $M\varepsilon \subseteq N$. Then $(Mg)\varepsilon = N(g\varepsilon)$ defines a homomorphism $\overline{\varepsilon}$ from $G/M$ to $G/N$. The homomorphism $\overline{\varepsilon}$ is said to be induced by $\varepsilon$. Let $\beta$ be a homomorphism from $G/M$ to $G/N$. The endomorphism $\beta^*$ of $G$ is said to be a lifting of $\beta$ to $G$ if $M\beta^* \subseteq N$ and $\beta^*$ induces $\beta$.

Throughout this chapter let $F$ be a free group with a free generating set \{x_1, \ldots, x_n\} and let $M$ and $N$ be normal subgroups of $F$.

Let $\varphi$ be a homomorphism from $F/M$ to $F/N$ and \{y_1, \ldots, y_n\} a set of elements in $F$ such that $(Mx_i)\varphi = Ny_i$. Then $Mw(x_1, \ldots, x_n)$ is mapped by $\varphi$ to $Nw(y_1, \ldots, y_n)$. Setting $x_i\varphi^* = y_i$ defines an endomorphism $\varphi^*$ of $F$ and $\varphi^*$
maps \( w(x_1, \ldots, x_n) \) to \( w(y_1, \ldots, y_n) \). If \( w(x_1, \ldots, x_n) \) is an element of \( M \), then \( w(y_1, \ldots, y_n) \) is an element of \( N \):

\[
N = M \varphi = (Mw(x_1, \ldots, x_n))\varphi = Nw(y_1, \ldots, y_n).
\]

This means that \( M\varphi^* \subseteq N \) and \( \varphi^* \) is a lifting of \( \varphi \).

If \( S \) is a normal subgroup of \( F \) contained in \( M \cap N \) such that \( S\varphi^* \subseteq S \), then \( \varphi^* \) induces an endomorphism \( \overline{\varphi}^* \) on \( F/S \) via \((Sx_i)\overline{\varphi}^* = Sy_i\). Clearly, \( \overline{\varphi}^* \) maps \( M/S \) into \( N/S \).

Let \( \varphi \) be an isomorphism from \( F/M \) to \( F/N \). It is a natural question to ask if \( \varphi \) has a lifting to an automorphism of \( F/S \). The following theorem can be used to provide an answer to this question.

6.2 Theorem (Gaschütz 1955)

If \( N \) is a finite normal subgroup of a group \( G \) and \( G \) can be generated by \( n \) elements, then for each generating set \( \{Ng_1, \ldots, Ng_n\} \) of \( G/N \) there is a generating set \( \{h_1, \ldots, h_n\} \) of \( G \) such that \( h_i \in Ng_i \) for \( 1 \leq i \leq n \).

In order to be able to apply this theorem, it is assumed that \( N/S \) is finite and that \( \varphi \) is an isomorphism from \( F/M \) to \( F/N \) such that every lifting of \( \varphi \) to \( F \) leaves \( S \) invariant. The latter is the case if \( S \) is fully invariant, i.e., invariant under all endomorphisms of \( F \). However, we do not want to impose this stronger condition on \( S \). The images of \( Mx_i \) under \( \varphi \) for \( 1 \leq i \leq n \) generate \( F/N \) because \( \varphi \) is an isomorphism. By Gaschütz' theorem applied to \( G = F/S \), elements \( y_i \in (Mx_i)\varphi \) can be chosen such that such that \( \{Sy_1, \ldots, Sy_n\} \) is a generating set for \( F/S \). As before, \( x_i \mapsto y_i \) defines a lifting \( \varphi^* \) of \( \varphi \) to \( F \) which induces an endomorphism \( \overline{\varphi}^* \) of \( F/S \). By choice of the \( y_i \), this endomorphism is surjective. It is clear that \( \overline{\varphi}^* \) maps \( M/S \) to \( N/S \). In general, it seems to be difficult to state conditions under which \( \overline{\varphi}^* \) is injective. However, if the group in question is Hopfian then the surjectivity of \( \overline{\varphi}^* \) implies the injectivity. For the present purpose we will assume that the involved groups are Hopfian where necessary. We summarize the discussion so far in the following lemma.

6.3 Lemma Let \( F, M \) and \( N \) be as above and \( S \) a normal subgroup of \( F \) such that

75
- $S$ is contained in $M \cap N$,
- the quotient group $F/S$ is hopfian and
- $N/S$ is finite.

Then for any isomorphism $\varphi$ from $F/M$ to $F/N$ such that $S$ is invariant under any lifting of $\varphi$ to $F$ there is an automorphism of $F/S$ that induces $\varphi$ and that maps $M/S$ to $N/S$.

If we assume that $S$ is fully invariant we get the following corollary.

6.4 Corollary Let $S$ be a fully invariant subgroup of $F$ and such that $F/S$ is Hopfian. Then two finite normal subgroups of $F/S$ lie in the same characteristic class if and only if their corresponding quotient groups are isomorphic.

Proof: If two normal subgroups of a group are conjugate under an automorphism, this automorphism induces an isomorphism between their quotient groups. The converse is true by the previous lemma. ■

Now let $R$ be a normal subgroup of $F$ containing $MN$ and suppose that $S$ is invariant under all endomorphisms of $F$ that leave $R$ invariant. If $(R/M)\varphi = R/N$, then the lifting $\varphi^*$ to an endomorphism of $F$ leaves $R$ invariant. Under the conditions of the lemma, this endomorphism can be chosen such that it induces an automorphism $\overline{\varphi^*}$ of $F/S$. Clearly, $\overline{\varphi^*}$ leaves $R/S$ invariant and induces an automorphism on $F/R$ or, vice versa, $\overline{\varphi^*}$ is a lifting of an automorphism of $F/R$.

6.5 Theorem Let $R$ and $S$ be normal subgroups of $F$, $R$ containing $S$, such that every lifting of any automorphism of $F/R$ to an endomorphism of $F$ leaves $S$ invariant. Furthermore, assume that $F/S$ is Hopfian.

Let $N$ be a set of normal subgroups of $F$ satisfying the following conditions.

- Every $M \in N$ contains $S$ and is contained in $R$.
- For every $M \in N$ the quotient $M/S$ is finite.
- Every isomorphism from $F/M$ to $F/N$ for $M, N \in N$ maps $R/M$ into $R/N$.

