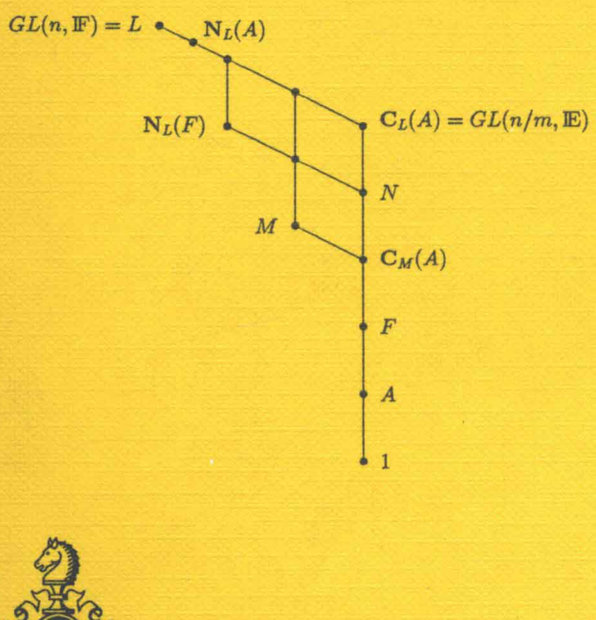
Lecture Notes in Mathematics 1519

M. W. Short

The Primitive Soluble Permutation Groups of Degree less than 256



Springer-Verlag

M. W. Short

The Primitive Soluble Permutation Groups of Degree less than 256

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Author

Mark W. Short
Mathematics Programme
Murdoch University
Murdoch, WA 6150, Australia

Mathematics Subject Classification (1991): 20-04, 20B35, 20D10

ISBN 3-540-55501-3 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-55501-3 Springer-Verlag New York Berlin Heidelberg

Printed in Germany

Typesetting: Camera ready by author/editor
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
46/3140-543210 - Printed on acid-free paper

Editorial Policy

for the publication of monographs

In what follows all references to monographs, are applicable also to multiauthorship volumes such as seminar notes.

§ 1. Lecture Notes aim to report new developments - quickly, informally, and at a high level. Monograph manuscripts should be reasonably self-contained and rounded off. Thus they may, and often will, present not only results of the author but also related work by other people. Furthermore, the manuscripts should provide sufficient motivation, examples and applications. This clearly distinguishes Lecture Notes manuscripts from journal articles which normally are very concise. Articles intended for a journal but too long to be accepted by most journals, usually do not have this "lecture notes" character. For similar reasons it is unusual for Ph. D. theses to be accepted for the Lecture Notes series.

§ 2. Manuscripts or plans for Lecture Notes volumes should be submitted (preferably in duplicate) either to one of the series editors or to Springer- Verlag, Heidelberg . These proposals are then refereed. A final decision concerning publication can only be made on the basis of the complete manuscript, but a preliminary decision can often be based on partial information: a fairly detailed outline describing the planned contents of each chapter, and an indication of the estimated length, a bibliography, and one or two sample chapters - or a first draft of the manuscript. The editors will try to make the preliminary decision as definite as they can on the basis of the available information.

§ 3. Final manuscripts should preferably be in English. They should contain at least 100 pages of scientific text and should include

- a table of contents;
- an informative introduction, perhaps with some historical remarks: it should be accessible to a reader not particularly familiar with the topic treated;
- a subject index: as a rule this is genuinely helpful for the reader.

Further remarks and relevant addresses at the back of this book.

Lecture Notes in Mathematics 1519

Contents

Chapter 1

Introduction

1.1 Motivation—a maximal subgroups algorithm

These notes are concerned with the problem of explicitly constructing all primitive soluble permutation groups of a given degree, with particular reference to those degrees less than 256. In this section we explain the motivation for tackling this problem.

Suppose we have a group G given by a finite presentation. What we can learn about G doesn't really depend on G but rather on its presentation and the theoretical and computational resources available. One might 'rate' presentations on a scale ranging from 'easy', where we can answer every question we ask, to 'impossible', where we cannot answer any of our questions. Where a presentation falls depends upon the resources at hand. In a sense, group presentation theory is about extending our resources and thereby shifting more and more group presentations towards the 'easy' end of the scale.

