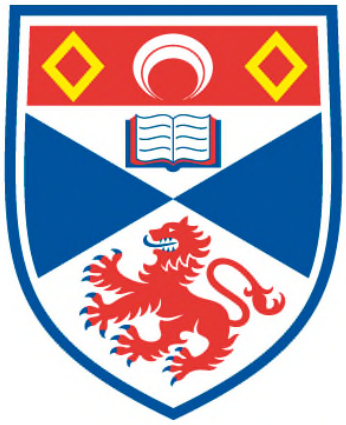
THE CONSTRUCTION OF FINITE SOLUBLE FACTOR GROUPS OF FINITELY PRESENTED GROUPS AND ITS APPLICATION

Alexander Wegner

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



1992

The Construction of Finite Soluble Factor Groups of Finitely Presented Groups and its Application

Alexander Wegner

June 16, 1992

Thesis submitted for the degree of doctor of philosophy at the University of St Andrews

Declaration

I ALEXANDER WEGNER hereby certify that this thesis has been composed by myself, that it is a record of my own work, and that it has not been accepted in partial or complete fulfilment of any other degree of professional qualification.

Signed ..... Date 16TH JUNE 1992

I was admitted to the Faculty of Science of the University of St. Andrews under Ordinance General No 12 on ..... and as a candidate for the degree of Ph.D. on .....

Signed ..... Date 16TH JUNE 1992

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate to the Degree of Ph.D.

Signature of Supervisor ..... Date 16/6/92

In submitting this thesis to the University of St. Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker.

Abstract

Computational group theory deals with the design, analysis and computer implementation of algorithms for solving computational problems involving groups, and with the applications of the programs produced to interesting questions in group theory, in other branches of mathematics, and in other areas of science. This thesis describes an implementation of a proposal for a Soluble Quotient Algorithm, i. e. a description of the algorithms used and a report on the findings of an empirical study of the behaviour of the programs, and gives an account of an application of the programs. The programs were used for the construction of soluble groups with interesting properties, e. g. for the construction of soluble groups of large derived length which seem to be candidates for groups having efficient presentations. New finite soluble groups of derived length six with trivial Schur multiplier and efficient presentations are described. The methods for finding efficient presentations proved to be only practicable for groups of moderate order. Therefore, for a given derived length soluble groups of small order are of interest. The minimal soluble groups of derived length less than or equal to six are classified.

Contents

Chapter 1

Introduction

Recent research indicates that machine computations and mathematical theory have proceeded hand in hand and have proved to be of great benefit to one another. Computer calculations have become an important element in mathematical research for various reasons :

- Computer calculations allow new, often unexpected mathematical phenomena to be observed.
- Richer, more complex examples of known phenomena can be explored. These examples which might illustrate or be of central importance to a theory were previously beyond computation and detailed comprehension.
- On the basis of exploration of examples and phenomena, new patterns are observed. This leads to the formulation of new theories and conjectures which are then the subject of formal mathematical investigation.
- The computer acts as a guide in the construction of a formal proof. It provides a tool that yields insight into the problem at hand. Furthermore, it enables mathematicians to understand the behaviour of the examples at a level deep enough to construct many new examples.

Computers have traditionally been associated with the solution of numerical problems such as the calculation of the roots of an equation, numerical interpolation and integration etc. However, a good deal of interesting work has been done using computers for essentially nonnumerical problems, such as sorting, translating languages, combinatorial analysis and solving mathematical problems in algebra. During the last three decades group theorists developed algorithms suitable for machine implementation to investigate the structure of groups (Todd-Coxeter method of coset enumeration, C. Sims' techniques for the algorithmic investigation of permutation groups, algorithms for finite soluble groups, etc.). The successful application of computers to group theory (classification of four-dimensional crystallographic groups and of finite simple groups, etc.) led to a wide acceptance among researchers of machine computation in algebra.

One of the objectives of computational group theory is the development of efficient algorithms for the purpose of calculating in groups and analysing their structure with the aid of a computer. The appearance of algorithms for computing with finite soluble groups (cf. [LNS 84]) emphasizes the fact that a finite soluble group can be investigated very efficiently if it is defined in terms of an AG-presentation, i.e. roughly a presentation that exhibits a composition series for the group. This raises the question of producing an AG-presentation for a finite soluble group that has been defined in some other way. Recently Sims described the implementation of an algorithm for computing a strong generating set and an AG-presentation for a finite soluble permutation group. The major gap in the present capabilities is the lack of an efficient analogue of the nilpotent quotient algorithm for soluble groups. Even though there are some proposals for a soluble quotient algorithm (cf. [Lee 84], [Ple 87]) which would construct an AG-presentation for a finitely presented soluble group they are not implemented and therefore it is unknown whether the methods are practical.

In early 1987 the author started on a project which aimed at an implementation of the basic algorithms of Plesken's proposal. By the end of 1987 a program

for the calculation of the extensions of finite soluble groups by finite elementary abelian groups became operational. The program was written in the C programming language and running in the UNIX programming environment. At this stage the requirements for the other parts of the project (in particular the calculation of the irreducible representations of finite soluble groups over finite fields) had been assessed and it was decided to implement the algorithms in the group theoretical programming system GAP which proved to be a fast and efficient tool to implement experimental versions of algorithms. At the end of 1988 the basic algorithms were implemented and a running version of a "soluble quotient algorithm" became available. The present version consists of about 3400 lines of code and about 2000 lines of documentation. Both, code and documentation, will be made available with GAP version 3.2. Apart from the programs and the documentation a library of finite soluble groups has been compiled in order to test and study the implementation. Since GAP contains in a much better form almost all that had been incorporated in SOGOS (cf. [LNS 84]) the "soluble quotient algorithm" makes the algorithms for computing with finite soluble groups accessible to finitely presented soluble groups.

This thesis outlines the state of the implementation, i.e. a description of the algorithms used and the experience gained with these algorithms, and gives an account of applications of the programs, however it will not contain code nor documentation of the programs since both are available within the GAP programming environment. The contents are arranged as follows : The remainder of this chapter contains a brief introduction to finite soluble groups and related notions such as AG-presentations and collection processes. A description of the proposed algorithm concludes this chapter. Chapter 2 describes the calculation of the extensions of finite soluble groups by finite elementary abelian groups. In chapter 3 the lifting of epimorphisms is investigated and the calculation of the irreducible representations of finite soluble groups over finite fields is described in chapter 4. The findings of an empirical study of the behaviour of the programs

are summarised in chapter 5. The programs were used for the construction of soluble groups with interesting properties, e.g. for the construction of soluble groups of large derived length which seem to be candidates for groups having efficient presentations. In chapter 6 new finite soluble groups of derived length six with trivial Schur multiplier and efficient presentations are described. The methods for finding efficient presentations proved to be only practicable for groups of moderate order. Therefore, for a given derived length soluble groups of small order are of interest. The minimal soluble groups of derived length at most six are classified in chapter 6.

The author assumes that the reader is familiar with the following topics, which are usually treated in a course on algebra : elementary group theory, rings and modules (cf. part I of [Jac 74] and [Joh 90]). For chapter 2 some background in the cohomology of groups (cf. chapter 6 in part II of [Jac 74]) would be helpful. For chapter 4 the reader is supposed to have knowledge of elementary representation theory such as that which may be obtained from reading introductory material in [Isa 76] or part II of [Jac 74]. The other prerequisites are rudiments of Galois theory (cf. chapter 4 in part I of [Jac 74]).

Acknowledgements I would like to express my thanks to Dr. E. F. Robertson whose help and encouragement I have greatly appreciated throughout the course of this work. Further I would like to thank Prof. Dr. J. Neubüser and Dr. C. M. Campbell for helpful discussions and advice. I would also like to express my gratitude to Dr. S. P. Glasby, Dr. W. Hanrath, Dr. R. B. Howlett and Dr. M. Schönert, who have contributed most valuable ideas and information during this study. Finally, I would like to acknowledge the support of grant EEC SC1-0003-C(EDB).

1.1 Finite Soluble Groups

The notion of solubility of groups was formulated by Galois in the earliest stages of the development of group theory. Indeed, the name 'soluble' reflects the intimate connection discovered by Galois between the possibility of solving polynomial equations by radicals and the solubility (in the sense defined below) of the groups associated by Galois with these equations. See chapter 4 of [Jac 74] for more information about Galois theory.

DEFINITION 1.1 Let G be a group. If $x, y \in G$, we define the *commutator* of x and y as $[x,y] = x^{-1}y^{-1}xy$. Let $H, K \leq G$. The *commutator subgroup* $[H,K]$ is the subgroup generated by all the commutators $[h,k]$ with $h \in H$ and $k \in K$. The particular subgroup $[G,G]$ generated by all commutators in G, is usually denoted by G' and called the *derived subgroup* of G. We define subgroups $G^{(i)}$ of G recursively by $G^{(0)} = G$ and $G^{(i)} = (G^{(i-1)})'$ for each integer $i > 0$. Every $G^{(i)}$ is characteristic in G. By definition

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots$$

is a descending sequence of characteristic subgroups of G. A group is said to be *soluble* if $G^{(l)} = 1$ for some integer l and the least integer such that $G^{(l)} = 1$ is called the *derived length* of G.

THEOREM 1.2 For a finite soluble group G the following statements are equivalent :

(i) The group G has a subnormal series with abelian factors.

(ii) The group G has a subnormal series with cyclic factors.

(iii) Every composition factor G_{i-1}/G_i of a composition series

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$$

is cyclic of prime order.

Proof cf. theorem 4.9 and 4.12 in part I of [Jac 74] □

Let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$ be a subnormal series of G with cyclic factors, that is, $G_i \lhd G_{i-1}$ and $G_{i-1} = \langle G_i, g_i \rangle$ for $i = 1, \ldots, n$. Then the sequence $(g_1, \ldots, g_n)$ is called an *AG-system* for G (cf. [LNS 84]). If p_i is the index of G_i in G_{i-1}, then in terms of the AG-system the group G has a presentation

$$\langle g_1, \ldots, g_n | {g_i}^{p_i} = w_{ii} (1 \leq i \leq n), {g_i}^{-1} g_j g_i = w_{ji} (1 \leq i < j \leq n) \rangle$$

where w_{ji} is a word of the form ${g_{i+1}}^{a(j,i,i+1)} \cdots {g_n}^{a(j,i,n)}$ with $0 \leq a(j,i,k) < p_k$ for all $k = i+1, \ldots, n$. We shall call such a presentation an *AG-presentation.* Every element of G can be expressed uniquely in the form ${g_1}^{a_1} \cdots {g_n}^{a_n}$ with $0 \leq a_k < p_k$ for $k = 1, \ldots, n$. We shall call this a *normal word* for the element. A *collection process* may be used to reduce an arbitrary word in the generators $g_1, \ldots, g_n$ of G to a normal word. Let w be an element of G expressed as a word in $g_1, \ldots, g_n$ and their inverses; w can be written in normal form by repeated cancellation and performing the following operations :

(i) Replace the subword $g_j g_i (i < j)$ by $g_i w_{ji}$

(ii) If $a < 0$, replace the subword ${g_i}^a$ by ${g_i}^{a+p_i} {w_{ii}}^{-1}$

(iii) If $a \geq p_i$, replace the subword ${g_i}^a$ by ${g_i}^{a-p_i} w_{ii}$.

This process always terminates in a normal word after a finite number of steps. If w contains more than one non-normal subword, we assume that there is a rule for determining which one to collect so that the process is well defined. Typical rules are "collect the rightmost minimal non-normal subword", or "collect the leftmost minimal non-normal subword" (see [LeS 90] for more information about collection strategies). Such a collection process can be used to compute the product gh or the inverse g^{-1} for any arbitrary elements $g = {g_1}^{e_1} \cdots {g_n}^{e_n}$ and

$h = {g_1}^{d_1} \cdots {g_n}^{d_n}$ of G by collecting the word ${g_1}^{e_1} \cdots {g_n}^{e_n} {g_1}^{d_1} \cdots {g_n}^{d_n}$ or the word ${g_n}^{-e_n} \cdots {g_1}^{-e_1}$, respectively.

1.2 The Construction of Finite Soluble Factor Groups of Finitely Presented Groups

We conclude this chapter by describing an algorithm to compute an AG-presentation for a finite soluble group G which is defined by a finite presentation. The principle idea is the computation of finite soluble factor groups of G by lifting epimorphisms $\varepsilon : G \to H$ onto extensions (see p. 12 for a definition) of H by finite irreducible H-modules, where H is given by an AG-presentation. We begin with an analysis.

Let G be a finite soluble group given by a finite presentation. Let $\widetilde{H}$ be a factor group of G and $\tilde{\varepsilon} : G \to \widetilde{H}$ be an epimorphism. Let $\widetilde{H} = \widetilde{H}_0 \rhd \widetilde{H}_1 \rhd \ldots \rhd \widetilde{H}_l = 1$ be a chief series for $\widetilde{H}$. Then $A = \widetilde{H}_{l-1}$ is a minimal normal subgroup of $\widetilde{H}$ and A is therefore characteristically simple (cf. Satz I.4.8 of [Hup 67]). A finite group is characteristically simple iff it is a direct product of finitely many isomorphic copies of simple groups (cf. Satz I.9.12 of [Hup 67]). Hence $A = A_1 \times \cdots \times A_d$ where the A_i are isomorphic simple groups. Since all subgroups of a soluble group are soluble, A_i is soluble for $i = 1, \ldots, d$. Then ${A_i}' \subset A_i$ and because of the simplicity of A_i we have ${A_i}' = 1$ and $A = A_1 \times \cdots \times A_d$ where the A_i are cyclic groups $\langle a_i \rangle$ of prime order p. The map μ defined by $(x_1, \ldots, x_d) \mapsto {a_1}^{x_1} \cdots {a_d}^{x_d}$ is an isomorphism from the additive group of the vector space V of dimension d over the field F_p with p elements onto A. If H is the factor group $\widetilde{H}/A$ and $\eta : \widetilde{H} \to H$ the natural projection, then we have a short exact sequence

$$1 \to V \xrightarrow{\mu} \widetilde{H} \xrightarrow{\eta} H \to 1$$

and $\widetilde{H}$ is an extension of H by V. For each element $x \in H$ choose an element $\tilde{h}_x \in \widetilde{H}$ such that $\eta(\tilde{h}_x) = x$. Since $\mu(V) = A \lhd \widetilde{H}$, $\tilde{h}_x^{-1}(\mu v)\tilde{h}_x \in \mu(V)$ and we have

a unique element $w \in V$ such that $\tilde{h}_x^{-1}(\mu v)\tilde{h}_x = \mu w$. It is straightforward to verify that the definition $v\varphi_x = w$ yields an automorphism of V and $\varphi : H \rightarrow GL(V)$ defined by $x \mapsto \varphi_x$ is a representation. The minimality of A in $\widetilde{H}$ implies that φ is an irreducible representation of H and A may be viewed as an irreducible $F_p[H]$-module. We conclude our analysis by noting that the map $\varepsilon : G \rightarrow H$ defined by $\varepsilon(g) = \eta(\tilde{\varepsilon}(g))$ is an epimorphism.

We now outline an algorithm to compute an AG-presentation for a finite soluble group which is defined by a finite presentation. Computing the commutator factor group G/G' is a matter of diagonalising the integer matrix resulting from the abelianised relations of the presentation for G (cf. chapter 3 in part I of [Jac 74] or chapter 6 of [Joh 90]). After this initialising step we may assume that an epimorphism $\varepsilon : G \rightarrow H$ has been computed and we repeat the following steps : For each prime divisor of $|G|$ we calculate the irreducible representations of H over the field F_p with p elements as outlined in chapter 4. For each irreducible representation we determine the extensions of H by the associated $F_p[H]$-module as outlined in chapter 2. Finally for each extension $\widetilde{H}$ we check whether the epimorphism ε lifts to an epimorphism $\tilde{\varepsilon} : G \rightarrow \widetilde{H}$, i.e. $\varepsilon = \eta\tilde{\varepsilon}$ (cf. chapter 3). If a lift $\tilde{\varepsilon}$ is found we replace ε by the epimorphism $\tilde{\varepsilon}$ and repeat the steps just described. If no lift is possible, we have calculated an isomorphism $\varepsilon : G \rightarrow H$.

A variation of this algorithm may be used to compute finite soluble factor groups of an arbitrary finitely presented group. Since we may not have information about the group under investigation (it may be infinite), we choose a set P of primes and restrict interest to P-factor groups.

Chapter 2

Extensions of Finite Soluble Groups by Finite Elementary Abelian Groups

In this chapter we present an algorithm for the calculation of the extensions of finite soluble groups by elementary abelian groups which was suggested by W. Plesken. In section 2.1 we explore Schreier's approach to the extension problem. Schreier described extensions in terms of factor sets and automorphisms which are subject to rather complicated conditions. In section 2.2 we shall restrict our attention to extensions of an arbitrary group G by an abelian group A. With such an extension we can associate an action of G on A by automorphisms and an element of the cohomology group $H^2(G, A)$. The main theorem establishes a one-to-one correspondence between the equivalence classes of extensions of G by A and the elements of $H^2(G, A)$. Using the associativity conditions for factor sets we may in principle calculate $H^2(G, A)$ in order to get an overview of all non-equivalent extensions of a finite soluble group G by a finite elementary abelian group A. This is a matter of solving a system of homogeneous linear equations, but this system of homogeneous linear equations is rather large, since each factor

set is determined by $|G|^2$ values in A. The basic idea of the algorithm which we describe in section 2.3 is the calculation of an isomorphic image of $H^2(G,A)$. A motivation for the isomorphism is the desire to describe extensions of a finite soluble group G by an elementary abelian group A by AG-presentations. We shall see that elements of $H^2(G,A)$ may be described by $n(n+1)/2$ elements in A, where n is the number of generators in an AG-system for G.

2.1 Extensions of Groups and Factor Sets

Among the subgroups of a group E there are some which are especially useful in deriving information about E : the so-called normal subgroups. We use the notation $N \trianglelefteq E$ to mean N is a normal subgroup of E. If $N \trianglelefteq E$, then we can define a corresponding group E/N which is called the factor group of E by N. In some sense, E is built up from the two groups N and E/N. This raises the extension problem : Given groups G and N determine the groups E for which there exists $M \trianglelefteq E$ such that $M \cong N$ and $E/M \cong G$. We shall call E an *extension* of G by N. For a given G and N there always exist extensions of G by N — for example, the direct product of G and N. However the group E is, in general, not uniquely determined by G and N; it therefore becomes desirable to give a complete survey of all distinct extensions of a given group G by a given group N. A first approach to the extension problem was made by Schreier (cf. [Sch 26]); his theory will be expounded in the present section.

We shall investigate extensions by means of short exact sequences of groups and homomorphisms. To begin with, we call a diagram of groups and homomorphisms $N \xrightarrow{\mu} E \xrightarrow{\pi} G$ *exact* if $\mu(N) = ker(\pi)$, that is, $\pi(e) = 1$ for $e \in E$ if and only if there exists a $n \in N$ such that $\mu(n) = e$. More generally, a sequence of groups and homomorphisms $\cdots \rightarrow G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \rightarrow \cdots$ is called *exact* if

for any three consecutive terms the sequence $G_{i-1} \overset{\varphi_{i-1}}{\to} G_i \overset{\varphi_i}{\to} G_{i+1}$ is exact. An exact sequence of the form $1 \to N \overset{\mu}{\to} E \overset{\pi}{\to} G \to 1$ is called a *short exact sequence.* This means that μ is a monomorphism, π is an epimorphism, and $\mu(N) = ker(\pi)$. Thus $\mu(N) \trianglelefteq E$ and $E/\mu(N) \cong G$, so E is an extension of G by N.

First we shall investigate the groups E which contain a normal subgroup isomorphic to N with factor group isomorphic to G. This is a good place to discuss briefly a notational convention which will be used in this chapter. It will be convenient to write certain maps on the right, that is, if $\alpha : S \to T$, then we denote the image of s under α by $s\alpha$. If $\beta : T \to U$, $t \mapsto t\beta$, then we define the composite map $\alpha\beta$ as the map having domain S and codomain U. Thus, by definition $s(\alpha\beta) = (s\alpha)\beta$.

THEOREM 2.1 Let $1 \to N \overset{\mu}{\to} E \overset{\pi}{\to} G \to 1$ be a short exact sequence. For each $x \in G$ choose an element $e_x \in E$ such that $\pi(e_x) = x$. Let $x, y \in G$ and consider the element $e_{xy}{}^{-1} e_x e_y$ of E. Applying π to this element gives $\pi(e_{xy}{}^{-1} e_x e_y) = 1$. Hence there is a unique element $\alpha(x,y) \in N$ such that $e_{xy}{}^{-1} e_x e_y = \mu(\alpha(x,y))$ or $e_x e_y = e_{xy}\mu(\alpha(x,y))$. Let $x \in G$, $n \in N$ and consider the element $e_x{}^{-1}(\mu n) e_x$. Since $\mu(N) \trianglelefteq E$, $e_x{}^{-1}(\mu n) e_x \in \mu(N)$ and we have a unique element $m \in N$ such that $e_x{}^{-1}(\mu n) e_x = \mu(m)$. The definition $n\varphi_x = m$ yields an automorphism of N and

$$(1) \qquad \alpha(xy,z)\alpha(x,y)\varphi_z = \alpha(x,yz)\alpha(y,z)$$

$$(2) \qquad n(\varphi_x\varphi_y) = \alpha(x,y)^{-1} n\varphi_{xy}\alpha(x,y)$$

for all $n \in N$ and $x, y, z \in G$.

Proof From the associative law in G it follows that

$$(e_x e_y)e_z = e_{xy}\mu(\alpha(x,y))e_z = e_{xyz}\mu(\alpha(xy,z)\alpha(x,y)\varphi_z)$$

and

$$e_x(e_y e_z) = e_x e_{yz}\mu(\alpha(y,z)) = e_{xyz}\mu(\alpha(x,yz)\alpha(y,z))$$

so that $\alpha(xy,z)\alpha(x,y)\varphi_z = \alpha(x,yz)\alpha(y,z)$. Moreover, we have

$$\mu(n(\varphi_x\varphi_y)) = (e_xe_y)^{-1}\mu(n)e_xe_y = \mu(\alpha(x,y)^{-1}n\varphi_{xy}\alpha(x,y)).$$

□

The map $\alpha : G\times G\to N$ is called a *factor set* relative to the transversal $\{e_x|x\in G\}$.

So far we have started from a given extension of G by N and have established a correspondence between this extension and a system of elements $\alpha(x,y)$, a so-called factor set, and a set of automorphisms φ_x of N. Conversely, let us assume now that in a group N a system of elements $\alpha(x,y)$ is chosen, where x and y range independently over all the elements of the group G and that every element $x\in G$ is associated with some automorphism φ_x of N for which conditions (1) and (2) are satisfied. We shall show that there exists an extension of G by N for which the given elements $\alpha(x,y)$ and the given automorphisms correspond to this extension in the above sense.

THEOREM 2.2 Let G and N be groups. Suppose $\alpha : G\times G \to N$ is a factor set and for every element $x\in G$ there is an automorphism φ_x of N such that for all $n\in N$ and $x,y,z\in G$ the conditions

$$(1)\ \ \alpha(xy,z)\alpha(x,y)\varphi_z = \alpha(x,yz)\alpha(y,z)$$

$$(2)\ \ n(\varphi_x\varphi_y) = \alpha(x,y)^{-1}n\varphi_{xy}\alpha(x,y)$$

are satisfied. Take $E = G\times N$, the set of pairs (x,n), $n\in N$, $x\in G$, and define a multiplication in E by $(x,n)(y,m) = (xy,\alpha(x,y)n\varphi_y m)$. Then E is a group and $N^* = \{(1,\alpha(1,1)^{-1}n)|n\in N\}\trianglelefteq E$ such that $N^*\cong N$ and $E/N^*\cong G$.

Proof The associativity of the multiplication follows easily from its definition and conditions (1) and (2).

From (2) with $x = y = 1$ it follows that

$$(n\varphi_1)\varphi_1 = n(\varphi_1\varphi_1) = \alpha(1,1)^{-1}n\varphi_1\alpha(1,1)$$

and since $n\varphi_1$ ranges over the whole group N as n does, we have

$$n\varphi_1 = \alpha(1,1)^{-1}n\alpha(1,1). \tag{3}$$

Further, from (1) it follows with $y = z = 1$ that

$$\alpha(x,1)\alpha(x,1)\varphi_1 = \alpha(x,1)\alpha(1,1)$$

and hence $\alpha(1,1) = \alpha(x,1)\varphi_1 = \alpha(1,1)^{-1}\alpha(x,1)\alpha(1,1)$ and since $\alpha(1,1)$ does not change when it is transformed by itself, we obtain

$$\alpha(x,1) = \alpha(1,1). \tag{4}$$

If (x,n) is an arbitrary element of E, then using (3) and (4) we have

$$(x,n)(1,\alpha(1,1)^{-1}) = (x,n)$$

so that $(1,\alpha(1,1)^{-1})$ is a right unit of E. Furthermore,

$$(x,n)(x^{-1},(n\varphi_{x^{-1}})^{-1}\alpha(x,x^{-1})^{-1}\alpha(1,1)^{-1}) = (1,\alpha(1,1)^{-1})$$

so that every element of E has a right inverse. This proves that E is a group.

It remains to show that E is the required extension of G by N. If we define $\mu : N \to E$ by $n \mapsto (1,\alpha(1,1)^{-1}n)$, then

$$\begin{aligned}\mu(n)\mu(m) &= (1,\alpha(1,1)(\alpha(1,1)^{-1}n)\varphi_1\alpha(1,1)^{-1}m) = \\ &= (1,\alpha(1,1)^{-1}nm) = \mu(nm)\end{aligned}$$

and from $\mu(n) = (1,\alpha(1,1)^{-1})$ it follows that $n = 1$. Therefore μ is an isomorphism of N onto the subgroup N^* of E.

Further, if we define $\pi : E \to G$ by $(x,n) \mapsto x$, then π is an epimorphism of E onto G with $ker(\pi) = N^*$. Hence N^* is a normal subgroup of E such that

$E/N^* \cong G$. If we use the notation $e_x = (x, 1)$, then it follows that $\{e_x | x \in G\}$ is a transversal for the cosets of N^* in E. The equation

$$e_x e_y = (xy, \alpha(xy, 1)\alpha(1, 1)^{-1}\alpha(x, y)) =$$
$$= (xy, 1)(1, \alpha(1, 1)^{-1}\alpha(x, y)) = e_{xy}\mu(\alpha(x, y))$$

shows that the factor set of this extension coincides with the given elements $\alpha(x, y)$. From (1) it follows with $x = y = 1$ that

$$\alpha(1, z)\alpha(1, 1)\varphi_z = \alpha(1, z)\alpha(1, z)$$

and hence $\alpha(1, 1)\varphi_z = \alpha(1, z)$. Hence the equation

$$\mu(n)e_x = (x, \alpha(1, x)(\alpha(1, 1)^{-1}n)\varphi_x) = (x, n\varphi_x) =$$
$$= (x, \alpha(x, 1)\alpha(1, 1)^{-1}n\varphi_x) = (x, 1)(1, \alpha(1, 1)^{-1}n\varphi_x) = e_x\mu(n\varphi_x)$$

shows that the transformation by e_x induces an automorphism of N that coincides with the original automorphism φ_x of N. □

The classification of extensions of a group G by a group N is usually carried to within equivalence. Two extensions E and E' of G by N are here called *equivalent* if there exists an isomorphism between E and E' that on N coincides with the identity automorphism and that maps onto each other the cosets of N corresponding to the same element of G.

Two short exact sequences $1 \to N \xrightarrow{\mu} E \xrightarrow{\pi} G \to 1$ and $1 \to N \xrightarrow{\mu'} E' \xrightarrow{\pi'} G \to 1$ are said to be *equivalent* if there exists an isomorphism $\psi : E \to E'$ such that

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \xrightarrow{\mu} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow 1 & & \downarrow \psi & & \downarrow 1 & & \\ 1 & \longrightarrow & N & \xrightarrow{\mu'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

is commutative (that is $\psi\mu = \mu'$ and $\pi'\psi = \pi$).

THEOREM 2.3 Two short exact sequences $1 \to N \xrightarrow{\mu} E \xrightarrow{\pi} G \to 1$ and $1 \to N \xrightarrow{\mu'} E' \xrightarrow{\pi'} G \to 1$ given by the factor sets $\alpha(x,y)$ and $\alpha'(x,y)$ and the automorphisms φ_x and φ'_x relative to the transversals $\{e_x|x\in G\}$ and $\{e'_x|x\in G\}$ are equivalent if and only if every element x of G can be associated with an element $\beta(x)$ of N in such a way that

$$(1) \quad n\varphi'_x = \beta(x)^{-1} n \varphi_x \beta(x)$$

$$(2) \quad \alpha'(x,y) = \beta(xy)^{-1}\alpha(x,y)\beta(x)\varphi_y\beta(y)$$

for all $n\in N$ and $x,y\in G$.

Proof Suppose there is an isomorphism $\psi : E \to E'$ such that $\psi\mu = \mu'$ and $\pi'\psi = \pi$. Then we have $\pi'(\psi(e_x)) = \pi(e_x) = x = \pi'(e'_x)$ and therefore $e'_x = \psi(e_x)\mu'(\beta(x))$ for a unique $\beta(x)\in N$. Properties (1) and (2) are immediate.

Conversely, suppose that every element $x\in G$ can be associated with an element $\beta(x)$ of N in such a way that conditions (1) and (2) are satisfied. Define $\psi : E \to E'$ by $e_x\mu(n) \mapsto e'_x\mu'(\beta(x)^{-1}n)$. It is easily checked that ψ is an isomorphism. Moreover, $\psi\mu = \mu'$ and $\pi'\psi = \pi$. Therefore the two short exact sequences are equivalent. □

A short exact sequence $1 \to N \xrightarrow{\mu} E \xrightarrow{\pi} G \to 1$ is said to *split* if there exists a homomorphism $\tau : G \to E$ such that $\pi\tau = 1$. Then $\tau(x)\tau(y) = \tau(xy)$ for any x, $y\in G$ and hence the factor set relative to the transversal $\{\tau(x)|x\in G\}$ is 1. Conversely, if this is the case, then we have a map $\tau : G \to E$ satisfying $\pi\tau = 1$ for which the $\alpha(x,y)$ are all 1, which means that τ is a homomorphism. It is readily seen that the short exact sequence splits if and only if there exists a subgroup H of E such that $E = H\mu(N)$ and $H\cap\mu(N) = 1$. In this case E is said to be the *semidirect* product of H and $\mu(N)$.

COROLLARY 2.4 Let $1 \to N \xrightarrow{\mu} E \xrightarrow{\pi} G \to 1$ be a short exact sequence given by the factor set $\alpha(x,y)$ and the automorphisms φ_x relative to the transversal $\{e_x | x \in G\}$. Then this short exact sequence splits if and only if every element $x \in G$ can be associated with an element $\beta(x)$ of N in such a way that $\beta(xy)^{-1}\alpha(x,y)\beta(x)\varphi_y\beta(y) = 1$ for all $x, y \in G$.

Proof The short exact sequence $1 \to N \xrightarrow{\mu} E \xrightarrow{\pi} G \to 1$ splits if and only if there exists a subgroup H of E such that $E = H\mu(N)$ and $H \cap \mu(N) = 1$. Then H is a transversal for $\mu(N)$ in E. If $\{e'_x | x \in G\}$ is another transversal for $\mu(N)$ in E, then $e'_x = e_x\mu(\beta(x))$ and $\alpha'(x,y) = \beta(xy)^{-1}\alpha(x,y)\beta(x)\varphi_y\beta(y)$ by theorem 2.3. Hence there exists a transversal $\{e'_x | x \in G\}$ with $\alpha'(x,y) = 1$ for all $x, y \in G$ if and only if there exist elements $\beta(x)$ which satisfy

$$\beta(xy)^{-1}\alpha(x,y)\beta(x)\varphi_y\beta(y) = 1.$$

□

This theory cannot be considered complete. The description of the distinct extensions of a given group G by a given group N is here reduced to the search for certain systems of elements and of automorphisms of N which are subject to rather complicated conditions and which, in general, do not simplify very much the survey of the totality of all nonequivalent extensions. In the following section we shall describe methods by which we can come closer to such a survey.

2.2 Extensions of Groups by Abelian Groups

In this section we shall study the extensions of an arbitrary group G by an abelian group A. With such an extension, we can associate an action of G on A by automorphisms and an element of the cohomology group $H^2(G,A)$ where A is regarded as a G-module by the action.

We begin with the cohomology groups and shall give the original definition of the cohomology groups of a group. For this purpose we require the concept of a G-module. If G is a group, we define a *G-module* A to be an abelian group (written additively) on which G acts as endomorphisms. This means that we have a map $(a, x) \mapsto ax$ of $A \times G$ into A such that

$$\begin{aligned} (a+b)x &= ax + bx \\ a(xy) &= (ax)y \\ a1 &= a \end{aligned}$$

for $x, y \in G$ and $a, b \in A$.

Let A be a G-module. For each $x \in G$, define a map $\varphi_x : A \to A$ by $a\varphi_x = ax$, $a \in A$. Then, because of the properties of the G-module A, we have $(a+b)\varphi_x = (a+b)x = ax + bx = a\varphi_x + b\varphi_x$, so that $\varphi_x \in End(A)$. The map φ_x is an automorphism of A : for it has as its inverse the map $\varphi_{x^{-1}}$. Moreover, we have $(a\varphi_x)\varphi_y = (ax)y = a(xy) = a\varphi_{xy}$ which shows that $\varphi : G \to Aut(A)$ defined by $x \mapsto \varphi_x$ is a homomorphism.

Conversely, let $\varphi : G \to Aut(A)$, $x \mapsto \varphi_x$ be a homomorphism. Then, for each $x \in G$ and $a \in A$, we define $ax = a\varphi_x$. This definition gives rise to a G-module structure on A.

Hence there is a one-to-one correspondence between G-modules and representations of G by automorphisms.

Now let A be a G-module. For any $n = 0, 1, 2, \ldots$ let $C^n(G, A)$ denote the set of maps $\underbrace{G \times \ldots \times G}_{n} \to A$. Every map of n elements of G with values in A shall be called an n-dimensional *cochain.* If we define addition of n-dimensional cochains by $(f + f')(g_1, \ldots, g_n) = f(g_1, \ldots, g_n) + f'(g_1, \ldots, g_n)$ for $f, f' \in C^n(G, A)$, then we obtain an abelian group $C^n(G, A)$. With every n-dimensional cochain f we can associate an $(n+1)$-dimensional cochain $\delta_n f$ called the *coboundary* of the cochain f and defined as follows

$$
\begin{aligned}
(\delta_n f)(g_1, \ldots, g_{n+1}) &= f(g_2, \ldots, g_{n+1}) \\
&+ \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i\, g_{i+1}, \ldots, g_{n+1}) \\
&+ (-1)^{n+1} f(g_1, \ldots, g_n)\, g_{n+1}.
\end{aligned}
$$

The map δ_n is a homomorphism of $C^n(G, A)$ into $C^{n+1}(G, A)$. Let $Z^n(G, A)$ denote its kernel and $B^{n+1}(G, A)$ its image in $C^{n+1}(G, A)$. We shall call an n-dimensional cochain an n-dimensional *cocycle* if $\delta_n f = 0$. For every $f \in C^n(G, A)$ we have $\delta_n(\delta_{n-1}(f)) = 0$ and therefore $B^n(G, A) \subseteq Z^n(G, A)$. Hence we can form the factor group $H^n(G, A) = Z^n(G, A)/B^n(G, A)$, which is called the n-th *cohomology group* of G with coefficients in A.

Let $1 \to A \xrightarrow{\mu} E \xrightarrow{\pi} G \to 1$ be a short exact sequence where A is abelian. For each $x \in G$ choose an element $e_x \in E$ such that $\pi(e_x) = x$. We first define an action of G on A. Let $x \in G$, $a \in A$ and consider the element ${e_x}^{-1}(\mu a)e_x$. Since $\mu(A) \trianglelefteq E$, ${e_x}^{-1}(\mu a)e_x \in \mu(A)$ and we have a unique element $b \in A$ such that ${e_x}^{-1}(\mu a)e_x = \mu(b)$. To obtain b we made a choice of an element $e_x \in E$ such that $\pi(e_x) = x$. If ${e'}_x$ is another element such that $\pi({e'}_x) = x$, then $\pi({e_x}^{-1}{e'}_x) = 1$ and hence there exists a unique $\beta(x) \in A$ such that ${e'}_x = e_x \mu(\beta(x))$. Thus we have a map $\beta : x \mapsto \beta(x)$ of G into A such that ${e'}_x = e_x \mu(\beta(x))$, $x \in G$. Since $\mu(A)$ is abelian, we have ${{e'}_x}^{-1}(\mu a){e'}_x = (e_x \mu(\beta(x)))^{-1}(\mu a)e_x \mu(\beta(x)) = {e_x}^{-1}(\mu a)e_x$. Thus the element b is independent of the choice of e_x. It is straightforward to verify that the definition $ax = b$ gives rise to a G-module structure on A. In other words, to the extension E of G by A corresponds a well-defined homomorphism of G into $Aut(A)$ which will be called the homomorphism associated with the extension.

Let x, $y \in G$ and consider the element ${e_{xy}}^{-1}e_x e_y$ of E. Applying π to this element gives $\pi({e_{xy}}^{-1}e_x e_y) = 1$. Hence there is a unique element $\alpha(x, y) \in A$ such that $e_x e_y = e_{xy}\mu(\alpha(x, y))$. If $z \in G$ also, then

$$
\alpha(xy, z)\alpha(x, y)z = \alpha(x, yz)\alpha(y, z).
$$

This relation shows that the map $\alpha : G \times G \to A$ such that $(x, y) \mapsto \alpha(x, y)$ is an element of $Z^2(G, A)$ as defined in the classical definition of $H^2(G, A)$. We now consider the alteration in α that results from changing the coset representatives e_x of $\mu(A)$ in E to e'_x for $x \in G$. Then we have a map $\beta : x \mapsto \beta(x)$ of G into A such that $e'_x = e_x \mu(\beta(x))$, $x \in G$ and α is replaced by α' where

$$\alpha'(x, y) = \beta(xy)^{-1} \beta(x) y \beta(y) \alpha(x, y).$$

This shows that α' and α determine the same element of $H^2(G, A)$ and the short exact sequence determines a unique element of $H^2(G, A)$.

THEOREM 2.5 Two extensions of G by an abelian group A are equivalent if and only if they determine the same action of G on A and the same element of $H^2(G, A)$. Let G be a group, A a G-module, and let Ext denote the set of extensions of G by A having a given G-module A as associated module. Then we have a one-to-one correspondence between the set of equivalence classes of extensions of G by A contained in Ext with the elements of $H^2(G, A)$.

Proof The result is immediate from theorem 2.1, 2.2 and 2.3. □

In this section we described the extensions of a group G by an abelian group A and we have seen, we can confine the classification of extensions of G by A to those non-equivalent extensions of G by A that have a given associated homomorphism of G into $Aut(A)$, i.e. the way in which the elements of G act on A is fixed.

2.3 Extensions of Finite Soluble Groups by Elementary Abelian Groups

Let G be a finite soluble group and let $G = G_0 \rhd G_1 \rhd \ldots \rhd G_n = 1$ be a subnormal series of G with cyclic factors, that is, $G_i \lhd G_{i-1}$ and $G_{i-1} = \langle G_i, g_i \rangle$ for

$i = 1, \ldots, n$. If $p_i = [G_{i-1} : G_i]$, then in terms of the AG-systems $(g_1, \ldots, g_n)$ the group G has a presentation

$$\langle g_1, \ldots, g_n | {g_i}^{p_i} = w_{ii} (1 \leq i \leq n), {g_i}^{-1} g_j g_i = w_{ji} (1 \leq i < j \leq n) \rangle$$

where w_{ji} is a word of the form ${g_{i+1}}^{a(j,i,i+1)} \ldots {g_n}^{a(j,i,n)}$ with $0 \leq a(j,i,k) < p_k$ for all $k = i+1, \ldots, n$. Let $A = A_1 \times \ldots \times A_d$ be an elementary abelian G-module where $A_i = \langle a_i \rangle$ is a cyclic group of order p. We assume that A is given by $d \times d$ matrices $(m_{ij}^{(k)})$ over the field F_p with p elements describing the action of the generators g_k of G. If E is an extension of G by A, then E has a presentation consisting of generators $x_1, \ldots, x_n, y_1, \ldots, y_d$ and relations

$$\begin{array}{lcll}
{x_i}^{p_i} & = & {x_{i+1}}^{a(i,i,i+1)} \ldots {x_n}^{a(i,i,n)} {y_1}^{z(i,i,1)} \ldots {y_d}^{z(i,i,d)} & 1 \leq i \leq n \\
{x_i}^{-1} x_j x_i & = & {x_{i+1}}^{a(j,i,i+1)} \ldots {x_n}^{a(j,i,n)} {y_1}^{z(j,i,1)} \ldots {y_d}^{z(j,i,d)} & 1 \leq i < j \leq n \\
{x_i}^{-1} y_j x_i & = & {y_1}^{m_{j1}^{(i)}} \ldots {y_d}^{m_{jd}^{(i)}} & \left\{ \begin{array}{l} 1 \leq j \leq d \\ 1 \leq i \leq n \end{array} \right. \\
{y_i}^{-1} y_j y_i & = & y_j & 1 \leq i < j \leq d \\
{y_i}^{p} & = & 1 & 1 \leq i \leq d
\end{array}$$

where $0 \leq z(j,i,k) < p$ for $k = 1, \ldots, n$ (cf. proposition 10.1 of [Joh 90]).