Then for $M$ and $N$ in $N$ the quotient groups $F/M$ and $F/N$ are isomorphic if and only if there is an automorphism $\alpha$ of $F/R$ with a lifting to an automorphism $\alpha^*$ of $F/S$ such that $(M/S)\alpha^* = N/S$. 76
Proof: If \( F/M \) and \( F/N \) are isomorphic, then there is an isomorphism \( \varphi \) from \( F/M \) to \( F/N \). It induces an automorphism \( \alpha \) on \( F/R \), because \( (R/M)\varphi = R/N \). By the lemma above, \( \varphi \) has a lifting \( \varphi^* \) to an automorphism of \( F/S \) because \( F/S \) is Hopfian and \( N/S \) is finite. Clearly, \( \varphi^* \) induces \( \alpha \) on \( F/R \) and maps \( M/S \) to \( N/S \).

If there is an automorphism of \( F/R \) that lifts to an automorphism \( \alpha^* \) of \( F/S \) mapping \( M/S \) to \( N/S \), then \( \alpha^* \) induces an isomorphism from \( F/M \) to \( F/N \).

Note that the conditions of the theorem do not require \( R \) to be a characteristic subgroup of \( F/S \). In fact, this would be too restrictive for practical purposes. Also note, that the condition that, for all \( M, N \in \mathcal{N}, R/M \) is mapped to \( R/N \) under any isomorphism from \( F/M \) to \( F/N \) is a stronger condition than the condition that \( R/M \) is characteristic in \( F/M \) for all \( M \in \mathcal{N} \).

If \( \mathcal{N} \) is a union of characteristic classes, then the liftings of all automorphisms of \( F/R \) to \( F/S \) act on \( \mathcal{N} \). Two subgroups \( M \) and \( N \) are in the same orbit if and only if \( F/M \) and \( F/N \) are isomorphic. This means that we can classify quotient groups of \( F/S \) modulo subgroups in \( \mathcal{N} \) by determining the orbits of all liftings of automorphisms of \( F/R \). This fact was used, for example, in the \( p \)-group generation algorithm as follows:

6.6 Corollary Assume that \( F/R \) is a finite \( p \)-group. Take \( S \) to be \( [R,F]_{RP} \) and take \( \mathcal{N} \) to be the set of all subgroups of \( F \), contained in \( R \) and containing \( S \), such that for each \( M \in \mathcal{N} \) the subgroup \( R/M \) of \( F/M \) is the last non-trivial term in the lower \( p \)-central series of \( F/M \).

Then all automorphisms of \( F/R \) can be lifted to automorphisms of \( F/S \). Two subgroups \( M \) and \( N \) lie in the same orbit of \( \mathcal{N} \) under the action of all such liftings if and only if the quotient groups \( F/M \) and \( F/N \) are isomorphic.

A detailed description of the \( p \)-group generation algorithm can be found in O'Brien (1990). The elements of \( \mathcal{N} \) are precisely the so-called allowable subgroups in O'Brien (1990, p. 690).

Possible candidates that can function as the normal subgroup \( S \) are

- \( S = R^m[R,R] \) for any integer \( m \), if \( F/R \) is finite;
$S = R^m[R, F]$ for any integer $m$, if $R$ is the normal closure of a finite set;


In Chapter 7 we will use the situation in the second case in order to determine all Schur covering groups of a given finite polycyclic group.

Theorem 6.1 reduces the determination of the isomorphism types of the quotient groups $F/N$ for $N \in \mathcal{N}$ to the problem of lifting the elements of the automorphism group $A$ of $F/R$ to automorphisms of $F/S$. Two different liftings $\beta^*$ and $\beta^{**}$ of an automorphism give raise to a lifting $\beta^{**}(\beta^*)^{-1}$ of the identity of $F/R$. Therefore, if $A$ is given by a generating set, it is sufficient to determine one lifting for each element of the generating set and all liftings of the identity of $F/R$. These generate the set $A^*$ of all liftings of automorphisms of $F/R$ to $F/S$ as a group.

In order to determine the orbits of $A^*$ on $\mathcal{N}$ each automorphism of $A^*$ has to be restricted to $R/S$. If $F/S$ has the property that the restriction of a lifting of an automorphism $\alpha$ is independent of the lifting, then the restriction to $R/S$ of any lifting of the identity is the identity on $R/S$. In this case it is sufficient to find one lifting for each automorphism of the generating set of $A$ and take their restrictions to $R/S$. However, this cannot be expected to happen in general.
Chapter 7:
Schur multiplicator and Schur covers

This chapter is concerned with the computation of the Schur multiplicator of polycyclic groups and the determination of all Schur covers of a given finite polycyclic group up to isomorphism. The computation of the Schur multiplicator uses the techniques developed in Chapter 4. For the classification of Schur covers up to isomorphism a generalization of the approach used in p-group generation (O'Brien, 1990) will be used.

7.1 The Schur multiplicator

Let $F$ be a free group of finite rank $n$ and $R$ a normal subgroup of $F$. Denote $F/R$ by $G$. The subgroup $R/[R,F]$ is a central subgroup of $F/[R,F]$. If $R$ is generated as a normal subgroup by $m$ elements, then $R/[R,F]$ is, as a central subgroup of $F/[R,F]$, generated by at most $m$ elements. The factor group $F/[F,F]$ is a free abelian group of rank $n$. The subgroup $R[F,F]/[F,F]$ of $F/[F,F]$ is free abelian and isomorphic to $R/(R \cap [F,F])$. If the free rank of $F/R[F,F]$ is $r$, then $R[F,F]/[F,F]$, and hence $R/(R \cap [F,F])$, is free abelian of rank $n - r$.

The following definition follows Beyl and Tappe (1982, p. 30).

7.1.1 Definition The subgroup $R \cap [F,F]/[R,F]$ of $F/[R,F]$ is called the Schur multiplicator $M(G)$ of $G$. 

79
It can be shown that the Schur multiplicator is independent of $F$ and $R$ and depends only on the isomorphism type of $G$, i.e., it is a group invariant (Beyl & Tappe, 1982, p. 30). The finiteness of $G$ is not required for this result. Since $R/M(G)$ is free abelian, it follows that the torsion subgroup of $R/[R, F]$ is contained in $M(G)$. For finite groups we have the following lemma.