Four of the most basic questions one asks about a group given by a finite presentation are:

— 'Is the group finite?';

— 'If the group is finite, what is its order?';

— 'What kinds of quotients does the group have?';

— 'What kinds of subgroups does the group have?'.

Whether G is finite or not, knowledge of its quotients and/or subgroups can be very useful in understanding its structure. The nilpotent quotient algorithm (see Newman (1976)) computes special descriptions of the finite p-quotients of groups given by finite presentations. This algorithm has proved to be an important tool, for example, in the investigation of Burnside groups. The procedure of coset enumeration, systematised by Todd and Coxeter (1936), allows one to compute the index in G of a subgroup H given by finitely many generating words, provided that this index is finite. It must be stressed, however, that the procedure is highly sensitive to the way in which G and H are specified: for any given amount of computing resources there is a presentation which would cause every coset enumerator to run out of space, and yet the presentation can be seen by other methods to define the trivial group.

In the early 1960s Sims developed an algorithm, based on coset enumeration, which takes as input a group G given by a finite presentation and a positive integer n, and outputs a list containing one representative of each conjugacy class of subgroups of G whose index is at most n. A similar algorithm was developed independently by Schaps (1968). The algorithm is now known as the *low index subgroups algorithm* and implementations of it are available in the group theory software systems CAYLEY (see Section 1.3) and SPAS (see Felsch (1989)). To be very brief, the method consists of a carefully organised backtrack search through all possible 'standardised' closed coset tables of at most n rows. A reasonably detailed description of the algorithm can be found in Neubüser (1982, Section 6, pp. 30–38). One problem with the method is that the backtrack search can be very slow. Another problem is that, as already mentioned, the performance of coset enumeration is sometimes very sensitive to the way in which G is specified.

Kovács, Neubüser and Newman (unpublished notes) have proposed an algorithm which computes certain *maximal* subgroups of low index. The algorithm takes as input a group G given by a finite presentation and a positive integer n, and outputs a list containing one representative of each conjugacy class of maximal subgroups M of G whose index is at most n and such that $G/\mathrm{core}_G(M)$ is soluble. While this algorithm is not as general as the low index subgroups algorithm, it is hoped that the method will be more efficient and therefore capable of yielding information for larger values of n than is currently possible. In what follows I give an outline of the proposal. Note that the algorithm has not been developed in detail.

If H is a subgroup of finite index n in G, then the action of G on the cosets of H yields a homomorphism from G to S_n, the symmetric group of degree n. The image of the homomorphism is transitive and the kernel is $\mathrm{core}_G(H)$.

If A and B are groups, denote by $\mathrm{Sur}(A, B)$ the set of all surjective homomorphisms from A to B. Note that $\mathrm{Aut}(B)$ has a natural action on this set via post-composition.

The following theorem contains an outline of the Kovács *et al.* proposal.

1.1.1 Theorem. *Let G be a group given by a finite presentation and let n be a positive integer. Suppose we have the following:*

(i) *a 'primary' list comprising one member from each isomorphism class of groups which have a faithful primitive permutation representation of degree at most n;*

(ii) *for each group on the list, a 'secondary' list comprising one member from each of its conjugacy classes of core-free maximal subgroups of index at most n;*

(iii) *for each group on the primary list, its automorphism group;*

(iv) *an algorithm which, given a group H on the primary list, finds one member from each* $\mathrm{Aut}(H)$*-orbit of* $\mathrm{Sur}(G, H)$*;*

(v) *an algorithm for constructing the complete inverse image under such a homomorphism of any given group on a secondary list.*

Then the following steps constitute an algorithm for locating exactly one member from each conjugacy class of maximal subgroups of G *of index at most* n:

initialise the set $\mathcal{M}$ *to the empty set;*

for each group H *on the primary list do:*

compute a set $\mathcal{S}$ *of representatives of the* $\mathrm{Aut}(H)$*-orbits of* $\mathrm{Sur}(G, H)$;

for each surjection $\sigma \in \mathcal{S}$ *do:*

for each group K *on the secondary list for* H *add* $K\sigma^{-1}$ *to* $\mathcal{M}$.