We proceed to calculate those sequences $(z(j,i,k) \mid 1 \leq k \leq d\,,\ 1 \leq i \leq j \leq n)$ for which the presentation above defines a group of order $|G||A|$, in other words, the presentation above describes an extension of G by A. Denote the set of these sequences by L. If E is an extension of G by A corresponding to the factor set α, then we obtain a map $\vartheta : Z^2(G,A) \rightarrow L$ defined by

$$\alpha \mapsto (z(j,i,k) \mid 1 \leq k \leq d\,,\ 1 \leq i \leq j \leq n).$$

It is easily verified that this map is an epimorphism.

DEFINITION 2.6 Let G be a group having a presentation

$$\langle g_1, \ldots, g_n | {g_i}^{p_i} = w_{ii} (1 \leq i \leq n), {g_i}^{-1} g_j g_i = w_{ji} (1 \leq i < j \leq n) \rangle$$

where w_{ji} is a word of the form ${g_{i+1}}^{a(j,i,i+1)} \cdots {g_n}^{a(j,i,n)}$ with $0 \leq a(j,i,k) < p_k$ for all $k = i+1, \ldots, n$. Such a presentation will be called a *power-conjugate* presentation. A power-conjugate presentation is said to be *consistent* if $|G| = p_1 \cdots p_n$.

A criterion for consistency may be obtained as follows. Let W be the set of normal words in the generators $g_1, \ldots, g_n$, that is the set of words of the form ${g_1}^{a_1} \cdots {g_n}^{a_n}$ with $0 \leq a_k < p_k$ for $k = 1, \ldots, n$. Note that W has order $p_1 \cdots p_n$. Any word in the generators can be transformed into a normal word using a collection process (cf. section 1.1). We define the product $u \cdot v$ of two elements $u, v \in W$ to be the result of collecting the word uv into normal form. If W is a group, then $W \cong G$, $|G| = p_1 \cdots p_n$ and the power-conjugate presentation for G is consistent. The following theorem shows that certain associativity conditions are sufficient to ensure that W is a group (cf. proposition 6 of [Lee 84]). The proof will follow very closely pp. 76-78 of [Vau 84].

THEOREM 2.7 (Consistency Test) A power-conjugate presentation is consistent iff the following associativity conditions are satisfied :

$$
\begin{array}{lrcll}
(1) & (g_i \cdot g_j) \cdot g_k & = & g_i \cdot (g_j \cdot g_k) & 1 \leq k < j < i \leq n \\
(2) & ({g_j}^{p_j - 1} \cdot g_j) \cdot g_k & = & {g_j}^{p_j - 1} \cdot (g_j \cdot g_k) & 1 \leq k < j \leq n \\
(3) & (g_i \cdot g_j) \cdot {g_j}^{p_j - 1} & = & g_i \cdot (g_j \cdot {g_j}^{p_j - 1}) & 1 \leq j < i \leq n \\
(4) & (g_i \cdot {g_i}^{p_i - 1}) \cdot g_i & = & g_i \cdot ({g_i}^{p_i - 1} \cdot g_i) & 1 \leq i \leq n.
\end{array}
$$

Proof We show that W is a group if the above associativity conditions are satisfied. For $r = 1, \ldots, n$ let W_r be the set of normal words ${g_r}^{a_r} \cdots {g_n}^{a_n}$. We assume that the associativity conditions hold, and we use induction to show that $W = W_1, W_2, \ldots, W_n$ are all groups.

Clearly, W_n is a cyclic group of order p_n. We suppose that W_{k+1} is a group for some $1 \leq k \leq n$, and we prove that W_k is a group.

We define a map $\theta_k : W_{k+1} \to W_{k+1}$ by $w \mapsto u$, where $g_k u$ is the normal word obtained from collecting wg_k. We show that θ_k is an automorphism of W_{k+1} as follows. First we show that, if $g_i g_j \cdots g_r g_s$ is a normal word in W_{k+1}, then $\theta_k(g_i g_j \cdots g_r g_s) = \theta_k(g_i) \cdot \theta_k(g_j) \cdots \theta(g_r) \cdot \theta_k(g_s)$. To calculate $\theta_k(g_i g_j \cdots g_r g_s)$, we must apply the collection process to $g_i g_j \cdots g_r g_s g_k$. We obtain

$$g_i g_j \cdots g_r g_s g_k = g_i g_j \cdots g_r g_k \theta_k(g_s) = g_i g_j \cdots g_k \theta_k(g_r) \cdot \theta_k(g_s).$$

At this point there is some ambiguity since there may be more than one minimal non-normal subword. There is one minimal non-normal subword involving g_k, and there may be also one in $\theta_k(g_r) \cdot \theta_k(g_s)$. However, if we identify $\theta_k(g_r) \cdot \theta_k(g_s)$ with an element of the group W_{k+1}, then the collection of any of its subwords does not change its value as an element of W_{k+1}. So we can ignore collection of subwords to the right of g_k. Also, there is never any minimal non-normal subword to the left of g_k at any stage in the collection process. So when the collection process is complete we obtain a word $g_k u$, where u is a normal word equal to $\theta_k(g_i) \cdot \theta_k(g_j) \cdots \theta(g_r) \cdot \theta_k(g_s)$ as an element of W_{k+1}. So $\theta_k(g_i g_j \cdots g_r g_s) = u$, and this is the required result.

Next notice that the associativity condition

$$(g_i \cdot g_j) \cdot g_k = g_i \cdot (g_j \cdot g_k)$$

is equivalent to the condition

$$\theta_k(g_j w_{ij}) = \theta_k(g_i) \cdot \theta_k(g_j)$$

and the associativity condition

$$({g_j}^{p_j - 1} \cdot g_j) \cdot g_k = {g_j}^{p_j - 1} \cdot (g_j \cdot g_k)$$

is equivalent to the condition

$$\theta_k(w_{jj}) = \theta_k(g_j)^{p_j}.$$

So $g_j \mapsto w_{jk}$ for $j = k+1, \ldots, n$ extends to the endomorphism θ_k of W_{k+1} since θ_k preserves the relations satisfied by the generators of W_{k+1} (cf. proposition 4.3 (Substitution Test) of [Joh 90]). Finally, the associativity condition

$$(g_i \cdot g_k) \cdot {g_k}^{p_k - 1} = g_i \cdot (g_k \cdot {g_k}^{p_k - 1})$$

is equivalent to the condition

$${\theta_k}^{p_k}(g_i) = {w_{kk}}^{-1} \cdot g_i \cdot w_{kk}.$$

Hence ${\theta_k}^{p_k}$ is an inner automorphism of W_{k+1} and therefore θ_k is an automorphism of W_{k+1}. Conditions (1) and (2) ensure that the map $g_j \mapsto w_{jk}$ defines an endomorphism of W_{k+1} and by condition (3) the p_kth power of this endomorphism is induced by w_{kk}.

Moreover, the associativity condition

$$(g_k \cdot {g_k}^{p_k - 1}) \cdot g_k = g_k \cdot ({g_k}^{p_k - 1} \cdot g_i)$$

is equivalent to the condition

$$\theta_k(w_{kk}) = w_{kk}.$$

We can form the split extension G of W_{k+1} by the infinite cycle x acting as θ_k. The element $x^{p_k} {w_{kk}}^{-1}$ is central in G, and $G/\langle x^{p_k} {w_{kk}}^{-1} \rangle$ is isomorphic to W_k. This proves that W_k is a group, and so, by induction, that W is a group. □

We apply theorem 2.7 to the power-conjugate presentation consisting of the generators $x_1, \ldots, x_n, y_1, \ldots, y_d$ and relations

$$\begin{array}{lcll}
{x_i}^{p_i} & = & {x_{i+1}}^{a(i,i,i+1)} \cdots {x_n}^{a(i,i,n)} {y_1}^{z(i,i,1)} \cdots {y_d}^{z(i,i,d)} & 1 \leq i \leq n \\
{x_i}^{-1} x_j x_i & = & {x_{i+1}}^{a(j,i,i+1)} \cdots {x_n}^{a(j,i,n)} {y_1}^{z(j,i,1)} \cdots {y_d}^{z(j,i,d)} & 1 \leq i < j \leq n \\
{x_i}^{-1} y_j x_i & = & {y_1}^{m_{j1}(i)} \cdots {y_d}^{m_{jd}(i)} & \begin{cases} 1 \leq j \leq d \\ 1 \leq i \leq n \end{cases} \\
{y_i}^{-1} y_j y_i & = & y_j & 1 \leq i < j \leq d \\
{y_i}^{p} & = & 1 & 1 \leq i \leq d
\end{array}$$

where the $z(j,i,k)$ for $k = 1,\ldots,d$ and $1 \leq i \leq j \leq n$ are regarded as indeterminates. By theorem 2.7 this power-conjugate presentation is consistent if and only if the following associativity conditions are satisfied :

$$\begin{array}{lrcll}
(1) & (x_i \cdot x_j) \cdot x_k & = & x_i \cdot (x_j \cdot x_k) & 1 \leq k < j < i \leq n \\
(2) & (x_j^{p_j - 1} \cdot x_j) \cdot x_k & = & x_j^{p_j - 1} \cdot (x_j \cdot x_k) & 1 \leq k < j \leq n \\
(3) & (x_i \cdot x_j) \cdot x_j^{p_j - 1} & = & x_i \cdot (x_j \cdot x_j^{p_j - 1}) & 1 \leq j < i \leq n \\
(4) & (x_i \cdot x_i^{p_i - 1}) \cdot x_i & = & x_i \cdot (x_i^{p_i - 1} \cdot x_i) & 1 \leq i \leq n.
\end{array}$$

The evaluation of these associativity conditions yields a system of homogeneous linear equations in the indeterminates $z(j,i,k)$ for $k = 1,\ldots,d$ and $1 \leq i \leq j \leq n$. The space of solutions of this system of homogeneous linear equations is L. Note that the associativity conditions involving $y_1,\ldots,y_d$ are superfluous since A is a G-module.

Next, we consider the group E given by the presentation consisting of the generators $x_1,\ldots,x_n,y_1,\ldots,y_d$ and relations

$$\begin{array}{rcll}
x_i^{p_i} & = & x_{i+1}^{a(i,i,i+1)} \cdots x_n^{a(i,i,n)} & 1 \leq i \leq n \\
x_i^{-1} x_j x_i & = & x_{i+1}^{a(j,i,i+1)} \cdots x_n^{a(j,i,n)} & 1 \leq i < j \leq n \\
x_i^{-1} y_j x_i & = & y_1^{m_{j1}(i)} \cdots y_d^{m_{jd}(i)} & \left\{ \begin{array}{l} 1 \leq j \leq d \\ 1 \leq i \leq n \end{array} \right. \\
y_i^{-1} y_j y_i & = & y_j & 1 \leq i < j \leq d \\
y_i^{p} & = & 1 & 1 \leq i \leq d.
\end{array}$$

Obviously, the map $\mu : A \to E$ defined by $a_i \mapsto y_i$ for $i = 1,\ldots,d$ extends to a monomorphism and $\pi : E \to G$ defined by $x_i \mapsto g_i$ for $i = 1,\ldots,n$ extends to an epimorphism such that $ker(\pi) = \mu(A)$. So we obtain a short exact sequence $1 \to A \xrightarrow{\mu} E \xrightarrow{\pi} G \to 1$. Moreover, the map $\tau : G \to E$ defined by $g_i \mapsto x_i$

for $i = 1, \ldots, n$ extends to a homomorphism such that $\pi\tau = 1$ and therefore the short exact sequence splits. This shows that the kernel of the epimorphism $\vartheta : Z^2(G, A) \to L$ must be contained in $B^2(G, A)$. Denote the image of $B^2(G, A)$ under ϑ by T and define $\overline{\vartheta} : H^2(G, A) \to L/T$ by $\alpha B^2(G, A) \mapsto \vartheta(\alpha)T$. Then $\overline{\vartheta}$ is obviously an isomorphism of $H^2(G, A)$ onto L/T.

In order to calculate T we proceed as follows. Since τ is a homomorphism the factor set α relative to the transversal $\{\tau(x)|x \in G\}$ of $\mu(A)$ in E is $\alpha = 1$. Let $1 \to A \xrightarrow{\mu'} E' \xrightarrow{\pi'} G \to 1$ be a short exact sequence and let α' be the factor set relative to the transversal $\{e'_x|x \in G\}$ of $\mu'(A)$ in E'. By theorem 2.3 this short exact sequence splits if and only if there exists a map $\beta : G \to A$ such that $\alpha'(x, y) = \beta(xy)^{-1}\beta(x)y\beta(y)$. Hence, if E' splits, then E' is equivalent to E via the isomorphism $\psi : E' \to E$ defined by $e'_x\mu'(v) \mapsto \tau(x)\mu(\beta(x)v)$, $x \in G$ and $v \in A$. Then the sequence $\vartheta(\alpha')$ is obtained by calculating

$$\psi({e'_{g_n}}^{-a(i,i,n)} \cdots {e'_{g_{i+1}}}^{-a(i,i,i+1)} {e'_{g_i}}^{p_i})$$

and

$$\psi({e'_{g_n}}^{-a(j,i,n)} \cdots {e'_{g_{i+1}}}^{-a(j,i,i+1)} {e'_{g_i}}^{-1} e'_{g_j} e'_{g_i})$$

for $1 \leq i \leq j \leq n$ as words in the generators $y_1, \ldots, y_d$ of E. Clearly, $\vartheta(\alpha')$ is uniquely determined by the values of β on the generators $g_1, \ldots, g_n$ of G. Hence, in order to calculate T we compute

$$(x_n\gamma(g_n))^{-a(i,i,n)} \cdots (x_{i+1}\gamma(g_{i+1}))^{-a(i,i,i+1)} (x_i\gamma(g_i))^{p_i}$$

and

$$(x_n\gamma(g_n))^{-a(j,i,n)} \cdots (x_{i+1}\gamma(g_{i+1}))^{-a(j,i,i+1)} (x_i\gamma(g_i))^{-1} x_j\gamma(g_j)x_i\gamma(g_i)$$

for $1 \leq i \leq j \leq n$ as words in the generators $y_1, \ldots, y_d$ of E for every map $\gamma : \{g_1, \ldots, g_n\} \to \mu(A)$.

EXAMPLE Let $G = \langle a, b\rangle$ be the alternating group of degree 4 with the defining relations $a^3 = b^2 = (ab)^3 = 1$. Take $r = a$, $s = b$ and $t = r^{-1}sr$; then it is easily verified that $r^{-1}tr = st$ and therefore $\langle s, t\rangle$ is a normal subgroup of G. Moreover, we have $s^2 = t^2 = 1$ and $st = ts$. Hence $\langle s, t\rangle$ is elementary abelian and $G \rhd \langle s, t\rangle \rhd \langle t\rangle \rhd 1$ is a subnormal series with cyclic factors. In terms of the AG-system (r, s, t) the group G has a presentation

$$\langle r, s, t | r^3 = s^2 = t^2 = 1, r^{-1}sr = t, r^{-1}tr = st, s^{-1}ts = t\rangle.$$

Let A be the cyclic group of order 2 and let G act on A.

In order to calculate the set of sequences L as described earlier we consider the presentation consisting of the generators x_1, x_2, x_3, y and relations

$$\begin{aligned}
{x_1}^3 &= y^{z_{11}} \\
{x_2}^2 &= y^{z_{22}} \\
{x_3}^2 &= y^{z_{33}} \\
{x_1}^{-1}x_2x_1 &= x_3y^{z_{21}} \\
{x_1}^{-1}x_3x_1 &= x_2x_3y^{z_{31}} \\
{x_2}^{-1}x_3x_2 &= x_3y^{z_{32}} \\
{x_i}^{-1}yx_i &= y \\
y^2 &= 1
\end{aligned}$$

for $i = 1, 2, 3$. The associativity conditions yield the following system of homogeneous linear equations (throughout the calculations we used collection from the left) : $z_{22} + z_{32} = 0, z_{22} + z_{33} = 0, z_{32} + z_{33} = 0$. For example, the equation $z_{22} + z_{32} = 0$ arises from the condition $(x_3 \cdot x_3) \cdot x_1 = x_3 \cdot (x_3 \cdot x_1)$ as follows

$$(x_3 \cdot x_3) \cdot x_1 = x_1 y^{z_{33}}$$

$$\begin{aligned}
x_3 \cdot (x_3 \cdot x_1) &= x_3x_1x_2x_3y^{z_{31}} = x_1x_2x_3x_2x_3 = \\
&= x_1{x_2}^2{x_3}^2y^{z_{32}} = x_1{x_3}^2y^{z_{22}+z_{32}} = x_1y^{z_{22}+z_{32}+z_{33}}.
\end{aligned}$$

The other equations arise from the conditions

$$\begin{aligned}(x_2 \cdot x_2) \cdot x_1 &= x_2 \cdot (x_2 \cdot x_1) \\ (x_3 \cdot x_1) \cdot {x_1}^2 &= x_3 \cdot (x_1 \cdot {x_1}^2)\end{aligned}$$

and $(x_2 \cdot x_1) \cdot {x_1}^2 = x_2 \cdot (x_1 \cdot {x_1}^2)$, respectively. The sequences

$$(z_{11}, z_{21}, z_{31}, z_{22}, z_{32}, z_{33}) = (1,0,0,0,0,0),$$

$(0,1,0,0,0,0), (0,0,1,0,0,0)$ and $(0,0,0,1,1,1)$ generate the space L of solutions of this system of homogeneous linear equations.

In order to calculate $T = \vartheta(B^2(G,A))$ we consider the group given by the presentation consisting of the generators x_1, x_2, x_3, y and relations

$$\begin{aligned}{x_1}^3 &= 1 \\ {x_2}^2 &= 1 \\ {x_3}^2 &= 1 \\ {x_1}^{-1} x_2 x_1 &= x_3 \\ {x_1}^{-1} x_3 x_1 &= x_2 x_3 \\ {x_2}^{-1} x_3 x_2 &= x_3 \\ {x_i}^{-1} y x_i &= y \\ y^2 &= 1\end{aligned}$$

for $i = 1,2,3$. Take $\gamma(r) = y^u$, $\gamma(s) = y^v$ and $\gamma(t) = y^w$; then we obtain

$$\begin{aligned}(x_1\gamma(r))^3 &= y^u \\ (x_2\gamma(s))^2 &= 1 \\ (x_3\gamma(t))^2 &= 1 \\ (x_3\gamma(t))^{-1}(x_1\gamma(r))^{-1} x_2\gamma(s) x_1\gamma(r) &= y^{v+w} \\ (x_3\gamma(t))^{-1}(x_2\gamma(s))^{-1}(x_1\gamma(r))^{-1} x_3\gamma(t) x_1\gamma(r) &= y^v \\ (x_3\gamma(t))^{-1}(x_2\gamma(s))^{-1} x_3\gamma(t) x_2\gamma(s) &= 1.\end{aligned}$$

Hence T is the subspace of L generated by the sequences

$$(z_{11}, z_{21}, z_{31}, z_{22}, z_{32}, z_{33}) = (1,0,0,0,0,0),$$

$(0,1,0,0,0,0)$ and $(0,1,1,0,0,0)$. As we have seen earlier the factor space L/T is isomorphic to $H^2(G,A)$ and therefore we have $H^2(G,A) \cong \langle (0,0,0,1,1,1) \rangle$.

Thus there are two equivalence classes of extensions of G by A. The sequence $(0,0,0,0,0,0)$ corresponds to the direct product $G \times A$ while the sequence $(0,0,0,1,1,1)$ corresponds to the representation group of G which is isomorphic to the special linear group $SL_2(3)$ of dimension 2 over F_3.

The method for the calculation of the extensions of a finite soluble group G by a finite elementary abelian G-module is easy to implement. The basic requirement is a collection process which allows to evaluate the associativity conditions in order to determine a set of homogeneous linear equations. In the remainder of this section we shall describe such a collection process.

We begin by studying the substitutions which involve relations in which some of the exponents of generators are indeterminates. Earlier in this section we have seen that we only need to evaluate the associativity conditions which involve the generators $x_1, \ldots, x_n$. Let ${x_{i_1}}^{r_1} \cdots {x_{i_l}}^{r_l}$ with $x_{i_j} \in \{x_1, \ldots, x_n\}$ be a non-normal word with positive exponents $r_1, \ldots, r_l$. Then there exists a minimal k such that either $r_k \geq p_{i_k}$ or $i_k \geq i_{k+1}$. Let ${x_j}^r = {x_{i_k}}^{r_k}$, ${x_i}^s = {x_{i_{k+1}}}^{r_{k+1}}$ and let v_{ji} be the word obtained from w_{ji} by substituting x_k for g_k, $k = 1, \ldots, n$; then we may proceed with the following substitutions

$$
\begin{aligned}
{x_j}^r &\leftarrow {x_j}^{r-p_j}\, v_{jj}\, {y_1}^{z(j,j,1)} \cdots {y_d}^{z(j,j,d)} && r \geq p_j \\
{x_j}^r {x_i}^s &\leftarrow {x_j}^{r+s} && i = j \\
{x_j}^r {x_i}^s &\leftarrow {x_j}^{r-1} x_i\, v_{ji}\, {y_1}^{z(j,i,1)} \cdots {y_d}^{z(j,i,d)} {x_i}^{s-1} && i < j.
\end{aligned}
$$

We now carry out the substitutions and obtain a word in $x_1, \ldots, x_n$ if $i = j$. If $r \geq p_i$ or $i < j$, then we obtain

$${x_{i_1}}^{r_1} \cdots {x_{i_l}}^{r_l} = {x_{i_1}}^{r_1} \cdots {x_j}^{r-p_j}\, v_{jj}\, {y_1}^{z(j,j,1)} \cdots {y_d}^{z(j,j,d)} {x_i}^s \cdots {x_{i_l}}^{r_l}$$

and

$$x_{i_1}{}^{r_1} \cdots x_{i_l}{}^{r_l} = x_{i_1}{}^{r_1} \cdots x_j{}^{r-1} x_i \, v_{ji} \, y_1{}^{z(j,i,1)} \cdots y_d{}^{z(j,i,d)} x_i{}^{s-1} \cdots x_{i_l}{}^{r_l}$$

respectively. Let $\mathbf{R} : G \to GL_d(p)$, $g_k \mapsto (m_{ij}{}^{(k)})$ for $k = 1, \ldots, n$ be the matrix representation associated with the G-module A and let v be a word in $x_1, \ldots, x_n$. Then $w(y_1{}^{z(j,i,1)} \cdots y_d{}^{z(j,i,d)})w^{-1} =$

$$y_1{}^{m_{11}z(j,i,1)} \cdots y_d{}^{m_{1d}z(j,i,1)} \cdots y_1{}^{m_{d1}z(j,i,d)} \cdots y_d{}^{m_{dd}z(j,i,d)}$$

where $(m_{ij}) = \mathbf{R}(w)^{-1}$ and w is obtained from v by substituting g_k for x_k, for $k = 1, \ldots, n$. Taking $v = x_{i_1}{}^{r_1} \cdots x_j{}^{r-p_j} v_{jj}$ and $x_{i_1}{}^{r_1} \cdots x_j{}^{r-1} x_i v_{ji}$ respectively we obtain expressions in $y_1, \ldots, y_d$ where the exponents of $y_1, \ldots, y_d$ are linear combinations of $z(j,i,1), \ldots, z(j,i,d)$ for $1 \leq i \leq j \leq n$. Moreover, we see that the required collection process consists of a mechanism for dealing with the conjugates of $y_1{}^{z(j,i,1)} \cdots y_d{}^{z(j,i,d)}$ and essentially a collection process with respect to the AG-presentation for G.

We now describe a collection process which we use to evaluate the associativity conditions in order to determine a system of homogeneous linear equations. We represent an expression in $y_1, \ldots, y_d$ where the exponents of $y_1, \ldots, y_d$ are linear combinations of $z(j,i,1), \ldots, z(j,i,d)$ for $1 \leq i \leq j \leq n$ by a sequence of matrices

$$\begin{array}{c} \\ y_1 \\ \vdots \\ y_d \end{array} \begin{array}{c} \begin{array}{ccccc} \cdots & & z(j,i,1) & \cdots & z(j,i,d) \end{array} \quad \cdots \\ \left[\begin{array}{c} \cdots \end{array} \right. \left(\begin{array}{ccc} \mathbf{M}[j][i]_{11} & \ldots & \mathbf{M}[j][i]_{1d} \\ \vdots & & \vdots \\ \mathbf{M}[j][i]_{d1} & \ldots & \mathbf{M}[j][i]_{dd} \end{array} \right) \begin{array}{c} \cdots \end{array} \left. \right] \end{array}$$

each row representing the exponent of y_k, $k = 1, \ldots, d$ (initially all entries are zero). Let $g_{i_1}{}^{r_1} \cdots g_{i_l}{}^{r_l}$ with $g_{i_j} \in \{g_1, \ldots, g_n\}$ be a non-normal word with positive exponents $r_1, \ldots, r_l$. Then there exists a minimal k such that either $r_k \geq p_{i_k}$ or $i_k \geq i_{k+1}$. Let $g_j{}^r = g_{i_k}{}^{r_k}$, $g_i{}^s = g_{i_{k+1}}{}^{r_{k+1}}$; then we define the required collection

process by the following operations

$$
\begin{aligned}
g_j{}^r &\leftarrow g_j{}^{r-p_j} w_{jj}\,; \mathbf{M}[j][j] := \mathbf{M}[j][j] + {}^t\mathbf{R}(g_{i_1}{}^{r_1} \cdots g_j{}^{r-p_j} w_{jj}\ )^{-1} && r \geq p_j \\
g_j{}^r g_i{}^s &\leftarrow g_j{}^{r+s} && i = j \\
g_j{}^r g_i{}^s &\leftarrow g_j{}^{r-1} g_i w_{ji}; \mathbf{M}[j][i] := \mathbf{M}[j][i] + {}^t\mathbf{R}(g_{i_1}{}^{r_1} \cdots g_j{}^{r-1} g_i w_{ji})^{-1} && i < j
\end{aligned}
$$

where ${}^t\mathbf{M}$ denotes the transposed matrix of $\mathbf{M}$.

Chapter 3

Lifting Epimorphisms

Let G be a finitely presented group $G = \langle g_1, \ldots, g_n | r_i(g_1, \ldots, g_n) = 1, 1 \leq i \leq m \rangle$ and let H be a finite soluble group with an AG-presentation

$$H = \langle h_1, \ldots, h_k | s_i(h_1, \ldots, h_k) = 1, 1 \leq i \leq l \rangle.$$

Let $\varepsilon : G \to H$ be an epimorphism given by the images $\overline{g}_i = \varepsilon(g_i) = w_i(h_1, \ldots, h_k)$ of g_i for $i = 1, \ldots, n$ and words $\hat{w}_1, \ldots, \hat{w}_k$ such that $h_i = \hat{w}_i(\overline{g}_1, \ldots, \overline{g}_n)$ for $i = 1, \ldots, k$. Let M be a finite irreducible $F_p[H]$-module, where F_p is the field with p elements for some prime p, and let

$$1 \to M \xrightarrow{\mu} \widetilde{H} \xrightarrow{\eta} H \to 1$$

be a short exact sequence. Finally, let $\tilde{h}_i \in \widetilde{H}$ for $i = 1, \ldots, k$ be members of a transversal $\{e_x | x \in H\}$ of $\mu(M)$ in $\widetilde{H}$ such that $\eta(\tilde{h}_i) = h_i$ for $i = 1, \ldots, k$ and assume that the factor set α relative to this transversal is given by $s_i(\tilde{h}_1, \ldots, \tilde{h}_k)$ for $i = 1, \ldots, l$ (cf. section 2.3). Given this data, it is a question of solving linear equations over the field F_p in order to check whether there exists an epimorphism $\tilde{\varepsilon} : G \to \widetilde{H}$ such that $\eta\tilde{\varepsilon} = \varepsilon$. A homomorphism $\tilde{\varepsilon}$ with $\eta\tilde{\varepsilon} = \varepsilon$ is said to *lift* the epimorphism ε.

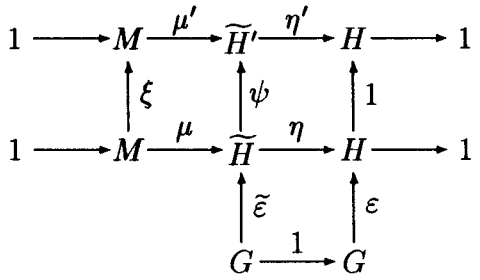
First, we show that in order to check whether an epimorphism ε can be lifted to an epimorphism $\tilde{\varepsilon}$ it is sufficient to consider representatives of the one-dimensional $End_{F_p[H]}(M)$-subspaces of $H^2(H,M)$.

We begin with a brief discussion of modules over rings. If V and W are modules over a ring R, then we write $Hom_R(V,W)$ to denote the set of R-homomorphisms of V into W. Then $Hom_R(V,W)$ is an abelian group with the addition defined by $v(f+g) = vf + vg$ for all $f,\ g \in Hom_R(V,W)$ and $v \in V$. In particular, $End_R(V) = Hom_R(V,V)$ is a ring with multiplication defined by $v(fg) = (vf)g$ for all $f,\ g \in End_R(V)$ and $v \in V$. Let V be a nonzero R-module. Then V is irreducible if its only R-submodules are 0 and V. An immediate consequence of Schur's lemma is that if V is an irreducible R-module, then $End_R(V)$ is a division ring.

Now, we apply this to the irreducible module M. Then $E = End_{F_p[H]}(M)$ is a division ring and E is a field by Wedderburn's theorem which asserts that finite division rings are commutative.

Let $\alpha \in Z^2(H,M)$ and $\xi \in E$. Define a map $\alpha\xi : H \times H \to M$ by $(x,y) \mapsto \alpha(x,y)\xi$. Then we have $(\alpha\xi)(xy,z) + (\alpha\xi)(x,y)z = (\alpha\xi)(x,yz) + (\alpha\xi)(y,z)$ and therefore $\alpha\xi \in Z^2(H,M)$. It is easily verified that $Z^2(H,M)$ together with the map $Z^2(H,M) \times E \to Z^2(H,M)$ defined by $(\alpha,\xi) \mapsto \alpha\xi$ is a vector space over E. Now, let $\alpha \in B^2(H,M)$, that is, there exists a map $\beta : H \to M$ such that $\alpha(x,y) = -\beta(xy) + \beta(x)y + \beta(y)$. Then we have $(\alpha\xi)(x,y) = -\beta(xy)\xi + (\beta(y)\xi)y + \beta(y)\xi$ and therefore $\alpha\xi \in B^2(H,M)$, showing that $B^2(H,M)$ is a subspace of $Z^2(H,M)$ and $H^2(H,M) = Z^2(H,M)/B^2(H,M)$ is a vector space over E.

Let $1 \to M \xrightarrow{\mu'} \widetilde{H}' \xrightarrow{\eta'} H \to 1$ be a short exact sequence and let $\alpha\xi$ be the factor set relative to the transversal $\{e'_x | x \in H\}$. Then $\psi : \widetilde{H} \to \widetilde{H}'$ defined by $e_x\mu(m) \mapsto e'_x\mu'(m\xi)$ is an isomorphism. Moreover, we have $\eta'\psi = \eta$ and $\psi\mu = \mu'\xi$ and therefore the following diagram is commutative.



If the epimorphism $\tilde{\varepsilon} : G \to \widetilde{H}$ lifts the epimorphism ε, then we have $\varepsilon = \eta\tilde{\varepsilon} = \eta'\psi\tilde{\varepsilon}$ and therefore $\psi\tilde{\varepsilon}$ also lifts the epimorphism ε.

Suppose that the homomorphism $\tilde{\varepsilon} : G \to \widetilde{H}$ lifts the epimorphism $\varepsilon : G \to H$. Take $\tilde{g}_i = w_i(\tilde{h}_1, \ldots, \tilde{h}_k)$ for $i = 1, \ldots, n$. Then we have

$$\eta(\tilde{\varepsilon}(g_i)) = \varepsilon(g_i) = w_i(h_1, \ldots, h_k) =$$
$$= w_i(\eta(\tilde{h}_1), \ldots, \eta(\tilde{h}_k)) = \eta(w_i(\tilde{h}_1, \ldots, \tilde{h}_k)) = \eta(\tilde{g}_i).$$

Thus $\tilde{\varepsilon}(g_i) = \tilde{g}_i m_i$ for $i = 1, \ldots, n$ and $m_i \in \mu(M)$.

By proposition 4.3 of [Joh 90] the map $g_i \mapsto \tilde{g}_i m_i$ for $i = 1, \ldots, n$ and $m_i \in \mu(M)$ extends to a homomorphism $G \to H$ if and only if

$$r_i(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n) = 1 \qquad (*)$$

for $i = 1, \ldots, m$. These equations for $(m_1, \ldots, m_n)$ yield linear equations over the field F_p for the coordinates of the m_i for $i = 1, \ldots, n$ in an implicitly given basis of $\mu(M)$ and ε lifts to a homomorphism if and only if $(*)$ is soluble. All possible lifts $\tilde{\varepsilon} : G \to \widetilde{H}$ are given by $\tilde{\varepsilon}(g_i) = \tilde{g}_i m_i$ for $i = 1, \ldots, n$, where $(m_1, \ldots, m_n)$ runs through the set $S(*)$ of solutions of $(*)$.

We now have to decide which solutions of the system of equations $(*)$ yield surjective lifts of the epimorphism $\varepsilon : G \to H$. Again, assume that $\tilde{\varepsilon} : G \to \widetilde{H}$ is a

homomorphism which lifts the epimorphism $\varepsilon : G \to H$. The group $\mu(M)$ is a normal subgroup of $\widetilde{H}$ and $\tilde{\varepsilon}(G)$ is a subgroup of $\widetilde{H}$. Then $\tilde{\varepsilon}(G)\mu(M)$ is a subgroup of $\widetilde{H}$ and by the isomorphism theorem $\tilde{\varepsilon}(G)\mu(M)/\mu(M) \cong \tilde{\varepsilon}(G)/\tilde{\varepsilon}(G) \cap \mu(M)$. Since $\eta(\tilde{\varepsilon}(G)) = H$ and the kernel of the restriction of η to $\tilde{\varepsilon}(G)$ is $\tilde{\varepsilon}(G) \cap \mu(M)$, we have $\widetilde{H} = \tilde{\varepsilon}(G)\mu(M)$. Therefore $\tilde{\varepsilon}(G) \cap \mu(M)$ is a normal subgroup of $\widetilde{H}$ and since M is an irreducible $F_p[H]$-module we have

$$\tilde{\varepsilon}(G) \cap \mu(M) = \begin{cases} \mu(M) \\ 1. \end{cases}$$

Case (1) : $\alpha \notin B^2(H, M)$. In this case $\tilde{\varepsilon}(G) \cap \mu(M) = \mu(M)$, that is $\mu(M) \leq \tilde{\varepsilon}(G)$ and $\tilde{\varepsilon}$ is necessarily an epimorphism. Therefore every solution of $(*)$ yields an epimorphism $\tilde{\varepsilon} : G \to \widetilde{H}$ given by $\tilde{\varepsilon}(g_i) = \tilde{g}_i m_i$ for $i = 1, \ldots, n$.

Case (2) : $\alpha \in B^2(H, M)$. In this case non-surjective lifts $\tilde{\varepsilon}$ arise, namely, the ones whose images are complements of $\mu(M)$ in $\widetilde{H}$. We assume that the elements $\tilde{h}_1, \ldots, \tilde{h}_k$ generate a complement of $\mu(M)$ in $\widetilde{H}$, that is, $s_i(\tilde{h}_1, \ldots, \tilde{h}_k) = 1$ for $i = 1, \ldots, l$.

If $\tilde{\varepsilon}(G) \cap \mu(M) = 1$, then $\eta : \tilde{\varepsilon}(G) \to H$ is an isomorphism and

$$\begin{aligned} 1 &= s_i(\tilde{h}_1, \ldots, \tilde{h}_k) \\ &= s_i(\eta^{-1}(h_1), \ldots, \eta^{-1}(h_k)) \\ &= s_i(\eta^{-1}(\hat{w}_1(\overline{g}_1, \ldots, \overline{g}_n)), \ldots, \eta^{-1}(\hat{w}_k(\overline{g}_1, \ldots, \overline{g}_n))) \\ &= s_i(\hat{w}_1(\tilde{\varepsilon}(g_1), \ldots, \tilde{\varepsilon}(g_n)), \ldots, \hat{w}_k(\tilde{\varepsilon}(g_1), \ldots, \tilde{\varepsilon}(g_n))) \end{aligned}$$

$$\begin{aligned} \tilde{g}_i m_i &= \eta^{-1}(\varepsilon(g_i)) \\ &= \eta^{-1}(w_i(h_1, \ldots, h_k)) \\ &= \eta^{-1}(w_i(\hat{w}_1(\overline{g}_1, \ldots, \overline{g}_n), \ldots, \hat{w}_k(\overline{g}_1, \ldots, \overline{g}_n))) \\ &= w_i(\hat{w}_1(\tilde{\varepsilon}(g_1), \ldots, \tilde{\varepsilon}(g_n)), \ldots, \hat{w}_k(\tilde{\varepsilon}(g_1), \ldots, \tilde{\varepsilon}(g_n))). \end{aligned}$$

therefore $(m_1, \ldots, m_n)$ is a solution of the equations

$$\left.\begin{aligned} &s_i(\hat{w}_1(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n), \ldots, \hat{w}_k(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n)) = 1 \\ &\tilde{g}_j m_j = w_j(\hat{w}_1(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n), \ldots \hat{w}_k(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n)) \end{aligned}\right\} \qquad (**)$$

for $i = 1, \ldots, l$ and $j = 1, \ldots, n$.

Conversely, if $(m_1, \ldots, m_n)$ is a solution of the equations $(**)$, then $\tau : H \to \widetilde{H}$ defined by $h_i \mapsto \hat{w}_i(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n)$ for $i = 1, \ldots, k$ is a homomorphism. Hence $\tilde{\varepsilon} : G \to \widetilde{H}$ defined by $\tilde{\varepsilon} = \tau\varepsilon$ is a homomorphism and $\tilde{\varepsilon}$ lifts the epimorphism ε since

$$\begin{aligned} \tilde{\varepsilon}(g_i) &= (\tau\varepsilon)(g_i) \\ &= \tau(w_i(h_1, \ldots, h_k)) \\ &= w_i(\tau(h_1), \ldots, \tau(h_k)) \\ &= w_i(\hat{w}_1(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n), \ldots, \hat{w}_k(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n)) \\ &= \tilde{g}_i m_i. \end{aligned}$$

Therefore $(m_1, \ldots, m_n)$ is a solution of $(*)$. Moreover, we have

$$\begin{aligned} \eta(\tau(h_i)) &= \eta(\hat{w}_i(\tilde{g}_1 m_1, \ldots, \tilde{g}_n m_n)) \\ &= \hat{w}_i(\eta(\tilde{g}_1), \ldots, \eta(\tilde{g}_n)) \\ &= \hat{w}_i(\eta(w_1(\tilde{h}_1, \ldots, \tilde{h}_k)), \ldots, \eta(w_n(\tilde{h}_1, \ldots, \tilde{h}_k))) \\ &= \hat{w}_i(w_1(h_1, \ldots, h_k), \ldots, w_n(h_1, \ldots, h_k)) \\ &= \hat{w}_i(\varepsilon(g_1), \ldots, \varepsilon(g_n)) \\ &= \varepsilon(\hat{w}_i(g_1, \ldots, g_n)) \\ &= h_i \end{aligned}$$

for $i = 1, \ldots, k$ and therefore $\tilde{\varepsilon}(G)$ is a complement of $\mu(M)$ in $\widetilde{H}$.