**7.1.2 Lemma** If $G$ is finite, then $M(G)$ is the torsion subgroup of $R/[R, F]$.

Proof: For a proof see Beyl and Tappe, p.97

The Schur multiplicator plays an important role in the literature. A wealth of material can be found in Karpilovski (1987, 1993) and Beyl and Tappe (1982).

In general it is difficult to compute the isomorphism type of $M(G)$ for given $G$. In recent years the Schur multiplicator has been computed for specific groups with the help of computers. Holt (1982) developed a program that computes $M(H)$ for a given permutation group $H$.

If $F/R$ is a polycyclic group given by a consistent polycyclic presentation, then the methods developed in Chapter 4 can be used to compute a consistent polycyclic presentation for $F/[R, F]$ and a presentation for $R/[R, F]$ as an abelian group. Then a presentation for $R/[R, F]$ in diagonal form can be computed from which the free rank of $R/[R, F]$ and the isomorphism type of the torsion subgroup of $R/[R, F]$ can be read off. The free rank of $M(G)$ is the difference of the free
rank of $R/[R, F]$ and the free rank of $R/M(G)$ which is, by the remarks at the beginning of this section, equal to $n - r$. For methods to compute the structure of $G/G'$ see Johnson (1990). A method for computing the Schur multiplicator of a $p$-group given by a polycyclic presentation is used in the routine NILPQUOT in Holt (1982).

7.2 Computing the Schur Multiplier for Polycyclic Groups

Let $(A, S)$ be a consistent polycyclic presentation and $A = ((X, \emptyset), (A, S), \sigma)$ a consistent quotient system. Chapter 4 explained the construction of the central covering system $A' = ((X, \emptyset), (A', S'), \sigma)$ of $A$. If $F$ is the free group on $X$ and $R$ the kernel of the surjective homomorphism (defined by) $\sigma$ from $F$ onto the group defined by $(A, S)$, then $A'$ represents $F/[R, F]$. Applying the consistency check to $A'$ results in a presentation for an abelian group on the generators $A' \backslash A$ which is isomorphic to $R/[R, F]$.

7.2.1 Example

We are going to compute the Schur multiplicator for the symmetric group on four letters. The following is a consistent polycyclic quotient system for it:

\begin{align*}
X &= \{a, b\}, \\
A &= (a, b, c, d), \\
S &= \{a^2 = c, \\
a^{-1}ba = b^2c, \quad &b^3 = 1, \\
a^{-1}ca = c, \quad &b^{-1}cb = d, \quad c^2 = 1, \\
a^{-1}da = cd, \quad &b^{-1}db = cd, \quad d^e = d, \quad d^2 = 1\}.
\end{align*}

The following is the universal central extension of the quotient system above:

\begin{align*}
X &= \{a, b\}, \\
A' &= (a, b, c, d, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8),
\end{align*}

81
\[ S' = \{ \quad a^2 = c, \]
\[ a^{-1}ba = b^2cx_4, \quad b^3 = x_1, \]
\[ a^{-1}ca = cx_5, \quad b^{-1}cb = d, \quad c^2 = x_2, \]
\[ a^{-1}da = cdx_6, \quad b^{-1}db = cdx_7, \quad d^c = dx_8, \quad d^2 = x_3, \]
\[ x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 \text{ central } \}.

Applying the consistency check to the above system gives the following relations for the generators \( x_1, \ldots, x_8 \):

\[
\begin{align*}
x_1 &= x_4^{-3}x_7^3x_8, \quad x_2 = x_7^{-2}x_8, \\
x_3 &= x_7^{-2}x_8, \quad x_5 = 1, \\
x_6 &= x_7x_8, \quad x_8^2 = 1.
\end{align*}
\]

From these relations we see that the abelian group generated by \( x_1, \ldots, x_8 \) as subgroup of the group defined by \((A', S')\) is isomorphic to \( C_\infty \times C_2 \). Since the symmetric group on four letters is finite, the Schur multiplicator is isomorphic to \( C_2 \), the torsion subgroup of \( C_\infty \times C_2 \).

### 7.2.2 Example

A second example is the computation of the Schur multiplicator of the infinite dihedral group given by the polycyclic presentation

\[ X = \{a, b\}, \]
\[ A = (a, b), \]
\[ S = \{a^2 = 1, \quad a^{-1}ba = b^{-1}\}. \]

Forming the universal central extension of this quotient system gives:

\[ X = \{a, b\}, \]
\[ A = (a, b, x_1, x_2), \]
\[ S = \{ \quad a^2 = x_1, \]
\[ a^{-1}ba = b^{-1}x_2, \]
\[ a^{-1}x_1a = x_1, \quad b^{-1}x_1b = x_1, \]
\[ a^{-1}x_2a = x_2, \quad b^{-1}x_2b = x_2 \}. \]
There is only one consistency check to perform which results in a trivial relation:

\[ bx_1 = ba^2 = ab^{-1}x_2 a = a^2bx_2^{-1}x_2 = x_1b = bx_1. \]

This means that the abelian subgroup generated by \( x_1 \) and \( x_2 \) is free abelian of rank 2. The largest abelian quotient of the infinite dihedral group is isomorphic to \( C_2 \times C_2 \). Thus we get that the free rank of the Schur multiplicator is \( 2 - (n - r) = 2 - 2 = 0 \) and that the Schur multiplicator of the infinite dihedral group is trivial.

7.2.3 Example As a third example we are going to compute the Schur multiplicator of a finite metacyclic group. The following is a consistent quotient system for a metacyclic group with a cyclic normal subgroup of order \( n \) and cyclic quotient group of order \( m \) as can be checked by the consistency test.

\[
X = \{a, b\},
\]
\[
A = (a, b),
\]
\[
S = \{a^m = b^s, \quad a^{-1}ba = b^r, \quad b^n = 1\}
\]
where \( n|s(r - 1) \) and \( n|(r^m - 1) \).

