

A Thesis Submitted for the Degree of PhD at the University of Warwick

Permanent WRAP URL:

<http://wrap.warwick.ac.uk/111609>

Copyright and reuse:

This thesis is made available online and is protected by original copyright.

Please scroll down to view the document itself.

Please refer to the repository record for this item for information to help you to cite it.

Our policy information is available from the repository home page.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

0

50040/84

NES G.R.

130

OF DEPOSIT

ILPOTENT

regulations

ation

the
) must
earliest
tation of

purposes

G. R. Jay

is thesis

le it is

CONTENTS

	<u>Page</u>
Acknowledgements	ii
Declaration	ii
Summary	iii
Conventions and Notation	iv
Introduction	1
CHAPTER I <u>The Main Theorems</u>	6
1. Definitions	7
2. The Frattini and Fitting Subgroups	11
3. Nilpotent Length and Derived Length	16
4. Injectors and Projectors	18
5. The Main Theorems	23
CHAPTER II <u>Standard Results and Methods</u>	39
1. Group Actions	40
2. p-groups	43
3. Representation Theory	49
4. The Method of Proof of Theorems A and B	56
CHAPTER III <u>Preparations for Theorems A and B</u>	63
1. Arithmetic	64
2. Group Theory	73
3. Representation Theory	83
4. Preparations for Theorem B	95
CHAPTER IV <u>The Proofs of Theorems A and B</u>	99
Bibliography	120

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Dr. T. O. Hawkes, for suggesting the topic of this thesis, and for his advice and guidance during its execution.

I gratefully acknowledge the receipt of an SERC Studentship.

DECLARATION

The work in this thesis is my own, except where specifically acknowledged. Part of the argument used in deducing Theorem C from Theorem B (in Section (I.5)) appeared in my M.Sc. Dissertation (University of Warwick, 1981).

SUMMARY

In 1969, Dade showed that the nilpotent length of a finite soluble group is bounded in terms of the composition length of a Carter subgroup. The main aim of this thesis is to prove a dual result to this involving nilpotent injectors instead of Carter subgroups: namely, we prove the following theorem.

THEOREM. Let E be a nilpotent injector of the finite soluble group G . Suppose that E can be generated by m elements, and that G has nilpotent length l . Then

$$l \leq 5m + 3.$$

Three other (similar) bounds are also proved. All four results are consequences of two theorems concerning the representation theory of a soluble group over a finite field.

CONVENTIONS

All groups are finite unless otherwise stated. All modules are finite dimensional.

In the large amount of arithmetic in this work, the period (.) will be used to denote multiplication (not a decimal point).

See the note after Hypotheses (II.2.7) for a convention concerning central products (which we denote by Υ).

NOTATION

Let H and G be groups. Let \mathbb{F} be a field and \mathbb{E} a field extension of \mathbb{F} . Let V be an $\mathbb{E}G$ -module. Let p be a prime, let m and n be integers, and let x be a real number.

$H \leq G$	H is a subgroup of G .
$H \trianglelefteq G$	H is a normal subgroup of G .
$H < G$	H is a proper subgroup of G .
$H \leq \cdot G$	H is a minimal subgroup of G .
$H < \cdot G$	H is a maximal subgroup of G .
The meaning of \triangleleft , $\triangleleft \cdot$, etc., should be obvious.	
$H \text{ char } G$	H is a characteristic subgroup of G .
$Z(G)$	the centre of G .
G'	the derived group of G .
$G^{(n)}$	the n^{th} derived group of G .

$\mathcal{O}(G)$	the Frattini subgroup of G (page 7).
$F(G)$	the Fitting subgroup of G (page 7).
$O_p(G)$	the largest normal p -subgroup of G (page 7).
$O_{p'}(G)$	the largest normal p' -subgroup of G (page 7).
$F_i(G)$	the i^{th} term in the upper nilpotent series of G (page 8).
$I_i(G)$	the i^{th} term in the lower nilpotent series of G .
$K_i(G)$	the i^{th} term in the lower central series of G .
$\text{Aut}(G)$	the automorphism group of G .
$\text{Syl}_p(G)$	the set of Sylow p -subgroups of G .
$C_G(H)$	(where $H \leq G$ or G acts on H) the centraliser of H in G .
$N_G(H)$	(where $H \leq G$) the normaliser of H in G .
$\text{Core}_G(H)$	The core of H in G (page 56).
$l(G)$	the nilpotent length of G (page 7).
$d(G)$	the derived length of G (page 8).
$m(G)$	the minimal number of generators of G .
$r(G)$	the rank of G (page 8).
$r_G(N/M)$	(where $M \leq N$ and $N, M \leq G$) the G -rank of N/M (page 8).
$l_p(G)$	the p -length of G .
$\mathcal{Y}(G)$	the composition length of G .
$\langle X \rangle$	(where $X \leq G$) the subgroup generated by X .
$G \wr H$	the regular wreath product of G and H . (See [17, T.15.6].)
$G \times H$	the central product of G and H . (See page 43 and note on page 46.)