If we denote the set of solutions of the equations $(**)$ by $S(**)$, then every element $(m_1, \ldots, m_n) \in S(*) \backslash S(**)$ yields an epimorphism $\tilde{\varepsilon} : G \to \widetilde{H}$ given by $g_i \mapsto \tilde{g}_i m_i$ for $i = 1, \ldots, n$.

This brings us to the concluding part in this section. In view of a repeated application of the lifting procedure outlined above it remains to calculate preimages of the generators in an AG-system for $\widetilde{H}$.

Suppose the epimorphism $\varepsilon : G \to H$ has been lifted to an epimorphism $\tilde{\varepsilon} : G \to \widetilde{H}$. If $x \in ker(\tilde{\varepsilon})$, then $\varepsilon(x) = (\eta\tilde{\varepsilon})x = \eta(\tilde{\varepsilon}x) = 1$ and therefore $x \in ker(\varepsilon)$. This shows that $ker(\tilde{\varepsilon}) \subset ker(\varepsilon)$. Moreover, $\eta(\tilde{\varepsilon}x) = 1$ implies $\tilde{\varepsilon}x \in \mu(M)$ and we have $\tilde{\varepsilon}(ker(\varepsilon)) = \mu(M)$. Since M is an irreducible $F_p[H]$-module, $\mu(M)$ is the normal closure $\overline{\{y\}}$ in $\widetilde{H}$ for every element $1 \neq y \in \mu(M)$. If w is an element of $ker(\varepsilon)$ such that $\tilde{\varepsilon}w = y$, then $ker(\varepsilon)/ker(\tilde{\varepsilon})$ is the normal closure $\overline{\{w \cdot ker(\tilde{\varepsilon})\}}$ in $G/ker(\tilde{\varepsilon})$ and we may compute a preimage for every element of $\mu(M)$ by producing a F_p-basis for $\mu(M)$ (cf. [Par 84]). Finally, we have

$$\eta(\tilde{\varepsilon}(\hat{w}_i(g_1, \ldots, g_n))^{-1}\tilde{h}_i) = \varepsilon(\hat{w}_i(g_1, \ldots, g_n))^{-1}h_i = 1$$

and therefore $h_i = \tilde{\varepsilon}(\hat{w}_i(g_1, \ldots, g_n))y'$ for some $y' \in \mu(M)$.

This obviously yields the required preimages provided we have a sufficient description for $ker(\tilde{\varepsilon})$. A normal subgroup generating set for $ker(\varepsilon)$ is obtained from the following theorem.

THEOREM 3.1

$$H = \langle \overline{g}_1, \ldots, \overline{g}_n | s_i(\hat{w}_1(\overline{g}_1, \ldots, \overline{g}_n), \ldots, \hat{w}_k(\overline{g}_1, \ldots, \overline{g}_n)),$$
$$\overline{g}_j = w_j(\hat{w}_1(\overline{g}_1, \ldots, \overline{g}_n), \ldots, \hat{w}_k(\overline{g}_1, \ldots, \overline{g}_n)); i = 1, \ldots, l; j = 1, \ldots, n \rangle.$$

Proof We have generating sets $X = \{h_1, \ldots, h_k\}$ and $Y = \{\overline{g}_1, \ldots, \overline{g}_n\}$ for H and $R(X) = \{s_i(h_1, \ldots, h_k) | i = 1, \ldots, l\}$ is a set of defining relations. Moreover, $h_i = \hat{w}_i(\overline{g}_1, \ldots, \overline{g}_n)$ for $i = 1, \ldots, k$ and $\overline{g}_i = w_i(h_1, \ldots, h_k)$ for $i = 1, \ldots, n$ are systems of equations expressing the generators X in terms of Y, and vice versa. Denote these systems of equations by $X = X(Y)$ and $Y = Y(X)$ respectively. We now apply Tietze transformations to the presentation $\langle X | R(X) \rangle$ in accordance

with the following scheme (cf. proposition 4.6 of [Joh 90]) :

$$
\begin{array}{lllllll}
X+: & X & Y & R(X) & Y=Y(X) & & \\
R+: & X & Y & R(X) & Y=Y(X) & X=X(Y) & \\
R+: & X & Y & R(X) & Y=Y(X) & X=X(Y) & R(X(Y)) \\
R-: & X & Y & & Y=Y(X) & X=X(Y) & R(X(Y)) \\
R+: & X & Y & & Y=Y(X) & X=X(Y) & R(X(Y)) \quad Y=Y(X(Y)) \\
R-: & X & Y & & & X=X(Y) & R(X(Y)) \quad Y=Y(X(Y)) \\
X-: & & Y & & & & R(X(Y)) \quad Y=Y(X(Y))
\end{array}
$$

□

In other words $ker(\varepsilon)$ is the normal closure of

$$\{s_i(\widehat{w}_1(g_1,\ldots,g_n),\ldots,\widehat{w}_k(g_1,\ldots,g_n)),$$
$$g_j{}^{-1}w_j(\widehat{w}_1(g_1,\ldots,g_n),\ldots,\widehat{w}_k(g_1,\ldots,g_n));i=1,\ldots,l;j=1,\ldots,n\}$$

in G.

EXAMPLE Let $G=\langle g_1,g_2\rangle$ be the alternating group of degree four with the defining relations ${g_1}^3={g_2}^2=(g_1g_2)^3=1$ and let $H=\langle h|s(h)=h^3\rangle$. The map $\varepsilon: G \to H$ defined by $g_1 \mapsto w_1(h)=h$ and $g_2 \mapsto w_2(h)=1$ extends to an epimorphism. Take $\widehat{w}(g_1,g_2)=g_1$ and let $\widetilde{H}$ be the semidirect product of H by an elementary abelian group $A=\langle a_1,a_2\rangle$ of type $(2,2)$ where the action of H on A is defined by $a_1{\cdot}h=a_2$ and $a_2{\cdot}h=a_1a_2$. Then $\widetilde{H}$ has the presentation

$$\langle \tilde{h},y_1,y_2|\tilde{h}^3={y_1}^2={y_2}^2=1,\tilde{h}^{-1}y_1\tilde{h}=y_2,\tilde{h}^{-1}y_2\tilde{h}=y_1y_2,{y_1}^{-1}y_2y_1=y_2\rangle.$$

It is easily verified that the system of equations $(*)$ only yields trivial equations and therefore every pair (m_1,m_2) with $m_1,\ m_2 \in \langle y_1,y_2\rangle$ yields a lift $\tilde{\varepsilon}: G \to \widetilde{H}$ defined by $g_1 \mapsto \tilde{h}m_1$ and $g_2 \mapsto m_2$. In order to find the nonsurjective lifts we consider the system of equations $(**)$ of which only the following equation is

nontrivial : $m_2 = \tilde{g}_2 m_2 = w_2(\hat{w}(\tilde{g}_1 m_1, \tilde{g}_2 m_2)) = 1$. Hence the nonsurjective lifts are the homomorphisms $\tilde{\varepsilon} : G \to \widetilde{H}$ defined by $g_1 \mapsto \tilde{h} m_1$ and $g_2 \mapsto 1$ with $m_1 \in \langle y_1, y_2 \rangle$. Let $\tilde{\varepsilon} : G \to \widetilde{H}$ defined by $g_1 \mapsto \tilde{h} y_1$ and $g_2 \mapsto y_1 y_2$. In order to calculate preimages for $\tilde{h}$, y_1 and y_2 we consider the images of the normal subgroup generating set for $ker(\varepsilon)$ in G. We have $\tilde{\varepsilon}(s(\hat{w}(g_1, g_2))) = \tilde{\varepsilon}({g_1}^3) = 1$,

$$\tilde{\varepsilon}({g_1}^{-1} w_1(\hat{w}(g_1, g_2))) = \tilde{\varepsilon}({g_1}^{-1} g_1) = 1$$

and finally $\tilde{\varepsilon}({g_2}^{-1} w_2(\hat{w}(g_1, g_2))) = \tilde{\varepsilon}({g_2}^{-1}) = y_1 y_2$. Then $y_1 = \tilde{h}^{-1}(y_1 y_2)\tilde{h} = \tilde{\varepsilon}({g_1}^{-1} {g_2}^{-1} g_1)$ and we have obtained preimages for the generators $y_1 y_2$ and y_1. In order to find a preimage for y_2 we express y_2 in terms of the generators $y_1 y_2$ and y_1. We have $y_2 = (y_1 y_2) y_1 = \tilde{\varepsilon}({g_2}^{-1}) \tilde{\varepsilon}({g_1}^{-1} {g_2}^{-1} g_1) = \tilde{\varepsilon}({g_2}^{-1} {g_1}^{-1} {g_2}^{-1} g_1)$. Finally, we have $\tilde{\varepsilon}(\hat{w}(g_1, g_2)) = \tilde{\varepsilon}(g_1) = \tilde{h} y_1$ and therefore $g_1({g_1}^{-1} g_2 g_1) = g_2 g_1$ is a preimage for $\tilde{h}$.

Chapter 4

The Construction of the Irreducible Representations of Finite Soluble Groups over Finite Fields

In this chapter an algorithm for the calculation of the irreducible representations of finite soluble groups over finite fields is presented. The principle tools are Clifford's results on the construction of the irreducible representations of a finite group from the irreducible representations of a normal subgroup. These results are summarised and applied in section 4.1 in order to develop an algorithm for the calculation of the irreducible representations of finite soluble groups over algebraically closed fields. The irreducible representations over arbitrary fields are considered in section 4.2. We shall see that the irreducible representations of a finite group over an algebraically closed field are absolutely irreducible. Moreover, in prime characteristic, we shall see that an absolutely irreducible representation of a group is realisable over its field of character values. This information may be used to construct (up to similarity) all the irreducible representations of a group

over any given finite field. With the help of our knowledge of section 4.1 and 4.2 we develop an algorithm for the calculation of the irreducible representations of finite soluble groups over finite fields in section 4.3.

Throughout this chapter the reader is supposed to have knowledge of elementary representation theory such as that which may be obtained from reading introductory material in [Isa 76] or part II of [Jac 74]. The other prerequisites are Galois theory and some familiarity with cohomology theory.

4.1 The Construction of the Irreducible Representations of Finite Soluble Groups over Algebraically Closed Fields

This section describes the connection between the irreducible representations of a finite group and the irreducible representations of a normal subgroup. The approach is based on an article by Clifford (cf. [Cli 37]). The first part of the section analyses the structure of the irreducible representations of a finite group in terms of the irreducible representations of a normal subgroup. Based on this analysis the second part describes the construction of the irreducible representations of a finite group from the irreducible representations of a normal subgroup. We conclude this section with an application of the theory which has been summarised in this section and describe an algorithm for the construction of the irreducible representations of finite soluble groups over algebraically closed fields : Going up a composition series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_l = \langle 1 \rangle$ of a soluble group G all irreducible representations of G_i are constructed from those of G_{i+1} by extending the G_i-invariant irreducibles of G_{i+1} to irreducibles of G_i and by inducing up the non-invariant irreducibles of G_{i+1}.

The first theorem describes the structure of an irreducible $F[G]$-module V on restriction to a normal subgroup N of a group G. The irreducible $F[G]$-module V is identified with an induced module ${V_j}^G$ for some irreducible $F[U_j]$-module V_j where U_j is a subgroup of G.

DEFINITION 4.1 Let N be a normal subgroup of a group G and let $\mathbf{R}$ be a representation of N. For a fixed element $g \in G$ the map defined by $n \mapsto \mathbf{R}^g(n) = \mathbf{R}(g^{-1}ng)$ is obviously a representation of N and is called a *conjugate representation* of $\mathbf{R}$ with respect to G.

THEOREM 4.2 Let $N \trianglelefteq G$ and let V be an irreducible $F[G]$-module.

(a) If W is an irreducible $F[N]$-submodule of V, then

$$V = \sum_{g \in G} gW.$$

Every gW is an irreducible $F[N]$-module and therefore V is a completely reducible $F[N]$-module. If $\mathbf{R}$ is the representation of N corresponding to W, then $\mathbf{R}^g$ corresponds to gW.

(b) Let $W_1, \ldots, W_k$ be representatives of the isomorphism classes of irreducible $F[N]$-submodules of V. Define the W_i-homogeneous component by

$$V_i = \sum_{\substack{W \subseteq V \\ W \cong W_i}} W$$

for $1 \leq i \leq k$. Then $V = V_1 \oplus \cdots \oplus V_k$ and the homogeneous components are transitively permuted by the action of G. Let U_j be the set $\{g \mid g \in G, gV_j = V_j\}$ and let $\mathbf{R}_j$ be the representation of N corresponding to W_j. Then $U_j = \{g \mid g \in G, \mathbf{R}_j{}^g \text{ is similar to } \mathbf{R}_j\}$ for $1 \leq j \leq k$, the homogeneous components V_j are irreducible $F[U_j]$-modules and

$$V \cong F[G] \otimes_{F[U_j]} V_j = {V_j}^G.$$

Proof See Satz V.17.3 of [Hup 67] for the details. □

EXAMPLE Let $G = \langle a, b \rangle$ be the Dihedral Group of order 6 with the defining relations $a^3 = b^2 = 1$, $b^{-1}ab = a^{-1}$. Consider the irreducible representation $\mathbf{R}$ over the field of complex numbers defined by

$$\mathbf{R}(a) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

and

$$\mathbf{R}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where ε is a primitive third root of unity in the field of complex numbers. The restriction of $\mathbf{R}$ to the normal subgroup $\langle a \rangle$ is obviously completely reducible and the irreducible components are defined by $\mathbf{S}(a) = \varepsilon$ and $\mathbf{S}^b(a) = \mathbf{S}(a^{-1}) = \varepsilon^{-1}$. Choose the transversal $\{1, b\}$ for the left cosets of $\langle a \rangle$ in G (that is, a set of representatives for these cosets). Then

$$\mathbf{S}^G(a) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} = \mathbf{R}(a)$$

and

$$\mathbf{S}^G(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \mathbf{R}(b).$$

Next consider a normal subgroup N of a finite group G and an irreducible $F[G]$-module V such that V_N is a homogeneous $F[N]$-module. In other words, if W is an irreducible $F[N]$-submodule of V_N, then

$$V = \sum_{g \in G} gW$$

where all the conjugates gW are $F[N]$-isomorphic to W. In the terminology of the previous theorem V corresponds to V_1 and G to U_1.

DEFINITION 4.3 Let G be a group and F a field. A *projective representation* of G is a map $\mathbf{P} : G \mapsto GL_n(F)$ such that

$$\mathbf{P}(g)\mathbf{P}(h) = \alpha(g,h)\mathbf{P}(gh)$$

for all g, $h \in G$, where $\alpha(g,h)$ is a non-zero element of F depending on the pair (g,h). Its degree is n and the map $(g,h) \mapsto \alpha(g,h)$ is called the *factor set* of the representation. Exactly as in the case with ordinary representations, two projective representations $\mathbf{P}$ and $\mathbf{Q}$ are similar if $\mathbf{Q} = \mathbf{X}^{-1}\mathbf{P}\mathbf{X}$ for some nonsingular matrix $\mathbf{X}$. Also $\mathbf{P}$ is irreducible if it is not similar to a projective representation in triangular block form

$$g \mapsto \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

for all $g \in G$.

The following lemma gives an instance of how projective representations arise in the study of ordinary representations.

LEMMA 4.4 (cf. theorem 11.2 of [Isa 76]) Let N be normal subgroup of G and let F be an algebraically closed field. Let $\mathbf{S}$ be an irreducible representation of N over F such that the conjugate $n \mapsto \mathbf{S}^g(n) = \mathbf{S}(g^{-1}ng)$ is similar to $\mathbf{S}$ for all $g \in G$. Then there exists a projective representation $\mathbf{P}$ of G such that

(a) $\mathbf{P}(n) = \mathbf{S}(n)$

(b) $\mathbf{P}(ng) = \mathbf{P}(n)\mathbf{P}(g)$

(c) $\mathbf{P}(gn) = \mathbf{P}(g)\mathbf{P}(n)$

for all $n \in N$ and $g \in G$. If α is the factor set of $\mathbf{P}$, then the values $\alpha(g,h)$ depend only on the cosets of $G \bmod N$ in which g and h lie. Furthermore, if $\mathbf{P}'$ is another projective representation satisfying (a), (b) and (c), then $\mathbf{P}'(g) = \mu(g)\mathbf{P}(g)$ for some map $\mu : G \mapsto F^*$, which is constant on cosets of N and the factor set of $\mathbf{P}'$ is $(g,h) \mapsto \alpha'(g,h) = \alpha(g,h)\mu(g)\mu(h)\mu(gh)^{-1}$.

Proof Choose a transversal T for N in G (that is, a set of coset representatives). Take $1 \in T$. For each $t \in T$, choose a nonsingular matrix $\mathbf{P}_t$ such that $\mathbf{P}_t{}^{-1}\mathbf{S}\mathbf{P}_t = \mathbf{S}^t$. Take $\mathbf{P}_1 = \mathbf{I}$. For $n \in N$ and $t \in T$ define $\mathbf{P}(tn) = \mathbf{P}_t\mathbf{S}(n)$. Properties (a), (b) and (c) are immediate. Properties (a), (b) and (c) yield

$$\mathbf{S}(n)\mathbf{P}(g) = \mathbf{P}(ng) = \mathbf{P}(gg^{-1}ng) = \mathbf{P}(g)\mathbf{S}(g^{-1}ng)$$

and

$$\mathbf{P}(g)^{-1}\mathbf{S}(n)\mathbf{P}(g) = \mathbf{S}(g^{-1}ng)$$

for all $g \in G$ and all $n \in N$. Also

$$\mathbf{P}(h)^{-1}\mathbf{P}(g)^{-1}\mathbf{S}(n)\mathbf{P}(g)\mathbf{P}(h) = \mathbf{S}(h^{-1}g^{-1}ngh).$$

Comparing with

$$\mathbf{P}(gh)^{-1}\mathbf{S}(n)\mathbf{P}(gh) = \mathbf{S}((gh)^{-1}ngh)$$

yields $\mathbf{P}(g)\mathbf{P}(h) = \alpha(g,h)\mathbf{P}(gh)$ for some $\alpha(g,h) \in F^*$ and thus $\mathbf{P}$ is a projective representation. By properties (b) and (c)

$$\alpha(gn,hm)\mathbf{P}(gnhm) = \mathbf{P}(gn)\mathbf{P}(hm) = \mathbf{P}(g)\mathbf{P}(nhm)$$

for m, $n \in N$ and g, $h \in G$. Furthermore

$$\begin{aligned}\mathbf{P}(g)\mathbf{P}(nhm) &= \mathbf{P}(g)\mathbf{P}(h)\mathbf{P}(h^{-1}nhm) = \\ &= \alpha(g,h)\mathbf{P}(gh)\mathbf{P}(h^{-1}nhm) = \alpha(g,h)\mathbf{P}(gnhm).\end{aligned}$$

Since $\mathbf{P}(gnhm)$ is nonsingular, $\alpha(gn,hm) = \alpha(g,h)$.

If $\mathbf{X}$ is any nonsingular matrix such that $\mathbf{X}^{-1}\mathbf{S}(n)\mathbf{X} = \mathbf{S}(g^{-1}ng)$ for all $n \in N$, then $\mathbf{X}\mathbf{P}(g)^{-1}$ commutes with all $\mathbf{S}(n)$ for all $n \in N$ and thus $\mathbf{X}\mathbf{P}(g)^{-1}$ is a scalar matrix. If $\mathbf{P}'$ also satisfies (a), (b) and (c), take $\mathbf{X} = \mathbf{P}'(g)$ and conclude that $\mathbf{P}'(g) = \mu(g)\mathbf{P}(g)$ for some $\mu(g) \in F^*$. For $n \in N$ and $g \in G$

$$\mu(gn)\mathbf{P}(gn) = \mathbf{P}'(gn) = \mathbf{P}'(g)\mathbf{P}'(n) = \mu(g)\mathbf{P}(g)\mathbf{P}(n).$$

Since $\mathbf{P}(gn) = \mathbf{P}(g)\mathbf{P}(n)$ is nonsingular, $\mu(gn) = \mu(g)$.

If α' is the factor set of $\mathbf{P}'$, then

$$\mu(g)\mu(h)\alpha(g,h)\mathbf{P}(gh) = \mu(g)\mu(h)\mathbf{P}(g)\mathbf{P}(h) =$$
$$= \mathbf{P}'(g)\mathbf{P}'(h) = \alpha'(g,h)\mathbf{P}'(gh) = \alpha'(g,h)\mu(gh)\mathbf{P}(gh).$$

Since $\mathbf{P}(gh)$ is nonsingular $\alpha'(gh) = \alpha(g,h)\mu(g)\mu(h)\mu(gh)^{-1}$. □

THEOREM 4.5 (cf. Satz V.17.5 of [Hup 67]) Let N be a normal subgroup of G and let F be an algebraically closed field. Let V be an irreducible $F[G]$-module and assume V_N is a direct sum of s isomorphic $F[N]$-modules. If $\mathbf{R}$ is the representation corresponding to V, then $\mathbf{R}(g) = \mathbf{Q}(g) \otimes \mathbf{P}(g)$ for all $g \in G$, where $\mathbf{Q}$ and $\mathbf{P}$ are irreducible projective representations of G and $\mathbf{Q}$ is a projective representation of G/N of degree s.

Proof Let $V_N = W_1 \oplus \cdots \oplus W_s$ where the W_i are isomorphic $F[N]$-modules. Then there exists a basis for the representation space V such that for $n \in N$

$$\mathbf{R}(n) = \begin{pmatrix} \mathbf{S}(n) & 0 & \cdots & 0 \\ 0 & \mathbf{S}(n) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \mathbf{S}(n) \end{pmatrix}.$$

With regard to this basis let $\mathbf{R}(g) = (\mathbf{R}_{ij}(g))$ ($i,j = 1,\ldots,s$). Since $\mathbf{R}(n)\mathbf{R}(g) = \mathbf{R}(g)\mathbf{R}(g^{-1}ng)$, it follows that $\mathbf{S}(n)\mathbf{R}_{ij}(g) = \mathbf{R}_{ij}(g)\mathbf{S}(g^{-1}ng) = \mathbf{R}_{ij}(g)\mathbf{S}^g(n)$. The conjugates $\mathbf{S}$ and $\mathbf{S}^g$ are similar and therefore there exists an invertible matrix $\mathbf{P}(g)$ such that $\mathbf{S}(n)\mathbf{P}(g) = \mathbf{P}(g)\mathbf{S}^g(n)$. Then

$$\mathbf{S}(n)\mathbf{R}_{ij}(g)\mathbf{P}(g)^{-1} =$$
$$= \mathbf{R}_{ij}(g)\mathbf{S}^g(n)\mathbf{P}(g)^{-1} = \mathbf{R}_{ij}(g)\mathbf{P}(g)^{-1}\mathbf{S}(n).$$

By Schur's lemma, since $\mathbf{S}$ is irreducible and F is algebraically closed, there exists an element $a_{ij}(g) \neq 0$ in F such that $\mathbf{R}_{ij}(g) = a_{ij}(g)\mathbf{P}(g)$. Define $\mathbf{Q}$ by $\mathbf{Q}(g) = (a_{ij}(g))$. Then $\mathbf{R}(g) = \mathbf{Q}(g) \otimes \mathbf{P}(g)$ for all $g \in G$.

Next, the mapping $g \mapsto \mathbf{P}(g)$ is shown to be a projective representation. If g and h are elements of G, then

$$\mathbf{S}(n)\mathbf{P}(g)\mathbf{P}(h)\mathbf{P}(gh)^{-1} = \mathbf{P}(g)\mathbf{S}(g^{-1}ng)\mathbf{P}(h)\mathbf{P}(gh)^{-1} =$$
$$= \mathbf{P}(g)\mathbf{P}(h)\mathbf{S}((gh)^{-1}ngh)\mathbf{P}(gh)^{-1} = \mathbf{P}(g)\mathbf{P}(h)\mathbf{P}(gh)^{-1}\mathbf{S}(n).$$

By Schur's lemma $\mathbf{P}(g)\mathbf{P}(h) = \alpha(g,h)\mathbf{P}(gh)$, where $\alpha(g,h) \in F^*$.

Because $\mathbf{P}$ is a projective representation of G with factor set α and $\mathbf{R}$ is an ordinary representation, $\mathbf{Q}$ is a projective representation of G with factor set α^{-1}. Since $\mathbf{S}^n(m) = \mathbf{S}(n)^{-1}\mathbf{S}(m)\mathbf{S}(n)$ for all n, $m \in N$, $\mathbf{P}(n) = \mathbf{S}(n)$ can be assumed for $n \in N$. Then $\mathbf{I} \otimes \mathbf{S}(n) = \mathbf{R}(n) = \mathbf{Q}(n) \otimes \mathbf{P}(n) = \mathbf{Q}(n) \otimes \mathbf{S}(n)$ implies $\mathbf{Q}(n) = \mathbf{I}$ and $\mathbf{Q}$ is actually a projective representation of G/N. The projective representations $\mathbf{Q}$ and $\mathbf{P}$ are irreducible, because a reduction of either one would imply a reduction of $\mathbf{R}$, contrary to the hypothesis that V is irreducible. □

EXAMPLE Let $G = \langle a, b \rangle$ be the Quaternion group of order 8 with the defining relations $b^{-1}ab = a^{-1}$, $a^4 = 1$ and $b^2 = a^2$. Consider the irreducible representation $\mathbf{R}$ over the field of complex numbers defined by

$$\mathbf{R}(a) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

and

$$\mathbf{R}(b) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

where ε is a primitive fourth root of unity in the field of complex numbers. The restriction of $\mathbf{R}$ to the normal subgroup $\langle a^2 \rangle$ is obviously completely reducible and up to similarity there is only one irreducible component. It is the representation $\mathbf{S}$ defined by $\mathbf{S}(a^2) = -1$. Choose the transversal $\{1, a, b, ba\}$ for the left cosets of $\langle a^2 \rangle$ in G and define a projective representation $\mathbf{P}$ of G by $\mathbf{P}(1) = \mathbf{P}(a) = \mathbf{P}(b) = \mathbf{P}(ba) = 1$ (cf. lemma 4.4). The factor set α of $\mathbf{P}$ on the cosets of $\langle a^2 \rangle$ in G may be given by the following table :

α	1	aN	bN	baN
N	1	1	1	1
aN	1	-1	-1	1
bN	1	1	-1	-1
baN	1	-1	1	-1

The map $\mathbf{Q}$ define by

$$\mathbf{Q}(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{Q}(a) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

$$\mathbf{Q}(b) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\mathbf{Q}(ba) = \begin{pmatrix} 0 & \varepsilon \\ \varepsilon & 0 \end{pmatrix}$$

is a projective representation of $G/\langle a^2 \rangle$ with factor set α^{-1}. Evidently $\mathbf{R}(g) = \mathbf{Q}(g) \otimes \mathbf{P}(g)$ for all $g \in G$.

Next, the procedure of starting from a known representation $\mathbf{R}$ of a group G and studying the restriction of $\mathbf{R}$ to a normal subgroup of G is reversed. Instead, the problem of embedding a given irreducible representation $\mathbf{S}$ of a normal subgroup N of G in an irreducible representation $\mathbf{R}$ of G is considered. The question is : Is there an irreducible representation $\mathbf{R}$ of G such that $\mathbf{S}$ occurs as an irreducible component of $\mathbf{R}_N$?

THEOREM 4.6 (cf. §4 of [Cli 37]) Let N be a normal subgroup of a finite group G and let $\mathbf{S}$ be an irreducible representation of N. Let U be the set of all

elements g in G such that the conjugate $n \mapsto \mathbf{S}^g(n) = \mathbf{S}(g^{-1}ng)$ is similar to $\mathbf{S}$. If it is possible to embed $\mathbf{S}$ in an irreducible representation $\mathbf{S}'$ of U, then $\mathbf{S}$ can be embedded in an irreducible representation of G.

Proof Let $\{r_1 = 1, r_2, \ldots, r_m\}$ be a transversal for U in G. Then the representations $\mathbf{S}^{(i)}$ of N defined by

$$\mathbf{S}^{(i)} : n \mapsto \mathbf{S}(r_i{}^{-1}nr_i) \qquad (i = 1, \ldots, m)$$

are the distinct conjugates of $\mathbf{S}$. By hypothesis there exists an irreducible representation $\mathbf{S}'$ of U such that $\mathbf{S}$ is an irreducible component of $\mathbf{S}'_N$. Since $\mathbf{S}$ is similar to all its conjugates relative to U, $\mathbf{S}'_N$ is necessarily a multiple of $\mathbf{S}$. Now, define $\mathbf{R}$ to be the induced representation $(\mathbf{S}')^G$, that is

$$\mathbf{R}(g) = \begin{pmatrix} \mathbf{R}_{11}(g) & \ldots & \mathbf{R}_{1m}(g) \\ \vdots & \ddots & \vdots \\ \mathbf{R}_{m1}(g) & \ldots & \mathbf{R}_{mm}(g) \end{pmatrix}$$

where

$$\mathbf{R}_{ij}(g) = \begin{cases} \mathbf{S}'(r_i{}^{-1}gr_j) & \text{if } r_i{}^{-1}gr_j \in U \\ 0 & \text{otherwise.} \end{cases}$$

For elements $n \in N$, $\mathbf{R}_{ij}(n) = 0$ if $i \neq j$ and

$$\mathbf{R}_{ii}(n) = \mathbf{S}'(r_i{}^{-1}nr_i) = \begin{pmatrix} \mathbf{S}^{(i)}(n) & & \\ & \ddots & \\ & & \mathbf{S}^{(i)}(n) \end{pmatrix}.$$

For elements u in U we have

$$\mathbf{R}(u) = \begin{pmatrix} \mathbf{S}'(u) & 0 & \ldots & 0 \\ 0 & \mathbf{S}'(r_2{}^{-1}ur_2) & \ldots & \mathbf{S}'(r_2{}^{-1}ur_m) \\ \vdots & \vdots & & \vdots \\ 0 & \mathbf{S}'(r_m{}^{-1}ur_2) & \ldots & \mathbf{S}'(r_m{}^{-1}ur_m) \end{pmatrix}.$$

To see that $\mathbf{R}$ is irreducible, let $\mathbf{R}'$ be an irreducible component of $\mathbf{R}$ such that $\mathbf{R}'_U$ contains $\mathbf{S}'$. But then $\mathbf{R}'_N$ will contain $\mathbf{S}'_N$ and hence by theorem 4.2 will contain $\mathbf{S}^{(1)} = \mathbf{S}, \mathbf{S}^{(2)}, \ldots, \mathbf{S}^{(m)}$. Therefore $\mathbf{R}'$ has the same degree as $\mathbf{R}$, and so $\mathbf{R}'$ must be similar to $\mathbf{R}$. □

This reduces the problem to that of embedding the irreducible representation $\mathbf{S}$ of N in an irreducible representation $\mathbf{S}'$ of U. To simplify the notation replace U by G and assume that the given irreducible representation $\mathbf{S}$ of N is similar to all its conjugates with respect to G.

THEOREM 4.7 (cf. §4 of [Cli 37]) Let N be a normal subgroup of a group G and let F be an algebraically closed field. Let $\mathbf{S} : G \mapsto GL_r(F)$ be an irreducible representation of N and assume that $\mathbf{S}$ is similar to all the conjugate representations with respect to G. Then there exists a projective representation $\mathbf{P}$ of G such that $\mathbf{P}(n) = \mathbf{S}(n)$ for all $n \in N$. Let $(g,h) \mapsto \alpha(g,h)$ be the factor set of $\mathbf{P}$. If $(g,h) \mapsto \alpha(g,h)^{-1}$ is the factor set of an irreducible projective representation $\mathbf{Q} : G/N \mapsto GL_s(F)$, then $\mathbf{S}$ can be embedded in an irreducible representation of G.

Proof Let $\mathbf{R}(g) = \mathbf{Q}(g) \otimes \mathbf{P}(g)$ for all $g \in G$. Evidently $\mathbf{R}$ is a matrix representation of G such that

$$\mathbf{R}(n) = \begin{pmatrix} \mathbf{S}(n) & & \\ & \ddots & \\ & & \mathbf{S}(n) \end{pmatrix}$$

for all $n \in N$. By Burnside's lemma the representation $\mathbf{R}$ is irreducible if and only if a linear relation among the components of $\mathbf{R}(g)$

$$\sum_{i,j,k,l} a_{ijkl} q_{ij}(g) p_{kl}(g) = 0 \qquad \begin{matrix} i,j = 1,\ldots,s \\ k,l = 1,\ldots,r \end{matrix}$$

implies $a_{ijkl} = 0$, where $\mathbf{Q}(g) = (q_{ij}(g))$ and $\mathbf{P}(g) = (p_{kl}(g))$. Let g_0 be a fixed

element of G, and n an element of N. Since $\mathbf{Q}(g_0 n) = \mathbf{Q}(g_0)$ we have

$$\sum_{i,j,k,l} a_{ijkl} q_{ij}(g_0) p_{kl}(g_0 n) = 0 \qquad \begin{matrix} i,j = 1,\ldots,s \\ k,l = 1,\ldots,r. \end{matrix}$$

Now $\mathbf{P}(g_0 n) = \mathbf{P}(g_0)\mathbf{S}(n)$, and since there are r^2 linearly independent matrices $\mathbf{S}(n)$ as n ranges over N (by Burnside's lemma), it follows that there are r^2 linearly independent matrices $\mathbf{P}(g_0 n)$. Hence

$$\sum_{i,j} a_{ijkl} q_{ij}(g_0) = 0 \qquad \begin{matrix} i,j = 1,\ldots,s \\ k,l = 1,\ldots,r. \end{matrix}$$

This holds for each g_0 in G, and since $\mathbf{Q}$ is irreducible $a_{ijkl} = 0$. □

Finally we consider the problem of finding all possible ways of embedding an irreducible representation of N over an algebraically closed field in irreducible representations of G (cf. §5 of [Cli 37]).

DEFINITION 4.8 Let N be a normal subgroup of a group G. The irreducible representations $\mathbf{R}$ and $\mathbf{T}$ of G are called *associate* relative to N if $\mathbf{R}_N$ and $\mathbf{T}_N$ have an irreducible component in common.

Consider the associates $\mathbf{R}$ and $\mathbf{T}$ of G relative to N and denote the common irreducible component by $\mathbf{S}$. By theorem 4.2(a), $\mathbf{R}_N$ and $\mathbf{T}_N$ have the same irreducible components, namely the conjugates of $\mathbf{S}$ relative to G. Let U be the group consisting of all elements g in G such that the conjugate $n \mapsto \mathbf{S}^g(n) = \mathbf{S}(g^{-1}ng)$ is similar to $\mathbf{S}$. By theorem 4.2(b) the associates $\mathbf{R}$ and $\mathbf{T}$ can be identified with the induced representations $(\mathbf{R}')^G$ and $(\mathbf{T}')^G$ where $\mathbf{R}'$ and $\mathbf{T}'$ are irreducible representations of U, which contain only components similar to $\mathbf{S}$ on restriction to N. Now fix a definite determination of an irreducible projective representation $\mathbf{P}$ of U such that $\mathbf{P}(n) = \mathbf{S}(n)$ for all $n \in N$. By theorem 4.5 there are irreducible projective representations $\mathbf{Q}_1$ and $\mathbf{Q}_2$ of G/N such that $\mathbf{R}'(u) = \mathbf{Q}_1(u) \otimes \mathbf{P}(u)$ and $\mathbf{T}'(u) = \mathbf{Q}_2(u) \otimes \mathbf{P}(u)$ for all $u \in U$.

Suppose there is an invertible matrix $\mathbf{M}$, such that $\mathbf{Q}_1(u) = \mathbf{M}^{-1}\mathbf{Q}_2(u)\mathbf{M}$ for all $u \in U$. Then $\mathbf{R}'$ and $\mathbf{T}'$ are obviously similar. If, on the other hand, $\mathbf{R}'$ and $\mathbf{T}'$ are similar, then there exists a nonsingular matrix $\mathbf{M}$ such that $\mathbf{Q}_1(u) \otimes \mathbf{P}(u) = \mathbf{M}^{-1}(\mathbf{Q}_2(u) \otimes \mathbf{P}(u))\mathbf{M}$. Thus $\mathbf{Q}_1$ and $\mathbf{Q}_2$ must evidently have the same degree. For elements $n \in N$ we have $\mathbf{I} \otimes \mathbf{S}(n) = \mathbf{M}^{-1}(\mathbf{I} \otimes \mathbf{S}(n))\mathbf{M}$. This means that $\mathbf{M}$ commutes with the matrices $\mathbf{I} \otimes \mathbf{S}(n)$ and so must be of the form $\mathbf{M}' \otimes \mathbf{I}$, where $\mathbf{M}'$ is of course a nonsingular matrix of degree s. Then $\mathbf{Q}_1(u) \otimes \mathbf{P}(u) = \mathbf{M}'^{-1}\mathbf{Q}_2(u)\mathbf{M}' \otimes \mathbf{P}(u)$ which implies $\mathbf{Q}_1(u) = \mathbf{M}'^{-1}\mathbf{Q}_2(u)\mathbf{M}'$ for all $u \in U$.

Therefore two associates of G relative to N differ only in the projective representation of U/N which they determine and they are similar if and only if the latter are similar.

We now describe an algorithm for the calculation of the irreducible representations of finite soluble groups over algebraically closed fields.

A finite group G is soluble if and only if every composition factor G_i/G_{i+1} of a composition series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_l = \langle 1 \rangle$ is cyclic of prime order. Going up a composition series of G one constructs all irreducible representations of G_i from the irreducible representations of G_{i+1}. For describing the passage from G_{i+1} to G_i assume that $N = G_{i+1}$ and $G = G_i$. Let $r = [G : N]$ and let $\mathbf{S}$ be an irreducible representation of N. Let U be the set of all elements g in G such that $n \mapsto \mathbf{S}^g(n) = \mathbf{S}(g^{-1}ng)$ is similar to $\mathbf{S}$. Since N is contained in U and r is a prime, either $U = N$ or $U = G$.

Case (1) : $U = N$. In this case the induced representation $\mathbf{S}^G$ is irreducible by theorem 4.6. The conjugate representations of $\mathbf{S}$ with respect to G induce up to representations similar to $\mathbf{S}^G$ by theorem 4.2.