We form the central extension of this quotient system

\[
X = \{a, b\},
\]
\[
A = (a, b, x_1, x_2, x_3),
\]
\[
S = \{a^m = b^s x_1, \quad a^{-1}ba = b^r x_2, \quad b^n = x_3\}
\]
\[
a^{-1}x_1 a = x_1, \quad b^{-1} x_1 b = x_1,
\]
\[
a^{-1}x_2 a = x_2, \quad b^{-1} x_2 b = x_2,
\]
\[
a^{-1}x_3 a = x_3, \quad b^{-1} x_3 b = x_3\}
\]

and perform the consistency test

\[ a^m a = b^s x_1 a = a(b^s x_2)^s x_1 = ab^r x_1 x_2^s = ab^r x_1 x_2^s x_3^{(r - 1)/n} \]
\[
\begin{align*}
aa^m &= ab^s x_1 \\
b^n b &= x_3 b = bx_3 \\
bb^n &= bx_3 \\
b^n a &= x_3 a = ax_3 \\
b^{n-1}(ba) &= a(b^r x_2)^n = a(b^n)^r x_2^n = ax_3^n x_3^r \\
b a^m &= b^{s+1} x_1 \\
(ba)a^{m-1} &= ab^r x_2 a^{m-1} = a^2 b^{r^2} x_2^{1+r} a^{m-2} = \ldots \\
&= a^m b^{r^m} x_2^M = b^{s+1} b^{m-1} x_1 x_2^M = b^{s+1} x_1 x_2^M x_3^N \\
\text{where } M &= \frac{(r^m - 1)}{(r - 1)} \text{ and } N = \frac{(r^m - 1)}{n}.
\end{align*}
\]

We get the following three relations on the generators \(x_1, x_2, x_3\):

\[
\begin{align*}
x_2^s x_3^{(r-1)/n}, & \quad x_2^n x_3^{-1}, & \quad x_2^M x_3^N.
\end{align*}
\]

It is easy to see that these relations define a cyclic group of order

\[
\gcd(r - 1, s, n, \frac{r^m - 1}{r - 1}, \frac{r^m - 1}{n}, \frac{s(r - 1)}{n}).
\]

This result was proved by Wamsley (1970) and Beyl (1973). Wamsley's proof relies on a free \(\mathbb{Z}\)-resolution for the metacyclic group while Beyl's proof uses spectral sequences.

The previous example demonstrates that it is possible to compute the Schur multiplicator for families of polycyclic groups given by a consistent polycyclic presentation that contains parameters. For instance, with this method it is also possible to determine the structure of the Schur multiplicator of all 2-generator \(p\)-groups of nilpotency class 2 for each prime \(p\).

If \(G\) is a 2-generator \(p\)-group of nilpotency class 2, it is easy to prove that there are positive integers \(\delta, \varepsilon, \lambda, \mu, \nu\) with \(\nu \leq \mu \leq \lambda\) and \(\delta, \varepsilon \leq \nu\) such that \(G\)
has the following consistent polycyclic presentation

\[(a, b, c \mid a^{p^\lambda} = c^{p^\delta}, \quad b^a = bc, \quad b^{p^\mu} = c^{p^\epsilon}, \quad c^a = c, \quad c^b = c, \quad c^{p^\nu}).\]

Applying the algorithm to this presentation yields the integer matrix

\[
\begin{bmatrix}
\frac{1}{2}p^\lambda(p^\lambda - 1) & p^\delta & p^{\lambda - \nu} \\
p^{-\epsilon} & \frac{1}{2}p^\mu(p^\mu - 1) & p^{\mu - \nu} \\
p^\delta & 0 & 0 \\
0 & p^\epsilon & 0
\end{bmatrix}.
\]

In computing the diagonal form of this matrix the following six cases for the structure of the Schur multiplicator \(M(G)\) of \(G\) arise.

If \(p > 2\) or if \(p = 2\), \(\delta \neq \lambda\) and \(\epsilon \neq \mu\), then there are three cases;

- if \(\epsilon \geq \delta\): \(M(G) \cong C_{p^\delta} \times C_{p^\delta} \times C_{p^{\mu - \nu}}\),
- if \(\epsilon \leq \delta\), \(\epsilon \leq \mu - \nu\): \(M(G) \cong C_{p^\epsilon} \times C_{p^\epsilon} \times C_{p^\omega}\),
  \(\text{where } \omega = \min(\lambda - \nu, \mu - \nu + \delta - \epsilon)\),
- if \(\epsilon \leq \delta\), \(\epsilon \geq \mu - \nu\): \(M(G) \cong C_{p^\epsilon} \times C_{p^{\mu - \nu}} \times C_{p^\omega}\),
  \(\text{where } \omega = \min(\delta, \epsilon + \lambda - \mu)\).

If \(p = 2\) and \(\delta = \lambda\) or \(\epsilon = \mu\), there are three further cases;

- if \(\delta = \lambda, \epsilon = \lambda\): \(M(G) \cong C_{2^{\epsilon - 1}} \times C_{2^\epsilon}\),
- if \(\delta = \lambda, \epsilon < \lambda\): \(M(G) \cong C_{2^\epsilon} \times C_{2^\epsilon}\),
- if \(\delta < \lambda, \mu = \epsilon\): \(M(G) \cong C_{2^\delta} \times C_{2^\delta}\).

A consequence of this result is that every abelian \(p\)-group that can be generated by at most three elements occurs as the Schur multiplicator of a 2-generator \(p\)-group of nilpotency class 2.

7.3 An implementation

The algorithm for the computation of the Schur multiplicator has been implemented as a program in the programming language C. The program takes a
polycyclic presentation for a finite polycyclic group $G$ and outputs the isomorphism type of $M(G)$.

The program was used to compute the Schur multiplicators for some exceptional soluble doubly transitive groups and for some maximal soluble subgroups of sporadic simple groups. All times are taken on a DECstation 5000/120.

The following list shows the Schur multiplicators for the three soluble doubly transitive groups in Huppert and Blackburn (1982, p. 385). The third column gives the number of new (central) generators that were defined in order to form the central covering system in each case. The fourth column lists the times that each computation takes.

<table>
<thead>
<tr>
<th>order</th>
<th>$M(G)$</th>
<th>central generators</th>
<th>time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^7 \cdot 3^4 \cdot 5$</td>
<td>1</td>
<td>66</td>
<td>8.4</td>
</tr>
<tr>
<td>$2^5 \cdot 3^4 \cdot 5$</td>
<td>$C_2 \times C_3$</td>
<td>55</td>
<td>4.5</td>
</tr>
<tr>
<td>$2^6 \cdot 3^4 \cdot 5$</td>
<td>$C_2 \times C_3$</td>
<td>66</td>
<td>8.0</td>
</tr>
</tbody>
</table>

The following list shows the Schur multiplicators for four soluble maximal subgroups in the sporadic simple groups $Co_2$, $Co_3$, $Fi_{22}$ and $Fi_{23}$, respectively.