Proof. Let M be a maximal subgroup of G of index $m \leq n$. Then the action of G on the cosets of M gives rise to a primitive permutation representation $\rho : G \to S_m$ whose kernel is $\mathrm{core}_G(M)$. Hence $G\rho$ is isomorphic to a group H on the list, say $G\rho\theta = H$, where θ is an isomorphism from $G\rho$ to H. Furthermore, $M\rho\theta$ is a core-free maximal subgroup of H of index m and so H-conjugate to one of the groups K on the secondary list for H. Thus the complete inverse images of $M\rho\theta$ and K are conjugate in G. Therefore the algorithm produces a subgroup $K\theta^{-1}\rho^{-1}$ of G conjugate to M.

Now suppose we have surjective homomorphisms $\sigma_i : G \to H_i$ $(i = 1, 2)$, where each H_i is on the primary list, and a group K_i on the secondary list for H_i such that $K_1\sigma_1^{-1}$ is conjugate to $K_2\sigma_2^{-1}$. It follows that the cores of $K_1\sigma_1^{-1}$ and $K_2\sigma_2^{-1}$ are equal, that is, $\ker\sigma_1 = \ker\sigma_2$, whence $H_1 \cong H_2$. Hence $H_1 = H_2$. Therefore the map $\alpha : H_1 \to H_1$ defined by $(g\sigma_1)\alpha := g\sigma_2$ is well-defined and an automorphism of H_1, that is, σ_1 and σ_2 are in the same $\mathrm{Aut}(H_1)$-orbit. Thus the algorithm produces pairwise non-conjugate maximal subgroups M of G of index at most n. ■

The algorithm could be modified to look for any subgroup of low index by replacing the word 'primitive' in item (i) by 'transitive' and by deleting the word 'maximal' in item (ii). However, the compilation of such a primary list would rapidly become unfeasible: since the regular representation of a group is transitive, the primary list would have to contain at least as many groups as there are isomorphism types of groups of order at most n. (The lower bound of Higman (1960) shows that there are at least eight million groups of order 512.) In addition, one would have to know the automorphism groups and core-free subgroups of all these groups. By contrast, relatively few groups have faithful primitive permutation representations, and those which do are of a quite restricted form. This suggests that it is reasonable to attempt the compilation of a primary list of primitive permutation groups. Dixon and Mortimer (1988) have determined the primitive groups of degree less than 1000 that have insoluble socles. Further details about lists of primitive permutation groups are given in the next section. We finish this section with some miscellaneous comments.

Kovács, Neubüser and Newman do not propose an algorithm for calculating $\mathrm{Sur}(G, H)$ when H is insoluble. Consequently, they envisage the primary list as consisting of all soluble groups having a faithful primitive permutation representation of degree at most n, and the output of the algorithm as consisting of one representative of each conjugacy class of maximal subgroups M of G of index at most n such that $G/\mathrm{core}_G(M)$ is soluble. This makes the compilation of the secondary lists particularly easy because every soluble group which has a faithful primitive permutation representation has a unique conjugacy class of core-free maximal subgroups, namely the point stabilisers (and the action on the cosets of any one of them yields the only isomorphism type of faithful primitive permutation representation of the group). Furthermore, the automorphism group of a primitive soluble permutation group is isomorphic to its normaliser in the relevant symmetric group. Hence the computation of automorphism groups amounts to the computation of normalisers in permutation groups (a seemingly less difficult problem).

The algorithm envisaged for the calculation of $\mathrm{Sur}(G, H)$ is based on Plesken's epimorphism lifting algorithm for soluble groups (Plesken (1987), Holt and Plesken (1989, Section 7.3, pp. 347–349)). This means that the primary list would have to be supplemented by certain quotients of primitive soluble groups.

The idea of looking for homomorphisms from a given group to groups on some list is illustrated in Havas and Kovács (1984), where metacyclic quotients of some knot groups are computed.

Kovács *et al.* also propose an algorithm for computing the intersection of those maximal subgroups M of G such that $M/\mathrm{core}_G(M)$ is on the primary list. This would give a canonical Frattini-free soluble quotient of G, and its computation forms the first step in their proposed soluble quotient algorithm.

Finally, I repeat that everything said so far about the algorithms proposed by Kovács *et al.* are outlines. Not many technical details have been worked out, and implementations are likely to be a long way off.