Case (2) : $U = G$. In this case the representation $\mathbf{S}$ is similar to the conjugate representation $\mathbf{S}^g$ for all $g \in G$. If $t \in G - N$, then $T = \{1, t, \ldots, t^{r-1}\}$

is a transversal for N in G. Choose a nonsingular matrix $\mathbf{P}_t$ such that $\mathbf{P}_t^{-1}\mathbf{S}\mathbf{P}_t = \mathbf{S}^t$ and take $\mathbf{P}_{t^i} = \mathbf{P}_t{}^i$ for $t^i \in T$. For $n \in N$ and $t^i \in T$ define $\mathbf{P}(t^i n) = \mathbf{P}_{t^i}\mathbf{S}(n)$. Then $\mathbf{P}$ is a projective representation satisfying (a), (b) and (c) of lemma 4.4. If $0 \leq i, j < r$ and $i + j < r$, then

$$\mathbf{P}(t^i)\mathbf{P}(t^j) = \mathbf{P}_t{}^i\mathbf{P}_t{}^j = \mathbf{P}_t{}^{i+j} = \mathbf{P}(t^{i+j}).$$

Since $r = [G : N]$, it follows that $t^r \in N$ and therefore $\mathbf{P}_t{}^{-r}\mathbf{S}(n)\mathbf{P}_t{}^r = \mathbf{S}(t^{-r}nt^r) = \mathbf{S}(t^r)^{-1}\mathbf{S}(n)\mathbf{S}(t^r)$ for all $n \in N$. By Schur's lemma $\mathbf{P}_t{}^r = e\mathbf{S}(t^r)$ for some $e \in F^*$. Now, if $0 \leq i, j < r$ and $i + j = r + r' \geq r$, then

$$\begin{aligned}\mathbf{P}(t^i)\mathbf{P}(t^i) = \mathbf{P}_t{}^{i+j} = \mathbf{P}_t{}^r\mathbf{P}_t{}^{r'} = \\ = e\mathbf{S}(t^r)\mathbf{P}(t^{r'}) = e\mathbf{P}(t^{r+r'}) = e\mathbf{P}(t^{i+j}).\end{aligned}$$

Therefore, if α is the factor set of $\mathbf{P}$, then we have

$$\alpha(t^iN, t^jN) = \begin{cases} 1 & i + j < r \\ e & i + j \geq r \end{cases} \qquad 0 \leq i, j < r.$$

Since F is algebraically closed, there is an element $c \in F^*$ such that $c^r = e$. Define another projective representations $\mathbf{P}'$ by $\mathbf{P}'(t^i n) = c^{-i}\mathbf{P}_t{}^i\mathbf{S}(n)$ for all $n \in N$ and $t^i \in T$. If α' is the factor set of $\mathbf{P}'$, then we have

$$\alpha(t^iN, t^jN) = 1 \qquad 0 \leq i, j < r.$$

This shows that every projective representation of a cyclic group can be normalised into an ordinary one. Moreover, every irreducible representation $\mathbf{Q}$ of G/N is of degree one. $\mathbf{Q}(g)$ is a r^{th} root of unity for each $g \in G$ and its value depends only on the coset of G mod N in which g lies. Therefore by theorem 4.7 and the discussion on associates every irreducible representation of G which contains a component similar to $\mathbf{S}$ on restriction to N is similar to a representation $\mathbf{R}$ defined by

$$\mathbf{R}(t^i n) = c^i\mathbf{P}_t{}^i\mathbf{S}(n)$$

for $t^i \in T$ and $n \in N$, where c is a r^{th} root of e. The number of distinct associates is 1 if r is the characteristic of F and r otherwise.

EXAMPLE Let $G = \langle a, b \rangle$ be the alternating group of degree four with the defining relations $a^2 = b^3 = (ab)^3 = 1$. Let $x = a$ and $y = b^{-1}xb$. Then $N = \langle x, y \rangle$ is an abelian normal subgroup of index 3 in G. The irreducible representations of N over the field of complex numbers are defined by

$$\begin{aligned} x &\mapsto 1, \quad y \mapsto 1; \\ x &\mapsto 1, \quad y \mapsto -1; \\ x &\mapsto -1, \quad y \mapsto 1; \\ x &\mapsto -1, \quad y \mapsto -1. \end{aligned}$$

Let $\mathbf{S}$ be the trivial representation of N. Then $\mathbf{S}$ is obviously similar to the conjugate representation $\mathbf{S}^g$ for all $g \in G$. Therefore Case (2) applies. Choose $\{1, b, b^2\}$ as a transversal for N in G. Choose $\mathbf{P}_b = 1$ and define a projective representation as outlined in the description above. Obviously $e = 1$ and the irreducible representations of G which contain a component similar to $\mathbf{S}$ on restriction to N are similar to the representations defined by

$$\begin{aligned} a &\mapsto 1, \quad b \mapsto 1; \\ a &\mapsto 1, \quad b \mapsto c; \\ a &\mapsto 1, \quad b \mapsto c^2, \end{aligned}$$

where c is a third root of unity.

Now, let $\mathbf{S}$ be the representation defined by $x \mapsto 1, y \mapsto -1$. Then $\mathbf{S}^b(x) = -1, \mathbf{S}^b(y) = -1, \mathbf{S}^{b^2}(x) = -1$ and $\mathbf{S}^{b^2}(y) = 1$. Hence Case (1) applies and the induced representation defined by

$$\mathbf{S}^G(a) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$\mathbf{S}^G(b) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

is an irreducible representation of G.

4.2 Extension of the Ground Field

So far in this chapter our attention was restricted almost exclusively to irreducible representations and modules over algebraically closed fields. In this section we consider irreducible representations over arbitrary fields. We study the behaviour of an irreducible representation of a group under extension of the ground field. In particular, if E/F is a field extension we explore the connection between the irreducible E-representations and F-representations of a group. The emphasis is on representations over finite fields and algorithms for computations with representations over finite fields.

This section is based on chapter 9 of [Isa 76] and begins with an introduction of the concepts of absolutely irreducible representations and splitting fields. We shall see that an algebraically closed field is a splitting field for every group and therefore the irreducible representations of a group over an algebraically closed field are absolutely irreducible. Thereafter we study the irreducible representations of a group over splitting fields and their extensions. We are led in a natural way to the question whether an absolutely irreducible representation is realisable over smaller fields. In prime characteristic, we shall see that some finite field is a splitting field for a group. Moreover, we prove that an absolutely irreducible representation $\mathbf{R}$ of a group G over a field $E \supseteq F$ of prime characteristic is realisable over the field generated by F and the character values $\chi(g)$ for all $g \in G$ where χ is the character afforded by $\mathbf{R}$ and describe an algorithm for the realisation of representations over smaller finite fields. After the introduction of the concept of

Galois conjugacy of characters we investigate the structure of an irreducible representation under extension of the ground field. We show that the representation is completely reducible; that all irreducible constituents occur with equal multiplicity and that the characters of the constituents constitute a Galois conjugacy class. As a consequence we shall see that an irreducible representation over a finite field may be described in terms of its absolutely irreducible constituents and describe an algorithm for the calculation of an absolutely irreducible constituent of an irreducible representation over a finite field.

Let $F \subseteq E$ and $\mathbf{R}$ be an F-representation of a group G. Then $\mathbf{R}$ maps G into a group of nonsingular matrices over F that are also nonsingular over E. Therefore $\mathbf{R}$ may be viewed as an E-representation of G. As such it will be denoted by $\mathbf{R}^E$. If $\mathbf{R}^E$ is irreducible, then clearly so is $\mathbf{R}$. However, $\mathbf{R}^E$ may well reduce, even if $\mathbf{R}$ is irreducible. To illustrate what can happen, let $G = \langle g \rangle$ be cyclic of order 3 and let $\mathbf{R}$ be the representation over the rational numbers defined by

$$\mathbf{R}(g) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

If E is the third cyclotomic field over the rational numbers, then $\mathbf{R}^E$ affords the character $\lambda + \lambda^{-1}$, where λ is a faithful linear character of G and so $\mathbf{R}^E$ is reducible.

DEFINITION 4.9 Let $\mathbf{R}$ be a representation of G over F. Then $\mathbf{R}$ is *absolutely irreducible* if $\mathbf{R}^E$ is irreducible for every field $E \supseteq F$.

We have already seen that an irreducible representation need not be absolutely irreducible. It is of importance, therefore, to obtain necessary and sufficient conditions for absolutely irreducibility.

THEOREM 4.10 Let $\mathbf{R}$ be an irreducible F-representation of degree n. Then the following assertions are equivalent :

(a) $\mathbf{R}$ is absolutely irreducible.

(b) $\mathbf{R}^E$ is irreducible for every finite degree extension E/F.

(c) The centraliser of $\mathbf{R}(G)$ in the matrix ring $M_n(F)$ of $n \times n$-matrices over F consists of scalar matrices.

(d) $\mathbf{R}(F[G]) = M_n(F)$.

Proof See theorem 9.2 of [Isa 76] for the details. □

DEFINITION 4.11 The field F is a *splitting field* for G if every irreducible F-representation of G is absolutely irreducible.

COROLLARY 4.12 (cf. corollary 9.4 of [Isa 76]) If F is an algebraically closed field, then F is a splitting field for every group.

Proof Since F has no proper finite degree extension, condition (b) of theorem 4.10 holds for every irreducible F-representation of G. □

Suppose F is a splitting field for G and $E \supseteq F$. Then every irreducible F-representation $\mathbf{R}$ determines an irreducible E-representation $\mathbf{R}^E$. A natural question is : If $\{\mathbf{R}_i\}$ is a set of representatives for the similarity classes of irreducible F-representations of G, is $\{\mathbf{R}_i{}^E\}$ a complete set of representatives for the irreducible E-representations of G ? In order to prove this, we need to discuss the irreducible constituents of possibly reducible representations.

If V is an $F[G]$-module, then a composition series for V is a chain of submodules $V = V_n > \ldots > V_1 > V_0 = 0$ such that each V_i/V_{i-1} is an irreducible module. The modules V_i/V_{i-1} are the factors of the series. The Jordan-Hölder theorem asserts that the factors of any two composition series for V are the same up to

isomorphism. If $\mathbf{R}$ is an F-representation of G corresponding to the $F[G]$-module V, then $\mathbf{R}$ is similar to a representation $\mathbf{T}$ in triangular block form

$$\mathbf{T}(g) = \begin{pmatrix} \mathbf{T}_1(g) & & * \\ & \ddots & \\ 0 & & \mathbf{T}_n(g) \end{pmatrix}$$

where the irreducible representations $\mathbf{T}_i$ correspond to the factors V_i/V_{i-1}. The matrices $\mathbf{T}(g)$ have zeros below the blocks on the main diagonal but may have nonzero entries above the diagonal blocks. Representations similar to the $\mathbf{T}_i$ are the irreducible constituents of $\mathbf{R}$. By the Jordan-Hölder theorem, the representation $\mathbf{R}$ has only finitely many irreducible constituents (up to similarity), namely those which appear in any single triangular representation similar to $\mathbf{R}$.

COROLLARY 4.13 (cf. corollary 9.5 of [Isa 76]) Let F be a field and G a group. Then

(a) Every irreducible $F[G]$-module is isomorphic to a factor module of the regular $F[G]$-module.

(b) There exist only finitely many similarity classes of irreducible F-representations of G.

(c) If $E \supseteq F$ and $\mathbf{T}$ is an irreducible E-representation of G, then $\mathbf{T}$ is a constituent of $\mathbf{R}^E$ for some irreducible F-representation $\mathbf{R}$.

Proof Statement (a) is immediate and statement (b) follows from (a) via the Jordan-Hölder theorem. Let $\mathbf{U}$ be any F-representation of G. The irreducible constituents of $\mathbf{U}^E$ may be found by taking the irreducible constituents $\mathbf{R}_i$ of $\mathbf{U}$ and then finding the irreducible constituents of the $\mathbf{R}_i{}^E$. Now (c) follows by applying this remark to the regular F-representation. □

The following result is a useful tool for establishing the similarity of two F-representations of G and for other purposes.

THEOREM 4.14 (cf. theorem 9.6 of [Isa 76]) Let $\mathbf{R}$ be an irreducible representation of $F[G]$ and let a be an element of $F[G]$. Then there exists b in $F[G]$ such that $\mathbf{R}(b) = \mathbf{R}(a)$ and $\mathbf{T}(b) = 0$ for every irreducible $F[G]$-representation $\mathbf{T}$ which is not similar to $\mathbf{R}$.

Proof Let $\{\mathbf{R}_i\}$ be a set of representatives for the similarity classes of irreducible $F[G]$-representations. Denote the Jacobson radical of $F[G]$ by $J(F[G])$. Let $A = F[G]/J(F[G])$, so that each $\mathbf{R}_i$ may be viewed as a representation of the algebra A. As such, the $\mathbf{R}_i$ are irreducible and pairwise nonsimilar. Since $J(A) = 0$, A is semisimple and therefore has minimal ideals M_i, such that $\mathbf{R}_j(M_i) = 0$ if $j \neq i$ and $\mathbf{R}_i(M_i) = \mathbf{R}_i(A) = \mathbf{R}_i(F[G])$. Now suppose $\mathbf{R} = \mathbf{R}_1$ and choose b in the preimage of M_1 in $F[G]$ with $\mathbf{R}(b) = \mathbf{R}(a)$. □

COROLLARY 4.15 (cf. corollary 9.7 of [Isa 76]) Let $\mathbf{R}$ and $\mathbf{T}$ be irreducible F-representations of G. Suppose $F \subseteq E$ and that $\mathbf{R}^E$ and $\mathbf{T}^E$ have a common irreducible constituent. Then $\mathbf{R}$ is similar to $\mathbf{T}$.

Proof Let $\mathbf{U}$ be an irreducible constituent of $\mathbf{R}^E$ and $\mathbf{T}^E$. If $\mathbf{R}$ and $\mathbf{T}$ are not similar, view them as representations of $F[G]$ and choose $b \in F[G]$ with $\mathbf{R}(b) = \mathbf{R}(1)$ and $\mathbf{T}(b) = 0$. Hence $\mathbf{U}(b)$ is an identity matrix and $\mathbf{U}(b) = 0$. This contradiction proves the result. □

COROLLARY 4.16 (cf. corollary 9.8 of [Isa 76]) Let F be a splitting field for G and let $\{\mathbf{R}_i\}$ be a set of representatives for the similarity classes of irreducible F-representations. If $E \supseteq F$, then E is a splitting field and $\{\mathbf{R}_i{}^E\}$ is a set of representatives for the irreducible E-representations of G.

Proof Since the $\mathbf{R}_i$ are absolutely irreducible, the $\mathbf{R}_i{}^E$ are absolutely irreducible. They are pairwise nonsimilar by corollary 4.15. Suppose $\mathbf{T}$ is any irreducible E-representation. By corollary 4.13(c), $\mathbf{T}$ is a constituent of $\mathbf{R}_i{}^E$ for some i. Since $\mathbf{R}_i{}^E$ is irreducible, it is similar to $\mathbf{T}$ and the proof is complete. □

Let $\mathbf{R}$ be a E-representation of G. Then $\mathbf{R}$ is said to be realisable in $F \subseteq E$ if there exists a F-representation $\mathbf{T}$ of G such that $\mathbf{R}$ is similar to $\mathbf{T}^E$. We can characterise splitting fields in terms of the concept of realisability as follows.

THEOREM 4.17 (cf. theorem 9.9 of [Isa 76]) Let E be a splitting field for G and let $F \subseteq E$. Then F is a splitting field if and only if every irreducible E-representation of G is similar to $\mathbf{T}^E$ for some F-representation $\mathbf{T}$.

Proof Suppose F is a splitting field. Then by corollary 4.16 every irreducible E-representation is as described. Conversely, let $\mathbf{U}$ be any irreducible F-representation and let $\mathbf{R}$ be an irreducible constituent of $\mathbf{U}^E$. By hypothesis, there exists an irreducible F-representation $\mathbf{T}$, such that $\mathbf{T}^E$ is similar to $\mathbf{R}$ and hence $\mathbf{T}^E$ and $\mathbf{U}^E$ have an irreducible constituent in common. By corollary 4.15, $\mathbf{T}$ is similar to $\mathbf{U}$, and thus $\mathbf{U}^E$ is absolutely irreducible. It follows that $\mathbf{U}$ is absolutely irreducible since the only F-matrices which centralise all $\mathbf{U}(g)$ are scalar. □

COROLLARY 4.18 (cf. corollary 9.10 of [Isa 76]) Let F be any field and G a group. Then some finite degree extension of F is a splitting field for G.

Proof Let $\overline{F}$ be the algebraic closure of F, so that $\overline{F}$ is a splitting field. Let $\{\mathbf{R}_i\}$ be a set of representatives for the similarity classes of irreducible $\overline{F}$-representations. By corollary 4.13(b), $|\{\mathbf{R}_i\}| < \infty$ and hence only finitely many elements of $\overline{F}$ occur as entries in any of the matrices $\mathbf{R}_i(g)$ for $g \in G$. Adjoin all of these elements to F so as to obtain the field E. Since $\overline{F}$ is algebraic over F, it follows that $[E : F] < \infty$. Since each $\mathbf{R}_i$ may be viewed as an E-representation of G, it follows from theorem 4.17 that E is a splitting field. □

Suppose now that E is an arbitrary extension field of F. Let $\mathbf{R}$ be an E-representation of G and let χ be the character of $\mathbf{R}$. Denote the extension field of F generated by the elements $\{\chi(g) | g \in G\}$ by $F(\chi)$. Then $F(\chi)$ is a finite algebraic

extension field of F, since each $\chi(g)$ is a sum of roots of unity. Moreover, if $\mathbf{R}$ is realisable in F, then $F(\chi) = F$. As the Quaternion group of order 8 will show $\mathbf{R}$ need not be realisable in F if $F(\chi) = F$.

EXAMPLE Let $G = \langle a, b \rangle$ be the Quaternion group of order 8 with the defining relations $b^{-1}ab = a^{-1}, a^4 = 1, b^2 = a^2$. Consider the irreducible representation $\mathbf{R}$ over the field of complex numbers defined by

$$\mathbf{R}(a) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$$

and

$$\mathbf{R}(b) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

where ε is a fourth root of unity in the field of complex numbers. Let $\mathbf{R}$ afford the character χ. The elements $1, a^2, a, b, ba$ are representatives of the conjugate classes of G and $\chi(1) = -\chi(a^2) = 2, \chi(a) = \chi(b) = \chi(ab) = 0$. Suppose $\mathbf{R}$ is realisable in the field of rational numbers. For a suitable basis,

$$\mathbf{R}(1) = \mathbf{I}, \quad \mathbf{R}(a^2) = -\mathbf{I}, \quad \mathbf{R}(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

can be assumed. From $ab = ba^{-1}$, it follows that

$$\mathbf{R}(b) = \begin{pmatrix} x & y \\ y & -x \end{pmatrix}.$$

Then $b^2 = a^2$ implies that $x^2 + y^2 = -1$, which is impossible for rational numbers x and y. Therefore $\mathbf{R}$ is not realisable in the field of rational numbers.

The next theorem asserts that $\mathbf{R}$ is realisable in a field F of prime characteristic if $F(\chi) = F$. We shall need the following lemmas.

LEMMA 4.19 (cf. lemma 9.12 of [Isa 76]) Let E be a splitting field for G. Then the characters of nonsimilar irreducible E-representations of G are nonzero, distinct and linearly independent over E.

Proof Let $\mathbf{R}_i$ be a set of representatives for the similarity classes of irreducible E-representations, and let χ_i be the character afforded by $\mathbf{R}_i$. View χ_i as being defined on all of $E[G]$. Since $\mathbf{R}_i(E[G])$ is a full matrix ring over E by theorem 4.10, $a_i \in E[G]$ may be chosen such that $\chi_i(a_i) = 1$. By theorem 4.14 $\chi_j(a_i) = 0$ may be assumed for $i \neq j$. The result is now immediate. □

This result is actually true without the assumption that E is a splitting field. The more general fact will be proved later (cf. corollary 4.29). If E is a splitting field for G, the notation $Irr_E(G)$ is used to denote the set of characters of the absolutely irreducible E-representations of G.

Let E be any field, σ an automorphism of E, and $\mathbf{R}$ an E-representation of G. The automorphism σ can be applied to every entry in the matrix $\mathbf{R}(g)$ for every $g \in G$. What results is a new representation, denoted $\sigma\mathbf{R}$.

LEMMA 4.20 Let E/F be a finite Galois extension and let $G = Gal(E/F)$. Let $\alpha : G \rightarrow GL_n(E)$ such that $\alpha(gh) = g\alpha(h)\alpha(g)$ for $g, h \in G$. Then there exists $\mathbf{X} \in GL_n(E)$ such that $\alpha(g) = g\mathbf{X}^{-1}\mathbf{X}$ for all $g \in G$.

Proof (cf. proposition X 1.3 of *Corps Locaux* by J. P. Serre) Let $\mathbf{M} \in M_n(E)$ and define $\mathbf{X} = \sum_{g \in G} g\mathbf{M}\alpha(g)$. Then $g\mathbf{X} = \mathbf{X}\alpha(g)^{-1}$ and α is as required if $\mathbf{M}$ can be chosen such that $\mathbf{X}$ is invertible.

Let m be an element of the row vector space E^n of dimension n over E and form $x(m) = \sum_{g \in G} gm\alpha(g)$. The elements $x(m), m \in E^n$, generate E^n : Let $\vartheta \in Hom(E^n, E)$ such that $0 = \vartheta(x(m))$ for all $m \in E^n$. If $e \in E$, then

$$0 = \vartheta(x(em)) = \vartheta(\sum_{g \in G} g(em)\alpha(g)) = \sum_{g \in G} ge\vartheta(gm\alpha(g)).$$

By Dedekind's Independence Theorem $\vartheta(gm\alpha(g)) = 0$ and since $\alpha(g)$ is invertible it follows that $\vartheta = 0$.

Let $w_1, \ldots, w_n \in E^n$ such that $\{y_1 = x(w_1), \ldots, y_n = x(w_n)\}$ is linearly independent over E. Let $\mathbf{M}$ be the matrix of the homomorphism defined by $v_i \mapsto w_i$

where $\{v_1, \ldots, v_n\}$ is the canonical base for E^n. Now calculate the matrix $\mathbf{X}$ as described above. Apparently

$$v_i\mathbf{X} = v_i(\sum_{g\in G} g\mathbf{M}\alpha(g)) = \sum_{g\in G} v_i g\mathbf{M}\alpha(g) = \sum_{g\in G} gw_i\alpha(g) = y_i$$

and therefore $\mathbf{X}$ is invertible. □

THEOREM 4.21 (cf. theorem 9.14 of [Isa 76]) Let $\mathbf{R}$ be an absolutely irreducible E-representation of G, where E is of prime characteristic. Suppose that $\mathbf{R}$ affords the character χ and that $\chi(g)\in F$ for all $g\in G$, where $F\subseteq E$. Then $\mathbf{R}$ is similar to $\mathbf{T}^E$ for some absolutely irreducible F-representation $\mathbf{T}$.

Proof First consider the case that $|E| < \infty$. Denote the Galois group $Gal(E/F)$ by A. If $\eta\in A$, then $\mathbf{R}$ and $\eta\mathbf{R}$ afford the same character and are therefore similar by lemma 4.19. Hence there exist nonsingular matrices $\mathbf{P}(\eta)$ such that $\eta\mathbf{R}(g) = \mathbf{P}(\eta)\mathbf{R}(g)\mathbf{P}(\eta)^{-1}$ for all $g\in G$ and all $\eta\in A$. For $\eta_1, \eta_2\in A$ we have

$$\mathbf{P}(\eta_1\eta_2)\mathbf{R}(g)\mathbf{P}(\eta_1\eta_2)^{-1} = \eta_1(\mathbf{P}(\eta_2)\mathbf{R}(g)\mathbf{P}(\eta_2)^{-1}) =$$
$$= \eta_1\mathbf{P}(\eta_2)\eta_1\mathbf{R}(g)\eta_1\mathbf{P}(\eta_2)^{-1} = \eta_1\mathbf{P}(\eta_2)\mathbf{P}(\eta_1)\mathbf{R}(g)\mathbf{P}(\eta_1)^{-1}\eta_1\mathbf{P}(\eta_2)^{-1}.$$

By theorem 4.10(c), $\eta_1\mathbf{P}(\eta_2)\mathbf{P}(\eta_1) = \alpha(\eta_1, \eta_2)\mathbf{P}(\eta_1\eta_2)$ for some $\alpha(\eta_1, \eta_2)\in E^*$. From $\mathbf{P}((\eta_1\eta_2)\eta_3) = \mathbf{P}(\eta_1(\eta_2\eta_3))$, it follows that

$$\alpha(\eta_1\eta_2, \eta_3)\alpha(\eta_1, \eta_2) = \alpha(\eta_1, \eta_2\eta_3)\eta_1\alpha(\eta_2, \eta_3).$$

Hence $\alpha\in Z^2(A, E^*)$, where A acts naturally on E^*. If $\mathbf{P}'(\eta)$ are other matrices such that $\eta\mathbf{R}(g) = \mathbf{P}'(\eta)\mathbf{R}(g)\mathbf{P}'(\eta)^{-1}$ for all $g\in G$ and all $\eta\in A$, then $\mathbf{P}'(\eta) = \mu(\eta)\mathbf{P}(\eta)$ for some $\mu : A \to E^*$ and the factor set α' determined by $\mathbf{P}'$ is

$$(\eta_1, \eta_2) \mapsto \alpha'(\eta_1, \eta_2) = \alpha(\eta_1, \eta_2)\eta_1\mu(\eta_2)\mu(\eta_1)\mu(\eta_1\eta_2)^{-1}.$$

Therefore the representation $\mathbf{R}$ determines an element $\alpha B^2(A, E^*)$ of the cohomology group $H^2(A, E^*)$. By Satz I.16.10 of [Hup 67] the cohomology group $H^2(A, E^*) = 1$. Hence the matrices $\mathbf{P}(\eta)$ can be chosen such that $\mathbf{P}(\eta_1\eta_2) =$

$\eta_1\mathbf{P}(\eta_2)\mathbf{P}(\eta_1)$. By lemma 4.20 there exists $\mathbf{X}\in GL_n(E)$ such that $\mathbf{P}(\eta) = \eta\mathbf{X}^{-1}\mathbf{X}$ for all $\eta\in A$. It follows that

$$\eta(\mathbf{X}\mathbf{R}(g)\mathbf{X}^{-1}) = \eta\mathbf{X}\eta\mathbf{R}(g)\eta\mathbf{X}^{-1} =$$
$$= \eta\mathbf{X}\mathbf{P}(\eta)\mathbf{R}(g)\mathbf{P}(\eta)^{-1}\eta\mathbf{X}^{-1} = \mathbf{X}\mathbf{R}(g)\mathbf{X}^{-1}.$$

Hence $\mathbf{T} = \mathbf{X}\mathbf{R}\mathbf{X}^{-1}$ is the desired representation of G over F.

Finally consider the case where E may be infinite. Since E may be replaced by a larger field, it is no loss to assume that E is algebraically closed. Let $K\subseteq E$ be the prime field and let $L\supseteq K$ be a splitting field with $[L : K] < \infty$ by corollary 4.18. Since E is algebraically closed, assume $L\subseteq E$. Since L is a splitting field, $\mathbf{R}$ is similar to $\mathbf{U}^E$ for some L-representation $\mathbf{U}$ and $\mathbf{U}$ affords χ which takes values in $L\cap F$. Since $|L| < \infty$, the first part of the proof yields an absolutely irreducible $(L\cap F)$-representation $\mathbf{T}$ such that $\mathbf{T}^L$ is similar to $\mathbf{U}$ and hence $\mathbf{T}^E$ is similar to $\mathbf{R}$. Now $\mathbf{T}^F$ is the desired F-representation. □

The proof for the case $|E| < \infty$ is actually an application of the remark V.14.14 of [Hup 67], p.548. The idea can be traced back to an article by A. Speiser (cf. [Spe 19]). The following algorithm for finding a conjugating matrix $\mathbf{X}$ is due to S. P. Glasby and R. B. Howlett. The description given here follows unpublished notes and written communication with Glasby and Howlett.

Let $\mathbf{R}$ be an absolutely irreducible E-representation of G, where $E = F_{q^r}$ is the field with q^r elements. Suppose $\mathbf{R}$ affords the character χ and that $\chi(g)\in F = F_q$, the field with q elements, for all $g\in G$. The Galois group $Gal(E/F)$ is generated by the automorphism $\eta : x \mapsto x^q$. The representations $\mathbf{R}$ and $\eta\mathbf{R}$ afford the same character and are therefore similar. Let $\mathbf{Z}$ be a matrix over E such that $\eta\mathbf{R}(g) = \mathbf{Z}\mathbf{R}(g)\mathbf{Z}^{-1}$ for all $g\in G$ and define

$$\mathbf{P}(\eta^i) = \begin{cases} \mathbf{I} & i = 0 \\ \eta^{i-1}\mathbf{Z}\cdots\eta\mathbf{Z}\mathbf{Z} & 0 < i\leq r-1. \end{cases}$$

If $0 \leq i, j < r$ and $i + j < r$, then

$$\eta^i \mathbf{P}(\eta^j)\mathbf{P}(\eta^i) = \mathbf{P}(\eta^{i+j}).$$

Since η has order r, it follows that

$$\mathbf{R}(g) = \eta^r \mathbf{R}(g) = \eta^{r-1}\mathbf{Z} \cdots \eta \mathbf{Z}\mathbf{Z}\mathbf{R}(g)\mathbf{Z}^{-1}\eta\mathbf{Z}^{-1} \cdots \eta^{r-1}\mathbf{Z}^{-1}$$

for all $g \in G$. Since $\mathbf{R}$ is absolutely irreducible, there exists a nonzero scalar $f \in E$ such that $\eta^{r-1}\mathbf{Z} \cdots \eta\mathbf{Z}\mathbf{Z} = f\mathbf{I}$. Now, if $0 \leq i, j < r$ and $i + j = r + r' \geq r$, then

$$\eta^i \mathbf{P}(\eta^j)\mathbf{P}(\eta^i) = \eta^{r'-1}\mathbf{Z} \cdots \eta\mathbf{Z}\mathbf{Z}f = \mathbf{P}(\eta^{r'})f = \mathbf{P}(\eta^{r+r'})f = \mathbf{P}(\eta^{i+j})f.$$

Therefore, if α is the factor set of $\mathbf{P}$, then

$$\alpha(\eta^i, \eta^j) = \begin{cases} 1 & i + j < r \\ f & i + j \geq r \end{cases} \qquad 0 \leq i, j < r.$$

Next, we will show that $f \in F$. By theorem 4.21 there is a representation $\mathbf{R}'$ over F such that $\mathbf{Y}\mathbf{R}\mathbf{Y}^{-1} = \mathbf{R}'$ for some nonsingular matrix $\mathbf{Y}$. Hence

$$\begin{aligned} \eta\mathbf{R}(g) &= \eta\mathbf{Y}^{-1}\eta\mathbf{R}'(g)\eta\mathbf{Y} = \\ &= \eta\mathbf{Y}^{-1}\mathbf{Y}\mathbf{R}(g)\mathbf{Y}^{-1}\eta\mathbf{Y} = \eta\mathbf{Y}^{-1}\mathbf{Y}\mathbf{R}(g)(\eta\mathbf{Y}^{-1}\mathbf{Y})^{-1} \end{aligned}$$

for all $g \in G$. Then $\eta^{r-1}(\eta\mathbf{Y}^{-1}\mathbf{Y}) \cdots \eta(\eta\mathbf{Y}^{-1}\mathbf{Y})\eta\mathbf{Y}^{-1}\mathbf{Y} = \eta^r\mathbf{Y}^{-1}\mathbf{Y} = \mathbf{I}$ and therefore $f = 1$ can be assumed. Suppose $\mathbf{Z}'$ is another matrix such that $\eta\mathbf{R}(g) = \mathbf{Z}'\mathbf{R}(g)\mathbf{Z}'^{-1}$ for all $g \in G$, then $\mathbf{Z}' = a\mathbf{Z}$ for some $a \in E$. Then

$$f' = \eta^{r-1}\mathbf{Z}' \cdots \eta\mathbf{Z}'\mathbf{Z}' = \eta^{r-1}a \cdots \eta a a \eta^{r-1}\mathbf{Z} \cdots \eta\mathbf{Z}\mathbf{Z} = N_{E/F}(a)f.$$

Hence f' is a F-multiple of f and therefore $f \in F$.

Let $b \in E$ such that $N_{E/F}(b) = f^{-1}$ and define

$$\mathbf{P}'(\eta^i) = \begin{cases} \mathbf{I} & i = 0 \\ \eta^{i-1}(b\mathbf{Z}) \cdots \eta(b\mathbf{Z})b\mathbf{Z} & 0 < i \leq r - 1. \end{cases}$$

If α' is the factor set of $\mathbf{P}'$, then $\alpha'(\eta^i, \eta^j) = 1$ for $0 \leq i, j < r$ and $i + j < r$. If $0 \leq i, j < r$ and $i + j = r + r' \geq r$, then

$$\eta^i \mathbf{P}'(\eta^j)\mathbf{P}'(\eta^i) = \eta^{r'-1}\mathbf{Z} \cdots \eta \mathbf{Z}\mathbf{Z} f \eta^{r'-1} b \cdots \eta b b N_{E/F}(b) =$$
$$= \eta^{r'-1}(b\mathbf{Z}) \cdots \eta(b\mathbf{Z})b\mathbf{Z} = \mathbf{P}'(\eta^{r'}) = \mathbf{P}'(\eta^{r+r'}) = \mathbf{P}'(\eta^{i+j}).$$

It follows from lemma 4.20 that there is a matrix $\mathbf{X}$ over E such that

$$\eta \mathbf{X} b \mathbf{Z} = \mathbf{X}. \qquad (*)$$

This equation may be viewed as a system of homogeneous linear equations over F. Since the dimension of E over F is r, finding $\mathbf{X}$ is equivalent to solving rn^2 homogeneous linear equations in rn^2 unknowns where n is the degree of the representation $\mathbf{R}$. Choose an invertible matrix $\mathbf{X}$ from the space of solutions, then $\mathbf{X}$ has the desired properties. The number of $\mathbf{X}$ satisfying $(*)$ is the number of $n \times n$ matrices over F, namely q^{n^2} : Suppose that $\mathbf{X}$ and $\mathbf{Y}$ satisfy $(*)$ where $\mathbf{X}$ is invertible, then $\eta(\mathbf{Y}\mathbf{X}^{-1}) = \eta\mathbf{Y}\eta\mathbf{X}^{-1} = \mathbf{Y}\mathbf{Z}^{-1}b^{-1}\eta\mathbf{X}^{-1} = \mathbf{Y}\mathbf{X}^{-1}$ and therefore $\mathbf{M} = \mathbf{Y}\mathbf{X}^{-1}$ is a matrix over F. Hence any solution $\mathbf{Y} = \mathbf{M}\mathbf{X}$ for some $\mathbf{M}$ over F. Conversely if $\mathbf{Y}$ is any matrix over F and $\mathbf{X}$ satisfies $(*)$, then $\mathbf{Y}\mathbf{X}$ also satisfies $(*)$ because $\eta(\mathbf{Y}\mathbf{X})b\mathbf{Z} = \eta\mathbf{Y}\eta\mathbf{X}b\mathbf{Z} = \mathbf{Y}\mathbf{X}$.

The size of the system of homogeneous linear equations can be reduced by the following observation. Elements of E may be regarded as r-tuples over F, and therefore $\mathbf{X}$ is effectively a $n \times rn$ matrix over F. Each row x of $\mathbf{X}$ has to satisfy $\eta x b \mathbf{Z} = x$. This is a system of rn homogeneous linear equations in rn unknowns : Let $(e_1, \ldots, e_r)$ be a basis of E over F and let $e = \sum_{l=1}^{r} c_l(e)e_l$ be the unique representation of $e \in E$. If $\mathbf{Z} = (z_{ij})$, then the equation $\eta x b \mathbf{Z} = x$ yields n equations in n unknowns $\sum_{k=1}^{n} \eta x_k b z_{ki} = x_i$ for $i = 1, \ldots, n$. If $x_k = \sum_{j=1}^{r} x_{kj}e_j$, where the x_{kj} are regarded as unknowns, then

$$\sum_{k=1}^{n} \eta x_k b z_{ki} = \sum_{k=1}^{n} \eta(\sum_{j=1}^{n} x_{kj}e_j)bz_{ki} =$$
$$= \sum_{k=1}^{n}\sum_{j=1}^{r} x_{kj}\eta(e_j)bz_{ki} = \sum_{l=1}^{r}\sum_{k=1}^{n}\sum_{j=1}^{r} c_l(\eta(e_j)bz_{ki})x_{kj}e_l.$$

Hence the equation $\eta x b \mathbf{Z} = x$ yields the equations

$$\sum_{k=1}^{n}\sum_{j=1}^{r} c_l(\eta(e_j)bz_{ki})x_{kj} = x_{il}$$

for $l = 1, \ldots, r$ and $i = 1, \ldots, n$.

If its space of solutions has dimension m, then the original system will have dimension mn. So $mn = n^2$ and therefore $m = n$. Now, if $(v_1, \ldots, v_n)$ is a base for this space of solutions then the $n \times rn$ matrix $\mathbf{X}$ having $v_1, \ldots, v_n$ as its rows will have rank n. It remains to show that it has rank n when viewed as a matrix over E. Since the F-rank is n, the only vector y over F satisfying $y\mathbf{X} = 0$ is $y = 0$. But $\mathbf{X} = \mathbf{M}\mathbf{X}'$ where $\mathbf{X}'$ is invertible and $\mathbf{M}$ has entries in F. If $\mathbf{M}$ were not invertible, then the nullspace of $\mathbf{X}$ over F would clearly be nonzero. So $\mathbf{M}$ is invertible and therefore $\mathbf{X}$ is too.

EXAMPLE Let $G = \langle a, b \rangle$ be the dihedral group of order 10 with the defining relations $a^5 = b^2 = (ab)^2 = 1$. The field $E = F_{2^4}$ of order 2^4 is the 15^{th} cyclotomic field over F_2. The 15^{th} cyclotomic polynomial $Q_{15}(x) = x^8+x^7+x^5+x^4+x^3+x+1$ and $Q_{15}(x) = (x^4+x+1)(x^4+x^3+1)$ is the decomposition of Q_{15} into irreducible factors in $F_2[x]$. Let z be a root of $x^4 + x + 1$. Then z is a primitive 15^{th} root of unity over F_2. Consider the representation $\mathbf{S}$ of $\langle a \rangle$ over E defined by $\mathbf{S}(a) = z^3$. By theorem 4.6 the representation $\mathbf{R} = \mathbf{S}^G$ is irreducible and

$$\mathbf{R}(a) = \mathbf{S}^G(a) = \begin{pmatrix} z^3 & 0 \\ 0 & z^{12} \end{pmatrix}$$

$$\mathbf{R}(b) = \mathbf{S}^G(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

There are four conjugate classes in G, which are given by $C_1 = \{1\}, C_b = \{b, ba, ba^2, ba^3, ba^4\}, C_a = \{a, a^4\}, C_{a^2} = \{a^2, a^3\}$. The values of the character of $\mathbf{R}$ are given by the following table.

C_1	C_b	C_a	C_{a^2}
0	0	z^{10}	z^5

Obviously the character has values in $F_2(z^5)$ which is the field of order four. Hence $\mathbf{R}$ is realisable over $F = F_{2^2}$. The Galois group $Gal(E/F)$ is generated by the automorphism $\eta : x \mapsto x^4$ and $(1, z)$ is a base of E over F.

$$\mathbf{Z} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is a matrix over E such that $\eta\mathbf{R}(g) = \mathbf{Z}\mathbf{R}(g)\mathbf{Z}^{-1}$ for all $g \in G$. We obtain $f\mathbf{I} = \eta\mathbf{Z}\mathbf{Z} = \mathbf{Z}^2 = \mathbf{I}$ and it follows that $f = 1$. This gives the following system of homogeneous linear equations

$$\begin{pmatrix} x_{11}, & x_{12}, & x_{21}, & x_{22} \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} x_{11}, & x_{12}, & x_{21}, & x_{22} \end{pmatrix}.$$

Then $((1,1,0,1),(1,0,1,0))$ is a base for the space of solutions and

$$\mathbf{X} = \begin{pmatrix} z^4 & z \\ 1 & 1 \end{pmatrix}$$

satisfies $\eta\mathbf{X}\mathbf{Z} = \mathbf{X}$. Then $g \mapsto \mathbf{X}\mathbf{R}(g)\mathbf{X}^{-1}$ is a representation over F since

$$\mathbf{X}\mathbf{R}(a)\mathbf{X}^{-1} = \begin{pmatrix} z^5 & 1 \\ z^{10} & 1 \end{pmatrix}$$

and

$$\mathbf{X}\mathbf{R}(b)\mathbf{X}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Now let F be any field and let $\mathbf{R}$ be an irreducible F-representation of G. Let $E \supseteq F$ be a splitting field for G. What does $\mathbf{R}^E$ look like ? We prove that $\mathbf{R}^E$

is completely reducible; that all irreducible constituents occur with equal multiplicity and that the characters of the constituents constitute a Galois conjugacy class over F.

We begin with a consequence of theorem 4.21. The exponent of a group G is the least positive integer n such that $g^n = 1$ for all $g \in G$.

COROLLARY 4.22 (cf. corollary 9.15 of [Isa 76]) Let G have exponent n and assume the polynomial $x^n - 1$ splits into linear factors in the field F. If F has prime characteristic, then it is a splitting field for G.

Proof Let $E \supseteq F$ be a splitting field and let $\chi \in Irr_E(G)$. Then $\chi(g)$ is a sum of n^{th} roots of unity and hence $\chi(g) \in F$. The result follows by theorem 4.21 and theorem 4.17. □

An entirely different proof shows that corollary 4.22 also holds in characteristic zero. This result by R. Brauer depends on his theorem on induced characters.