<table>
<thead>
<tr>
<th>order</th>
<th>$M(G)$</th>
<th>central generators</th>
<th>time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^5 \cdot 3^5$</td>
<td>1</td>
<td>45</td>
<td>4.5</td>
</tr>
<tr>
<td>$2^{10} \cdot 3^3$</td>
<td>$C_2 \times C_2$</td>
<td>91</td>
<td>26.7</td>
</tr>
<tr>
<td>$2^8 \cdot 3^9$</td>
<td>$C_6 \times C_3$</td>
<td>153</td>
<td>130.8</td>
</tr>
<tr>
<td>$2^{11} \cdot 3^{13}$</td>
<td>1</td>
<td>300</td>
<td>2334.8</td>
</tr>
</tbody>
</table>

7.4 Schur covering groups

Now we will consider Schur covers of finite polycyclic groups and devise a method to classify the isomorphism types of Schur covers of a given finite polycyclic group.

7.4.1 Definition Let $F$ be a free group and $R$ a normal subgroup of $F$. A group $E$ with a normal subgroup $M$ such that

- $M \cong M(F/R)$,
- $M \leq Z(E) \cap [E,E]$ and
- $E/M \cong F/R$, 

86
is called a Schur covering group of $F/R$ or, short, a Schur cover of $F/R$.

We continue to denote $F/R$ by $G$. The existence of Schur covers is assured by the following theorem.

7.4.2 Theorem

a) $M(G)$ is complemented in $R/[R,F]$.

b) If $C \leq F$ such that $C \geq [R,F]$ and $C/[R,F]$ is a complement for $M(G)$ in $R/[R,F]$, then $F/C$ is a Schur cover for $G$.

c) If $E$ is a Schur cover for $F/R$, then there is a subgroup $[R,F] \leq C \leq F$ such that $E \cong F/C$ and $C/[R,F]$ is a complement for $M(G)$ in $R/[R,F]$.

Proof:

a) Clear because $R/M(G)$ is free abelian.

b) It is clear that $R/C \leq Z(F/C)$. This and the following computation show that $R/C \leq [F/C,F/C] \cap Z(F/C)$;

$$R/C = C(R \cap [F,F])/C \leq C[F,F]/C = [F/C,F/C].$$

Now the observation that $(F/C)/(R/C) \cong F/R$ completes the proof of part b).

c) Let $E$ be a Schur cover of $G$ and $M \leq Z(E) \cap [E,E]$ with $M \cong M(G)$. Furthermore, let $\tau$ be a projection from $E$ onto $G$ with $\ker \tau = M$.

Let $\{x_1, \ldots, x_n\}$ be a free generating set for $F$ and choose $e_i \in E$ such that $e_i \tau = Rx_i$ for $1 \leq i \leq n$. The set $\{e_1, \ldots, e_n\}$ generates $E$ because $M$ is a subgroup of $\Phi(E)$ by Theorem 1.2.2. Therefore, $x_i \sigma = e_i$ defines a surjective homomorphism from $F$ onto $E$. We will prove that $C = \ker \sigma$ satisfies the claim.

Now $x_i \sigma \tau = e_i \tau = Rx_i$ and $\ker \tau = M$ show that $R \sigma = M$ and $R = M \sigma^{-1}$. The subgroup $[R,F]$ is contained in $\ker \sigma$, as the equation $[R,F] \sigma = [R \sigma,F \sigma] = [M,E] = 1$ shows. The subgroup $M$ of $E$ is the image of $([F,F] \cap R)$ under $\sigma$ because $([F,F] \cap R) \sigma = [E,E] \cap M = M$. This implies, since $M$ is isomorphic to $M(G)$ and hopfian by Theorem 2.1.3, that $\ker \sigma \cap ([F,F] \cap R) = [R,F]$. We also see that $R = (\ker \sigma)([F,F] \cap R)$. This completes the proof.
7.4.3 Example  

In Example 7.2.1 the subgroup generated by \( x_4 \) and \( x_7 \) is a complement to the Schur multiplicator which is generated by \( x_8 \). Forming the factor group modulo the (normal) subgroup generated by \( x_4 \) and \( x_7 \) and using the relations that came out of the consistency check gives the following consistent polycyclic presentation for a Schur cover of the symmetric group on 4 letters.

\[
X = \{a, b\},
\]

\[
A = (a, b, c, d, x_8),
\]

\[
S = \{a^2 = c,
\]

\[
a^{-1}ba = b^2c,
\]

\[
b^3 = x_8,
\]

\[
a^{-1}ca = c,
\]

\[
(a^{-1}cb = d),
\]

\[
c^2 = x_8,
\]

\[
a^{-1}da = cdx_8,
\]

\[
b^{-1}db = cd,
\]

\[
c^{-1}dc = dx_8,
\]

\[
d^2 = x_8,
\]

\[
a^{-1}x_8a = x_8,
\]

\[
b^{-1}x_8b = x_8,
\]

\[
c^{-1}x_8c = x_8,
\]

\[
d^{-1}x_8d = x_8, \quad x_8^2 \}.
\]

It is possible that two different complements \( C_1, C_2 \) for the Schur multiplicator in \( R/[R, F] \) yield Schur covers \( F/C_1 \) and \( F/C_2 \) that are isomorphic to each other. For finite \( F/R \) we will describe an action of a group on the set of complements of \( M(G) \) such that the isomorphism classes of Schur covers correspond
to the orbits under this action. This approach was successfully used in the p-group generation algorithm (O'Brien, 1990). The following was partly inspired by Proposition 4.2 in Beyl and Tappe (1982) which describes certain equivalence classes of stem extensions. From now on, we assume that all groups are finite.

Let $C$ be the set of subgroups of $F$ containing $[R, F]$ that are complements modulo $[R, F]$ for the Schur multiplier of $F/R$ in $R/[R, F]$ and let $D$ be the intersection of these complements.