1.2 Primitive permutation groups

Permutation groups arose out of the study of roots of polynomials, but soon became objects of independent interest. Early researchers were interested in listing all permutation groups of a given degree. The highest degree for which such a list was made is 11 (Cole (1895), Miller and Ling (1901)). The intransitive groups of a given degree arise (in a suitable sense) from transitive groups of smaller degrees. Consequently, transitive groups received more attention than intransitive ones; lists of all of them were made up to degree 15 (Miller (1897a), Martin (1901), Kuhn (1904)). In a similar way, the imprimitive transitive groups of a given degree arise from primitive groups of smaller degrees. In the early 1970s Sims, with the aid of a computer, prepared a list of all primitive groups up to degree 50. Previously the primitive groups had only been listed up to degree 20 (Bennett (1912)). Worthy of special mention is Jordan (1871a), who determined the number of conjugacy classes of primitive maximal soluble permutation groups for all degrees up to one million. A detailed account of the history of listing permutation groups can be found in Appendix A.

The socle of a primitive permutation group is of fundamental importance. This is exploited in the O'Nan-Scott Theorem (see Liebeck, Praeger and Saxl (1988)), in which primitive groups are classified into types according to the structures of their socles and the intersections of these with point stabilisers. Broadly speaking, primitive groups divide naturally into two types: those with insoluble socles, and those with soluble socles. As mentioned in the previous section, Dixon and Mortimer (1988) have determined all groups of the first kind whose degree is less than 1000.

If a primitive permutation group has soluble socle, then the degree of the group is a prime power, p^n say. Furthermore, the socle is elementary abelian of order p^n, and is complemented. The socle may then be treated as an n-dimensional vector space over $GF(p)$, and every complement as an irreducible subgroup of $GL(n,p)$. Consequently, the study of primitive permutation groups with soluble socles reduces to the study of irreducible subgroups of $GL(n,p)$. This reduction is essentially due to Galois.

The irreducible subgroups of $GL(n,p)$ also divide naturally into two kinds: those that are insoluble, and those that are soluble. There are many results concerning irreducible insoluble subgroups of $GL(n,p)$, but complete lists of groups of this kind seem to be scarce, especially for $p > 2$. The irreducible insoluble subgroups of $GL(n,2)$ have been listed for $n \leq 10$ (Kondrat′ev (1986b)). The only direct attempt at listing irreducible soluble subgroups of $GL(n,p)$ seems to have been by Harada and Yamaki (1979), who count the irreducible soluble subgroups of $GL(n,2)$ for $n \leq 6$. However, in light of the theorem of Galois mentioned above, Sims' list of primitive permutation groups of degree up to 50 indirectly yields a list of the irreducible soluble subgroups of $GL(n,p)$ for $p^n \leq 50$. Consequently, and since the determination of the subgroups of $GL(1,p)$ is a trivial matter, the irreducible soluble subgroups of $GL(n,p)$ are known for $p^n < 81$. The history of listing linear groups is reviewed briefly in Appendix A.

These notes investigate the irreducible soluble subgroups of $GL(n,p)$, or, equivalently, the primitive soluble permutation groups. Although these groups have not featured extensively in lists, there is in fact a very large body of theory about their structure. During the years 1861–1917 this theory was developed almost single-handedly by Jordan, who was inspired by Galois' work on primitive soluble permutation groups and their connection with polynomials soluble by radicals. Jordan's work seems to have attracted very little interest until 1947, when Suprunenko began publishing papers containing extensions of it to the case of arbitrary fields. Suprunenko also formulated Jordan's results in more modern notation. Since that time a number of people, such as Dixon (1971), have contributed results to this theory.

These notes have two main objectives, both of which are motivated by the Kovács *et al.* proposal for a maximal subgroups algorithm discussed in the previous section. One of these objectives is to develop efficient algorithms that take as input a positive integer n and a prime p, and produce a list of the irreducible soluble subgroups of $GL(n, p)$. The other main objective is to execute these algorithms for those n and p such that $p^n < 256$, and to provide electronic access to the list of groups so obtained. A secondary objective is to 'match', as far as possible, the list of Dixon and Mortimer mentioned above.