\mathbb{F}^+	the additive group of \mathbb{F} .
\mathbb{F}^\times	the multiplicative group of \mathbb{F} .
$[\mathbb{E} : \mathbb{F}]$	the degree of \mathbb{E} over \mathbb{F} .
$\text{Gal}(\mathbb{E} : \mathbb{F})$	the Galois group of \mathbb{E} over \mathbb{F} .
$\text{GL}(n, \mathbb{F})$	the general linear group of dimension n over \mathbb{F} .
$\text{Sp}(2n, \mathbb{F})$	the symplectic linear group of dimension $2n$ over \mathbb{F} (see page 47).
V_H	(where $H \leq G$) V considered as an $\mathbb{F}H$ -module.
$U G$	(where $H \leq G$ and U is an $\mathbb{F}H$ -module) the $\mathbb{F}G$ -module induced from U .
$\ker(G \text{ on } V)$	the kernel of the action of G on V .
\oplus	direct sum (of $\mathbb{F}G$ -modules).
$*$	tensor product (of $\mathbb{F}G$ -modules).
$\text{Hom}_{\mathbb{F}G}(V, W)$	(where V and W are $\mathbb{F}G$ -modules) the set of linear maps θ from V into W such that $v\theta g = v\theta$ for all $v \in V, g \in G$.
$\dim_{\mathbb{F}}(V)$	the dimension of V as a vector space over \mathbb{F} . (We will write $\dim(V)$ if the field is clear.)
$\text{codim}_{\mathbb{F}}(W)$	(where W is a submodule of V) $\dim_{\mathbb{F}}(V/W) = \dim_{\mathbb{F}}(V) - \dim_{\mathbb{F}}(W)$.
$V \cong_G W$	(where V and W are $\mathbb{F}G$ -modules) V and W are isomorphic as $\mathbb{F}G$ -modules.
\mathcal{N}	the class of all nilpotent groups.
\mathbb{F}_q	the (finite) field of order q .
\mathbb{R}	the real numbers.
\mathbb{Z}	the integers.

\mathbb{Z}_n	the cyclic group of order n .
$m n$	m divides n .
$m \nmid n$	m does not divide n .
$p^i \parallel n$	i is the largest natural number such that $p^i \mid n$.
$\lfloor x \rfloor$	the largest integer not greater than x .
$\lceil x \rceil$	the smallest integer not less than x .
\log_n	logarithm to base n .
\log	natural logarithm.

\mathbb{Z}_n	the cyclic group of order n .
$m n$	m divides n .
$m \nmid n$	m does not divide n .
$p^i n$	i is the largest natural number such that $p^i n$.
$\lfloor x \rfloor$	the largest integer not greater than x .
$\lceil x \rceil$	the smallest integer not less than x .
\log_n	logarithm to base n .
\log	natural logarithm.

INTRODUCTION

The main aim of this thesis is to prove the following theorem.

THEOREM. Let E be a nilpotent injector of the finite soluble group G . Suppose that E can be generated by m elements, and that G has nilpotent length l . Then

$$l \leq 5m + 3.$$

(This appears as Part (ii) of Theorem C on page 23.)

We recall that the nilpotent length of a finite soluble group G can be defined as the shortest length i of a normal series $1 = N_0 \leq N_1 \leq \dots \leq N_i = G$ of G such that each factor group N_j/N_{j-1} is nilpotent ($1 \leq j \leq i$). (See also page 7.) A nilpotent injector of a soluble group G is a maximal nilpotent subgroup of G containing the Fitting subgroup of G . The nilpotent injectors form a single conjugacy class in G , and may be viewed as the duals of the Carter subgroups. (See Section (J.4).) Like Carter subgroups, they may be seen as a measure of the nilpotence of a group.

In [5], Dade proved the following theorem.

THEOREM. Let G be a finite soluble group, and let n be the composition length of a Carter subgroup of G . Suppose that the nilpotent length of G is l . Then

$$l \leq 10(2^n - 1) - 4n.$$

As we have described above, nilpotent injectors and Carter subgroups are duals of one another. The main motivation behind this work was to prove a dual to Dade's theorem with nilpotent injectors in place of Carter subgroups. It is in fact quite easy to show that the nilpotent length of a finite soluble group is bounded in terms of the composition length of a nilpotent injector. We prove this as (I.5.6(iii)). Our main theorem, stated at the beginning of this introduction, provides a superior dual to this, since the minimal number of generators of a group is normally much less than its composition length.