7.4.4 Lemma If $m$ is the exponent of $M(G)$, then $D = [R, F]R^m$.

Proof: Let $C ∈ C$. Then $R/C ≅ M(G)$ and therefore $R^m ≤ C$. It follows that $C ≥ [R, F]R^m$ and $D ≥ [R, F]R^m$.

Now let $\{a_1, \ldots, a_n\}$ be a basis for a complement of $M(G)$ and let $d$ be an element of $D/[R, F]$. It is possible to write $d$ as a product $a_1^{x_1} \ldots a_n^{x_n} b$ with $x_i ∈ Z$ and $b ∈ M(G)$. Because $d$ is an element of the subgroup generated by $\{a_1, \ldots, a_n\}$, it follows that $b$ is trivial.

For any $1 ≤ i ≤ n$ and $e ∈ M(G)$ the set $\{a_1, \ldots, a_i e, \ldots, a_n\}$ is a basis for a complement and $d$ can be written as $a_1^{y_1} \ldots (a_i e)^{y_i} \ldots a_n^{y_n}$. Comparing exponents yields $y_j = x_j$ for $1 ≤ j ≤ n$ and $e^{y_i} = 1$.

It follows from the latter that $m | y_i$ for all $1 ≤ i ≤ n$ and hence $d ∈ [R, F]R^m/[R, F]$. ■

Let $Z$ be the complete preimage in $F$ of the centre of $F/[R, F]$.

7.4.5 Lemma

a) $Z/R ≤ Z(F/R)$.

b) $Z/C = Z(F/C)$ for all $C ∈ C$.

c) $Z/D = Z(F/D)$.

d) $[S, F] = [R, F]$ for all $R ≤ S ≤ Z$.

Proof:

a) $R$ is a subgroup of $Z$ and therefore $Z/R ≤ Z(F/R)$.

b) Now let $zC ∈ Z(F/C)$. Then $[z, g] ∈ C$ for all $g ∈ F$. Since $Z(F/C)$ is finite, there is a positive integer $e$ such that $z^e ∈ C$. Now, by Lemma 2.3.1

a), $[z^2, g] = [z, g][z, g, z][z, g]$ and $[z, g, z] ∈ [C, F] ≤ [R, F]$. It follows by induction that

$[z, g]^e[R, F] = [z^e, g][R, F] = [R, F]$. 

89
Therefore, \([z,g][R,F] \in \text{Tor}(R/[R,F])\) and \([z,g] \in C \cap (R \cap [R,F]) = [R,F].\) Hence \(z[R,F] \in Z(F/[R,F]).\)

c) The crucial step of the proof of b) is that \(C \cap (R \cap [R,F])\) is equal to \([R,F].\) Replacing \(C\) by \(D\) (or, in fact, any other subgroup of \(F\) containing \([R,F]\) and intersecting \(R \cap [R,F]\) in \([R,F]\)) gives a proof of c).

d) It has to be shown that \([S,F] \subseteq [R,F].\) It is clear that \([S,F] \leq C\) since \(S/C \leq Z(F/C).\) This and \([S,F] \leq [F,F]\) implies \([S,F] \leq C \cap [F,F] = [R,F].\)

\(\blacksquare\)

Define \(Z^* = Z \cap R[F,F].\) The Schur multiplicator of \(F/Z^*\) is

\[
(Z^* \cap [F,F])/[Z^*,F] = (Z^* \cap [F,F])/[R,F]
\]

by part d) of the previous lemma.

\[7.4.6 \text{ Lemma}\]

Let \(C \in C.\) Then \(C/[R,F]\) is a complement of \(M(F/Z^*)\) in \(Z^*/[R,F].\)
Proof:

\[ C \cap (Z^* \cap [F,F]) = (C \cap Z^*) \cap [F,F] \]
\[ \subseteq C \cap [F,F] = [R,F] \]
\[ C(Z^* \cap [F,F]) = C(R \cap [F,F])(Z^* \cap [F,F]) \]
\[ = R(Z^* \cap [F,F]) \]
\[ = RZ^* \cap R[F,F] = Z^* \]

Let \( C^* \) be the set of subgroups of \( F \) containing \([R,F]\) which, modulo \([R,F]\), are complements for the Schur multiplicator of \( F/Z^* \) in \( Z^*/[R,F] \) and let \( D^* \) be the intersection of these complements. Lemma 7.4.6 shows that \( C \subseteq C^* \) and hence \( D^* \subseteq D \). Let \( m^* \) be the exponent of \( M(F/Z^*) \). By Lemma 7.4.4 we have that \( D^* = (Z^*)^{m^*}[R,F] \). If \( m = m^* \), then \( D = R^m[R,F] \subseteq (Z^*)^m[R,F] = D^* \) and \( D = D^* \).

7.4.7 Theorem Let \( C_1, C_2 \in C^* \) and let \( \varphi : F/C_1 \longrightarrow F/C_2 \) an isomorphism. Then there is an automorphism \( \alpha \) of \( F/D^* \) such that \( C_1 \alpha = C_2 \).
Proof: The group \( F/D^* \) is finite and \( C_1 \cap C_2 \supseteq D^* \). Any isomorphism \( \varphi \) from \( F/C_1 \) to \( F/C_2 \) maps the center of \( F/C_1 \) to the center of \( F/C_2 \). Therefore, any lifting of \( \varphi \) to \( F \) leaves \( Z^* \) invariant and also \( D^* = (Z^*)^{m^*}[Z^*,F] \). The theorem now follows from Lemma 6.3.
7.4.8 Theorem Let $A$ be the set of all liftings of automorphisms of $F/Z^*$ to $F/D^*$. Then $A$ acts on $C^*$. Two complements $C_1$ and $C_2$ in $C^*$ lie in the same orbit under this action if and only if the quotient group $F/C_1$ is isomorphic to $F/C_2$.

Proof: Let $\alpha$ be an automorphism of $F/Z^*$. Any lifting of $\alpha$ to an endomorphism of $F$ maps $Z^*$ and therefore $Z^* \cap [F,F]$ and $D^* = (Z^*)^m[R,F]$ into itself. That implies that any lifting $\alpha^*$ of $\alpha$ to an automorphism of $F/D^*$ normalizes $D^*(Z^* \cap [F,F])/D^*$ and maps a complement of $D^*(Z^* \cap [F,F])/D^*$ to a complement. This shows that $A$ acts on $C^*$. Now the theorem follows from Theorem 6.5.