1.3 Summary of contents

As mentioned in the previous section, the primitive soluble permutation groups are in one-to-one correspondence with the irreducible soluble linear groups over finite prime fields. In Chapter 2 we exhibit that correspondence in detail, and then proceed to investigate groups of the latter kind. First we summarise the relevant parts of the theory already developed by Jordan and Suprunenko regarding the structure of maximal irreducible soluble linear groups over finite fields. Then we extend that theory as necessary to accomplish the two main objectives stated in the previous section. Table 1.1 shows the primes p and positive integers n for which $p^n < 256$.

n	p
1	2, ..., 251
2	2, ..., 13
3	2, 3, 5
4	2, 3
5	2, 3
6	2
7	2

Table 1.1: The values of p and n for which $p^n < 256$

In Chapters 3, 4 and 5 we investigate the irreducible soluble subgroups of $GL(2, \mathbb{F})$, where $\mathbb{F}$ is any finite field. These investigations lead to a list containing exactly one group from each conjugacy class of irreducible soluble subgroups of $GL(2, \mathbb{F})$.

Chapter 6 presents some results about the maximal irreducible soluble subgroups of $GL(q, \mathbb{F})$, where q is an odd prime. The irreducible soluble subgroups of $GL(3, 3)$, $GL(3, 5)$ and $GL(5, 3)$ are determined.

In Chapter 7 we determine the imprimitive soluble subgroups of $GL(4,2)$ and $GL(4,3)$. We carry out this determination with the help of an algorithm that has been implemented in the group theory system CAYLEY (see below).

In Chapter 8 we develop some 'listing' theorems for the primitive soluble subgroups of $GL(4,\mathbb{F})$ which are similar in nature to those found for $GL(2,\mathbb{F})$.

The algorithm developed in Chapter 7 is used again in Chapter 9, this time to find the irreducible soluble subgroups of $GL(6,2)$.

The final chapter discusses the provision of electronic access to the list of groups. This requires a discussion of CAYLEY, which is a computer system that has extensive capabilities in computing with groups. A full description of this system can be found in Cannon (1984). CAYLEY has a language in which users can write their own programs. An important kind of sub-program is a *procedure.* A procedure is simply a sequence of instructions which one can invoke as part of a larger program. CAYLEY also has a facility called a *library* whereby a user can contribute data and procedures to official releases of the system. All users can then access this information and manipulate it according to their own needs. For example, Sims' list of primitive permutation groups mentioned in Section 1.2 is available as the library PRMGPS. Another example is TWOGPS, a library consisting of the groups of order dividing 128, their automorphism groups, and some procedures for manipulating these groups (see Newman and O'Brien (1989)). The releases of CAYLEY following Version 3.8-531 will contain a library that provides access to the primitive soluble permutation groups of degree less than 256. This library is described in Section 10.2. At a later stage the list of groups may also be released as part of the group theory computer system GAP, which is described in Nickel, Niemeyer and Schönert (1988). The final chapter concludes with a note on work in progress on the irreducible soluble subgroups of $GL(8,2)$ (that is, the primitive soluble permutation groups of degree 256).

Appendix A presents a history of the determination of permutation groups and linear groups. Appendix B contains some auxiliary results necessary for the work on $GL(4,\mathbb{F})$ in Chapter 8. Appendix C contains some program listings.

1.4 Conventions and Notation

Throughout these notes all actions are on the right unless specified otherwise. Consequently, if g and h are elements of a group, we define the conjugate g^h of g by h to be $h^{-1}gh$.

If G, N and H are groups and G has a normal subgroup N_0 isomorphic to N such that G/N_0 is isomorphic to H, then we write $G = N \cdot H$. If G has a subgroup isomorphic to H which intersects N_0 trivially, then G is a *semidirect product* of N and H, and we write $G = N \rtimes H$.

If V is an n-dimensional vector space over the field $\mathbb{F}$, we use the notations $GL(V)$ and $GL(n, \mathbb{F})$ to denote the group of all invertible linear transformations of V, or equivalently, the group of all n by n invertible matrices over $\mathbb{F}$. If $\mathbb{F}$ is finite of order p^k, we also use the notation $GL(n, p^k)$.