Let $\mathbf{R}$ be an E-representation of G. Suppose $\mathbf{R}$ affords the E-character χ and that χ takes values in $F \subseteq E$. If $\tau \in Aut(F)$, it is not obvious that $\tau\chi$ is an E-character of G.

LEMMA 4.23 (cf. lemma 9.16 of [Isa 76]) Let E be a splitting field for G and let $\chi \in Irr_E(G)$. Suppose $\chi(g) \in F \subseteq E$ for all $g \in G$ and let $\tau \in Aut(F)$. Then $\tau\chi \in Irr_E(G)$.

Proof Let $\overline{E}$ be an algebraic closure of E and let $\overline{F} \subseteq \overline{E}$ be an algebraic closure of F. Then $Irr_E(G) = Irr_{\overline{E}}(G) = Irr_{\overline{F}}(G)$ by corollary 4.16. Since τ is extendible to an automorphism of $\overline{F}$, the result follows. □

Let $F \subseteq E$ be a field extension and suppose χ is an E-character of G. Note that $F(\chi)$ is contained in a splitting field for a polynomial of the form $x^n - 1$ over F. Since this polynomial yields a Galois extension with an abelian Galois group, it follows that $F(\chi)$ is a finite degree Galois extension of F and the Galois group $Gal(F(\chi)/F)$ is abelian.

DEFINITION 4.24 Let E be a splitting field for G and let $F \subseteq E$. If χ and ψ are in $Irr_E(G)$, then χ and ψ are said to be *Galois conjugate over* F if $F(\chi) = F(\psi)$ and there exists $\sigma \in Gal(F(\chi)/F)$ such that $\sigma\chi = \psi$. It is clear that this defines an equivalence relation on $Irr_E(G)$.

LEMMA 4.25 (cf. lemma 9.17 (c) of [Isa 76]) Let E be a splitting field for G and let $\chi \in Irr_E(G)$. If S is the equivalence class of χ with respect to Galois conjugacy over F where $F \subseteq E$, then $|S| = [F(\chi) : F]$.

Proof We have that S is the orbit of χ under $Gal(F(\chi)/F)$. By definition of $F(\chi)$, the stabiliser of χ in $Gal(F(\chi)/F)$ is trivial and so

$$|S| = |Gal(F(\chi)/F)| = [F(\chi) : F].$$

□

LEMMA 4.26 (cf. lemma 9.18 of [Isa 76]) Let $F \subseteq E$ with $[E : F] = r < \infty$ and let ρ be a regular representation of E over F. Let $\mathbf{R}$ be an irreducible E-representation of G and let $\mathbf{U} = \rho\mathbf{R}$. In other words, the representation $\mathbf{U}$ of G is obtained by taking $\mathbf{R}$ and replacing the entries by the matrices representing them in the regular representation ρ of E over F. Then

(a) $deg\ \mathbf{U} = r \cdot deg\ \mathbf{R}$

(b) $\mathbf{U}$ has a unique (up to similarity) irreducible constituent. It is the F-representation $\mathbf{T}$ such that $\mathbf{R}$ is a constituent of $\mathbf{T}^E$ and $deg\ \mathbf{T} \mid r \cdot deg\ \mathbf{R}$.

(c) If $\mathbf{R}$ affords the E-character χ and $F(\chi) = F$, then $\mathbf{U}$ affords $r\chi$.

Proof Statement (a) is immediate. Let $\mathbf{T}$ be a (unique up to similarity) irreducible F-representation of G such that $\mathbf{R}$ is a constituent of $\mathbf{T}^E$. By theorem 4.14, choose $b \in F[G] \subseteq E[G]$, such that $\mathbf{T}(b) = \mathbf{T}(1)$ and $\mathbf{T}'(b) = 0$ for every irreducible F-representation $\mathbf{T}'$ not similar to $\mathbf{T}$. Since $\mathbf{R}$ is a constituent of $\mathbf{T}^E$

and $\mathbf{T}(b)$ is an identity matrix, then so is $\mathbf{R}(b)$ an identity matrix. Hence $\mathbf{U}(b)$ is an identity matrix and $\mathbf{T}_i(b) \neq 0$ for every irreducible constituent $\mathbf{T}_i$ of $\mathbf{U}$. Thus every $\mathbf{T}_i$ is similar to $\mathbf{T}$ and (b) is proved.

For (c), let ρ be the regular representation of E over F determined by the basis $(e_1, \ldots, e_k)$ and let n be the degree of $\mathbf{R}$. Write $\mathbf{R}(g) = (\mathbf{R}_{ij}(g))$ for $g \in G$ and $\rho(e) = (\rho_{ij}(e))$ for $e \in E$. If $\mathbf{U}$ affords the character ψ, then

$$\psi(g) = \sum_{i=1}^{r} \sum_{j=1}^{n} \rho_{ii}(\mathbf{R}_{jj}(g)).$$

Moreover,

$$\chi(g)e_k = (\sum_{j=1}^{n} \mathbf{R}_{jj}(g))e_k = \sum_{l=1}^{r} \sum_{j=1}^{n} \rho_{lk}(\mathbf{R}_{jj}(g))e_l$$

and since $\sum_{j=1}^{n} \mathbf{R}_{jj}(g) = \chi(g) \in F$, it follows that $\chi(g) = \sum_{j=1}^{n} \rho_{kk}(\mathbf{R}_{jj}(g))$ for each $k = 1, \ldots, n$. The result now follows. □

COROLLARY 4.27 (cf. corollary 9.20 of [Isa 76]) Let $\mathbf{R}$ be an absolutely irreducible E-representation of G which affords the character χ. Let $F \subseteq E$ be such that $F(\chi) = F$. Then there exists an irreducible F-representation $\mathbf{T}$, such that $\mathbf{R}$ is the unique (up to similarity) irreducible constituent of $\mathbf{T}^E$. In particular, $\mathbf{T}$ affords $m\chi$ for some integer m.

Proof If F has prime characteristic, then by theorem 4.21, there exists a F-representation $\mathbf{T}$ such that $\mathbf{T}^E$ is similar to $\mathbf{R}$.

Assume now that $char(F) = 0$. It will suffice to show for some positive integer n that the character $n\chi$ is afforded by some F-representation $\mathbf{U}$. This is sufficient since by the linear independence of $Irr_L(G)$ for a splitting field $L \supseteq E$, it follows that every irreducible constituent of $\mathbf{U}^L$ affords χ and so is similar to $\mathbf{R}^L$. One may thus take $\mathbf{T}$ to be any irreducible constituent of $\mathbf{U}$ and quote corollary 4.15 to complete the proof.

To produce $\mathbf{U}$, let $K \supseteq F$ be a splitting field with $[K : F] = n < \infty$ and assume that $E, K \subseteq L$ for some field L. By corollary 4.16, L is a splitting field for G and

$\chi \in Irr_L(G) = Irr_K(G)$. Let $\mathbf{R}'$ be a K-representation which affords χ and let ρ be a regular representation of K over F. Then $\mathbf{U} = \rho\mathbf{R}'$ affords $n\chi$ by lemma 4.26(c) and the result follows. □

THEOREM 4.28 (cf. theorem 9.21 of [Isa 76]) Let $F \subseteq E$, where E is a splitting field for G. Let $\mathbf{T}$ be an irreducible F-representation of G. Then

(a) The irreducible constituents of $\mathbf{T}^E$ all occur with equal multiplicity m.

(b) If $char(E) \neq 0$, then $m = 1$.

(c) The characters $\chi_i \in Irr_E(G)$ afforded by the irreducible constituents of $\mathbf{T}^E$ constitute a Galois conjugacy class over F and so the fields $F(\chi_i)$ are equal.

(d) Let $L = F(\chi_i)$. The irreducible constituents of $\mathbf{T}^L$ occur with multiplicity 1.

(e) If $\mathbf{U}$ is any irreducible constituent of $\mathbf{T}^L$ then $\mathbf{U}^E$ has a unique irreducible constituent. Its multiplicity is m.

(f) $\mathbf{T}^L$ and $\mathbf{T}^E$ are completely irreducible.

Proof Let $\mathbf{R}$ be an irreducible constituent of $\mathbf{T}^E$ and suppose $\mathbf{R}$ affords the character $\chi \in Irr_E(G)$. Let $L = F(\chi)$ and let $\mathbf{U}$ be an irreducible constituent of $\mathbf{T}^L$ such that $\mathbf{R}$ is a constituent of $\mathbf{U}^E$. By corollary 4.27, $\mathbf{R}$ is the unique irreducible constituent of $\mathbf{U}^E$. Let m be its multiplicity. If $char(E) \neq 0$, then theorem 4.21 yields $m = 1$ and $\mathbf{U}$ is absolutely irreducible.

Let $\chi = \chi_1, \ldots, \chi_n$ be the distinct Galois conjugates of χ over F, so that $n = [L : F]$ by lemma 4.25. For $\sigma \in Gal(L/F)$, form the L-representations $\sigma\mathbf{U}$. As σ runs over $Gal(L/F)$ we obtain n representations $\sigma\mathbf{U}$ affording the characters $m\chi_i, i = 1, \ldots, n$. Since $m = 1$, if $char(E) \neq 0$, the $m\chi_i$ are distinct in all cases and thus the $\sigma\mathbf{U}$ are pairwise nonsimilar. Also, each $(\sigma\mathbf{U})^E$ has a unique irreducible constituent and it occurs with multiplicity m.

We claim that the $n = [L : F]$ representation $\sigma\mathbf{U}$ are exactly the irreducible constituents of $\mathbf{T}^L$ and that each occurs with multiplicity 1. Since the irreducible

constituents of $(\sigma\mathbf{U})^E$ and $(\tau\mathbf{U})^E$ are nonsimilar if $\sigma \neq \tau$, statements (a)–(e) will follow when the claim is established.

Since $\mathbf{U}$ is a constituent of $\mathbf{T}^L$ and $\sigma(\mathbf{T}^L) = \mathbf{T}^L$ for $\sigma \in Gal(L/F)$ it follows that $\sigma\mathbf{U}$ is a constituent of $\mathbf{T}^L$ for every σ. Therefore $n \cdot deg\ \mathbf{U} \leq deg\ \mathbf{T}$. By corollary 4.26, $deg\ \mathbf{T}$ divides $n \cdot deg\ \mathbf{U}$ and thus $n \cdot deg\ \mathbf{U} = deg\ \mathbf{T}$. Therefore the $\sigma\mathbf{U}$ are the only irreducible constituents of $\mathbf{T}^L$.

All that remains is to show that $\mathbf{T}^L$ and $\mathbf{T}^E$ are completely reducible. This follows from Maschke's theorem if $char(E) = 0$ so we assume that $char(E) \neq 0$. Let V be an $L[G]$-module corresponding to $\mathbf{T}^L$ and let W be the sum of all the irreducible submodules of V. Note that W is completely reducible and it suffices to show $W = V$. Since $\sigma(\mathbf{T}^L) = \mathbf{T}^L$ for every $\sigma \in Gal(L/F)$ every irreducible constituent of V is actually an irreducible submodule of V. Hence V/W is trivial. The proof for $\mathbf{R}^E$ is similar since $\mathbf{U}^E$ is irreducible in this case. □

We obtain some consequences now. The first generalises theorem 4.19.

COROLLARY 4.29 (cf. corollary 9.22 of [Isa 76]) Let F be any field. Then the characters of nonsimilar irreducible F-representations of G are nonzero, distinct and linearly independent over F.

Proof Let $E \supseteq F$ be a splitting field for G. By theorem 4.28, the characters of nonsimilar irreducible F-representations of G are nonzero multiples of sums of disjoint subsets of $Irr_E(G)$. The result follows from lemma 4.19. □

The next corollary will be used in order to describe an irreducible representation in terms of its absolutely irreducible constituents.

COROLLARY 4.30 (cf. problem 9.6 of [Isa 76]) Let $F \subseteq E$ with $[E : F] = r < \infty$ and let ρ be a regular representation of E over F. Let $\mathbf{R}$ be an irreducible

E-representation of G which affords the character χ. If $E = F(\chi)$, then $\mathbf{U} = \rho\mathbf{R}$ is irreducible.

Proof By lemma 4.26, $deg\ \mathbf{U} = [F(\chi) : F]deg\ \mathbf{R}$ and $\mathbf{U}$ has a unique (up to similarity) irreducible constituent. It is the F-representation $\mathbf{T}$ such that $\mathbf{R}$ is a constituent of $\mathbf{T}^E$. By theorem 4.28 the irreducible constituents of $\mathbf{T}^E$ occur with multiplicity 1 and the characters afforded by the irreducible constituents of $\mathbf{T}^E$ constitute a Galois conjugacy class over F. Then, by lemma 4.25(c), $deg\ \mathbf{T} = [F(\chi) : F]deg\ \mathbf{R} = deg\ \mathbf{U}$. Therefore $\mathbf{U}$ is similar to $\mathbf{T}$. □

Let $\mathbf{R}$ be an irreducible F-representation of G where F is a finite field and let χ be the character of an (absolutely) irreducible constituent $\mathbf{T}$ of $\mathbf{R}^E$ where $E \supseteq F$ is a splitting field for G. Let $L = F(\chi)$ and let ρ be a regular representation of L over F. By theorem 4.28, $\mathbf{T}$ is similar to $\mathbf{T'}^E$ for some absolutely irreducible L-representation $\mathbf{T'}$. By lemma 4.26 and corollary 4.30 the representation $\mathbf{U} = \rho\mathbf{T'}$ is irreducible and $\mathbf{T'}$ is a constituent of $\mathbf{U}^L$. Since $\mathbf{T}$ is a common irreducible constituent of $\mathbf{U}^E$ and $\mathbf{R}^E$ it follows that $\mathbf{U}$ is similar to $\mathbf{R}$.

We conclude this section with an algorithm for the calculation of an absolutely irreducible constituent of an irreducible representation.

COROLLARY 4.31 (cf. problem 9.8 of [Isa 76]) Let F be of prime characteristic and let $\mathbf{R}$ be an irreducible F-representation of G. Let D be the centraliser of $\mathbf{R}(G)$ in the matrix ring $M_n(F)$ where $n = deg\ \mathbf{R}$. Let χ be the character of an irreducible constituent of $\mathbf{R}^E$ where $E \supseteq F$ is a splitting field for G. Then $F(\chi) \cong D$.

Proof Let $L = F(\chi)$. By theorem 4.28(f) the representation $\mathbf{R}^L$ is completely

reducible and therefore there exists a matrix $\mathbf{X}\in GL_n(L)$ such that

$$\mathbf{X}^{-1}\mathbf{R}(g)\mathbf{X} = \begin{pmatrix} \mathbf{R}_1(g) & & 0 \\ & \ddots & \\ 0 & & \mathbf{R}_r(g) \end{pmatrix}$$

for all $g\in G$. By theorem 4.28 (d) and (e) the irreducible constituents $\mathbf{R}_i$ are absolutely irreducible and pairwise nonsimilar. If $\mathbf{D}\in D$, then

$$\begin{pmatrix} \mathbf{R}_1(g) & & 0 \\ & \ddots & \\ 0 & & \mathbf{R}_r(g) \end{pmatrix} \mathbf{X}^{-1}\mathbf{D}\mathbf{X} = \mathbf{X}^{-1}\mathbf{D}\mathbf{X} \begin{pmatrix} \mathbf{R}_1(g) & & 0 \\ & \ddots & \\ 0 & & \mathbf{R}_r(g) \end{pmatrix}.$$

Therefore $\mathbf{X}^{-1}\mathbf{D}\mathbf{X}$ is a matrix of the form

$$\begin{pmatrix} l_1\mathbf{I} & & 0 \\ & \ddots & \\ 0 & & l_r\mathbf{I} \end{pmatrix}$$

where $l_i\in L$ for $i = 1,\ldots,r$. Since D is a field $\mathbf{D} \mapsto l_1$ is a monomorphism of rings and it follows that $dim_F D \leq dim_F L$.

Take $\mathbf{T} = \mathbf{R}_1$ and let ρ be a regular representation of L over F. Then there exists an invertible matrix $\mathbf{Y}$ such that $\mathbf{R}(g) = \mathbf{Y}^{-1}\rho(\mathbf{T}(g))\mathbf{Y}$ for all $g\in G$. If $l\in L$, then $\mathbf{R}(g)\mathbf{Y}^{-1}\rho(l\mathbf{I})\mathbf{Y} = \mathbf{Y}^{-1}\rho(l\mathbf{I})\mathbf{Y}\mathbf{R}(g)$ for all $g\in G$. Then $l \mapsto \mathbf{Y}^{-1}\rho(l\mathbf{I})\mathbf{Y}$ is a monomorphism and $dim_F L \leq dim_F D$. □

Let F be of prime characteristic and let $\mathbf{R}$ be an irreducible F-representation of G. Let D be the centraliser of $\mathbf{R}(G)$ in the matrix ring $M_n(F)$ where $n = deg\,\mathbf{R}$. Let $\mathbf{T}$ be an irreducible constituent of $\mathbf{R}^E$ where $E\supseteq F$ is a splitting field for G. By theorem 4.21 the representation $\mathbf{T}$ is similar to $\mathbf{U}^E$ for some absolutely irreducible representation $\mathbf{U}$ over $F(\chi)$ where χ is the character of $\mathbf{T}$.

Since $F(\chi)/F$ is a finite Galois extension $F(\chi)/F$ has a primitive element, that is $F(\chi) = F(u)$ for some $u\in F(\chi)$. Then $(1, u, \ldots, u^{r-1})$ is a base for $F(\chi)/F$ where $r = [F(\chi) : F]$. Note that $F(\chi)\cong D$ by corollary 4.31. Let $f(x)$ be the

minimal polynomial of u over F and $\overline{f}(x)$ the corresponding polynomial in $D[x]$ (under the isomorphism which extends the natural isomorphism between F and $F\cdot\mathbf{I}$ and maps $x \mapsto x$). If $\mathbf{D}$ is a root of $\overline{f}(x)$ in D, then the natural isomorphism between F and $F\cdot\mathbf{I}$ extends to an isomorphism $F(\chi)\cong D$ sending $u \mapsto \mathbf{D}$. Hence $(1, \mathbf{D}, \ldots, \mathbf{D}^{r-1})$ is a base for $D/F\cdot\mathbf{I}$.

Let V be an $F(u)[G]$-modules corresponding to $\mathbf{U}$ and let $(v_1, \ldots, v_m)$ be a base for V over $F(u)$. Then

$$(v_1, uv_1, \ldots, u^{r-1}v_1, \ldots, v_m, uv_m, \ldots, u^{r-1}v_m)$$

is a base for V over F and the representation of G corresponding to V over F with respect to this base is

$$g \mapsto \begin{pmatrix} \rho(\mathbf{U}_{11}(g)) & \ldots & \rho(\mathbf{U}_{1n}(g)) \\ \vdots & & \vdots \\ \rho(\mathbf{U}_{n1}(g)) & \ldots & \rho(\mathbf{U}_{nn}(g)) \end{pmatrix}.$$

Moreover, this representation is similar to $\mathbf{R}$ and therefore $n = rm$.

Let W be the n-dimensional column vector space over F and let $(w_1, \ldots, w_n)$ be a base for W over F such that $\mathbf{R}$ is the representation afforded by the $F[G]$-module W with respect to this base. Suppose that

$$B = (w'_1, \mathbf{D}w'_1, \ldots, \mathbf{D}^{r-1}w'_1, \ldots, w'_i, \mathbf{D}w'_i, \ldots, \mathbf{D}^{r-1}w'_i)$$

is linearly independent. Choose $w \in \{w_1, \ldots, w_n\}$ such that $B \cup \{w\}$ is linearly independent. Then $B \cup \{w, \mathbf{D}w, \ldots, \mathbf{D}^{r-1}w\}$ is linearly independent. Hence there is a base for W over F of the form

$$(w'_1, \mathbf{D}w'_1, \ldots, \mathbf{D}^{r-1}w'_1, \ldots, w'_m, \mathbf{D}w'_m, \ldots, \mathbf{D}^{r-1}w'_m)$$

where $w'_1, \ldots, w'_m \in \{w_1, \ldots, w_n\}$. If $\mathbf{R}'$ is the representation of G corresponding to W with respect to this base, then

$$\mathbf{R}'(g) = \begin{pmatrix} \rho(\mathbf{U}_{11}(g)) & \ldots & \rho(\mathbf{U}_{1n}(g)) \\ \vdots & & \vdots \\ \rho(\mathbf{U}_{n1}(g)) & \ldots & \rho(\mathbf{U}_{nn}(g)) \end{pmatrix}.$$

In other words, the representation $\mathbf{U}$ of G over $F(\chi)$ is obtained by taking $\mathbf{R}'$ and replacing the matrices $\rho(\mathbf{U}_{ij}(g))$ which represent the elements $\mathbf{U}_{ij}(g)$ of $F(\chi)$ in a regular representation of $F(\chi)$ over F by $\mathbf{U}_{ij}(g)$.

EXAMPLE Let $G = \langle a, b \rangle$ be the dihedral group of order 10 with the defining relations $a^5 = b^2 = (ab)^2 = 1$. Consider the irreducible representation $\mathbf{R}$ over the field F_2 of order two defined by

$$\mathbf{R}(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

and

$$\mathbf{R}(b) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

A base for the centraliser D of $\mathbf{R}(G)$ in the matrix ring $M_4(F_2)$ is given by

$$(\mathbf{I}, \mathbf{D} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}).$$

Hence D is isomorphic to the field F_{2^2} of order four, which is the 3^{rd} cyclotomic field over F_2. The 3^{rd} cyclotomic polynomial $Q_3(x) = x^2 + x + 1$ is irreducible over F_2. If z be a root of $Q_3(x)$, then z is a primitive 3^{rd} root of unity over F_2.

Let W be the 2-dimensional column vector space over F_2 and let $(w_1, \ldots, w_4)$ be a base for W over F_2 such that $\mathbf{R}$ is the representation afforded by the $F_2[G]$-module W with respect to this base. Then $(w_1, \mathbf{D}w_1, w_2, \mathbf{D}w_2)$ is another base

and the representation $\mathbf{R}'$ corresponding to W with respect to this basis is

$$\mathbf{R}'(a) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \rho(z) & \rho(1) \\ \rho(z^2) & \rho(1) \end{pmatrix}$$

and

$$\mathbf{R}'(b) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \rho(1) & \rho(1) \\ \rho(0) & \rho(1) \end{pmatrix}$$

where ρ is the regular representation of F_{2^2} determined by the base $(1, z)$. Therefore the representation $\mathbf{U}$ defined by

$$\mathbf{U}(a) = \begin{pmatrix} z & 1 \\ z^2 & 1 \end{pmatrix}$$

and

$$\mathbf{U}(b) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

is an absolutely irreducible constituent of $\mathbf{R}^{F_{2^2}}$.

4.3 The Construction of the Irreducible Representations of Finite Soluble Groups over Finite Fields

In section 4.1 we described an algorithm for the construction of the irreducible representations of finite soluble groups over algebraically closed fields : Going up a composition series $G = G_0 \rhd G_1 \rhd \cdots \rhd G_l = \langle 1 \rangle$ of a soluble group G all irreducible representations of G_i are constructed from those of G_{i+1} by extending

the G_i-invariant irreducibles of G_{i+1} to irreducibles of G_i and by inducing up the non-invariant irreducibles of G_{i+1}.

In section 4.2 we studied the relation between the irreducible E-representations and F-representations of a group where E is a field extension of F. We have a one-to-one correspondence between the irreducible representations of a group over a field F and the absolutely irreducible representations over a field E, where E is a splitting field for the group. The absolutely irreducible constituents of an irreducible representation form a Galois conjugate class over F. Moreover, we showed that an irreducible representation $\mathbf{R}$ over a finite field F can be described in terms of an absolutely irreducible constituent $\mathbf{T}$ over a finite extension field L over F. The information needed to construct the representation $\mathbf{R}$ from an absolutely irreducible constituent $\mathbf{T}$ is the realisation of $\mathbf{T}$ over $L = F(\chi)$ where χ is the character afforded by $\mathbf{T}$.

In this section we modify the algorithm described in section 4.1 in order to derive an algorithm for the construction of the irreducible representations of finite soluble groups over finite fields. The principle idea is to calculate representatives for the Galois conjugate classes of absolutely irreducible representations of G_i from those of G_{i+1} and to realise them over their fields of character values.

For describing the passage from G_{i+1} to G_i we assume that $N = G_{i+1}$ and $G = G_i$. With the help of our knowledge of section 4.1 and 4.2 we investigate the absolutely irreducible representations of G in which a given absolutely irreducible representation of a normal subgroup N of prime index can be embedded. We summarise the results in the following theorem.

THEOREM 4.32 Let $N \lhd G$ such that G/N is a cyclic group of prime order r. Let $t \in G - N$ and let γ be the automorphism of N defined by $x \mapsto t^{-1}xt$. Let F be a finite field and let $\mathbf{S}$ be an absolutely irreducible representation of N over a finite extension field $E \supseteq F$ such that $E = F(\chi)$ where χ is the character afforded

by $\mathbf{S}$. Then one of the following occurs :

(1) If $\mathbf{S}\gamma$ is not similar to $\eta\mathbf{S}$ for all $\eta \in Gal(E/F)$, then the induced representation $\mathbf{S}^G$ is absolutely irreducible. If ψ is the character of $\mathbf{S}^G$, then

$$F(\psi) = E.$$

(2) If $\mathbf{S}\gamma$ is similar to $\eta\mathbf{S}$ for some $1 \neq \eta \in Gal(E/F)$, then $\mathbf{S}^G$ is absolutely irreducible. If ψ is the character of $\mathbf{S}^G$, then $F(\psi) = E' \subset E$ with $[E : E'] = r$.

(3) If $\mathbf{S}\gamma$ is similar to $\mathbf{S}$, then there exists an invertible matrix $\mathbf{P}_t$ such that $\mathbf{S}\gamma = \mathbf{P}_t{}^{-1}\mathbf{S}\mathbf{P}_t$. Moreover, $\mathbf{P}_t{}^r = e\mathbf{S}(t^r)$ for some $e \in E$. Let c be a r^{th} root of e which lies in E or possibly in an extension field of E. Then every irreducible representation of G which contains a component similar to $\mathbf{S}$ on restriction to N is similar to a representation defined by $\mathbf{R}_c : t^i n \mapsto c^i \mathbf{P}_t{}^i \mathbf{S}(n)$ for $i = 0, \ldots, r-1$ and $n \in N$. If ψ is the character of $\mathbf{R}_c$, then

$$F(\psi) = E(c).$$

The characters of the representations $\mathbf{R}_c$ and $\mathbf{R}_{c'}$ are Galois conjugate over F if and only if c and c' have the same minimum polynomial over E.

Moreover, the Galois conjugacy classes over F which are determined by the characters ψ in (1), (2) and (3) are independent of the choice of the representative of the Galois conjugacy class of χ over F.

Proof The assertions about the representations in (1), (2) and (3) are easily checked by appealing to the algebraically closed case (cf. section 4.1). Case (1) and (2) correspond to the inducing case there while case (3) corresponds to the extension case there and nothing has to be added. In order to prove the assertions about the fields $F(\psi)$ we construct the Galois conjugacy classes of ψ over F.

Suppose that $\mathbf{S}\gamma$ is not similar to $\eta\mathbf{S}$ for all $\eta \in Gal(E/F)$. Let $\mathbf{S}$ be a constituent of $\mathbf{U}^E$ for some irreducible representation $\mathbf{U}$ over F. By theorem 4.28 the irreducible constituents of $\mathbf{U}^E$ occur with multiplicity 1 and the characters afforded by the irreducible constituents of $\mathbf{U}^E$ constitute a Galois conjugacy class over F. Since $\mathbf{S}\gamma$ is an absolutely irreducible constituent of $(\mathbf{U}\gamma)^E$ and $\mathbf{S}\gamma$ is not similar to $\eta\mathbf{S}$ for all $\eta \in Gal(E/F)$ the representation $\mathbf{U}\gamma$ is not similar to $\mathbf{U}$ by corollary 4.15. Hence $O = \{\eta\chi\gamma^i | \eta \in Gal(E/F), i = 0, \ldots, r-1\}$ is a set of $r[E : F]$ characters. Let γ_g be the automorphism of N defined by $x \mapsto g^{-1}xg$ for $g \in G$. We obtain a map of $G \times O$ into O defined by $(g, \varphi) \mapsto g\varphi = \varphi\gamma_g$. This map satisfies the conditions $1\varphi = \varphi$ and $(gh)\varphi = g(h\varphi)$ for $\varphi \in O$ and $g, h \in G$. Hence G acts on O and O decomposes into orbits of length r under the action of G. The characters $\eta\chi$ for $\eta \in Gal(E/F)$ are representatives of these orbits. Thus the induced characters $(\eta\chi)^G = \eta(\chi^G)$ are distinct and $\{\eta(\chi^G) | \eta \in Gal(E/F)\}$ is the orbit of $\psi = \chi^G$ under $Gal(E/F)$. Hence, if S is the Galois conjugacy class of ψ over F, then $[E : F] = |S| = [F(\psi) : F]$ by lemma 4.25.

Now, suppose that $\mathbf{S}\gamma$ is similar to $\eta\mathbf{S}$ for some $1 \neq \eta \in Gal(E/F)$ and let O be the Galois conjugacy class of χ over F. We obtain a map of $G \times O$ into O defined by $(g, \varphi) \mapsto g\varphi = \varphi\gamma_g$. This map satisfies the conditions $1\varphi = \varphi$ and $(gh)\varphi = g(h\varphi)$ for $\varphi \in O$ and $g, h \in G$. Hence G acts on O and O decomposes into orbits of length r under the action of G. Let $\chi_1 = \chi, \ldots, \chi_k$ be representatives of these orbits. Then the induced characters $(\chi_i)^G$ are distinct and since $(\chi_i)^G = (\sigma\chi)^G = \sigma(\chi^G)$ for some $\sigma \in Gal(E/F)$, $\{\chi_i{}^G | i = 1, \ldots, k\}$ is the orbit of $\psi = \chi^G$ under $Gal(E/F)$. Hence, if S is the Galois conjugacy class of ψ over F, then $[E : F] = r \cdot k = r|S| = r[F(\psi) : F]$ by lemma 4.25.

Finally, suppose that $\mathbf{S}\gamma$ is similar to $\mathbf{S}$. Since $\eta\mathbf{S}\gamma = \eta\mathbf{P}_t{}^{-1}(\eta\mathbf{S})\eta\mathbf{P}_t$ for all $\eta \in Gal(E/F)$, the representations $\eta\mathbf{S}\gamma$ and $\eta\mathbf{S}$ are similar. Let $\bar{c}$ be a r^{th} root of $\eta(e)$ which lies in E or possibly in an extension field of E. Then every irreducible representation of G which contains a component similar to $\eta\mathbf{S}$ on restriction to N is similar to a representation defined by $t^i n \mapsto \bar{c}^i\eta(\mathbf{P}_t{}^i\mathbf{S}(n))$ for $i = 0, \ldots, r-1$

and $n \in N$. If $\sigma \in Gal(E(c)/F)$, then $\sigma \mathbf{R}_c(t^i n) = \sigma(c)^i \sigma(\mathbf{P}_t{}^i \mathbf{S}(n))$. The restriction of σ on E is an automorphism $\eta \in Gal(E/F)$. Since $\sigma(c)^i \sigma(\mathbf{P}_t{}^i \mathbf{S}(n)) = \sigma(c)^i \eta(\mathbf{P}_t{}^i \mathbf{S}(n))$ and $\sigma(c)^r = \sigma(c^r) = \sigma(e) = \eta(e)$ it follows that $\sigma \mathbf{R}_c$ is an extension of $\eta \mathbf{S}$. Hence, if ψ is the character of $\mathbf{R}_c$ and S is the Galois conjugacy class of ψ over F, then $[E(c) : F] = |S| = [F(\psi) : F]$ by lemma 4.25.

If c and c' have the same minimum polynomial, then there is an automorphism σ of $E(c)$ extending the identity mapping of E and sending $c \mapsto c'$. Then $\sigma \mathbf{R}_c = \mathbf{R}_{c'}$ and the characters of $\mathbf{R}_c$ and $\mathbf{R}_{c'}$ are Galois conjugate over F. Conversely, let ψ_c and $\psi_{c'}$ be the characters of $\mathbf{R}_c$ and $\mathbf{R}_{c'}$ respectively and let $\sigma \in Gal(E(c)/F)$ such that $E(c) = F(\psi_c) = F(\psi_{c'}) = E(c')$ and $\sigma \psi_c = \psi_{c'}$. Since $\mathbf{S}(E[N])$ is a full matrix ring over E, for every $e \in E$ we may choose $n \in E[N]$ such that $\mathbf{S}(n) = e\mathbf{E}_{11}$ is the matrix having e as its $(1,1)$-entry and all other entries 0. Then $\sigma(e) = \sigma\psi_c(n) = \psi_{c'}(n) = e$ and therefore $\sigma \in Gal(E(c)/E)$. Moreover, we may choose $n \in E[N]$ such that $\mathbf{P}_t \mathbf{S}(n) = \mathbf{E}_{11}$ and it follows that $\sigma(c) = \sigma\psi_c(tn) = \psi_{c'}(tn) = c'$. Hence c and c' have the same minimal polynomial over E. □

In view of a repeated application of theorem 4.32 and in order to obtain the irreducible representations of G over F (we have to compose the absolutely irreducible representations of G with a regular representation of E, E' or $E(c)$ over F respectively) it remains to outline the realisation of the induced representation $\mathbf{S}^G$ over E' in case (2) and to describe the fields $E(c)$ in case (3).

Case (2) : Initially we handled case(2) in a rather tedious way : Since $\mathbf{S}\gamma$ is similar to $\eta \mathbf{S}$ for some $1 \neq \eta \in Gal(E/F)$ there is a matrix $\mathbf{Z}$ such that $\eta \mathbf{S} = \mathbf{Z}(\mathbf{S}\gamma)\mathbf{Z}^{-1}$. Choose a base for E/F and let ρ be a regular representation of E over F determined by this base. Let $\mathbf{Y}$ be the matrix of η^{-1} with respect to the chosen base. Then $\rho(\eta(x)) = \mathbf{Y}^{-1} \rho(x) \mathbf{Y}$ for all $x \in E$. In other words $\mathbf{Y}$ induces the automorphism η on the matrix representation

of E by conjugation. Then $\mathbf{X} = (\mathbf{I}\otimes\mathbf{Y})\rho\mathbf{Z}$ is a matrix such that

$$\mathbf{X}^{-1}(\rho\mathbf{S})(n)\mathbf{X} = (\rho\mathbf{S}\gamma)(n).$$

Note that by corollary 4.30 and 4.26 the representation $\rho\mathbf{S}$ is irreducible and that $\mathbf{S}$ is an absolutely irreducible constituent of $(\rho\mathbf{S})^E$. Moreover, if D is the centraliser of $(\rho\mathbf{S})(N)$ in the matrix ring $M_{d[E:F]}(F)$ where $d = deg\,\mathbf{S}$, then $D\cong F(\chi) = E$ by corollary 4.31. Since $t^r\in N$, we have

$$\mathbf{X}^{-r}(\rho\mathbf{S})(n)\mathbf{X}^r = \rho(\mathbf{S}(t^{-r}nt^r)) =$$
$$= \rho(\mathbf{S}(t^r))^{-1}(\rho\mathbf{S})(n)\rho(\mathbf{S}(t^r))$$

and therefore $\mathbf{X}^r = \mathbf{E}\rho(\mathbf{S}(t^r))$ for some $0 \neq \mathbf{E}\in D$. Since $\{(\rho\mathbf{S})(n)|n\in N\} = \{(\rho\mathbf{S}\gamma)(n)|n\in N\}$ it follows that D is the centraliser of $\rho\mathbf{S}\gamma$ in the matrix ring $M_{d[E:F]}(F)$. Hence, $\mathbf{X}$ conjugates D into itself and therefore $\mathbf{X}$ induces an automorphism of D. Since $\mathbf{X}^r$ centralises D it follows that $\mathbf{X}$ either induces an automorphism of order r or $\mathbf{X}$ centralises D.

A central simple algebra A over a field F is a simple algebra A for which $Z(A) = F$ and $[A : F] < \infty$. If B is a simple subalgebra of a central simple algebra A, then $[A : F] = [B : F][C_A(B) : F]$ by theorem 4.11 of [Jac 74]II. We apply this theorem as follows. If $A = M_{[E:F]}(F)$, then A is a central simple algebra and $B = \rho(E)$ is a simple subalgebra of A. Therefore $[C_A(B) : F] = [E : F]$ and it follows that $C_A(B) = B$. Note that D actually consists of matrices of the form $\rho(x\mathbf{I})$ for $x\in E$. Hence, if $\mathbf{X}$ centralises D, then $\mathbf{X} = \rho(\mathbf{X}')$ for some matrix $\mathbf{X}'\in M_d(E)$ and it follows that $\mathbf{S}$ is similar to $\mathbf{S}\gamma$. Since $\mathbf{S}$ is similar to $\eta\mathbf{S}$ for some $1 \neq \eta\in Gal(E/F)$ it follows that $\mathbf{X}$ induces an automorphism of order r of D. Let D' be a subalgebra of D with $[D : D'] = r$ and let $N_{D/D'}$ denote the norm map. Since $\mathbf{X}$ centralises $\mathbf{E}$ we may choose $\mathbf{C}\in D$ such that $N_{D/D'}(\mathbf{C}) = \mathbf{E}$ and replace $\mathbf{X}$ by $\mathbf{C}^{-1}\mathbf{X}$ in order to arrange that $\mathbf{E} = 1$. Now, define a representation $\mathbf{R}$ of G over F by $\mathbf{R}(nt^i) = \rho(\mathbf{S}(n))\mathbf{X}^i$ for $i = 0,\ldots,r-1$ and $n\in N$. It is easily checked that

$\mathbf{R}$ is indeed a representation of G and an absolutely irreducible constituent of $\mathbf{R}$ may be found by applying the algorithm described on page 76.

EXAMPLE Let $G = \langle a, b \rangle$ be the Dihedral group of order 10 with the defining relations $a^5 = b^2 = (ab)^2 = 1$. The field $E = F_{2^4}$ of order 2^4 is the 15^{th} cyclotomic field over F_2. The 15^{th} cyclotomic polynomial $Q_{15}(x) = x^8+x^7+x^5+x^4+x^3+x+1$ and $Q_{15}(x) = (x^4+x+1)(x^4+x^3+1)$ is the decomposition of Q_{15} into irreducible factors in $F_2[x]$. Let z be a root of $x^4 + x + 1$. Then z is a primitive 15^{th} root of unity over F_2. Consider the representation $\mathbf{S}$ of $\langle a \rangle$ over E defined by $\mathbf{S}(a) = z^3$. Then $\mathbf{S}^b(a) = \mathbf{S}(b^{-1}ab) = z^{12} = \eta(z^3) = \eta(\mathbf{S}(a))$ where η is the automorphism of E sending x to x^4. Choose $(1, z, z^2, z^3)$ for a base of E over $F = F_2$ and let ρ be the regular representation of E over F determined by this base. The matrix of η^{-1} with respect to the chosen base is

$$\mathbf{Y} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $\mathbf{X} = \mathbf{Y}$ is a matrix such that $\mathbf{X}^{-1}(\rho\mathbf{S})(a)\mathbf{X} = (\rho\mathbf{S})(b^{-1}ab)$. Moreover, $\mathbf{X}^2 = \mathbf{I}$ and therefore $\mathbf{E} = \mathbf{I}$. Now, we define $\mathbf{R}$ by

$$\mathbf{R}(a) = (\rho\mathbf{S})(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

and $\mathbf{R}(b) = \mathbf{X}$. Using the algorithm described on page 76 we obtain an absolutely irreducible constituent $\mathbf{U}$ of $\mathbf{R}$ defined by

$$\mathbf{U}(a) = \begin{pmatrix} z^5 & 1 \\ z^{10} & 1 \end{pmatrix}$$

and

$$\mathbf{U}(b) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The problem with this approach is the calculation of the centraliser D of $(\rho\mathbf{S})(N)$ in the matrix ring $M_{d[E:F]}(F)$, in particular if F is the prime field F_p of order p. Alternatively we may apply the algorithm described on page 65 in order to obtain the realisation of $\mathbf{S}^G$ over E'. The following treatment of Case (2) is due to R. B. Howlett (private communication).