If $R$ is properly contained in $Z^*$ then the isomorphism types of Schur covers of $F/R$ correspond to those orbits which contain a complement that is contained in $R$.

7.5 An extended example

In this section the isomorphism classes of Schur covers of the direct product $G$ of the alternating group $A_4$ on four letters with a copy of itself will be determined.

The following is a consistent polycyclic quotient system for $G$:

$$X = \{a, b, d, e\},$$
$$A = (a, b, c, d, e, f),$$
$$S = \{a^3, b^a = c, b^2, c^a = bc, c^b = c, c^2, d^a = d, d^b = d, d^c = d, d^3, e^a = e, e^b = e, e^c = e, e^d = f, e^2, f^a = f, f^b = f, f^c = f, f^d = ef, f^e = f, f^2 \}$$

The automorphism group of $A_4$ is isomorphic to the symmetric group $S_4$ on four letters. The map $a \mapsto (123), b \mapsto (12)(34), c \mapsto (14)(23)$ is an embedding into $S_4$. A generating set for $S_4$ is $\{(123), (34)\}$. The automorphisms of $A_4$ induced by these permutations are:
The automorphisms of $G$ in terms of the second polycyclic presentation are:

$$
\begin{align*}
\alpha : u & \mapsto u \\
v & \mapsto v \\
w & \mapsto y \\
x & \mapsto xy \\
y & \mapsto wy \\
z & \mapsto wyz
\end{align*}
\begin{align*}
\beta : u & \mapsto u^2v^2wz \\
v & \mapsto v \\
x & \mapsto wx \\
y & \mapsto wy \\
z & \mapsto wxyz
\end{align*}
\begin{align*}
\gamma : u & \mapsto u \\
v & \mapsto uv^2wxyz \\
w & \mapsto wz \\
x & \mapsto x \\
y & \mapsto z \\
z & \mapsto xz
\end{align*}

Now we compute the universal central extension of the quotient system above:

$$
X = \{u,v\},
$$

$$
A' = (u,v,w,x,y,z,t_1,\ldots,t_{17}),
$$

$$
S' = \{ u^3 =: t_1, \\
v^u =: vx, \quad v^3 =: w, \\
w^u =: y, \quad w^v =: wt_6, \quad w^2 =: t_2, \\
x^u =: z, \quad x^v =: yzt_7, \quad x^w =: xt_8, \\
y^u =: wyt_9, \quad y^v =: yt_{10}, \quad y^w =: yt_{11}, \\
z^u =: xzt_{13}, \quad z^v =: wxyzt_{14}, \quad z^w =: zt_{15}, \\
z^2 =: t_3, \\
y^z =: yt_{12}, \quad y^2 =: t_4, \\
z^z =: zt_{16}, \quad z^y =: zt_{17}, \quad z^2 =: t_5 \}
$$

The consistency check gives the following relation matrix in row Hermite normal
The automorphisms of $G$ in terms of the second polycyclic presentation are:

\[
\begin{align*}
\alpha : u & \mapsto u \\
v & \mapsto vwy \\
w & \mapsto y \\
x & \mapsto xy \\
y & \mapsto wy \\
z & \mapsto wyz \\
\beta : u & \mapsto u^2v^2wx \\
v & \mapsto v \\
x & \mapsto wx \\
w & \mapsto wz \\
y & \mapsto wy \\
z & \mapsto wxyz \\
\gamma : u & \mapsto u \\
v & \mapsto uv^2wxyz \\
w & \mapsto wz \\
x & \mapsto x \\
y & \mapsto z \\
z & \mapsto z \\
\end{align*}
\]

Now we compute the universal central extension of the quotient system above:

\[X = \{u, v\},\]
\[A' = (u, v, w, x, y, z, t_1, \ldots, t_{17}),\]
\[S' = \{ u^3 =: t_1, \]
\[v^u =: vx, \quad v^3 =: w, \]
\[w^u =: y, \quad w^v =: wt_6, \quad w^2 =: t_2, \]
\[x^u =: z, \quad x^v =: yzt_7, \quad x^w =: xt_8, \]
\[y^u =: wyt_9, \quad y^v =: yt_{10}, \quad y^w =: yt_{11}, \]
\[z^u =: xzt_{13}, \quad z^v =: wxyzt_{14}, \quad z^w =: zt_{15}, \]
\[x^2 =: t_3, \]
\[y^x =: yt_{12}, \quad y^2 =: t_4, \]
\[z^x =: zt_{16}, \quad z^y =: zt_{17}, \quad z^2 =: t_5 \}\]

The consistency check gives the following relation matrix in row Hermite normal

94
form (with columns 9 and 14 swapped):

\[
\begin{array}{cccccccccccccccc}
t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 & t_{14} & t_{10} & t_{11} & t_{12} & t_{13} & t_9 & t_{15} & t_{16} & t_{17} \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & -1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]

The elementary divisors of the corresponding Smith normal form are 2 and 6. There are, as expected, two free generators: \( t_1 \) and \( t_9 \). The torsion subgroup is generated by \( t_{13} \) and \( t_{17} \) which are of order 6 and 2, respectively. Since the Schur multiplicator has exponent 6, two relations are added to the polycyclic presentation in order to make the two generators \( t_1 \) and \( t_9 \) elements of order 6. Applying the relations to the polycyclic presentation above gives the following consistent polycyclic presentation:

\[
X = \{u, v\},
\]

\[
A' = (u, v, w, x, y, z, t_1, t_9, t_{13}, t_{17}),
\]

\[
S' = \{u^3 = t_1, v^u = vx, v^3 = w, w^u = y, w^v = xzt_9, x^u = z, x^v = yzt_9, y^u = wyt_9, y^v = yt_{17}, y^w = yt_{17}, z^u = xzt_{13}, z^v = wxyzt_{13}^2t_9^2t_{17}, z^w = z, x^2 = t_{13}, y^x = y^2 = t_9^{-2}t_{17} - t_{17}, z^x = z^2 = t_{13}, t_1^6, t_9^6, t_{13}^6, t_{17}^2\}
\]
Now the automorphisms of $G$ have to be lifted to the central cover.