In fact we prove three other (similar) bounds to our main theorem, concerning the structure of nilpotent injectors, Sylow subgroups, and the nilpotent and derived length of G . (See Theorem C, page 23.) The four parts of Theorem C all follow from a 'modular' representation theorem, Theorem B, which in turn is based on a 'classical' representation theorem, Theorem A.

The contents of this thesis are organised as follows.

In Section 5 of Chapter I, we state the three main theorems and, assuming the representation theorems A and B, we deduce the group-theoretic consequences, Theorem C. The first four sections of Chapter I introduce the basic concepts and results concerning

finite soluble groups that we need in Section 5 (and elsewhere).

Chapter II contains standard results on representation theory (such as Clifford's theorem) and group theory (especially Hall's theorem on p -groups with all characteristic abelian subgroups cyclic). Then in (II.4) we give an account of the method of proof of Theorems A and B.

The real work is done in Chapters III and IV. Theorem B follows quite quickly from Theorem A, so it is the proof of Theorem A that takes up most of these two chapters. Now Theorem A concerns a soluble group KP acting faithfully and irreducibly on a module V over a finite field, where K is a normal Hall p' -subgroup of KP , and P is a Sylow p -subgroup of KP . In this situation we want to show that the number $|V|/|P|^2$ increases with the derived length of K .

In Section 1 of Chapter III, we prove some arithmetical bounds which lead, essentially, to bounds for $|P|$ in terms of $|V|$ in the above situation in the case $K = 1$. These will be used at various points in the proof of Theorem A, and elsewhere. In (III.2) we prove the main lemma for the 'homogeneous' case of Theorem A. Lemma (III.2.5) gives us a chief factor of K to which we can apply induction in this case. In (III.3) we prove estimates for $|W|$ in terms of $|V|$ under various hypotheses on P , Y , and V . The most important of these is a 'derived length one version'

of Theorem A, namely (III.3.6). The final section of Chapter III consists of results used in proving Theorem B.

Chapter IV consists of the proofs of Theorems A and B, and three examples relating to Theorem A.

A more detailed introduction to the motivation and methods of this work can be obtained from (I.5) (omitting proofs) and (II.4).

finite soluble groups that we need in Section 5 (and elsewhere).

Chapter II contains standard results on representation theory (such as Clifford's theorem) and group theory (especially Hall's theorem on p -groups with all characteristic abelian subgroups cyclic). Then in (II.4) we give an account of the method of proof of Theorems A and B.

The real work is done in Chapters III and IV. Theorem B follows quite quickly from Theorem A, so it is the proof of Theorem A that takes up most of these two chapters. Now Theorem A concerns a soluble group KP acting faithfully and irreducibly on a module V over a finite field, where K is a normal Hall p' -subgroup of KP , and P is a Sylow p -subgroup of KP . In this situation we want to show that the number $|V|/|P|^2$ increases with the derived length of K .

In Section 1 of Chapter III, we prove some arithmetical bounds which lead, essentially, to bounds for $|P|$ in terms of $|V|$ in the above situation in the case $K = 1$. These will be used at various points in the proof of Theorem A, and elsewhere. In (III.2) we prove the main lemma for the 'homogeneous' case of Theorem A. Lemma (III.2.5) gives us a chief factor of K to which we can apply induction in this case. In (III.3) we prove estimates for $|M|$ in terms of $|V|$ under various hypotheses on P , Y , and V . The most important of these is a 'derived length one version'

of Theorem A, namely (III.3.6). The final section of Chapter III consists of results used in proving Theorem B.

Chapter IV consists of the proofs of Theorems A and B, and three examples relating to Theorem A.

A more detailed introduction to the motivation and methods of this work can be obtained from (I.5) (omitting proofs) and (II.4).

CHAPTER I

THE MAIN THEOREMS

This chapter has two aims. Firstly, Sections 1-4 constitute an introduction to some basic concepts and results concerning finite soluble groups that we shall need. Secondly, in Section 5, we assume the representation theorems whose proofs constitute the bulk of this work, and deduce consequences about the structure of finite soluble groups.

I.1 DEFINITIONS

A complete list of notation can be found on page iv. Here, we define and discuss some less well-known items.

Let G be a group.