Case (2) : If $\mathbf{S}\gamma$ is similar to $\eta\mathbf{S}$ for some $1 \neq \eta \in Gal(E/F)$, then there is a matrix $\mathbf{Z}$ such that $\eta\mathbf{S} = \mathbf{Z}(\mathbf{S}\gamma)\mathbf{Z}^{-1}$. Since $r = [G : N]$, it follows that

$$\eta^r\mathbf{S}(n) = \eta^{r-1}\mathbf{Z}\cdots\eta\mathbf{Z}\mathbf{Z}\,\mathbf{S}(t^{-r}nt^r)\,(\eta^{r-1}\mathbf{Z}\cdots\eta\mathbf{Z}\mathbf{Z})^{-1} =$$
$$= \eta^{r-1}\mathbf{Z}\cdots\eta\mathbf{Z}\mathbf{Z}\mathbf{S}(t^r)^{-1}\,\mathbf{S}(n)\,(\eta^{r-1}\mathbf{Z}\cdots\eta\mathbf{Z}\mathbf{Z}\mathbf{S}(t^r)^{-1})^{-1}.$$

We know that $\eta^r = 1$ because otherwise $\mathbf{S}$ would be realisable over a subfield of E contrary to the hypothesis $E = F(\chi)$. Hence $\eta^r\mathbf{S} = \mathbf{S}$ and $\eta^{r-1}\mathbf{Z}\cdots\eta\mathbf{Z}\mathbf{Z}\,\mathbf{S}(t^r)^{-1} = f\mathbf{I}$ for some $f \in E^*$. The scalar f is in E', the fixed field of η because, if we apply η to $\mathbf{W} = \eta^{r-1}\mathbf{Z}\cdots\eta\mathbf{Z}\mathbf{Z}$ we get

$$\eta\mathbf{W} = \eta^r\mathbf{Z}\cdots\eta\mathbf{Z} = \mathbf{Z}\mathbf{W}\mathbf{Z}^{-1}.$$

Moreover, $\eta\mathbf{S}(t^r)^{-1} = (\mathbf{Z}\mathbf{S}(t^{-1}t^rt)\mathbf{Z}^{-1})^{-1} = \mathbf{Z}\mathbf{S}(t^r)^{-1}\mathbf{Z}^{-1}$ and therefore

$$\eta(f\mathbf{I}) = \eta(\mathbf{W}\mathbf{S}(t^r)^{-1}) = \mathbf{Z}\mathbf{W}\mathbf{S}(t^r)^{-1}\mathbf{Z}^{-1} = f\mathbf{I}$$

showing that $\eta(f) = f$. Choosing $c \in E$ such that $N_{E/E'}(c) = f$ where $N_{E/E'}$ denotes the norm map and replacing $\mathbf{Z}$ by $c^{-1}\mathbf{Z}$ we may arrange that $f = 1$. Choose a base for E/E' and let ρ be the regular representation of E by $r \times r$ matrices over E' determined by this base. Furthermore, let $\mathbf{Y}$ be the

matrix of η^{-1} with respect to the chosen base. Then $\rho(\eta(x)) = \mathbf{Y}^{-1}\rho(x)\mathbf{Y}$ for all $x \in E$. In other words $\mathbf{Y}$ induces the automorphism η on the matrix representation of E by conjugation. Now, define a representation $\mathbf{R}$ of G over E' by $\mathbf{R}(nt^i) = \rho(\mathbf{S}(n))(\mathbf{I} \otimes \mathbf{Y}^i)\rho(\eta^{i-1}\mathbf{Z} \cdots \eta\mathbf{Z}\mathbf{Z})$ for $i = 0, \ldots, r-1$ and $n \in N$. It is easily checked that $\mathbf{R}$ is indeed a representation of G equivalent to the induced representation $\mathbf{S}^G$.

For case (3), we begin with the following lemma on extraction of roots in finite fields (cf. section 63 of *Linear Groups with an exposition of Galois field theory* by L. E. Dickson).

LEMMA 4.33 Given a positive integer m the element $a \in F_q^*$ is the m^{th} power of some element of F_q if and only if $a^{(q-1)/d} = 1$ where $d = (q-1, m)$ is the greatest common divisor of $q-1$ and m.

Proof Let a be a m^{th} power of some element $z \in F_q^*$. We have

$$(q-1)m = (q-1, m)[q-1, m]$$

where $[q-1, m]$ is the least common multiple of $q-1$ and m. Hence

$$a^{(q-1)/d} = z^{m(q-1)/d} = z^{[q-1,m]} = 1.$$

Conversely, let z be a primitive root of F_q. Then the elements z^{di} for $i = 1, \ldots, (q-1)/d$ are the distinct roots of the equation $x^{(q-1)/d} = 1$. We next prove that each root is a m^{th} power in F_q. We can determine integers l and t satisfying the equation $t(q-1) + lm = d$. Hence $z^{di} = (z^{t(q-1)+lm})^i = (z^{lm})^i = (z^{li})^m$. □

Case (3) : If $r \mid |E^*|$, then $r \neq p$ and E contains r distinct roots of unity. Let r^k be the biggest r power dividing $|E^*|$.

A. If the order of e in E^* is divisible by r^k, then $e^{|E^*|/r} \neq 1$ and therefore $x^r - e$ has no root in E by lemma 4.33. Then $x^r - e$ is irreducible over E by lemma 2 of [Jac 74]I, p. 253.

B. If the order of e in E^* is not divisible by r^k, then $e^{|E^*|/r} = 1$ and therefore E contains r roots of $x^r - e$.

If $r \not| |E^*|$, then raising elements to the r^{th} power is an automorphism of the multiplicative group of E and there is a unique $c \in E$ such that $c^r = e$.

A. If $r = p$, then $x^r - e = (x - e)^r$ and no further roots exist in E or extension fields of E.

B. If $r \neq p$, then there are r distinct roots of unity in an extension field of E. The r^{th} cyclotomic polynomial $(x^r - 1)/(x - 1)$ factors into $\phi(r)/l$ distinct irreducible polynomials in $E[x]$ of the same degree l. The r^{th} cyclotomic field $E^{(r)}$ over E is the splitting field for any such irreducible factor over E and $[E^{(r)} : E] = l$ where l is the least positive integer such that $q^l \equiv 1 \mod r$ (cf. theorem 2.47 of [LiN 83]).

Factorisation of polynomials can be achieved by Berlekamp's algorithm (cf. chapter 4 of [LiN 83]).

EXAMPLE Let $G = \langle a, b \rangle$ be the Dihedral group of order 10 with the defining relations $a^5 = b^2 = (ab)^2 = 1$. The field $E = F_{2^4}$ of order 2^4 is the 15^{th} cyclotomic field over F_2. The 15^{th} cyclotomic polynomial $Q_{15}(x) = x^8+x^7+x^5+x^4+x^3+x+1$ and $Q_{15}(x) = (x^4+x+1)(x^4+x^3+1)$ is the decomposition of Q_{15} into irreducible factors in $F_2[x]$. Let z be a root of $x^4 + x + 1$. Then z is a primitive 15^{th} root of unity over F_2. Consider the representation $\mathbf{S}$ of $\langle a \rangle$ over E defined by $\mathbf{S}(a) = z^3$. Then $\mathbf{S}^b(a) = \mathbf{S}(b^{-1}ab) = z^{12} = \eta(z^3) = \eta(\mathbf{S}(a))$ where η is the automorphism of E sending x to x^4. Take $\mathbf{Z} = \mathbf{I}$; then $\eta\mathbf{S} = \mathbf{Z}\mathbf{S}^b\mathbf{Z}^{-1}$ and $f = 1$. Let ρ be the regular representation of E by 2×2 matrices over F_{2^2} determined by the base $(1, z)$ of E over F_{2^2}. Furthermore, let $\mathbf{Y}$ be the matrix of η^{-1} with respect to this

base. Then the representation $\mathbf{R}$ of G defined by

$$\mathbf{R}(a) = \rho(\mathbf{S}(n)) = \begin{pmatrix} z^5 & 1 \\ z^{10} & 1 \end{pmatrix}$$

and

$$\mathbf{R}(b) = \mathbf{Y} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

is absolutely irreducible. There are four conjugate classes in G which are given by $C_1 = \{1\}, C_b = \{b, ba, ba^2, ba^3, ba^4\}, C_a = \{a, a^4\}$ and $C_{a^2} = \{a^2, a^3\}$. The values of the character ψ of $\mathbf{R}$ are given by the following table.

C_1	C_b	C_a	C_{a^2}
0	0	z^{10}	z^5

Obviously, $\mathbf{R}$ is a representation over F_{2^2} and $F_2(\psi) = F_{2^2}$.

Now, let $\mathbf{S}$ be the representation of $\langle\, a \,\rangle$ over E defined by $\mathbf{S}(a) = z^6$. Then $\mathbf{S}^b(a) = \mathbf{S}(b^{-1}ab) = z^9 = \eta(z^6) = \eta(\mathbf{S}(a))$ and we obtain an absolutely irreducible representation $\mathbf{R}$ of G defined by

$$\mathbf{R}(a) = \rho(\mathbf{S}(a)) = \begin{pmatrix} 0 & z^{10} \\ z^5 & z^5 \end{pmatrix}$$

and

$$\mathbf{R}(b) = \mathbf{Y} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The values of the character ψ of $\mathbf{R}$ are given by the following table.

C_1	C_b	C_a	C_{a^2}
0	0	z^5	z^{10}

Finally consider the trivial representation of $\langle\, a \,\rangle$. The trivial representation of $\langle\, a \,\rangle$ is G-invariant. Take $\mathbf{P}_t = \mathbf{I}$; then $e = 1$ and $c = 1$ is obviously the unique element in E such that $c^r = e$. Moreover, since the characteristic of E is 2 there are no further roots in E or extension fields of E. Hence the trivial representation of G is the only extension of the trivial representation of $\langle\, a \,\rangle$.

Hence we obtain three absolutely irreducible representations of G. By corollary 15.11 of [Isa 76] the number of similarity classes of irreducible K-representations of G for every splitting field K of characteristic p is the number of classes of p-regular elements of G (that is, elements of order not divisible by p). The classes of 2-regular elements of G are C_1, C_a and C_{a^2} and therefore we have calculated all absolutely irreducible representations of G.

In order to compute the irreducible representations of G we have to decide whether a given irreducible representation $\mathbf{S}$ of N is similar to $\mathbf{S}\gamma$. The following suggestion (cf. [Ple 87]) is feasible : Since the algorithm on N provides the irreducible representations of N over E and the characters of the representations are distinct by corollary 4.29 we may choose random elements in N such that the irreducible representations are distinguished by their degrees and traces of the images of these elements under the irreducible representations. Note that this is asking for much less than representatives of the conjugate classes. We may also use this technique to distinguish the representations $\{\eta\mathbf{S}|\eta\in Gal(E/F)\}$ and decide the similarity of $\mathbf{S}\gamma$ and $\eta\mathbf{S}$.

To compute an intertwining matrix in case (3) (that is a matrix $\mathbf{X}$ such that $\mathbf{S}\gamma = \mathbf{X}^{-1}\mathbf{S}\mathbf{X}$) we may regard $\mathbf{X}$ as a $d\times d$ matrix $(\mathbf{X}_{ij})$, the $\mathbf{X}_{ij}$ unknowns, and consider the system of homogeneous linear equations

$$\begin{pmatrix} \mathbf{X}_{11} & \dots & \mathbf{X}_{1d} \\ \vdots & & \\ \mathbf{X}_{d1} & \dots & \mathbf{X}_{dd} \end{pmatrix} (\mathbf{S}\gamma)(n) - \mathbf{S}(n) \begin{pmatrix} \mathbf{X}_{11} & \dots & \mathbf{X}_{1d} \\ \vdots & & \\ \mathbf{X}_{d1} & \dots & \mathbf{X}_{dd} \end{pmatrix} = 0$$

where d is the degree of the representation $\mathbf{S}$. For each $n\in N$ the evaluation of the left-hand side of the above equation yields a matrix whose $(i,j)^{th}$ entry is a linear combination of the $\mathbf{X}_{ij}$ and which must be equal to zero. It suffices to evaluate this formula for the generators of N coming from the $\mathbf{AG}$-system of N. Any solution of this system of homogeneous linear equations in the $\mathbf{X}_{ij}$ will give

rise to an intertwining matrix. An intertwining matrix in case (2) (that is a matrix $\mathbf{Z}$ such that $\mathbf{S}\gamma = \mathbf{Z}^{-1}(\eta\mathbf{S})\mathbf{Z}$) may be obtained in a similar way.

Chapter 5

An Empirical Study of the Implementation

The basic three parts of W. Plesken's proposal for a Soluble Quotient Algorithm (cf. chapter 2-4) are implemented in the GAP version 2.6 programming environment. The programs are used to implement an algorithm to compute an AG-Presentation for a finite soluble group which is defined by a finite presentation. In order to gain a better understanding of the algorithm we have undertaken an investigation into the implementation of the algorithm. In this chapter we report the findings from sample runs of the programs on a 25 MHz SUN SPARC station. We begin with a more detailed description of the algorithm to set the stage. The following sections give details on the performance analysis and report on the problems that have been found. A major problem has been located and will be addressed in the concluding section of this chapter.

The basic idea of the Soluble Quotient Algorithm proposed by W. Plesken is to lift epimorphisms : Suppose an epimorphism $\varepsilon : G \rightarrow H$ from a finitely presented finite soluble group G onto a finite soluble H is given and let P be the set of prime divisors of $|G|$. For each prime $p \in P$ we calculate the irreducible rep-

resentations of H over the field F_p. Every irreducible representation $\mathbf{R}$ of H over the field F_p is given by an absolutely irreducible representation $\mathbf{T}$ which is realised over its field of character values $F_p(\chi)$ where χ is the character afforded by $\mathbf{T}$ and $\mathbf{R} = \rho\mathbf{T}$ where ρ is a regular representation of $F_p(\chi)$ over F_p. The motivation for this approach is that it was found to be beneficial for the subsequent calculations to compute with representations of small degree over large fields rather than representations of large degree over small fields. For every irreducible representation the second cohomology group $H^2(H, M)$ of H with coefficients in the associated module M is determined. For a representative $\alpha B^2(H, M)$ of every one-dimensional $End_{F_p[H]}(M)$-subspace of $H^2(H, M)$ we check whether the epimorphism ε lifts to an epimorphism $\tilde{\varepsilon} : G \rightarrow \widetilde{H}$ where $\widetilde{H}$ is an extension of H by M corresponding to the factor set α. If such a lift is found the epimorphism ε is replaced by $\tilde{\varepsilon}$ and we repeat the steps just described. If no lift is possible, we have calculated an isomorphism $\varepsilon : G \rightarrow H$.

The performance of the algorithm as described above has been analysed by running selections of examples. In [Jam 88] Jamali calculated presentations for maximal subgroups of nonabelian finite simple groups. Initially, we used a selection of these groups to analyse the performance of the programs. For the purpose of this report we chose a smaller selection of six examples. A group of order 1296 and derived length six (cf. [Ken 90]) :

$$\langle x, y | (xy)^2 y^{-6} = x^4 y^{-1} x y^{-9} x^{-1} y = 1 \rangle.$$

The groups $G(-2, 2, -1)$, $G(-2, 3, -1)$ and $G(2, 2, -3)$ of derived length three and order 1320, 5832 and 6912, where

$$G(l, m, n) = \langle a, b | a b^m a^{-1} b^{-1} a^{-n} b^{1-l} = b a^m b^{-1} a^{-1} b^{-n} a^{1-l} = 1 \rangle.$$

These groups have been investigated by Campbell in (cf. [Cam 75]). The groups $\langle u, v | u^2vu^{-1}vu^{-1}v^{-1}uv^{-2} = u^2v^{-1}uv^{-1}uvu^{-1}v^2 = 1\rangle$ and

$$\langle u, v | uv^2(uv^{-1})^2 = (u^2v)^2u^{-1}vu^2(vuv)^{-1} = 1\rangle$$

of derived length five and order 2400 and 3000 which are due to Kenne (private communication).

Table T

order	T_1	T_2	T_3	T_4
1296:	106.117	7271.067	113.131	7495.450
1320:	231.400	4715.764	680.003	5642.100
2400:	13406.716	51935.300	665.189	66033.567
3000:	238.485	22045.733	363.985	22691.616
5832:	1193.166	73608.382	1231.452	76081.050
6912:	926.550	83369.229	275.769	84589.783

Table T lists CPU times (in seconds) for the calculation of AG-presentations for these groups. T_1, T_2, T_3 and T_4 are the computing times for the calculation of the irreducible representations of finite soluble groups over finite fields, the calculation of the extensions of finite soluble groups by finite irreducible modules, lifting of epimorphisms and the total execution time. From this table, it is seen that at present most of the time is spent on the calculation of the extensions of finite soluble groups by finite irreducible modules.

The calculation of the extensions of the finite soluble group H by a finite irreducible H-module M is based on the consistency test (cf. section 2.3). The evaluation of the associativity conditions yields a system of homogeneous linear equations and we obtain an epimorphism $\vartheta : Z^2(H, M) \rightarrow L$ where L is the vector space of solutions of the system of homogeneous linear equations. The second cohomology group $H^2(H, M)$ of H with coefficients in M is isomorphic to $L/\vartheta(B^2(H, M))$.

In order to evaluate the associativity conditions which yield homogeneous linear equations we designed a particular collection process which is based on a collection process with respect to the AG-presentation for H. For the first implementation we used collection from the right, but later it was found that collection from the right is not practicable for certain groups. Consider the split extension H of a cyclic group $\langle x \rangle$ of order 13 by an elementary abelian group of order 3^3 where the action of x is given by the matrix

$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Then H has the following presentation consisting of the generators x, y_1, y_2, y_3 and the relations $x^{13} = {y_1}^3 = {y_2}^3 = {y_3}^3 = [y_3, y_2] = [y_3, y_1] = [y_2, y_1] = 1$, $x^{-1}y_1x = y_3, x^{-1}y_2x = y_1{}^2y_3{}^2$ and $x^{-1}y_3x = y_2{}^2$. We now evaluate the associativity condition $(y_3x)x^{12} = y_3(xx^{12})$. We have $y_3(xx^{12}) = y_3x^{13} = y_3$. On the other hand we have $(y_3x)x^{12} = (xy_2{}^2)x^{12} = xy_2{}^2x^{12}$. A program written in the C programming language carried out 356.608.065 substitutions in order to produce y_3. The program which implements collection from the left carried out only 93 substitutions !

Table C

order	T_1	T_2	T_3	T_4	T_5	T_6
1296:	41.733	31.115	7198.219	7077.111	73.514	47.594
1320:	57.501	37.411	4620.852	4467.389	78.978	74.485
2400:	241.596	189.452	51504.252	50995.358	409.540	99.354
3000:	141.118	99.501	21805.114	21183.347	541.291	80.476
5832:	265.370	353.463	72989.549	72522.359	344.081	123.109
6912:	216.166	538.914	82614.149	82120.019	336.016	158.114

During the sample runs we collected additional information (Table C) for the extensions of finite soluble groups by finite irreducible modules. T_1, T_2 and

T_3 are the computing times for the calculation of quotient spaces, the calculation of the subspaces $\vartheta(B^2(H,M))$ and the calculation of the vector spaces L. T_4, T_5 and T_6 are the computing times for building and solving the systems of homogeneous linear equations which arise from the consistency tests, the matrix calculations and the collection process from the left (these are the constituents of the collection process for the evaluation of the associativity conditions). From Table C it can be seen that most of the computing time is spent on building and solving systems of homogeneous linear equations. The problem is caused by the large number of equations and indeterminates of the systems of homogeneous linear equations. There are $d(\binom{n}{3} + 2\binom{n}{2} + n) = \frac{d}{6}n(n^2 + 3n + 2)$ homogeneous linear equations in $\frac{d}{2}n(n+1)$ indeterminates arising from a consistency test (n is the number of generators in the AG-system for H and $d = rank(M)$).

With regard to future development, different proposals by Holt (cf. [Hol 85]) and Plesken (cf. Method (B) in [Ple 87]) could be implemented and compared with the one described in section 2.3. Other useful algorithms to implement would be criteria for trivial cohomology : For example, if M is a faithful irreducible H-module, then $H^2(H,M) = 0$ by Satz II.3.3 in [Hup 67]. More criteria may be found in [Gas 52].

The lifting of epimorphisms (cf. chapter 3) is based on solving systems of linear equations. Given an epimorphism $\varepsilon : G \to H$, a finite irreducible H-module M and a factor set α, we construct an extension $\widetilde{H}$ of H by M corresponding to the factor set α. Subsequently the system of linear equations which arises from the equations (*) (see p. 35) is solved. In addition we solve the system of linear equations which arises from the equations (**) (see p. 37) if $\alpha \in B^2(H,M)$. If the epimorphism $\varepsilon : G \to H$ lifts to an epimorphism $\tilde{\varepsilon} : G \to \widetilde{H}$, then preimages for the generators in the AG-system for $\widetilde{H}$ are calculated.

Table L

order	T_1	T_2	T_3	T_4	T_5	T_6
1296:	1.252	5.865	1.850	2.550	96.601	5.013
1320:	5.632	18.950	4.334	6.517	642.183	2.387
2400:	4.552	21.849	4.753	6.517	624.416	3.102
3000:	3.218	41.093	12.704	8.902	294.018	4.050
5832:	7.562	55.563	8.409	9.417	1139.517	10.984
6912:	3.002	31.415	6.802	4.445	217.134	12.971

Table L shows CPU times for the lifting of epimorphisms. T_1 is the computing time for the initialisation of the calculations (e.g. computation of the images of the generators of G under ε in H). T_2 and T_3 are the computing times for the construction of an AG-presentation for $\widetilde{H}$ and the construction of $\widetilde{H}$ as an object within GAP (cf. the function ag() in [NNS 88]). Finally T_4, T_5 and T_6 are the computing times for building and solving the systems of linear equations coming from the equations $(*)$ and $(**)$ and the calculation of preimages.

Apparently, constructing and solving the systems of linear equations coming from the equations $(**)$ is the most expensive task. This is due to the number of equations of the system of linear equations. There are

$$d(n(n+1)/2+n) = \frac{d}{2}(n^2+3n)$$

linear equations arising from the equations $(**)$ (n is the number of generators in the AG-system for H and $d = rank(M)$).

Initially, the preimages for the generators in the AG-system for $\widetilde{H}$ were calculated using the noncommutative Gauss algorithm (NCGA) which constructs an AG-system from a finite generating set for a subgroup of a finite soluble group by repeated formation of powers and commutators (cf. [LNS 84]). If the epimorphism $\varepsilon : G \rightarrow H$ lifts to an epimorphism $\tilde{\varepsilon} : G \rightarrow \widetilde{H}$, then the images of the generators of G under $\tilde{\varepsilon}$ generate $\widetilde{H}$ and the NCGA will produce the initial

AG-system for $\widetilde{H}$. By formation of corresponding powers and commutators of preimages we obtain preimages for the generators in the AG-system for $\widetilde{H}$. The major disadvantage of this technique is that the preimages tend to get rather long. Better results are obtained with the technique described in chapter 3.

The calculation of the irreducible representations of finite soluble groups over finite fields is based on the calculation of representatives of the Galois conjugate classes of absolutely irreducible representations. These representatives are calculated using Clifford's theory for the construction of the irreducible representations of a group from the irreducible representations of a normal subgroup. Going up a composition series $H = H_0 \rhd H_1 \rhd \ldots \rhd H_l = 1$ of a finite soluble group H the representatives of the Galois conjugate classes of absolutely irreducible representations of H_i are constructed from those of H_{i+1} by extending the H_i-invariant representatives of H_{i+1} to representatives of H_i and by inducing up the non-invariant representatives of H_{i+1}. Contrary to the calculation of the irreducible representations of a group over algebraically closed fields we have to consider the character fields of the representatives. There are three cases :

(1) The conjugate with respect to H_i of a representative with character field E is not similar to any Galois conjugate of the representative. In this case the induced representative is absolutely irreducible and cannot be realised over subfields of E.

(2) The conjugate with respect to H_i of a representative with character field E is similar to a Galois conjugate of the representative for a nontrivial Galois automorphism. In this case the induced representative is absolutely irreducible and has to be realised over a subfield of E.

(3) A representative of a Galois conjugate class of H_{i+1} with character field E is invariant. In this case extensions of the representative are constructed and their character fields are extension fields of E.

Table M

order	T_1	T_2	T_3	T_4	T_5	T_6
1296:	7.595	4.670	1.464	59.603	16.801	15.599
1320:	26.603	9.704	5.016	118.124	18.284	52.439
2400:	15.966	12.384	4.099	13296.550	12.868	64.185
3000:	68.533	12.168	11.100	55.246	22.169	68.499
5832:	772.168	34.628	31.734	164.122	66.735	121.516
6912:	224.351	22.364	22.588	627.931	7.932	18.079

Table M shows CPU times for the calculation of the irreducible representations of finite soluble groups over finite fields. T_1, T_2 and T_4 are the computing times for testing similarity of irreducible representations, for the calculation of conjugate representations of irreducible representations of H_{i+1} with respect to H_i and for the calculation of intertwining matrices. T_3, T_5 and T_6 are the computing times for the subsequent calculations in case (1), (2) and (3). It can be seen that at present testing similarity and finding intertwining matrices are the areas for further investigations (initially we had difficulties handling case (2) in an efficient way).

The algorithm for the calculation of an AG-presentation for a finitely presented finite soluble group G produces a chief series

$$H = H'_0 \rhd H'_1 \rhd \ldots \rhd H'_m = 1$$

for a factor group H of G. There is a one-to-one correspondence between the representations of H/H'_i and the representations of H/H'_{i+1} with kernel containing H'_i/H'_{i+1}. Furthermore, under this correspondence, irreducible representations correspond to irreducible representations. This fact may be used to improve the calculation of the irreducible representations of finite soluble groups over finite fields : Going down the chief series we calculate the irreducible representations of H'_i/H'_{i+1}, discard the trivial representation and apply the techniques described

in chapter 4 to the remaining representations. Note that the restriction of a representation of H/H'_{i+1} to H'_i/H'_{i+1} is a multiple of the trivial representation if and only if the kernel of the representation contains H'_i/H'_{i+1}. If we keep information from earlier stages (e.g. the irreducible representations of H/H_j, $j < m$) we only have to apply the algorithm above for $i = j+1, \ldots, m$. This "top down" algorithm reduces the burden on the similarity test since there are at any time less representations to consider than in the "bottom up" algorithm.

With regard to future development we also mention Baum's dissertation (cf. [Bau 91]). He describes an algorithm for the calculation of the irreducible representations of finite supersoluble groups. Every supersoluble group has a chief series with cyclic factors. Moreover, every irreducible representation of a supersoluble group is monomial, i.e. every element of a supersoluble group is mapped under an irreducible representation onto a matrix which has exactly one nonzero entry in each row and column. In order to test similarity he used these facts and designed a recursive procedure for the calculation of intertwining matrices. This algorithm is considered to be the reason for the spectacular performance of his programs. His techniques may perhaps be generalised to the calculation of the irreducible representations of a finite soluble group along a chief series.

In view of an application of the programs the following remarks are relevant. The algorithm proceeds by "trial and error" : Whenever an epimorphism of G onto a finite soluble group H is constructed, one tries to lift it onto extensions of H by finite irreducible H-modules. Earlier in this chapter we have seen that the most expensive tasks depend on the rank of the H-modules. In the course of the computations modules of increasing rank occur, but the epimorphism actually does not lift onto extensions of H by these modules. It therefore appears to be reasonable to impose an upper bound on the degree of the modules. The irreducible representations of degree less than or equal to b may be calculated as

follows. We observe that as we go up a composition series

$$H = H_0 \rhd H_1 \rhd \ldots \rhd H_l = 1$$

of a soluble group H the degree of the representations increases. Hence as we pass from H_{i+1} to H_i we may discard the irreducibles of H_i of degree larger than b. Since this modified algorithm performed on H_{i+1} provides all irreducible representations of H_{i+1} of degree less than or equal to b we may use the techniques described in chapter 4 in order to test similarity.

The preceding remarks on the rank of the modules and the degree of the representations respectively may be translated in the language of groups. If

$$H = H'_0 \rhd H'_1 \rhd \ldots \rhd H'_m = 1$$

is a chief series for H, then the chief factors are elementary abelian. If $|H'_i/H'_{i+1}| = {p_i}^{r_i}$, then $r(G) = \max r_i$ is called the rank of H. The bound b introduced above thus sets a bound on the rank of the factor groups of G. The groups mentioned in the beginning of this chapter all have rank two. Using this information we can compute AG-presentations for these groups much faster. Table T' lists CPU times for the calculation of AG-presentations for these groups (cf. Table T).

Table T'

order	T_1	T_2	T_3	T_4
1296:	10.316	122.949	25.166	160.950
1320:	16.184	111.001	101.735	232.483
2400:	12.350	247.083	77.283	341.917
3000:	8.700	106.135	22.497	139.517
5832:	71.535	205.868	124.102	409.066
6912:	89.950	487.415	68.500	652.183

Chapter 6

Applications

In 1978 Johnson and Robertson gave a survey of known finite groups of deficiency zero. They observed that all known finite soluble groups of deficiency zero had derived length less than or equal to four and asked whether there is bound on the derived length of a finite soluble group of deficiency zero. The first example of a finite group of derived length five and deficiency zero was given by Kenne in 1988. In [Ken 90] Kenne gave examples of finite groups of derived length six and deficiency zero. He considered non-abelian p-groups G of order p^3 and exponent $p \in \{3, 5\}$ and constructed split extensions of subgroups of the automorphism group $Aut(G)$ by G. He then applied techniques described in [Ken 86] in order to find efficient presentations for these groups. In section 6.1 we use the programs for the calculation of finite soluble factor groups of finitely presented groups to find finite soluble groups of increasing derived length and trivial Schur multiplier. The method suggested by Kenne is then used to find efficient presentations for the constructed groups. We give further examples of finite groups of deficiency zero having derived length five and six. In the course of the computations we noticed that Kenne's method is only applicable for groups of moderate order. Therefore, for a given derived length the minimal soluble groups appeared to be of interest. In section 6.2 we classify the minimal soluble groups of derived length less than or equal to six.

6.1 Efficient Finite Soluble Groups

The *deficiency of a finite presentation* $\langle X|R\rangle$ is defined to be $|X|-|R|$, and the *deficiency* $def(G)$ *of a group* G is the maximum of $|X|-|R|$ taken over all finite presentations of G. It is easy to show that if $\langle X|R\rangle$ is a finite presentation for a finite group, then $|X|\leq|R|$. Therefore finite groups have non-positive deficiency. An upper bound for $def(G)$ is given in terms of the rank of the Schur multiplier $M(G)$ of G. In 1907 Schur showed (cf. Satz V.25.2 in [Hup 67]) that if G is a group with a presentation $\langle X|R\rangle$, then

$$|X|-|R| \leq -rank(M(G)). \tag{1}$$

A group G is said to be *efficient* if equality holds in (1).

In 1978 Johnson and Robertson (cf. [JoR 79]) gave a survey of known finite groups of deficiency zero. They observed that all known finite soluble groups of deficiency zero had derived length less than or equal to four and asked whether there is a bound on the derived length of a finite soluble group of deficiency zero. The first example of a finite group of derived length five and deficiency zero was given by Kenne in 1988. In [Ken 90] Kenne gave examples of finite groups of derived length six and deficiency zero.

In this section, we give further examples of finite groups of deficiency zero having derived length five and six. We also give an example of a soluble group of derived length seven and deficiency one and a possible candidate for a soluble group of derived length seven and deficiency zero. The programs for the calculation of finite soluble factor groups of finitely presented groups are used to find efficient soluble groups of increasing derived length in the following way. We start with a known group G (e.g. the symmetric group S_3 of degree three or the alternating group A_4 of degree four). Using the programs we calculate an AG-presentation for G which is used to determine the extensions of G by finite irreducible $F_p[G]$-modules (e.g. $p\in\{2,3\}$). For each extension we compute the

derived length and choose a small group of larger derived length. A method suggested by Kenne (cf. [Ken 86]) is then used to find an efficient presentation for the selected group and the procedure is repeated.

We will require a method for calculating the Schur multiplier $M(G)$ of a group G. One possible approach depends upon a presentation for G by generators and relations. First we mention a few elementary facts about the Schur multiplier. A thorough treatment of the general theory of the Schur multiplier appears in section V.23 of [Hup 67]. Satz V.23.5 (a) and (c) show that the Schur multiplier $M(G)$ is abelian and finite, while (d) shows that there exists a representation group C of G, that is, $C/A \cong G$ for suitable $A \leq C' \cap Z(C)$ with $A \cong M(G)$. Moreover, the proof of Satz V.23.5 (e) shows that if π is a homomorphism of a group H onto G such that $ker(\pi) \leq H' \cap Z(H)$, then $ker(\pi)$ is a homomorphic image of the Schur multiplier of G and H is a homomorphic image of some representation group of G. This describes the underlying theory of the Schur multiplier; it remains to discuss its actual calculation. Using a Todd-Coxeter coset enumeration program the Schur multiplier may be calculated from the largest group H such that $H/A \cong G$ for suitable $A \leq H' \cap Z(H)$.

EXAMPLE Consider the alternating group A_4 with generators r and s satisfying the relations $r^3 = s^2 = (rs)^3 = 1$. A representation group of A_4 has a presentation of the form $\langle r, s, t | r^3 t^{\alpha_1} = s^2 t^{\alpha_2} = (rs)^3 t^{\alpha_3} = [t, r] = [t, s] = 1 \rangle$ for suitable α_i, $i = 1, 2, 3$. We calculate an invertible 3×3 integer matrix $\mathbf{P}$ such that the product $\mathbf{P} \cdot \mathbf{M}$ of $\mathbf{P}$ and the relation matrix $\mathbf{M}$ determined by the presentation for A_4 is a triangular matrix :

$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & 1 \\ -2 & -3 & 2 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 2 \\ 3 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Let $\mathbf{P}^{-1} = (p_{ij})$ and take $\alpha_i = p_{i3}$ for $i = 1, 2, 3$. Hence some representation group of A_4 has the presentation $\langle r, s, t | r^3t = s^2t^{-1} = (rs)^3 = [t, r] = [t, s] = 1 \rangle$. Coset enumeration shows that $|M(A_4)| = 2$.

The problem of determining a method whereby it can be efficiently recognised whether a group G is isomorphic to another group H is called the isomorphism problem. Since the groups in this section are 2-generator groups the isomorphism problem is easily solved. The idea is to search for elements in H which generate a group of order $|G|$ and satisfy a set of defining relations for G. Suppose $G = \langle x, y \rangle$, where $|x| = n$ and $|y| = m$. It is sufficient to take the set of representatives of the classes of elements of order n of H as possible images of x and the set of all elements of order m of H as possible images of y. The group H must be given explicitly enough that multiplication can be carried out and equality of elements can be decided. For example, if H is finite and soluble, it suffices that H is given by an AG-presentation. Moreover, the groups in this section will have faithful permutation representations of reasonable degree.

We start with the symmetric group S_3 of degree three (the split extension of $GL_1(3)$ by its natural module) with generators r and s satisfying the relations $r^3 = s^2 = (rs)^2 = 1$. The Schur multiplier $M(S_3) = 1$. In order to show that S_3 is efficient we have to show that S_3 has a presentation with two generators and two relations. In [CaR 82] Campbell and Robertson describe a technique for reducing the number of relations in a presentation. Let H be the group obtained by combining two relations as follows $H = \langle a, b | a^3b^2 = (ab)^2 = 1 \rangle$. Clearly, S_3 is a homomorphic image of H and H is a homomorphic image of some representation group of S_3. Thus H is isomorphic to S_3 because $M(S_3) = 1$.

Since $S_3 \cong GL_2(2)$ we know that S_3 has a faithful irreducible representation $\mathbf{R}$ of degree two over F_2 defined by

$$a \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$b \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The split extension G of S_3 by the module associated with this representation of S_3 is generated by r, s, t_1 and t_2 subject to the defining relations $r^3s^2 = (rs)^2 = 1, r^{-1}t_ir = \prod t_j^{\mathbf{R}(a)_{ij}}, s^{-1}t_is = \prod t_j^{\mathbf{R}(b)_{ij}}, t_i^2 = 1$ for $i = 1,2$ and $[t_2, t_1] = 1$. Coset enumeration shows that $x = st_1$ and $y = rs$ generate G and that G has defining relations $x^4 = y^2 = (xy)^3 = 1$. Hence G is isomorphic to S_4 (note that S_4 has derived length three).

The Schur multiplier of S_4 is isomorphic to the cyclic group of order two and therefore S_4 is efficient. The symmetric group S_4 of degree four has two representation groups :

(1) Let G be the group generated by r, s and t subject to the defining relations $r^4 = t, s^2 = (rs)^3 = [t, r] = [t, s] = t^2 = 1$. Coset enumeration shows that $x = s$ and $y = sr^{-1}$ generate G. The following efficient presentation for G was found $\langle x, y | x^2y^3 = ((xy)^2x^{-1}y^{-1})^2 = 1 \rangle$. The map

$$x \mapsto \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$$

$$y \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

extends to an isomorphism $\mathbf{R}$ onto the general linear group $GL_2(3)$ of dimension two over the field F_3 of order three.

(2) Let G_1 be the group generated by r, s and t subject to the defining relations $r^4 = s^2 = t, (rs)^3 = [t,r] = [t,s] = t^2 = 1$. Coset enumeration shows that $x = sr^{-1}$ and $y = tr^{-1}$ generate G_1. The following efficient presentation for G_1 was found $\langle x, y | x^2yx^{-1}y = xy^3xy^{-1} = 1 \rangle$.

The representation groups of S_4 have derived length four and faithful permutation representations for these groups can be obtained by enumeration of the cosets with respect to the Sylow 3-subgroups. Other groups of derived length four are obtained by the split extensions of S_4 by the faithful irreducible $F_3[S_4]$-modules. These groups are isomorphic to maximal subgroups of $PSU_4(2)$ and A_9, respectively (cf. [Jam 88]).

A group of derived length five is obtained by constructing the split extension $3^2 : GL_2(3)$ of $GL_2(3)$ by the modules associated with the faithful irreducible representation of $GL_2(3)$ as defined above. This group is generated by r, s, t_1 and t_2 subject to the defining relations $r^2s^3 = ((rs)^2r^{-1}s^{-1})^2 = 1, r^{-1}t_ir = \prod t_j^{\mathbf{R}(x)_{ij}}, s^{-1}t_is = \prod t_j^{\mathbf{R}(y)_{ij}}, t_i^3 = 1$ for $i = 1,2$ and $[t_2,t_1] = 1$. Jamali (cf. [Jam 88]) found the following presentation for the maximal subgroup of order 432 of the projective special linear group $PSL_3(3)$ of dimension three over the field F_3 of order three

$$H = \langle x, y | x^2y^3 = (xy)^3(xy^{-1}xy)^2x^{-1}yxy^{-1}x^{-1}y(x^{-1}y^{-1})^3x^{-1}y = 1 \rangle.$$

Coset enumeration shows that the map $x \mapsto r$ and $y \mapsto st_1t_2^{-1}$ extends to an isomorphism of H onto $3^2 : GL_2(3)$.

Note that $GL_2(3)$ actually has two faithful irreducible representations of degree two over the field F_3, but the split extensions of $GL_2(3)$ by the associated modules are isomorphic. Another group of derived length five is obtained by constructing the split extension of G_1 by the module associated with the faithful irreducible representation of degree four over F_3.

We now consider the extensions of $3^2 : GL_2(3)$ by the module associated with the alternating representation of $3^2 : GL_2(3)$ over the field F_3. There are the following non-isomorphic groups of derived length six :

(1) Let G be the group generated by r, s and t subject to the defining relations $r^2s^3 = (rs)^3(rs^{-1}rs)^2r^{-1}srs^{-1}r^{-1}s(r^{-1}s^{-1})^3r^{-1}s = [t,r] = t, [t,s] = t^3 = 1$. Coset enumeration shows that $x = s^2rsrsr$ and $y = s^2rsr$ generate G. The following efficient presentation for G was found $\langle x,y|(xy)^2xy^{-2}x^{-1}y = x^2yx^{-2}yx^2y^{-2} = 1\rangle$.

(2) Let G be the group generated by r, s and t subject to the defining relations $(rs)^3(rs^{-1}rs)^2r^{-1}srs^{-1}r^{-1}s(r^{-1}s^{-1})^3r^{-1}s = [t,r] = t, r^2s^3 = [t,s] = t^3 = 1$. Coset enumeration shows that $x = ts^{-1}rsrsr$ and $y = ts^{-1}rsr$ generate G. The following efficient presentation for G was found $\langle x,y|xy(x^{-1}y)^2xy^{-2} = x^2yx^{-1}y^{-3}xy^2 = 1\rangle$.