$\alpha : u \mapsto ut_9^2t_{13}$  
$\beta : u \mapsto u^2v^2wxt_9t_{13}^5t_{17}$  
$\gamma : u \mapsto ut_9^3t_{13}$  
$v \mapsto vwyt_{13}$  
$w \mapsto yt_9^3t_{17}$  
$x \mapsto xyt_9t_{17}$  
$y \mapsto wyt_9t_{13}^2$  
$z \mapsto wyzt_9^2$  
$t_1 \mapsto t_1t_9^3t_{13}$  
$t_9 \mapsto t_9t_{13}^3t_{17}$  
$t_{13} \mapsto t_{13}$  
$t_{17} \mapsto t_{17}$

The action of each lifting on the subgroup generated by \( \{t_1, t_9, t_{13}, t_{17}\} \) is written down in matrix form with respect to this generating system:

\[
\alpha : \begin{bmatrix}
1 & 3 & 3 \\
1 & 3 & 1 \\
1 & 1 & 1
\end{bmatrix} \quad \beta : \begin{bmatrix}
2 & 4 & 0 & 0 \\
1 & 3 & 5 \\
5 & 1 & 1
\end{bmatrix} \quad \gamma : \begin{bmatrix}
1 & 3 & 3 & 0 \\
5 & 2 & 3 & 1 \\
5 & 3 & 1
\end{bmatrix}
\]

It is clear that the lifting of beta is the only one not defining an automorphism.
Therefore, we use an "Ansatz" to find a lifting for $\beta$ which is an automorphism.

\[
\begin{align*}
    u &\mapsto u^2 v^2 w x t_9 t_1^5 t_3^6 t_5^4 t_1^3 t_2^2 t_3 t_4^4 b_4 \\
v &\mapsto v t_9^4 t_1^4 t_2^2 t_3^6 t_4^4 b_6 t_8^7 b_8 \\
w &\mapsto w t_3^4 t_1 t_7^2 (3b_6)^4 (3b_7)^5 t_2^4 t_4^4 b_8 \\
x &\mapsto [v, u] \mapsto w x t_9 t_3^2 t_1 v t_1^3 t_2^2 (3b_6)^4 (3b_7)^5 t_5^4 t_4^4 b_8 \\
y &\mapsto w u t_4^4 t_1^3 (3b_5) t_2^2 (3b_6)^4 (3b_7)^5 t_4^4 b_8 \\
z &\mapsto x u \mapsto x t_4^2 t_1 v t_1^3 t_2^2 (3b_6)^4 (3b_7)^5 t_4^4 b_8 \\
t_1 &\mapsto u v^3 t_4^4 t_1^3 t_2^4 (3b_5) t_2^2 (3b_6)^4 (3b_7)^5 t_4^4 b_8 \\
t_9 &\mapsto y^{-1} w^{-1} y u t_1^3 t_2^2 (3b_5) t_2^2 (3b_6)^4 (3b_7)^5 t_4^4 b_8 \\
t_{13} &\mapsto x^{-1} z u t_5^3 t_1^3 t_2^2 (3b_5) t_2^2 (3b_6)^4 (3b_7)^5 t_4^4 b_8 \\
t_{17} &\mapsto [z, y] \mapsto t_{17}
\end{align*}
\]

This yields the following matrix for $\beta$:

\[
\begin{bmatrix}
2 + 3b_5 & 4 + 3b_6 & 3b_7 & b_8 \\
-3b_5 & 1 - 3b_6 & 3 - 3b_7 & -3b_8 \\
5 & 1
\end{bmatrix}
\]

Choosing $b_5 = 1$ and $b_6 = b_7 = b_8 = 0$ gives the following matrix:

\[
\begin{bmatrix}
5 & 4 \\
-3 & 1 & 3 \\
5 & 1
\end{bmatrix}
\]

Clearly, this lifting of $\beta$ is an isomorphism.

Now we are going to lift the identity. For this we only have to consider homomorphisms from the commutator quotient into the subgroup generated by $\{t_1, t_9, t_{13}, t_{17}\}$. The commutator quotient is generated by the cosets of $u$ and $v$ and it holds that $t_1 = u^3$ and $t_9^{-1} = v^3$ modulo the commutator subgroup. We use the following "Ansatz":

\[
\begin{align*}
    u &\mapsto u t_1^{a_1} t_9^{a_2} t_{13}^{a_3} t_{17}^{a_4} \\
v &\mapsto v t_1^{b_1} t_9^{b_2} t_{13}^{b_3} t_{17}^{b_4}
\end{align*}
\]
Then
\[ t_1 \mapsto t_1^{(3a_1+1)}, t_9^{(3a_2)}, t_{13}^{(3a_3)}, t_{17}^{(3a_4)} \]
\[ t_9 \mapsto t_1^{(-3b_1)}, t_9^{(-3b_2+1)}, t_{13}^{(-3b_3)}, t_{17}^{(-3b_4)} \]
\[ t_{13} \mapsto t_{13} \]
\[ t_{17} \mapsto t_{17} \]

The corresponding matrix is:
\[
\begin{bmatrix}
1 + 3a_1 & 3a_2 & 3a_3 & a_4 \\
-3b_1 & 1 - 3b_2 & -3b_3 & b_4 \\
1 & 1 & 1 & 1
\end{bmatrix}
\]

Using all those automorphisms to calculate the orbits on the complements it turns out that there are three orbits for which we list representatives:
\[ \langle t_1, t_9 \rangle, \langle t_1 t_{13}, t_9 \rangle, \langle t_1 t_{13}, t_9 t_{13} \rangle \]

The difference between these three groups can be explained in terms of their Sylow 3-groups. All three are semidirect products of a non-abelian group of order 27 and a non-abelian group of order 64. The isomorphism class of the Sylow 2-group is the same in all three cases. The Sylow 3-group has exponent 3 in the first case and exponent 9 in the two other cases. The two last cases differ in the following way. Modulo the 2-component of the Schur multiplicator both groups have elementary abelian minimal normal subgroups of order 4. Their respective centralizers are cyclic of order 9 and elementary abelian in one case and both cyclic of order 9 in the other case.


100


Gregory Karpilovsky (1993), *Group Representations, Volume 2*, North-Holland Mathematics Studies, **177**.