$\Phi(G)$ will denote the Frattini subgroup of G . If $G \neq 1$, it is defined to be the intersection of all maximal subgroups of G . By convention, we put $\Phi(1) = 1$. Since any automorphism of G takes maximal subgroups to maximal subgroups, it follows that $\Phi(G)$ is a characteristic subgroup of G .

$F(G)$ will denote the Fitting subgroup of G .

Let N and M be normal subgroups of G which are both nilpotent. It is trivial that NM is also normal in G , and it is well-known [17, II.4.1] that NM is again nilpotent. We define $F(G)$ to be the product of all normal nilpotent subgroups of G . By the above, $F(G)$ is again normal and nilpotent. Thus $F(G)$ is the largest normal nilpotent subgroup of G .

$O_p(G)$ and $O_{p'}(G)$ (where p is a prime). In a similar manner to $F(G)$, we define $O_p(G)$ to be the largest normal p -group of G , and $O_{p'}(G)$ to be the largest normal p' -subgroup of G . (A p' -group is a group whose order is coprime to p .) We also define $O_{p',p}(G)$ by

$$O_{p',p}(G)/O_{p'}(G) = O_p(G/O_{p'}(G)).$$

$l(G)$. If G is soluble we will denote the nilpotent length of G by $l(G)$. We give two definitions. It is easy to check that they are equivalent, and we shall use them interchangeably.

Firstly, $l(G)$ is the shortest length i of a series

$$1 = N_0 \leq N_1 \leq \dots \leq N_i = G$$

of normal subgroups N_0, \dots, N_i such that N_j/N_{j-1} is nilpotent ($1 \leq j \leq i$).

For the second definition we first note that when G is soluble and $G \neq 1$, we have $F(G) \neq 1$. This is because any minimal normal subgroup of G is abelian, and so contained in $F(G)$. This means that if we put $F_0(G) = 1$ and define $F_i(G)$ for $i \geq 1$ by

$$F_i(G)/F_{i-1}(G) = F(G/F_{i-1}(G)),$$

we will obtain an ascending series, the upper nilpotent series of G ,

$$1 = F_0(G) \leq F_1(G) \leq \dots,$$

and since $F_i(G) > F_{i-1}(G)$ unless $F_i(G) = G$, we must have $F_i(G) = G$ for some i . Then $l(G)$ is the least such i .

Because of this second definition $l(G)$ is sometimes known as the Fitting height of G .

$m(G)$ will denote the minimal number of generators of G .

$d(G)$. If G is soluble, we will denote the derived length of G by $d(G)$. If we put $G = G_0$, and define G_i for $i \geq 1$ by

$$G_i = (G_{i-1})',$$

then $d(G)$ is the least i such that $G_i = 1$.

$r(G)$ and $r_G(N/M)$. If G is soluble we denote the rank of G by $r(G)$. If N and M are normal subgroups of G with $N \supseteq M$, then $r_G(N/M)$ denotes the G -rank of N/M .

Suppose that G is soluble and that N and M are normal subgroups of G with $N \supseteq M$. Then we can choose a chief series passing through N and M , so that we have

Firstly, $l(G)$ is the shortest length i of a series

$$1 = N_0 \triangleleft N_1 \triangleleft \dots \triangleleft N_i = G$$

of normal subgroups N_0, \dots, N_i such that N_j/N_{j-1} is nilpotent ($1 \leq j \leq i$).

For the second definition we first note that when G is soluble and $G \neq 1$, we have $F(G) \neq 1$. This is because any minimal normal subgroup of G is abelian, and so contained in $F(G)$. This means that if we put $F_0(G) = 1$ and define $F_i(G)$ for $i \geq 1$ by

$$F_i(G)/F_{i-1}(G) = F(G/F_{i-1}(G)),$$

we will obtain an ascending series, the upper nilpotent series of G ,

$$1 = F_0(G) \triangleleft F_1(G) \triangleleft \dots,$$

and since $F_i(G) > F_{i-1}(G)$ unless $F_i(G) = G$, we must have $F_i(G) = G$ for some i . Then $l(G)$ is the least such i .

Because of this second definition $l(G)$ is sometimes known as the Fitting height of G .

$m(G)$ will denote the minimal number of generators of G .

$d(G)$. If G is soluble, we will denote the derived length of G by $d(G)$. If we put $G = G_0$, and define G_i for $i \geq 1$ by

$$G_i = (G_{i-1})',$$

then $d(G)$ is the least i such that $G_i = 1$.

$r(G)$ and $r_G(N/M)$. If G is soluble we denote the rank of G by $r(G)$. If N and M are normal subgroups of G with $N \triangleright M$, then $r_G(N/M)$ denotes the G -rank of N/M .