(3) Let G_2 be the group generated by r, s and t subject to the defining relations $(rs)^3(rs^{-1}rs)^2r^{-1}srs^{-1}r^{-1}s(r^{-1}s^{-1})^3r^{-1}s = [t,r] = t, r^2s^3t = [t,s] = t^3 = 1$. In [Ken 90] Kenne gave the following efficient presentation for a group of order 1296 and derived length six :

$$H = \langle x,y|(xy)^2y^{-6} = x^4y^{-1}xy^{-9}x^{-1}y = 1\rangle.$$

Coset enumeration shows that the map $x \mapsto ts^{-1}r, y \mapsto s^2rsrs^{-1}(rs)^3r$ extends to an isomorphism of H onto G_2.

Faithful permutation representations for these groups can be obtained by enumeration of the cosets with respect to the Sylow 2-subgroups.

The group G_2 of derived length six may be used to construct a small group of derived length seven. It has a faithful irreducible representation $\mathbf{R}$ of degree six over the field of order two F_2 defined by

$$x\mapsto\begin{pmatrix}0&1&1&0&1&1\\1&0&1&1&0&1\\1&1&1&1&1&1\\0&1&0&1&0&1\\1&1&1&0&0&1\\0&1&1&1&1&0\end{pmatrix}$$

$$y\mapsto\begin{pmatrix}1&0&0&1&0&1\\0&1&1&1&1&1\\1&0&1&1&1&0\\0&1&1&0&0&1\\1&0&1&0&1&1\\0&1&0&1&1&0\end{pmatrix}.$$

The split extension G of G_2 by the module associated with this representation is generated by r, s and $t_1,\ldots,t_6$ subject to the defining relations $(rs)^2s^{-6} = r^4s^{-1}rs^{-9}r^{-1}s = 1, r^{-1}t_ir = \prod t_j^{\mathbf{R}(x)_{ij}}, s^{-1}t_is = \prod t_j^{\mathbf{R}(y)_{ij}}, t_i^2 = 1$ for $i = 1,\ldots,6$ and $[t_j,t_i] = 1$ for $1\leq j < i\leq 6$. Coset enumeration shows that $x = rs$ and $y = s^{-1}t_1$ generate G and that G has defining relations $x^2 = y^6 = (xyxy^{-1}xy^2)^2 =$

$$(xy)^2(xy^3)^2(xy^{-1})^3y^{-1}xy^{-1}(xy^{-2})^2y^{-1} =$$

$(xy)^2(xy^2)^2yxy(xy^{-2})^2y^{-1}xy^2(xy^{-2})^2 = 1$. The Schur multiplier of G is isomorphic to the cyclic group of order two and therefore an efficient presentation has two generators and three relations. It is easily verified that the relation $(xyxy^{-1}xy^2)^2$ is redundant. Let H be the group obtained by combining two relations as follows $H = \langle a,b|a^2b^6 = (ab)^2(ab^3)^2(ab^{-1})^3b^{-1}ab^{-1}(ab^{-2})^2b^{-1} = (ab)^2(ab^2)^2bab(ab^{-2})^2b^{-1}ab^2(ab^{-2})^2 = 1\rangle$. Clearly G is a homomorphic image of

H and H is a homomorphic image of some representation group of G. In [JaR 89] Jamali and Robertson describe a technique which allows one to determine whether H is isomorphic to G by using a coset enumeration program (see also lemma 2.2 in [CaR 82]). Let $\eta : H \rightarrow G$ be the epimorphism defined by $a \mapsto x$ and $b \mapsto y$. Take $h = b^2$; then $\eta(h) = y^2$ has order 3 and $\gcd(|\eta(h)|, m) = 1$ where $m = |M(G)|$. If $[H : \langle h^m \rangle]$ can be found, then $|H| = [H : \langle h^m \rangle]|\eta(h)|$. Coset enumeration shows that $[H : \langle h^m \rangle] = 27648$, proving that $H \cong G$. Note that G_2 actually has three faithful irreducible representations of degree six over F_2, but the split extensions of G_2 by the associated modules are isomorphic.

We may also start with the alternating group A_4 of degree four (the split extension of $SL_2(2)$ by its natural module) with generators r and s satisfying the relations $r^3 = s^2 = (rs)^3 = 1$. The Schur multiplier $M(A_4)$ is isomorphic to the cyclic group of order two and therefore A_4 is efficient.

The representation group G of A_4 is generated by r, s and t subject to the defining relations $s^2 = t, r^3 = (rs)^3 = [t, r] = [t, s] = t^2 = 1$. Coset enumeration shows that $x = rsr$ and $y = s^{-1}$ generate G. The following efficient presentation for G was found $\langle x, y | x^3 = y^2, (x^{-1}y)^3 = 1 \rangle$. The representation group of A_4 has derived length three and a faithful permutation representation for this group can be obtained by enumeration of the cosets with respect to the Sylow 3-subgroups. It is easily verified that the map

$$x \mapsto \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

$$y \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

extends to an isomorphism $\mathbf{R}$ onto the special linear group $SL_2(3)$ of dimension two over the field F_3 of order three. Another group of derived length three is the split extension of A_4 by its faithful irreducible $F_3[A_4]$-module.

The split extension $3^2 : SL_2(3)$ by the module associated with the representation above is generated by r, s, t_1 and t_2 subject to the defining relations $r^3 = s^2, (r^{-1}s)^3 = 1, r^{-1}t_i r = \prod t_j^{\mathbf{R}(x)_{ij}}, s^{-1}t_i s = \prod t_j^{\mathbf{R}(y)_{ij}}, t_i^2 = 1$ for $i = 1, 2$ and $[t_2, t_1] = 1$. Jamali (cf. [Jam 88]) found the following presentation for the maximal subgroup of order 216 of the alternating group A_9 of degree nine :

$$H = \langle x, y | y^3 = (yx)^4 x^{-3} = (yxy)^2 x^{-2} (yxy)^{-2} x^{-1} = 1 \rangle.$$

Coset enumeration shows that the map $x \mapsto r^2, y \mapsto r t_2 s^{-1}$ extends to an isomorphism of $3^2 : SL_2(3)$, which has derived length four, onto H.

The Schur multiplier of $3^2 : SL_2(3)$ is isomorphic to the cyclic group of order three and therefore $3^2 : SL_2(3)$ is efficient. $3^2 : SL_2(3)$ has the following representation groups :

(1) Let G be the group generated by r, s and t subject to the defining relations $s^3 = t, (sr)^4 r^{-3} = (srs)^2 r^{-2} (srs)^{-2} r^{-1} t = [t, r] = [t, s] = t^3 = 1$. Coset enumeration shows that $x = r^2 s^{-1}$ and $y = rsrt^{-1}$ generate G. The following efficient presentation for G was found

$$\langle x, y | xy^2 x^{-1} y^2 xy^{-1} = xyxy^{-1} x^{-1} y^{-2} x^{-1} y^{-1} = 1 \rangle.$$

(2) Let G be the group generated by r, s and t subject to the defining relations $(srs)^2 r^{-2} (srs)^{-2} r^{-1} = t, s^3 = (sr)^4 r^{-3} t = [t, r] = [t, s] = t^3 = 1$. Coset enumeration shows that $x = s^{-1}$ and $y = sr^{-1}$ generate G. The following efficient presentation was found

$$\langle x, y | (xy)^2 x^{-2} y^{-5} = xy^2 x^{-1} y^3 x^{-1} y^2 = 1 \rangle.$$

(3) Let G_3 be the group generated by r, s and t subject to the defining relations $(sr)^4 r^{-3} = t, s^3 t = (srs)^2 r^{-2} (srs)^{-2} r^{-1} = [t, r] = [t, s] = t^3 = 1$. Jamali (cf. [Jam 88]) found the following presentation for a maximal subgroup of order 648 of $PSU_4(2)$:

$$H = \langle x, y | x^3 y (x^{-1} y)^2 = x^2 yxyx^{-1} y^{-1} x^{-1} yxy = 1 \rangle.$$

Coset enumeration shows that the map $x \mapsto sr$ and $y \mapsto rs^{-1}r^{-1}sr^{-1}$ extends to an isomorphism of G_3 onto H.

All three groups have derived length five and faithful permutation representations for these groups can be found by enumeration of the cosets with respect to the Sylow 2-subgroups.

The group G_3 of derived length five may be used to construct a group of derived length six. It has a faithful irreducible representation $\mathbf{R}$ of degree six over the field of order two F_2 defined by

$$x \mapsto \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and

$$y \mapsto \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The split extension $2^6 : G_3$ of G_3 by the module associated with this representation is generated by r, s and $t_1, \ldots, t_6$ subject to the defining relations $r^3s(r^{-1}s)^2 = r^2srsr^{-1}s^{-1}r^{-1}srs = 1, r^{-1}t_ir = \prod t_j^{\mathbf{R}(x)_{ij}}, s^{-1}t_is = \prod t_j^{\mathbf{R}(y)_{ij}}, t_i^2 = 1$ for $i = 1, \ldots, 6$ and $[t_j, t_i] = 1$ for $1 \leq j < i \leq 6$. Coset enumeration shows that $x = r^3t_3$ and $y = t_1rs$ generate $2^6 : G_3$ and that $2^6 : G_3$ has defining relations $(xy)^3y^6 = xyx^{-1}yxy^3xyx^{-1}yxy^{-1} = x^2y^{-2}xyx^{-1}y^3xy^{-1}x^{-1}y^2 = 1$. The Schur multiplier of $2^6 : G_3$ is isomorphic to the cyclic group of order two and therefore

$2^6 : G_3$ is efficient. Note that G_3 has three faithful irreducible representations of degree six over F_2, but the split extensions of G_3 by the associated modules are isomorphic.

The representation group G of $2^6 : G_3$ is generated by r, s and t subject to the defining relations $(rs)^3 s^6 t = rsr^{-1}srs^3rsr^{-1}srs^{-1}t = r^2s^{-2}rsr^{-1}s^3rs^{-1}r^{-1}s^2 = [r,t] = [s,t] = 1$. The group G has derived length seven and trivial Schur multiplier, but we were unable to find an efficient presentation for G. A faithful permutation representation for G can be obtained by enumeration of the cosets with respect to the Sylow 3-subgroups.

We shall now derive some results on extensions of finite soluble groups by finite irreducible modules. We begin with an elementary observation. If g, $h \in G$, the commutator of g and h is defined by $[g,h] = g^{-1}h^{-1}gh$. If $\pi : G \to H$ is an epimorphism, then $\pi([g,h]) = [\pi(g), \pi(h)]$. Hence $\pi(G') \subseteq H'$. Moreover, every commutator $[x,y]$ for x, $y \in H$ is in $\pi(G')$. Then $\pi(G') = (\pi(G))' = H'$, so π restricted to G' is an epimorphism of G' onto H'. By induction we have

$$\pi(G^{(i)}) = (\pi(G))^{(i)} = H^{(i)}.$$

Let $1 \to M \xrightarrow{\mu} G \xrightarrow{\pi} H \to 1$ be a short exact sequence where H is a finite soluble group of derived length n and M is a finite H-module. Then $1 = H^{(n)} = (\pi(G))^{(n)} = \pi(G^{(n)})$ and therefore $G^{(n)} \subseteq \mu(M)$. Hence G has derived length n or $n+1$.

THEOREM 6.1 Let $1 \to M \xrightarrow{\mu} G \xrightarrow{\pi} H \to 1$ be a short exact sequence where H is a finite soluble group of derived length n and M is a finite irreducible H-module. If G has derived length n, then $H^{(n-1)}$ is contained in the kernel of the representation associated with the action of H on M.

Proof Let $N = \mu(M)$. The $(n-1)st$ derived subgroup $H^{(n-1)}$ is contained in the kernel of the representation associated with the action of H on M if and only

if $[N, G^{(n-1)}] = 1$. Consider the normal subgroup $G^{(n-1)} \cap N$ of G. Since N is a minimal normal subgroup, $G^{(n-1)} \cap N$ is either N or 1.

Now, $G^{(n-1)} \cap N = N$ implies $N \leq G^{(n-1)}$ and thus $[N, G^{(n-1)}] \leq [G^{(n-1)}, G^{(n-1)}] = G^{(n)} = 1$. In the case $G^{(n-1)} \cap N = 1$, we have $[N, G^{(n-1)}] \leq G^{(n-1)} \cap N$ by Hilfssatz III.1.6(f) in [Hup 67]. □

Theorem 6.1 explains the observation that an extension of a finite soluble group of derived length n by a faithful irreducible module has derived length $n + 1$. The reverse of the assertion does not hold for arbitrary extensions. Consider the symmetric group S_4 of degree four. The Schur multiplier $M(S_4)$ is isomorphic to the cyclic group of order two and the representation groups of S_4 have derived length four. But the reverse holds for split extensions.

THEOREM 6.2 Let H be a finite soluble group of derived length n and let M be a finite irreducible H-module. If $H^{(n-1)}$ is contained in the kernel of the representation associated with the action of H on M, then the split extension of H by M has derived length n.

Proof Suppose the short exact sequence $1 \to M \xrightarrow{\mu} G \xrightarrow{\pi} H \to 1$ splits and let $N = \mu(M)$. Then $G^{(n-1)} \cap N$ is either N or 1.

If $G^{(n-1)} \cap N = 1$, then the preimage of $H^{(n-1)}$ is the semidirect product of $G^{(n-1)}$ and N. By the second isomorphism theorem we have

$$H^{(n-1)} \cong G^{(n-1)} N/N \cong G^{(n-1)}/G^{(n-1)} \cap N \cong G^{(n-1)}$$

and therefore $G^{(n)} = 1$.

If $G^{(n-1)} \cap N = N$, then $N \leq G^{(n-1)}$ and therefore $G^{(n-1)} N = G^{(n-1)}$. We conclude that $G^{(n-1)}$ is isomorphic to the semidirect product of $H^{(n-1)}$ and N. But the action of $H^{(n-1)}$ on N is trivial and thus $G^{(n-1)}$ is isomorphic to the direct product $H^{(n-1)} \times N$ and therefore $G^{(n-1)}$ is abelian. □

We have already seen that faithful irreducible modules are useful for the construction of finite soluble groups. The calculations which led to the groups pre-

sented in this section suggest that extensions of finite soluble groups by finite faithful irreducible modules split.

COROLLARY 6.3 If $1 \to M \xrightarrow{\mu} G \xrightarrow{\pi} H \to 1$ is a short exact sequence where H is a finite soluble group and M a finite faithful irreducible H-module, then the short exact sequence splits (i. e. $H^2(H, M) = 0$).

Proof Obviously $N = \mu(M)$ is a minimal normal subgroup of G such that $N = C_G(N)$. The result follows from Satz II.3.3 in [Hup 67]. □

Satz II.3.3 also shows how to obtain a faithful permutation representation for a finite soluble group G which has a minimal normal subgroup N with $C_G(N)$.

Next we obtain a result on the normal subgroup structure of the groups presented in this section.

THEOREM 6.4 Let $1 \to M \xrightarrow{\mu} G \xrightarrow{\pi} H \to 1$ be a short exact sequence where H is a finite soluble group of derived length n and M is a finite irreducible H-module. If G has derived length $n + 1$ and the commutator series is the only normal series of H, then the commutator series is the only normal series of G.

Proof Let $N = \mu(M)$. Since G has derived length $n + 1$ and N is a minimal normal subgroup of G, we have $G^{(n)} = N$. All we have to show is that N is the unique minimal normal subgroup of G. Let K be a minimal normal subgroup of G and consider the normal subgroup $N \cap K$ of G. Since N is a minimal normal subgroup, we have $N \cap K$ is either N or 1.

If $N \cap K = N$, then $N \leq K$ and $N = K$ since K is a minimal normal subgroup of G. If $N \cap K = 1$, we consider the product NK which is a normal subgroup of G. Since $N \subset NK$ it must coincide with one of the commutator subgroups $G^{(i)}$, $i = 0, \ldots, n-1$. However, $[N, K] \subseteq N \cap K$ by Hilfssatz III.1.6(f) in [Hup 67] and therefore NK is abelian — a contradiction. □

Using theorem 6.4 we see that by construction the commutator subgroups are the only normal subgroups of the groups presented in this section. Note that finite groups with a unique minimal normal subgroup have faithful irreducible representations. If F is a field such that $char(F) \nmid |G|$, then the regular representation is completely reducible. Suppose every irreducible representation of G over F has a nontrivial kernel. Then the kernel of every irreducible representation contains the minimal normal subgroup and therefore the regular representation of G over F has a nontrivial kernel — a contradiction.

Another problem being investigated using the techniques in this section is that of constructing examples of soluble groups for which the orders of the derived factors decrease. To be more specific, we are looking for examples of soluble groups G for which $a_1 \geq a_2 \geq \ldots \geq a_{n-1}$, where $a_i = [G^{(i)} : G^{(i+1)}]$ and n is reasonably large, say $n \geq 4$. This problem is due to E. A. Bertram (University of Hawaii at Manoa) and is related to the problem of finding "good" lower bounds to the number of conjugate classes of soluble groups.

By Hilfssatz I.9.9 of [Hup 67] we have $(G \times H)' = G' \times H'$ for given groups G and H. Hence we may start with a soluble group of derived length 4 (e. g. the general linear group $GL_2(3)$ for dimension 2 over the field F_3). The sequence of orders of derived factor groups of $GL_2(3)$ is $(2, 3, 4, 2)$. The group generated by x, y subject to the defining relations $x^2 = y^m = 1$ and $x^{-1}yx = y^{-1}$ is a finite group of order $2m$ (the Dihedral group D_{2m}). The group D_{2m} has a cyclic normal subgroup $N = \langle y \rangle$ of order m and $\langle x \rangle$ is a complement of N in G. We conclude that D_{2m} is metabelian and that $[D_{2m} : D_{2m}'] = 2$ if m is odd and $[D_{2m} : D_{2m}'] = 4$ if m is even. The elements of D_{2m} are

$$1 , y , y^2 , \ldots , y^{m-1} , xy , \ldots , xy^{m-1}.$$

Since $y^{-1}(xy^i)y = y^{-1}xy^{i+1} = xy^{i+2}$ we see that xy^i is conjugate to xy^{i+2} for

every i. Also, since $xy^ix = y^{-i}$ we see that y^i is conjugate to y^{-i}. If m is odd, then the conjugate classes are $\{1\}, \{xy, \ldots, xy^{m-1}\}, \{y^i, y^{-i}\}$ for $1 \leq i \leq (m-1)/2$ and D_{2m} has $2 + (m-1)/2 = (m+3)/2$ conjugate classes. If m is even, the conjugate classes are $\{1\}, \{x, xy^2, \ldots, xy^{m-2}\}, \{xy, xy^3, \ldots, xy^{m-1}\}, \{y^{m/2}\}, \{y^i, y^{-i}\}$ for $1 \leq i \leq (m-2)/2$ and D_{2m} has $4 + (m-2)/2 = (m+6)/2$ conjugate classes. The sequence of orders of derived factor groups of $GL_2(3) \times D_6$ is $(4, 9, 4, 2)$ and $GL_2(3) \times D_6$ has $8 \cdot 3 = 24$ conjugate classes.

With the help of Theorem 6.2 we may also start with a group G of derived length 4 (e. g. the general linear group $GL_2(3)$ of dimension 2 over F_3) and construct split extensions of G by finite irreducible $F_p[G]$-modules. Obviously the split extension of $GL_2(3)$ by the modules associated with the trivial representations over the fields F_2 and F_3 yield groups for which the sequences of orders of derived factor groups are $(4, 3, 4, 2)$ and $(6, 3, 4, 2)$ respectively. The split extension of $GL_2(3)$ by the module associated with the alternating representation over the field F_3 has 15 conjugate classes and the sequence of orders of derived factor groups is $(2, 9, 4, 2)$. The split extension of $GL_2(3)$ by the module associated with the irreducible representation of degree 2 over F_2 has the sequence $(2, 3, 16, 2)$. The split extensions of $GL_2(3)$ by the modules associated with the irreducible representations of degree 3 over F_3 have the sequence $(2, 3, 4, 54)$. Note that every representation mentioned above is a faithful irreducible representation of some derived factor group of $GL_2(3)$. This observation brings us to the concluding theorem in this section.

THEOREM 6.5 Let H be a finite soluble group and M a finite irreducible H-module. Suppose the short exact sequence $1 \to M \xrightarrow{\mu} G \xrightarrow{\pi} H \to 1$ splits. If $H^{(i)}$ is and $H^{(i-1)}$ is not contained in the kernel of the representation associated with the action of H on M, then $G^{(i)} \cong H^{(i)} \times M$.

Proof Since $H^{(i-1)}$ is not contained in the kernel of the representation associated with the action of H on M, there exist $x \in N = \mu(M)$ and $y \in G^{(i-1)}$ such that

$[x,y] \neq 1$. Therefore $[x,y]$ is a nontrivial element of $G^{(i-1)} \cap N$. Since N is a minimal normal subgroup of G, we conclude that $N \subseteq G^{(i-1)}$. But this implies $[x,y] \in G^{(i)}$ and therefore $[x,y]$ is a nontrivial element of $G^{(i)} \cap N$. We conclude that $N \subseteq G^{(i)}$ and that $G^{(i)}$ is isomorphic to the semidirect product of $H^{(i)}$ and M. But the action of $H^{(i)}$ on M is trivial and thus $G^{(i)} \cong H^{(i)} \times M$. □

6.2 Minimal Soluble Groups

By a minimal soluble group of derived length d we mean a soluble group of smallest order and derived length d. For example, the symmetric group S_3 of degree 3 is the smallest nonabelian group. Therefore S_3 is the minimal soluble group of derived length 2. In this section we investigate the minimal soluble groups of derived length less than or equal to 6.

The following problem sparked off our interest in minimal soluble groups. A group G with a finite presentation $\langle X|R\rangle$ is said to be efficient if $|R| = |X| + rank(M(G))$, where $M(G)$ is the Schur multiplier of G. The first example of a finite group of derived length 5 having an efficient presentation and trivial Schur multiplier was given by P. Kenne in 1988. In [Ken 90] Kenne gave examples of finite groups of derived length 6 having efficient presentations and trivial Schur multiplier. Programs for the calculation of finite soluble quotients of finitely presented groups have been developed in the **GAP** programming system. These programs were used to find soluble groups with trivial Schur multiplier and a method suggested by Kenne (cf. [Ken 86]) was then used to find efficient presentations for these groups. In this method a small number of generating pairs for a group are chosen and for each generating pair a presentation is constructed and modified towards obtaining an efficient presentation. This method is only practicable for groups of moderate order. Therefore, for a given derived length d soluble groups of small order and derived length d are of interest.

Throughout this section we use the notation of [Gla 89] : The derived and composition length of a finite soluble group G are denoted by $d(G)$ and $n(G)$ respectively. When no confusion arises, the symbols d and n will be used in preference to $d(G)$ and $n(G)$. We restate some results on upper bounds for $d(G)$ in terms of $n(G)$ which will be used in this section. Given a group G of order p^n and derived length d, Hall showed (cf. Satz III.7.11 of [Hup 67]) that $n \geq 2^{d-1} + d - 1$. It is well known that a soluble group with composition length n may have much larger derived length than a nilpotent group with the same composition length. It is proved in Theorem 2 of [Gla 89] that $d \leq \lceil 2n/3 \rceil$, where $\lceil x \rceil$ denotes the least integer greater than or equal to x. Table I shows some values for the function $h(n) = \lceil 2n/3 \rceil$. Since $h(n)$ is a non-decreasing function, only the smallest value of n for which $h(n) = m$ are listed.

Table I

n	1	2	4	5	7	8
$h(n)$	1	2	3	4	5	6

The following result (cf. Lemma 1(b) of [Gla 89]) is used to prove Theorem 2 of [Gla 89]. If G is a soluble group of derived length 3 and G'' is cyclic, then G'/G'' is not cyclic. In order to prove this, Lemma 1(a) is needed : Let N be a normal subgroup of a group G. If $N \leq Z(G)$ and G/N is cyclic, then G is abelian. With the help of this knowledge we can now investigate the minimal soluble groups of derived length less than or equal to 6.

As we mentioned in the introduction the symmetric group S_3 of degree 3 is the minimal soluble group of derived length 2.

The symmetric group S_4 of degree 4 and the special linear group $SL_2(3)$ of dimension 2 over the field of order 3 have derived length 3. By Theorem 2 of

[Gla 89] the composition length of a soluble group of derived length 3 is at least 4 and therefore S_4 and $SL_2(3)$ are minimal soluble groups of derived length 3. Let G be a minimal soluble group of derived length 3. Then $n(G/G'') \geq 2$ by Theorem 2 of [Gla 89] and therefore $n(G'')$ is either 1 or 2. If $n(G'') = 1$, then G is a covering group of the alternating group A_4 of degree 4. It follows that G is isomorphic to $SL_2(3)$. If $n(G'') = 2$, then G is isomorphic to the split extension of the symmetric group S_3 of degree 3 by its natural module over the field of order 2. It follows that G is isomorphic to the symmetric group S_4 of degree 4.

The Schur multiplier of the symmetric group S_4 of degree 4 is isomorphic to the cyclic group of order 2. There are exactly two nonisomorphic covering groups of S_4 both of which have derived length 4. By Theorem 2 of [Gla 89] the composition length of a soluble group of derived length 4 is at least 5 and therefore the covering groups of S_4 are minimal soluble groups of derived length 4. Let G be a minimal soluble group of derived length 4. Then $n(G/G^{(3)}) \geq 4$ by Theorem 2 of [Gla 89] and therefore $n(G^{(3)}) = 1$. It follows that G is a covering group of S_4.

Next we show that a minimal soluble group of derived length 5 is isomorphic to the split extension of the general linear group $GL_2(3)$ of dimension 2 over the field of order 3 by its natural module. Note that by Theorem 2 of [Gla 89] the composition length of a group of derived length 5 is at least 7. First of all we show that a group of smallest order, derived length 5 and composition length 7 is isomorphic to the split extension of $GL_2(3)$ by its natural module. In order to show that this group is minimal of derived length 5 we show that there are no groups of smaller order, derived length 5 and composition length larger than 7.

LEMMA 6.6 If G is a finite soluble group of smallest order such that $d(G) = 5$ and $n(G) = 7$, then G is isomorphic to the split extension of the general linear group $GL_2(3)$ of dimension 2 over the field of order 3 by its natural module.

Proof Let G be a finite soluble group of smallest order such that $d(G) = 5$ and $n(G) = 7$. By Theorem 2 of [Gla 89], $n(G/G^{(4)}) \geq 5$ and therefore $n(G^{(4)})$ is either 1 or 2. If $n(G^{(4)}) = 1$, then $G^{(4)}$ is a cyclic group of order q. By Theorem 2 of [Gla 89], $n(G/G^{(3)}) \geq 4$ and so $n(G^{(3)}/G^{(4)}) \leq 2$. Since $G^{(4)}$ is cyclic, $G^{(3)}/G^{(4)}$ is not cyclic by Lemma 1(b) of [Gla 89]. Therefore $G^{(3)}/G^{(4)}$ is abelian of type (p,p). If $p \neq q$, then $G^{(3)}$ is abelian, since $G^{(3)}$ is a split extension of $G^{(3)}/G^{(4)}$ by $G^{(4)}$ and $G^{(3)}$ centralises $G^{(4)}$ — a contradiction. Hence $G^{(3)}$ is a group of order p^3. Moreover, $Z(G^{(3)}) = G^{(4)}$ by Lemma 1(a) of [Gla 89] and $G^{(3)}$ is extraspecial by Satz III.3.14(a) of [Hup 67]. If $p \geq 3$, then $|G| = |G/G^{(3)}||G^{(3)}| \geq 24 \cdot p^3 \geq 648$ — a contradiction. Therefore $p = 2$ and $G^{(3)}$ is isomorphic to the dihedral group D_8 of order 8 or the quaternion group Q_8 of order 8. Since $G^{(3)}$ is not contained in $C_G(G^{(3)})$ the derived length of $G/C_G(G^{(3)})$ is larger than or equal to 4. This yields a contradiction as the automorphism groups of D_8 and Q_8 are isomorphic to D_8 and the symmetric group S_4 of degree 4 respectively. This shows that $n(G^{(4)}) = 2$. If $G^{(4)}$ is cyclic, then $G^{(3)}/G^{(4)}$ is not cyclic by Lemma 1(b) of [Gla 89] and $n(G^{(3)}) \geq 4$. But then $n(G) = n(G/G^{(3)}) + n(G^{(3)}) \geq 8$ — a contradiction. Hence $G^{(4)}$ is abelian of type (p,p). If $p \geq 5$, then $|G| = |G/G^{(4)}||G^{(4)}| \geq 48 \cdot 5^2 = 1200$ — a contradiction. Now, suppose $p = 2$. Since $n(G/G^{(3)}) \geq 4$, $G^{(3)}/G^{(4)}$ is cyclic and it follows that $G^{(3)}$ is isomorphic to the alternating group A_4 of degree 4. Since $G^{(3)}$ is not contained in $C_G(G^{(3)})$ the derived length of $G/C_G(G^{(3)})$ is larger than or equal to 4. This yields a contradiction as the automorphism group of A_4 is isomorphic to S_4. Hence $p = 3$ and $G/G^{(4)}$ is a covering group of S_4. Note that the commutator subgroups are the only normal subgroups of the covering groups of S_4. If $G^{(4)} < C_G(G^{(4)})$, then $G^{(3)}$ is abelian — a contradiction. Hence $G^{(4)} = C_G(G^{(4)})$ and therefore $G/G^{(4)}$ is isomorphic to $GL_2(3)$. It follows that $G^{(4)}$ is a minimal normal subgroup and $G^{(4)}$ has a complement in G by Satz II.3.3 of [Hup 67]. □

THEOREM 6.7 If G is a minimal soluble group of derived length 5, then G is isomorphic to the split extension of the general linear group $GL_2(3)$ of dimension 2 over the field of order 3 by its natural module.

Proof By Lemma 6.6 it remains to show that there are no groups of order less than 432, derived length 5 and composition length larger than 7. Let G be a group of order $384 = 2^7 3$ and derived length 5. If P is a Sylow 2–subgroup of G, then $[G : N_G(P)]$ is either 1 or 3. If $[G : N(P)] = 1$, then P is a normal subgroup of G and G/P is isomorphic to the cyclic group of order 3. It follows that G' is contained in P and $|G'| \geq 2^{11}$ by Satz III.7.11 of [Hup 67] — a contradiction. If $[G : N_G(P)] = 3$, then we get an action of G on the coset space of G relative to P. The homomorphism associated with the action is an epimorphism of G onto the symmetric group S_3 of degree 3 and G'' is contained in the kernel of the epimorphism. By Satz III.7.11 of [Hup 67], $|G''| \geq 2^6$ and therefore G'' coincides with the kernel. Moreover, the proof of Satz III.7.11 shows that $G''/G^{(3)}$ is elementary abelian of order p^2. By Satz III.11.9 of [Hup 67], G'' is metacyclic — a contradiction. Hence, there are no groups of order $384 = 2^7 3$ and derived length 5 and the split extension of $GL_2(3)$ by its natural module over the field of order 3 is the minimal group of derived length 5. □

We now show that a minimal soluble group of derived length 6 is isomorphic to an extension of the minimal soluble group of derived length 5 by the alternating module over the field of order 3. Note that by Theorem 2 of [Gla 89] the composition length of a group of derived length 6 is at least 8. First of all we show that a group of smallest order, derived length 6 and composition length 8 is isomorphic to an extension of the minimal soluble group of derived length 5 by the alternating module over the field of order 3. In order to show that these groups are minimal of derived length 6 we show that there are no groups of smaller order, derived length 6 and composition length larger than 8. We begin with the following lemma.

LEMMA 6.8 If G is a group of order 72, then $d(G) < 4$.

Proof If P is a Sylow 3-subgroup of G, then $[G : N_G(P)]$ is either 1 or 4. If $[G : N_G(P)] = 1$, then P is an abelian normal subgroup of G and $|G/P| = 2^3$. Since $d(G/P) \leq 2$, it follows that $d(G) \leq 3$. If $[G : N_G(P)] = 4$, then we get an action of G on the coset space of G relative to P. The homomorphism associated with the action is an epimorphism of G onto a subgroup of the symmetric group S_4 of degree 4 which has four conjugate subgroups of index 4. Thus, the epimorphism is onto S_4. If G has derived length 4, then G is either a covering group of S_4 or G' is a covering group of the alternating group A_4, contrary to the fact that the Schur multiplier of S_4 and A_4 is isomorphic to the cyclic group of order 2. □

LEMMA 6.9 If G is a finite soluble group of smallest order such that $d(G) = 6$ and $n(G) = 8$, then G is isomorphic to an extension of the minimal soluble group of derived length 5 by the alternating module over the field of order 3.

Proof Let G be a finite soluble group of smallest order such that $d(G) = 6$ and $n(G) = 8$. By Theorem 2 of [Gla 89], $n(G/G^{(5)}) \geq 7$ and therefore $n(G^{(5)}) = 1$. Since $G^{(5)}$ is cyclic of order q, $G^{(4)}/G^{(5)}$ is not cyclic by Lemma 1(b) of [Gla 89]. By Theorem 2 of [Gla 89], $n(G/G^{(4)}) \geq 5$ and therefore $G^{(4)}/G^{(5)}$ is abelian of type (p, p). If $p \neq q$, then $G^{(4)}$ is abelian, since $G^{(4)}$ is a split extension of $G^{(4)}/G^{(5)}$ by $G^{(5)}$ and $G^{(4)}$ centralises $G^{(5)}$ — a contradiction. Hence $G^{(4)}$ is a group of order p^3. Moreover, $Z(G^{(4)}) = G^{(5)}$ by Lemma 1(a) of [Gla 89] and $G^{(4)}$ is extraspecial by Satz III.3.14(a) of [Hup 67]. If $p = 2$, then $G^{(4)}$ is isomorphic to the dihedral group D_8 of order 8 or the quaternion group Q_8 of order 8. Since $G^{(4)}$ is not contained in $C_G(G^{(4)})$ the derived length of $G/C_G(G^{(4)})$ is larger than or equal to 5. This yields a contradiction as the automorphism groups of D_8 and Q_8 are isomorphic to D_8 and the symmetric group S_4 of degree 4 respectively. This shows that $p = 3$ and $G/G^{(5)}$ is isomorphic to the minimal soluble group of derived length 5. □

THEOREM 6.10 If G is a minimal soluble group of derived length 6, then G is isomorphic to an extension of the minimal soluble group of derived length 5 by the alternating module over the field of order 3.

Proof By Lemma 6.9 it remains to show that there are no groups of order less than 1296, derived length 6 and composition length larger than 8. We have to consider groups of order $768 = 2^8 3$, $1152 = 2^7 3^2$ and $1280 = 2^8 5$. By Satz III.7.11 of [Hup 67], there are no groups of order 768 and 1280 respectively of derived length 6. Finally, let G be a group of order 1152 and derived length 6. Since $|G/G^{(5)}| \geq 432$, it follows that $G^{(5)}$ is cyclic of order 2. Therefore $G^{(4)}/G^{(5)}$ is not cyclic by Lemma 1(b) of [Gla 89]. By Theorem 2 of [Gla 89], $n(G/G^{(4)}) \geq 5$ and therefore $n(G^{(4)}/G^{(5)})$ is either 2 or 3. If $n(G^{(4)}/G^{(5)}) = 2$, then $G^{(4)}/G^{(5)}$ is abelian of type (p,p). If $p \neq 2$, then $G^{(4)}$ is abelian, since $G^{(4)}$ is a split extension of $G^{(4)}/G^{(5)}$ by $G^{(5)}$ and $G^{(4)}$ centralises $G^{(5)}$ — a contradiction. Hence $G^{(4)}$ is a group of order 2^3. Since $G^{(4)}$ is not contained in $C_G(G^{(4)})$ the derived length of $G/C_G(G^{(4)})$ is larger than or equal to 5. This yields a contradiction as the automorphism groups of D_8 and Q_8 are isomorphic to D_8 and S_4 respectively. Hence, $n(G^{(4)}/G^{(5)}) = 3$. If $|G^{(4)}/G^{(5)}| = 2 \cdot 3^2$, then $|G/G^{(4)}| \geq 2^{11}$ by Satz III.7.11 of [Hup 67] — a contradiction. If $|G^{(4)}/G^{(5)}| = 2^2 3$, then $G^{(4)}/G^{(5)}$ is abelian of type (2,2,3) since $G^{(4)}/G^{(5)}$ is not cyclic. Hence $G^{(4)}$ is isomorphic to the direct product of the cyclic group of order 3 and D_8 or Q_8 respectively. Since $G^{(4)}$ is not contained in $C_G(G^{(4)})$ the derived length of $G/C_G(G^{(4)})$ is larger than or equal to 5. This yields a contradiction as the automorphism group of $G^{(4)}$ is isomorphic to the direct product of the cyclic group of order 2 and D_8 or S_4 (cf. Satz I.9.4 of [Hup 67]). It follows that $|G^{(4)}/G^{(5)}| = 2^3$ and $|G/G^{(4)}| = 2^3 3^2 = 72$. This yields a contradiction by Lemma 6.8. □

The classification of the minimal soluble groups of derived length 7 remains an open problem. Using results on soluble subgroups of 2-dimensional general

linear groups, Glasby proved (cf. Lemma 6 of [Gla 89]) that the composition length of $G^{(4)}$ is at least 6 if G has derived length 7, and thus he is able to improve the previous bound to $d \leq \lceil (n+3)/2 - 3/(n+2) \rceil = g(n)$. The bound $d \leq g(n)$ is not best possible since $g(11) = 7$ and Glasby showed (cf. Appendix A) that there is no group with composition length 11 and derived length 7. In [Gla 89], Glasby described a group of order $2^{11}3^{13}$ and derived length 10 which has factors of derived length 7 and order $2^{10}3^4$, showing that $|G| \leq 2^{10}3^4$ if G is a minimal soluble group of derived length 7.

Bibliography

[Atk 84] M. D. Atkinson
Computational Group Theory
Academic Press 1984

[Bau 91] U. Baum
Existenz und effiziente Konstruktion schneller Fouriertransformationen überauflösbarer Gruppen
Dissertation, Universität Bonn 1991

[Cam 75] C. M. Campbell
Application of the Todd-Coxeter coset enumeration algorithm
PhD thesis, University of St. Andrews 1975

[CaR 82] C. M. Campbell, E. F. Robertson
The efficiency of simple groups of order $< 10^5$
Comm. Algebra 10(1982),217 - 225

[Cli 37] A. H. Clifford
Representations induced in an invariant subgroup
Annals of Mathematics 38(1937),533 - 550

[Gas 52] W. Gaschütz
Zur Erweiterungstheorie der endlichen Gruppen
J. Math. 190(1952),93 - 107

[Gla 89] S. P. Glasby
The composition and derived lengths of a soluble group
J. Algebra 120(1989),406 - 413

[Hol 85] D. F. Holt
The Mechanical Computation of 1st and 2nd Cohomology Groups
J. Symbolic Computation 1(1985),351 - 361

[Hup 67] B. Huppert
Endliche Gruppen I
Springer Verlag 1967

[HWM 73] N. E. Steenrod, P. R. Halmos, M. M. Schiffer, J. A. Dieudonné
How to Write Mathematics
American Mathematical Society 1973

[Isa 76] I. M. Isaacs
Character Theory of Finite Groups
Academic Press 1976

[Jac 74] N. Jacobson
Basic Algebra I+II
Freeman & Co. 1974/80

[Jam 88] A. Jamali
Computing with simple groups : maximal subgroups and presentations
PhD thesis, University of St. Andrews 1988

[JaR 89] A. Jamali, E. F. Robertson
Efficient presentations for certain simple groups
Comm. Algebra 17(1989),2521 - 2528

[Joh 90] D. L. Johnson
Presentations of Groups
Cambridge University Press 1990

[JoR 79] D. L. Johnson, E. F. Robertson
Finite groups of deficiency zero
LMS Lecture Notes Vol. 36,275 - 289
Cambridge University Press 1979

[Ken 86] P. E. Kenne
Efficient presentations for three simple groups
Comm. Algebra 14(1986),797 - 800

[Ken 90] P. E. Kenne
Some new efficient soluble groups
Comm. Algebra 18(1990),2747 - 2753

[Lee 84] C. R. Leedham-Green
A Soluble Group Algorithm
in [Atk 84], pp. 85 - 101

[LeS 90] C. R. Leedham-Green, L. H. Soicher
Collection from the Left and Other Strategies
J. Symbolic Computation 9(1990),665 - 675

[LiN 83] R. Lidl, H. Niederreiter
Finite Fields
Addison-Wesley 1983

[LNS 84] R. Laue, J. Neubüser, U. Schoenwaelder
Algorithms for Finite Soluble Groups and the **SOGOS** *system*
in [Atk 84], pp. 105 - 135

[NNS 88] W. Nickel, A. Niemeyer, M. Schönert
The **GAP** *User Manual*
Lehrstuhl D für Mathematik, RWTH Aachen 1988

[Par 84] R. A. Parker
The Computer Calculation of Modular Characters
in [Atk 84], pp. 267 - 274

[Ple 87] W. Plesken
Towards a Soluble Quotient Algorithm
J. Symbolic Computation 4(1987),111 - 122

[Sch 26] O. Schreier
Über die Erweiterungen von Gruppen I
Monatsh. Math. Phys. 34(1926),165 - 190

[Spe 19] A. Speiser
Zahlentheoretische Sätze aus der Gruppentheorie
Math. Z. 5(1919),1 - 6

[Vau 84] M. R. Vaughan-Lee
An Aspect of the Nilpotent Quotient Algorithm
in [Atk 84], pp. 75 - 83

Appendix A

An Article submitted to the London Mathematical Society

ON THE MINIMAL SOLUBLE GROUPS OF DERIVED LENGTH AT MOST SIX

S. P. GLASBY and A. WEGNER

16 June 1992

ABSTRACT. For $d \leq 6$, we classify the soluble groups of derived length d and minimal order. Also for $d \leq 6$, we classify the soluble groups of derived length d and minimal composition length.