The *dihedral group* D_{2n} of order $2n$ ($n \geq 3$) is the group

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

The *generalised quaternion group* Q_{4n} of order $4n$ ($n \geq 2$) is the group

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

The group Q_8 is called the *quaternion group.*

The *semidihedral group* SD_{8n} of order $8n$ ($n \geq 2$) is the group

$$\langle a, b \mid a^2 = 1, \; b^a = b^{-1+2n}, \; b^{4n} = 1 \rangle .$$

We denote by SA_{8n} the group of order $8n$ ($n \geq 2$) given by

$$\langle a, b \mid a^2 = 1, \; b^a = b^{1+2n}, \; b^{4n} = 1 \rangle .$$

We say that a group G has a *central decomposition* $(H_1, \ldots, H_n)$ if

1. each H_i is a normal subgroup of G;
2. $G = H_1 \cdots H_n$;
3. for each i and j, $H_i \cap H_j \leq Z(H_i) \cap Z(H_j)$;
4. for each i and j, $H_i \cap H_j$ equals $Z(H_i)$ or $Z(H_j)$.

We also say that G is the *central product* of the H_i, and write $G = H_1 \curlyvee \ldots \curlyvee H_n$. Note that many authors do not impose the fourth condition.

The *holomorph* of a group G, written $\mathrm{Hol}(G)$, is the semidirect product of G and its automorphism group.

We say that a group is *monolithic* if it has a unique minimal normal subgroup.

If a, b and c are positive integers such that a^b divides c but that a^{b+1} does not divide c, then we say that a^b *sharply divides* c, and write $a^b \,\|\, c$.

We also need some notation for referring to CAYLEY objects. Libraries will be denoted by upper case, for example, PRMGPS. Built-in functions will be denoted by a sans serif font, for example, lattice. Procedures will be denoted by an upper-case typewriter font, for example, GETIRR. Names of algebraic objects, such as sets, will be printed in a lower-case typewriter font, for example, `irred`.

An index of notation is included at the beginning of the index. Most notation is standard, and can be found, for example, in Robinson (1982).

1.5 Polycyclic presentations for finite soluble groups

A convenient way of describing finite soluble groups is to use *polycyclic presentations*, introduced by Jürgensen (1970) who used the term AG-system to describe them.

A polycyclic presentation for a group G is a presentation $\{\mathcal{X}, \mathcal{R}\}$, where $\mathcal{X} = \{a_1, a_2, \ldots, a_n\}$ say, and where the relations in $\mathcal{R}$ are of the following two kinds:

$$\begin{aligned} a_i^{r(i)} &= \textstyle\prod_{k=i+1}^{n} a_k^{\alpha(i,i,k)} \quad 1 \le i \le n; \\ a_i^{-1} a_j a_i &= \textstyle\prod_{k=i+1}^{n} a_k^{\alpha(i,j,k)} \quad 1 \le i < j \le n. \end{aligned}$$

In these relations each $r(i)$ is a positive integer and each $\alpha(i,j,k)$ $(i \le j)$ is an integer modulo $r(k)$. The set $\mathcal{X}$ is sometimes called a *polycyclic generating sequence* for G. If some of the $r(i)$ and $\alpha(i,j,k)$ are not assigned specific numeric values, but rather can be chosen from some set, then we call $\{\mathcal{X}, \mathcal{R}\}$ a *parametrised polycyclic presentation*, although we shall usually omit the word "parametrised". For example, $\langle a \mid a^r = 1 \rangle$ is a parametrised polycyclic presentation for a cyclic group of order r. Thus we can describe infinitely many groups with a single polycyclic presentation.

We call $\{\mathcal{X}, \mathcal{R}\}$ *consistent* if $|G| = \prod_{i=1}^{n} r(i)$. If $\{\mathcal{X}, \mathcal{R}\}$ is consistent, then every element g of G can be written uniquely in the form

$$g = \prod_{i=1}^{n} a_i^{\varepsilon_i},$$

where $0 \le \varepsilon_i \le r(i) - 1$. The *normal form* of g (with respect to $\mathcal{X}$) refers to either the word $a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$ or the sequence $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$.

Note that a finite group has a polycyclic presentation if and only if it is soluble, and that every finite soluble group has a consistent polycyclic presentation. Unfortunately, however, not all polycyclic presentations are consistent. All soluble groups discussed in detail in these notes will be described using consistent polycyclic presentations.

1.6 Acknowledgements

The work reported on in these notes was done while I was a PhD student at The Australian National University, Canberra, Australia. I am deeply indebted to my supervisors L. G. Kovács and M. F. Newman for all their guidance and inspiration. I am also indebted to Werner Nickel, Alice C. Niemeyer, E. A. O'Brien and the referees for their constructive comments.