1. INTRODUCTION

A soluble group G is said to have *minimal order* (respectively *minimal composition length*) amongst the soluble groups of derived length d, if every soluble group H of derived length d has order (respectively composition length) at least that of G. We denote by $\mathcal{MO}(d)$ (respectively $\mathcal{MC}(d)$) the set of all soluble groups of derived length d with minimal order (respectively composition length). Since the composition factors of a finite soluble group have prime order, the composition length of a soluble group of order $p_1^{k_1} \cdots p_r^{k_r}$ is $k_1 + \cdots + k_r$ if the p_i are prime. Clearly the elements of $\mathcal{MC}(1)$ comprise the groups of prime order, and $\mathcal{MO}(1)$ contains only the group of order 2. The elements of $\mathcal{MC}(2)$ are nonabelian of order pq where p and q are primes and p divides $q-1$, while $\mathcal{MO}(2)$ has only one element: the symmetric group S_3 of degree 3.

In this paper, we describe the elements of $\mathcal{MC}(d)$ and $\mathcal{MO}(d)$ for $d \leq 6$, and give an incomplete description of the elements of $\mathcal{MC}(7)$ and $\mathcal{MO}(7)$. While it seems unlikely that $\mathcal{MO}(d)$ is always a subset of $\mathcal{MC}(d)$, we observe that this is the case for $d \leq 6$. One may also observe that the elements of $\mathcal{MC}(d)$, $1 \leq d \leq 6$, have a unique chief series which coincides with the derived series. While it is easy to show that $G^{(d-1)}$ is the unique minimal normal subgroup of an element G of $\mathcal{MC}(d)$ (respectively $\mathcal{MO}(d)$), since $G/G^{(d-1)}$ need not be an element of $\mathcal{MC}(d)$ (respectively $\mathcal{MO}(d)$), it is not obvious that there should be a unique chief series for G.

One motivation for the study of minimal soluble groups, apart from their intrinsic interest, is for the calculation of deficiency zero presentations. It was conjectured by Johnson and Roberston [8], that a finite soluble group with deficiency zero has bounded derived length. Kenne [10] showed this bound is at least 6 by exhibiting a

1980 *Mathematics Subject Classification* (1985 *Revision*). 20 D10, 20 F15.
The second author gratefully acknowledges the support of grant EEC SC1-0003-C(EDB) .

deficiency zero presentation for a group, which turns out to be an element of $\mathcal{MO}(6)$. In [9] Kenne suggested a method for constructing deficiency zero presentations which is practical only for groups of "small" order. The second author used this method to show that all three elements of $\mathcal{MO}(6)$ have deficiency zero presentations and trivial Schur multipliers (see Section 5).

Throughout the paper we use the notation of [2] where the derived and composition length of a finite soluble group G are denoted by $d(G)$ and $n(G)$ respectively. The ith derived subgroup of G is denoted by $G^{(i)}$, and $n(G^{(i-1)}/G^{(i)})$ is abbreviated by n_i.

2. Minimal soluble groups of derived length 3 and 4

In this section we describe the elements of $\mathcal{MC}(d)$ and $\mathcal{MO}(d)$ where d equals 3 or 4. First, we prove the following Lemma.

Lemma 0.

(*i*) *If $i \geq 2$, then $G^{(i-1)}/G^{(i)}$ and $G^{(i)}/G^{(i+1)}$ are not both nontrivial cyclic groups, and so $(n_i, n_{i+1}) \neq (1,1)$.*

(*ii*) *If $i \geq 2$ and $(n_i, n_{i+1}) = (2,1)$, then $G^{(i-1)}/G^{(i+1)}$ is extraspecial of order p^3 and so $G^{(i-1)}/G^{(i)}$ is abelian of type (p,p).*

(*iii*) *If $(n_i, n_{i+1}) = (1,a)$ where $a > 0$ and $G^{(i-1)}/G^{(i)}$ is the unique minimal normal subgroup of $G/G^{(i)}$, then $G/G^{(i)}$ acts faithfully on $G^{(i)}/G^{(i+1)}$. If, in addition, $G^{(i)}/G^{(i+1)}$ is a Hall subgroup of $G^{(i-1)}/G^{(i+1)}$ and $G^{(i-1)}/G^{(i)}$ acts fixed-point-freely on $G^{(i)}/G^{(i+1)}$, then $G/G^{(i+1)}$ is a split extension of $G^{(i)}/G^{(i+1)}$ by $G/G^{(i)}$.*

Proof. (*i*) Suppose that $G^{(i)}/G^{(i+1)}$ is cyclic. Since $\mathrm{Aut}(G^{(i)}/G^{(i+1)})$ is abelian, we have $G' \leq C_G(G^{(i)}/G^{(i+1)})$ and so

$$G^{(i)}/G^{(i+1)} \leq Z(G'/G^{(i+1)}) \leq Z(G^{(i-1)}/G^{(i+1)}) \qquad \text{as } i \geq 2.$$

Therefore $G^{(i-1)}/G^{(i)}$ is not cyclic, otherwise $G^{(i-1)}/G^{(i+1)}$ would be abelian.
(*ii*) Since $G^{(i)}/G^{(i+1)}$ is cyclic, (*i*) shows that

$$G^{(i)}/G^{(i+1)} \leq Z(G^{(i-1)}/G^{(i+1)})$$

and $G^{(i-1)}/G^{(i)}$ is noncyclic. Thus the abelian group $G^{(i-1)}/G^{(i)}$ has type (p,p). If $G^{(i)}/G^{(i+1)}$ has prime order q, then $p = q$, otherwise $G^{(i-1)}/G^{(i+1)}$ would be abelian. Therefore $G^{(i-1)}/G^{(i+1)}$ is a nonabelian group of order p^3, and so is extraspecial.
(*iii*) By replacing G by $G/G^{(i+1)}$, we may assume that $G^{(i)}$ is a nontrivial abelian subgroup. Let $C = C_G(G^{(i)})$. Then $G^{(i)} \leq C \leq_! G$ so either

$$G^{(i)} = C \quad \text{or} \quad G^{(i-1)} \leq C.$$

If $G^{(i-1)} \leq C$, then since $G^{(i-1)}/G^{(i)}$ is cyclic, it follows that $G^{(i-1)}$ is abelian, a contradiction. Hence $C = G^{(i)}$ and so $G/G^{(i)}$ acts faithfully on $G^{(i)}/G^{(i+1)}$.

Suppose now that $G^{(i-1)}/G^{(i)}$ has order p and $G^{(i)}$ has order coprime to p. Let H be a Sylow p-subgroup of $G^{(i-1)}$. By the Frattini argument $G = G^{(i)}K$ where $K = N_G(H)$. Now $G^{(i)} \cap K$ and H are normal subgroups of K whose orders are coprime, so H centralizes $G^{(i)} \cap K$. However, H acts fixed-point-freely on $G^{(i)}$, so $G^{(i)} \cap K = \{1\}$, and therefore G is a split extension of $G^{(i)}$ by K. □

Theorem 1. *$G \in \mathcal{MC}(3)$ if and only if either*

(*i*) *$(n_1, n_2, n_3) = (1, 1, 2)$ and G is a split extension $V \cdot H$ where V is abelian of type (r, r) and $H \in \mathcal{MC}(2)$ acts faithfully and irreducibly on V, or*

(*ii*) *$(n_1, n_2, n_3) = (1, 2, 1)$ and G is a split extension $N\langle\alpha\rangle$ where N is extraspecial of order q^3 and α is an automorphism of N of prime order which acts fixed-point-freely on N/N'.*

Furthermore, $\mathcal{MO}(3) = \{S_4, SL_2(3)\}$ where S_4 is the symmetric group of degree 4 and $SL_2(3)$ is the special linear group of degree 2 over the field of three elements.

Proof. If $d(G) = 3$, then by Lemma 0(*i*), $n_2 + n_3 \geq 3$ so $n(G) = n_1 + n_2 + n_3 \geq 4$. Thus any group G, such as S_4, with $d(G) = 3$ and $n(G) = 4$ is an element of $\mathcal{MC}(3)$. Hence if $G \in \mathcal{MC}(3)$, then $n(G) = 4$ and so (n_1, n_2, n_3) equals $(1, 1, 2)$ or $(1, 2, 1)$.

CASE (*i*) $(n_1, n_2, n_3) = (1, 1, 2)$. Then the abelian group $G^{(2)}$ is noncyclic by Lemma 0(*i*) and so has type (r, r) where r is a prime. Now $G^{(2)}$ is a minimal normal subgroup of G because if N were a nontrivial normal subgroup of G properly contained in $G^{(2)}$, then $d(G/N) = 3$ and $n(G/N) = 3$, a contradiction. Clearly $G/G^{(2)} \in \mathcal{MC}(2)$ and by Lemma 0(*iii*), $G/G^{(2)}$ acts faithfully (and irreducibly) on $G^{(2)}$, and G is a split extension of $G^{(2)}$ by $G/G^{(2)}$. Conversely, if V is an abelian group of type (r, r) and $H \in \mathcal{MC}(2)$ acts faithfully and irreducibly on V, then the split extension $G = V \cdot H$ is an element of $\mathcal{MC}(3)$. (Note that $|H'|$ and $|V|$ are coprime so $V = C_V(H') \times [H', V]$. Since H acts irreducibly $[H', V]$ is trivial or V, and since H acts faithfully $[H', V] = V$. This shows that $G^{(2)} = V$ and hence that $d(G) = 3$.)

CASE (*ii*) $(n_1, n_2, n_3) = (1, 2, 1)$. Then by Lemma 0(*ii*), G' is an extraspecial group of order q^3 for some prime q. If G/G' has prime order p, then $p \neq q$ and G is a split extension of G' by an automorphism α of order p. Now α must act fixed-point-freely on the abelian group $V = G'/G^{(2)}$ of type (q, q), otherwise $[\alpha, V]$ would be a proper subspace of V and $|G'| < q^3$. Conversely, if N is extraspecial of order q^3 and α is an automorphism of N of prime order p which acts fixed-point-freely on N/N', then $p \neq q$ and the split extension $N\langle\alpha\rangle$ is an element of $\mathcal{MC}(3)$.

Amongst the groups in $\mathcal{MC}(3)$, those of smallest order are S_4 in Case (*i*) and $SL_2(3)$ in Case (*ii*). Since groups with composition length greater than 4 have order greater than $24 = |S_4| = |SL_2(3)|$, it follows that $\mathcal{MO}(3) = \{S_4, SL_2(3)\}$. □

Theorem 2. *$G \in \mathcal{MC}(4)$ if and only if $(n_1, n_2, n_3, n_4) = (1, 1, 2, 1)$ and G is an extension of an extraspecial group N of order r^3 by $H \in \mathcal{MC}(2)$ where H acts faithfully and irreducibly on N/N'. Furthermore, $\mathcal{MO}(4) = \{GL_2(3), \widehat{S_4}\}$ where $GL_2(3)$ and $\widehat{S_4}$ are the two covering groups of S_4.*

Proof. If $d(G) = 4$, then by Lemma $0(i)$, $n_2 + n_3 \geq 3$ so $n(G) \geq 5$. Thus any group G, such as $GL_2(3)$, with $d(G) = 4$ and $n(G) = 5$ is an element of $\mathcal{MC}(4)$. Hence if $G \in \mathcal{MC}(4)$, then $n(G) = 5$ and the only choice for (n_1, n_2, n_3, n_4) which complies with Lemma $0(i)$, is $(1,1,2,1)$. By Lemma $0(ii)$, $G^{(2)}$ is extraspecial of order r^3. Clearly, $G/G^{(2)} \in \mathcal{MC}(2)$ and $G/G^{(4)} \in \mathcal{MC}(4)$. By Theorem 1, $G/G^{(2)}$ acts faithfully and irreducibly on $G^{(2)}/G^{(3)}$. Conversely, if N is extraspecial of order r^3 and $H \in \mathcal{MC}(2)$ is a group of automorphisms of N which acts faithfully and irreducibly on N/N', then an extension of N by H is an element of $\mathcal{MC}(4)$.

Suppose now that G has smallest order amongst the elements of $\mathcal{MC}(4)$. Then $G^{(2)}$ has order 8 and is isomorphic to either the dihedral group D_8, or the quaternion group Q_8. Now $\mathrm{Aut}(D_8) \cong D_8$ and $\mathrm{Aut}(Q_8) \cong S_4$, so the only way a group $H \in \mathcal{MC}(2)$ can act faithfully and irreducibly on $G^{(2)}/G^{(3)}$ is if $G^{(2)} \cong Q_8$ and $H \cong S_3$. There are two nonisomorphic groups which are extensions of Q_8 by S_3 where S_3 acts faithfully and irreducibly on Q_8/Q_8': one is a split extension and is isomorphic to $GL_2(3)$, while the other group, which we call $\widehat{S_4}$, is a nonsplit extension. These groups are the covering groups of S_4. Since groups with composition length greater than 5 have order greater than $48 = |GL_2(3)| = |\widehat{S_4}|$, it follows that $\mathcal{MO}(4) = \{GL_2(3), \widehat{S_4}\}$. □

3. Minimal soluble groups of derived length 5 and 6

Theorem 3. *$G \in \mathcal{MC}(5)$ if and only if either*

(*i*) *$(n_1, \ldots, n_5) = (1,1,2,1,2)$ and G is a split extension $V \cdot H$ where $H \in \mathcal{MO}(4)$ and V is a faithful absolutely irreducible two-dimensional $GF(s)H$-module where s is a prime, or*

(*ii*) *$(n_1, \ldots, n_5) = (1,2,1,2,1)$ and G is an extension of an extraspecial group N of order s^3 and exponent s by the symplectic group $Sp_2(3)$, where $Sp_2(3)$ acts faithfully and absolutely irreducibly on N/N'.*

Furthermore, $\mathcal{MO}(5)$ contains only one group: the split extension $V \cdot GL_2(3)$, where V is the natural module for $GL_2(3)$.

Proof. If $d(G) = 5$, then it follows from [2, Theorem 2] that $n(G) \geq 7$. If V is the natural module for $GL_2(3)$, then the split extension $G = V \cdot GL_2(3)$ satisfies $d(G) = 5$ and $n(G) = 7$. Hence if $G \in \mathcal{MC}(5)$, then $n(G) = 7$. If $G \in \mathcal{MC}(5)$, then it follows from Lemma $0(i)$ that $(n_1, \ldots, n_5)$ equals either $(1,1,2,1,2)$ or $(1,2,1,2,1)$.

Case (*i*) $(n_1, \ldots, n_5) = (1,1,2,1,2)$. Now $G^{(2)}/G^{(4)}$ is an extraspecial group of order r^3 by Lemma $0(ii)$ and $G^{(4)}$ is abelian of type (s,s). It follows that $r \neq s$ and $G/G^{(4)} \in \mathcal{MC}(4)$. Thus $G^{(3)}/G^{(4)}$ is the unique minimal normal subgroup of the extraspecial group $G^{(2)}/G^{(4)}$ and by Lemma $0(iii)$, $G^{(2)}/G^{(4)}$ acts faithfully, and hence irreducibly, on $G^{(4)}$. One may show that an ordinary faithful irreducible representation of an extraspecial group is necessarily absolutely irreducible. Furthermore, each faithful absolutely irreducible representation of an extraspecial group of order r^3 has degree r by [6, V Satz 16.14]. Therefore $r = 2$ and $G^{(2)}/G^{(4)} \cong D_8$ or Q_8. Since $G/G^{(2)}$ acts faithfully on $G^{(2)}/G^{(3)}$, we must have $G^{(2)}/G^{(4)} \cong Q_8$ and

$G/G^{(2)} \cong S_3$. By Theorem 2, $G/G^{(4)} \in \mathcal{M}O(4)$. By Lemma $0(iii)$, $G/G^{(4)}$ acts faithfully, and hence absolutely irreducibly, on $G^{(4)}$. It can be shown (see [3], for example) that $GL_2(3)$ (respectively $\widehat{S_4}$) has a faithful absolutely irreducible two-dimensional representation over the prime field $GF(s)$ if and only if s is odd and -2 (respectively 2) is a square in $GF(s)$.

Conversely, suppose that $H \in \mathcal{M}O(4)$ and V is a faithful absolutely irreducible two-dimensional $GF(s)H$-module. Then the split extension $G = V \cdot H$ satisfies $d(G) = 5$ and $n(G) = 7$. (Note that $H^{(3)} = Z(H)$ has order 2 and so the nontrivial central element induces the transformation -1 on V. As H acts faithfully, $s \neq 2$, and so $[H^{(3)}, V] = V$. Therefore $G^{(4)} = V$ and $d(G) = 5$.)

CASE (ii) $(n_1, \ldots, n_5) = (1,2,1,2,1)$. By Lemma $0(ii)$, $G'/G^{(3)}$ and $G^{(3)}$ are extraspecial groups of order, say, r^3 and s^3 respectively. Arguing as above, $r = 2$ and $s \neq 2$. Therefore $G'/G^{(3)} \cong Q_8$ and G/G' has order 3 so $G/G^{(3)}$ is isomorphic to $Sp_2(3) \cong SL_2(3)$. By Lemma $0(iii)$, $G/G^{(3)}$ acts faithfully on $G^{(3)}/G^{(4)}$. This representation is irreducible otherwise G has a normal subgroup M such that $G^{(4)} < M < G^{(3)}$, and G/M contradicts Lemma $0(i)$. Therefore $G^{(3)}$ has no characteristic subgroups strictly between $G^{(3)}$ and $G^{(4)}$, and so $G^{(3)}$ is the extraspecial group of exponent s. In addition, $G/G^{(3)}$ acts absolutely irreducibly on $G^{(3)}/G^{(4)}$. (Otherwise, if F is the algebraic closure of $GF(p)$, then $G/G^{(3)}$ would be isomorphic to a subgroup of the matrix group

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in F,\ ac \neq 0 \right\}$$

and so $d(G/G^{(3)}) \leq 2$, a contradiction.)

Conversely, if V is a faithful irreducible two-dimensional $GF(s)Sp_2(3)$-module, then $s \neq 2$. One may show (cf. [4, Section 7]) that $Sp_2(3)$ preserves a nondegenerate alternating bilinear form on V, and hence $Sp_2(3)$ acts on the extraspecial group N of order s^3 and exponent s by [4, Sections 2,3]. Arguing as above, it follows that if G is an extension of N by $Sp_2(3)$ where $Sp_2(3)$ acts faithfully and irreducibly on N/N', then $G \in \mathcal{M}C(5)$. If $s \neq 3$, then G is a split extension while if $s = 3$, there are three possible extensions.

We now classify the elements of $\mathcal{M}O(5)$. First, we show that the group in $\mathcal{M}C(5)$ of smallest order is the split extension $G = V \cdot GL_2(3)$, with natural action. If K is a group occurring in Case (ii), then $|K| = 2^3 3 s^3 > 2^4 3^3 = |G|$. If K is a group occurring in Case (i), then $|K| = 2^4 3 s^2 \geq 2^4 3^3 = |G|$. Thus equality holds if and only if $s = 3$, in which case K is a split extension $V \cdot H$ where V is abelian of type $(3,3)$ and H is isomorphic to a subgroup of $GL_2(3)$. Since $|H| = |GL_2(3)|$, H is isomorphic to $GL_2(3)$ as claimed.

It remains to prove that there is no group G with $d(G) = 5$, $n(G) > 7$ and $|G| < 2^4 3^3$. If G were such a group, then $|G| = 2^7 3$. If P were a Sylow 2–subgroup of G, then $|G : N_G(P)|$ is either 1 or 3. If $|G : N(P)| = 1$, then P is a normal subgroup of G and G/P has order 3. It follows that G' is contained in P and $|G'| \geq 2^{11}$ by [6, III Satz 7.11], a contradiction. If $|G : N_G(P)| = 3$, then G acts by left translation on the left cosets of P in G. This induces a homomorphism ρ

of G *onto* S_3. Now $G^{(2)} \leq \ker(\rho)$ and $|G^{(2)}| \geq 2^6$ by [**6**, III Satz 7.11]. Therefore $G^{(2)} = \ker(\rho)$. Moreover, the proof of [**6**, III Satz 7.11] shows that $G^{(2)}/G^{(3)}$ is elementary abelian of order 2^2. By [**6**, III Satz 11.9], $G^{(2)}$ is metacyclic, a contradiction. Hence, there are no groups of order $2^7 3$ and derived length 5, and so $\mathcal{MO}(5) = \{V \cdot GL_2(3)\}$ as claimed. □

Theorem 4. *$G \in \mathcal{MC}(6)$ if and only if G is an extension of the extraspecial group of order s^3 and exponent s by $H \in \mathcal{MO}(4)$ where H acts faithfully and absolutely irreducibly on N/N'. There are precisely three groups in $\mathcal{MO}(6)$, namely the extensions of the extraspecial group N of order 3^3 and exponent 3 by $GL_2(3)$, where $GL_2(3)$ acts naturally on N/N'.*

Proof. If $d(G) = 6$, then $n(G) \geq 8$ by [**2**, Theorem 2]. First, we assume there is a group G with $d(G) = 6$ and $n(G) = 8$. Then, after determining the structure of G, we show that G does indeed exist.

If $d(G) = 6$ and $n(G) = 8$, then it follows from Lemma $0(i)$ that $(n_1, \ldots, n_6) = (1, 1, 2, 1, 2, 1)$. Hence, $G/G^{(5)}$ and G' are elements of $\mathcal{MC}(5)$. By Theorem $3(i)$, $G/G^{(4)} \in \mathcal{MO}(4)$ and by Theorem $3(ii)$, $G^{(4)}$ is extraspecial of order s^3 and exponent s. Also, $G/G^{(4)}$ acts faithfully, and hence absolutely irreducibly, on $G^{(4)}/G^{(5)}$ by Lemma $0(ii)$.

Conversely, let $H \in \mathcal{MO}(4)$. As remarked above, for appropriate primes s there is a faithful absolutely irreducible degree-two representation of H over $GF(s)$. It is shown in [**4**] that this representation preserves, up to a sign, a nondegenerate alternating bilinear form. By [**4**, Sections 2,3] there is an extraspecial group N of order s^3 and exponent s containing H in its automorphism group. Therefore, extensions of N by H where H acts faithfully and irreducibly on N/N' do indeed exist. If G were such an extension, then it follows from the proof of Theorem 3 that $d(G) = 6$. This classifies the elements of $\mathcal{MC}(6)$. Note that if $s \neq 3$, then G is a split extension of N by H. If $s = 3$, then $H \cong GL_2(3)$ and there are three extensions of N by H: one split and two nonsplit extensions.

If $G \in \mathcal{MC}(6)$, then $|G| = 2^4 3 s^3$ where s is odd, so the three groups with $s = 3$ have minimal order amongst the elements of $\mathcal{MO}(6)$. To show that these three groups are elements of $\mathcal{MO}(6)$, we must show there are no groups G satisfying $d(G) = 6$, $n(G) > 8$ and $|G| < 2^4 3^4$. It follows from [**6**, III Satz 7.11] that G is not nilpotent. Therefore $|G|$ equals $2^8 3$, $2^7 3^2$ or $2^8 5$, and so $n(G) = 9$.

By Theorem 3, $|G/G^{(5)}| \geq 2^4 3^3$ and since $|G| < 2^4 3^4$, we must have $|G^{(5)}| = 2$. We may assume that G has a unique minimal normal subgroup. Therefore this is $G^{(5)}$ and $O_{2'}(G)$ is trivial. Let $P = O_2(G)$ and let $|P/\Phi(P)| = 2^r$. We use the fact that G/P acts faithfully on the r-dimensional vector space $P/\Phi(P)$ by [**6**, VI Hilfssatz 6.5], and consider four cases.

CASE (i) $d(P) \geq 4$. By [**6**, III Satz 7.11], $n(P) \geq 2^3 + 3 = 11$. This is a contradiction as $9 = n(G) \geq n(P) \geq 11$.

CASE (ii) $d(P) = 3$. Now $d(G/P) \geq 3$ so $n(G/P) \geq 4$. In addition, $n(P) \geq 6$ so

$$9 = n(G) = n(G/P) + n(P) \geq 6 + 4,$$

a contradiction.

CASE (*iii*) $d(P) = 2$. Now $d(G/P) \geq 4$ so $n(G/P) \geq 5$. Since G/P is a soluble subgroup of $GL_r(2)$ with $n(G/P) \geq 5$, it follows that $r \geq 4$. Hence $n(P) \geq 5$ and so $n(G) \geq 10$, a contradiction.

CASE (*iv*) $d(P) = 1$. Now $d(G/P) \geq 5$ so $n(G/P) \geq 7$. The argument of Case (*iii*) shows that $r \geq 4$. Therefore $n(P) \geq 4$ and so $n(G) \geq 11$, a contradiction.

Hence, no such group exists, and the proof is complete. □

4. MINIMAL SOLUBLE GROUPS OF DERIVED LENGTH 7

In this section we show that if $G \in \mathcal{MC}(7)$, then $12 \leq n(G) \leq 13$. The lower bound is proved in Theorem 7 below. Guided by the proof of Theorem 7, we construct a family G_p of groups with $d(G_p) = 7$, $|G_p| = 2^3 3^4 p^6$ and $n(G_p) = 13$, thereby establishing the upper bound. We show that if $G \in \mathcal{MO}(7)$, then $|G| \leq 2^{10}3^4$ by constructing a group K with $d(K) = 7$ and $|K| = 2^{10}3^4$. In [4, Section 7] soluble groups with arbitrarily large derived lengths are constructed from extraspecial groups. A group H of order $2^{11}3^{13}$ and derived length 10 is described which has such a group K as the quotient group $H/H^{(7)}$. Although K is not an element of $\mathcal{MC}(7)$, we have $|K| < 2^3 3^4 7^6 \leq |G_p|$, and by a conspiracy of small primes, K may be an element of $\mathcal{MO}(7)$ which is not an element of $\mathcal{MC}(7)$.

Before proving Theorem 7, we establish two preliminary results.

Lemma 5. *A p-group of order p^6 and derived length 3 has maximal class.*

Proof. Suppose P is such a p-group. It follows from the proof of [6, III Satz 7.11] that $|P/P'| = p^2$, $|P'/P^{(2)}| = p^3$ and $|P^{(2)}| = p$. Now $\gamma_2(P)/\gamma_3(P)$ is cyclic since $|P/\gamma_2(P)| = p^2$. Therefore,

$$P^{(2)} = [\gamma_2(P), \gamma_2(P)] = [\gamma_2(P), \gamma_3(P)] \leq \gamma_5(P),$$

and so $\gamma_5(P)$ is nontrivial. Hence P is of maximal class. Note that such groups can be classified using Blackburn's paper [1]. In particular, p is not equal to 2 or 3. □

Lemma 6. *Let G be a p-soluble group such that $O_{p'}(G) = \{1\}$. If $P = O_p(G)$ and $P/\Phi(P)$ has order p^r, then G/P is isomorphic to a completely reducible subgroup of $GL_r(p)$.*

Proof. By [6, VI Hilfssatz 6.5] $\overline{G} = G/P$ acts faithfully on the r-dimensional vector space $V = P/\Phi(P)$. Suppose that W is an s-dimensional $\overline{G}$-invariant subspace of V corresponding to a normal subgroup of G lying between $\Phi(P)$ and P. Now $\overline{G}$ is a subgroup of the parabolic group H which stabilizes the flag $\{0\} \leq W \leq V$. Since H acts on W and V/W, there is a homomorphism

$$\phi: H \to GL(W) \times GL(V/W)$$

whose kernel is isomorphic to the matrix group

$$\begin{pmatrix} I_s & * \\ 0 & I_{r-s} \end{pmatrix}$$

of order $p^{s(r-s)}$. Since $O_p(\overline{G})$ is trivial, the restriction of ϕ to $\overline{G}$ is injective. Hence $\overline{G}$ is isomorphic to a completely reducible subgroup of $GL(V)$. □

Theorem 7. *If G has derived length 7, then its composition length is at least 12.*

Proof. It suffices to prove that if $G \in \mathcal{MC}(7)$, then $n(G) \geq 12$. Our proof is similar in style to [2, Theorem 8]. Now $G^{(6)}$ is the unique minimal normal subgroup of G. Therefore $G^{(6)}$ is an elementary abelian p-group and $O_{p'}(G) = \{1\}$. Let $P = O_p(G)$, and let $|P/\Phi(P)| = p^r$. We consider five cases.

CASE (i) $d(P) \geq 5$. By [6, III Satz 7.11], $n(G) \geq n(P) \geq 2^4 + 4 > 12$.

CASE (ii) $d(P) = 4$. Then $n(P) \geq 11$. Since $d(G/P) \geq 3$ we have $n(G/P) \geq 4$ so $n(G) = n(G/P) + n(P) \geq 4 + 11 > 12$.

CASE (iii) $d(P) = 3$. Then $n(P) \geq 6$ and $d(G/P) \geq 4$ so $n(G/P) \geq 5$. Thus $n(G) \geq 5 + 6 = 11$. We must rule out the case when $n(G) = 11$. In this case $n(P) = 6$, and it follows from Lemma 5 that P is a p-group of maximal class. Hence $P/\Phi(P)$ has order p^2 and $C_P(\gamma_2(P)/\gamma_4(P))$ is a characteristic subgroup of index p. By Lemma 6, G/P is isomorphic to a subgroup of the group of $GL_1(p) \times GL_1(p)$. This shows that $d(G/P) \leq 1$, a contradiction. Therefore $n(G) \geq 12$ as claimed.

CASE (iv) $d(P) = 2$. Now G/P is a soluble subgroup of $GL_r(p)$ with $d(G/P) \geq 5$. It follows from [11] that $r \geq 3$, and so $n(P) \geq 4$. By [2], $n(G/P) \geq 7$ and hence $n(G) \geq 11$.

We must rule out the case when $n(G) = 11$. In this case $r = 3$ and both $\Phi(P)$ and P' have order p. If $Z(P)$ also has order p, then P would be an extraspecial group of order p^4, a contradiction. Hence $Z(P)$ lies strictly between $\Phi(P)$ and P. By Lemma 6, G/P is isomorphic to a subgroup of $GL_1(p) \times GL_2(p)$. By [11] it follows that $d(G/P) \leq 4$, a contradiction. Hence $n(G) \geq 12$ holds in this case too.

CASE (v) $d(P) = 1$. Since $d(G/P) \geq 6$, we have $n(G/P) \geq 8$ by [2] and $r \geq 4$ by [11]. Therefore $n(G) \geq 12$ and the proof is complete. □

We now construct a group G with $d(G) = 7$ and $n(G) = 13$.

Example. Let V be an r-dimensional vector space over the finite field $GF(q)$. Then the homogeneous component $\Lambda^2 V$ of the exterior algebra ΛV has dimension $\binom{r}{2}$. We construct a group of order q^m where $m = r + \binom{r}{2}$ by setting $P = V \times \Lambda^2 V$, and defining multiplication by the rule

$$(v_1, w_1)(v_2, w_2) = (v_1 + v_2, w_1 + w_2 + v_1 \wedge v_2) \qquad \text{where } v_1, v_2 \in V, w_1, w_2 \in \Lambda^2 V.$$

This makes P into a special group of order q^m. Note that when q is even, P is elementary abelian, and when q is odd

$$P' = \Phi(P) = Z(P) = \{(0, w) \mid w \in \Lambda^2 V\}$$

is elementary abelian. There is a right action of $GL_r(q)$ on the group P defined by

$$(v, w)g = (vg, w(g \wedge g))$$

which gives rise to a split extension $P \cdot GL_r(q)$.

Suppose now that $H \in \mathcal{M}C(5)$ and the subgroup $H^{(3)}$ is extraspecial of order 3^3 and exponent 3. Then H is one of the three extension of $H^{(3)}$ by $Sp_2(3)$. (There are at most three such extensions because if $gH^{(3)}$ has order 3 in $H/H^{(3)}$, then $g^3 \in Z(H^{(3)})$, so there are three choices for g^3. Indeed, the resulting three groups are nonisomorphic.) One may determine the odd primes p for which there is an absolutely irreducible faithful representation $\phi: H \to GL_3(p)$. (A necessary condition for the existence of ϕ is that $p \equiv 1 (\mathrm{mod}\ 3)$, and if H is a split extension of $H^{(3)}$ by $H/H^{(3)}$, this condition is also sufficient. If H is a nonsplit extension, then $p \equiv 1 (\mathrm{mod}\ 9)$ is sufficient.) If $q = p$ and $r = 3$, then the group P above has order p^6 and the subgroup $G = P \cdot H$ of $P \cdot GL_3(p)$ has order $2^3 3^4 p^6$, and so $n(G) = 13$. If $r = 3$ and g has matrix A relative to the basis e_1, e_2, e_3 for V, then the matrix of $g \wedge g$ relative to the basis $e_2 \wedge e_3, e_3 \wedge e_1, e_1 \wedge e_2$ for $\Lambda^2 V$ is $\det(A)(A^{-1})^t$. Now a nontrivial element $g \in H^{(4)} = Z(H)$ induces a scalar transformation $\omega 1$ on V where ω is a primitive cube root of 1, and so $g \wedge g$ induces $\omega^2 1$ on $\Lambda^2 V$. This shows that $G^{(5)} = P$, and so $d(G) = 7$. Note also that the smallest prime p for which the group G_p exists is $p = 7$.

5. Deficiency zero presentations

In this section we show that the soluble groups of derived length 6 and minimal order have deficiency zero presentations.

By Theorem 3, the split extension $V \cdot GL_2(3)$, where V is the natural module for $GL_2(3)$, is the only element of $\mathcal{M}O(5)$. The maximal subgroups of order 432 of the projective special linear group $PSL_3(3)$ are isomorphic to $V \cdot GL_2(3)$. Indeed, there is a monomorphism from $V \cdot GL_2(3)$ into $SL_3(3) (\cong PSL_3(3))$ defined by

$$(x, A) \mapsto \begin{pmatrix} \det(A)A & 0 \\ x & \det(A) \end{pmatrix}.$$

Jamali [7] found the deficiency zero presentation $\langle R, S \mid R^2 S^3 = T = 1 \rangle$ for $V \cdot GL_2(3)$ where T is the word

$$T = (RS)^3 (RS^{-1}RS)^2 R^{-1} S R S^{-1} R^{-1} S (R^{-1} S^{-1})^3 R^{-1} S,$$

and where R and S are identified with the matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 \\ -1 & -1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

By Theorem 4, the elements G_0, G_1 and G_2 of $\mathcal{M}O(6)$ are extensions of $V \cdot GL_2(3)$ by the alternating module over the field with 3 elements. The second author developed programmes for calculating finite soluble quotients of finitely presented

groups in the **GAP** programming system (cf. [13] and [12]). These programmes were used to compute the appropriate extensions G_i, $0 \leq i \leq 2$, of $V \cdot GL_2(3)$. The G_i, $0 \leq i \leq 2$, have presentations

$$G_i = \langle R, S \mid R^2S^3 = T^i, [T,R] = T, [T,S] = T^3 = 1 \rangle,$$

where T is defined above. The following deficiency zero presentations were found

$$G_0 = \langle X, Y \mid XY(X^{-1}Y)^2XY^{-2} = X^2YX^{-1}Y^{-3}XY^2 = 1 \rangle \quad \text{and}$$
$$G_1 = \langle X, Y \mid (XY)^2XY^{-2}X^{-1}Y = X^2YX^{-2}YX^2Y^{-2} = 1 \rangle,$$

and Kenne [10] found the following deficiency zero presentation

$$G_2 = \langle X, Y \mid (XY)^2Y^{-6} = X^4Y^{-1}XY^{-9}X^{-1}Y = 1 \rangle.$$

Coset enumeration may be used to show that the maps

$$X \mapsto TS^{-1}(RS)^2R, \quad Y \mapsto TS^{-1}RSR$$
$$X \mapsto S^2(RS)^2R, \quad Y \mapsto S^2RSR$$
$$X \mapsto TS^{-1}R, \quad Y \mapsto S^2RSRS^{-1}(RS)^3R$$

define isomorphisms between the respective presentations of G_0,G_1 and G_2.

Note that G_2 is isomorphic to the quotient group $H/H^{(6)}$ where H is the group described in Section 4, and is a split extension of the exponent-3 extraspecial group by $GL_2(3)$. The group $K = H/H^{(7)}$ was shown to have Schur multiplier of order 2 (and $H/H^{(8)}$ is a covering group). We showed that $H'/H^{(8)}$ has a trivial Schur multiplier, but were unable to find a deficiency zero presentation for it.

ACKNOWLEDGEMENT

The first author would like to thank R.B. Howlett for a discussion which led to the idea of the example in Section 4, and the second author is grateful to E.F. Robertson for comments relating to Section 5.

REFERENCES

1. N. Blackburn, *On a special class of p-groups*, Acta Math. **100** (1958), 45–92.
2. S.P. Glasby, *The composition and derived lengths of a soluble group*, J. Algebra **120** (1989), 406–413.
3. S.P. Glasby, *On the faithful representations of* $2_\epsilon^{1+2n} \cdot O_{2n}^\epsilon(2)$ *and* $4 \circ 2^{1+2n} \cdot Sp_{2n}(2)$ *of degree* 2^n, submitted.
4. S.P. Glasby and R.B. Howlett, *Extraspecial towers and Weil representations*, to appear in J. Algebra.
6. B. Huppert, *Endliche Gruppen I*, Springer–Verlag, 1967.

7. A. Jamali, *Computing with simple groups : maximal subgroups and presentations, PhD thesis*, University of St. Andrews, 1988.

8. D.L. Johnson and E.F. Robertson, *Finite groups of deficiency zero, in C.T.C. Wall (Ed.) Homological Group Theory, pp.275–289, London Mathematical Society Lecture Note Series*, vol. 36, Cambridge University Press, Cambridge, 1978.

9. P.E. Kenne, *Efficient presentations for three simple groups*, Comm. Algebra **14** (1986), 797–800.

10. P.E. Kenne, *Some new efficient soluble groups*, Comm. Algebra **18** (1990), 2747–2753.

11. M.F. Newman, *The soluble length of a soluble linear group*, Math. Z. **126** (1972), 59–70.

12. W. Nickel, A. Niemeyer, M.Schönert, *The* **GAP** *User Manual*, Lehrstuhl D für Mathematik, RWTH Aachen, 1988.

13. W. Plesken, *Towards a Soluble Quotient Algorithm*, J. Symbolic Comp. **4** (1987), 111–122.

SCHOOL OF MATHEMATICS AND STATISTICS, THE UNIVERSITY OF SYDNEY, N.S.W. 2006, AUSTRALIA

MATHEMATICAL INSTITUTE, UNIVERSITY OF ST. ANDREWS, ST. ANDREWS KY16 9SS, SCOTLAND