Suppose that G is soluble and that N and M are normal subgroups of G with $N \triangleright M$. Then we can choose a chief series passing through N and M , so that we have

$$M = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = N,$$

where each G_i/G_{i-1} ($1 \leq i \leq n$) is a chief factor of G . Since G is soluble, each G_i/G_{i-1} is an elementary abelian p_i -group for some prime p_i . If G_i/G_{i-1} has order $p_i^{r_i}$ (for suitable integers r_i), then

$$r_G(N/M) = \max_{1 \leq i \leq n} r_i.$$

It follows from the Jordan-Holder theorem that the definition is independent of the choice of the chief series.

Finally, we set

$$r(G) = r_G(G/1).$$

$l_p(G)$ will denote the p -length of G (where p is a prime). It can be defined as the smallest integer n such that there exists a series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_n \trianglelefteq M_n = G$$

of normal subgroups of G where M_i/N_i is a p' -group ($0 \leq i \leq n$), and N_i/M_{i-1} is a p -group ($1 \leq i \leq n$).

Group action. Let A be a group. We will say that A acts on G if there is given a homomorphism from A into the automorphism group of G . If this is the case we can form the semi-direct product of G and A which we will denote by GA , where the action of A on G is written as conjugation. Thus G is a normal subgroup of GA , and $G \cap A = 1$.

We define

$$[G, A] = \langle \{g^{-1}g^a; g \in G, a \in A\} \rangle.$$

Similarly, if V is a vector space on which A acts, we write

$$[V, A] = \langle \{v - va; v \in V, a \in A\} \rangle.$$

(This definition coincides with the definition of $[G, A]$)

if V is regarded as an abelian group and written multiplicatively.)

If B acts on $[G, A]$, it will be convenient to write $[[G, A], B] = [G, A, B]$.

Finally, a subgroup H of G is called A-invariant if $h^a \in H$ whenever $h \in H$ and $a \in A$. Note that if N is a normal A-invariant subgroup of G , then A acts naturally on both G/N and N .

I.2. THE FRATTINI AND FITTING SUBGROUPS

Nearly all the material in this section comes from [17, III.3 & III.4]. Some of the results (and proofs) hold without restriction to soluble groups, but for simplicity's sake we will assume throughout this section that all groups are soluble. In general, we will refer to Huppert's book for proofs, but some proofs or sketch proofs are included here where this seems illuminating.

We concentrate on $\Phi(G)$ first.

(I.2.1) Let G be a group.

(i) $\Phi(G)$ consists of those elements of G which are redundant in any generating set for G . Precisely

$$\Phi(G) = \{g \in G; G = \langle X, g \rangle \Rightarrow G = \langle X \rangle \text{ for all } X \in G\}.$$

(ii) If $N \leq \Phi(G)$ and $N \cong G$, then $m(G) = m(G/N)$.

Proof (i) [17, III.3.2(a)].

(ii) Immediate from (i).

The next result is probably the most fundamental fact about $\Phi(G)$.

(I.2.2) $\Phi(G)$ is nilpotent.

Proof We aim to show that all Sylow subgroups of $\Phi(G)$ are normal in $\Phi(G)$, which will prove that $\Phi(G)$ is nilpotent.

Let P be a Sylow p -subgroup of $\Phi(G)$ for some prime p . Let $g \in G$. Then, since $\Phi(G)$ is normal in G , we have $P^g \leq \Phi(G)$. So, by Sylow's theorem, $P^g = P^x$ for some $x \in \Phi(G)$. Then

$P^{gx^{-1}} = P$, so $gx^{-1} \in N_G(P)$. Thus $g = (gx^{-1})x \in N_G(P)\phi(G)$.

Therefore we have $G = N_G(P)\phi(G)$ and, using (I.2.1(i)), we have $G = N_G(P)$. So P is normal in G , and therefore in $\phi(G)$, as required.

(I.2.3) If $N \triangleleft G$, then $\phi(N) \leq \phi(G)$.

Proof [17, III.3.3(b)].

(I.2.4) If $A \triangleleft G$ is abelian and $A \cap \phi(G) = 1$, then A possesses a complement in G , i.e., there exists $H \leq G$ such that $G = HA$ and $H \cap A = 1$.

Proof [17, III.4.4].

Our last result on $\phi(G)$ concerns the case when G is a p -group.

(I.2.5) Let G be a p -group. Then $G/\phi(G)$ is elementary abelian, and $\phi(G)$ is the smallest normal subgroup of G with elementary abelian factor group.

Proof [17, III.3.14(a)].

We turn our attention to $F(G)$. Firstly, we give two useful descriptions of this group.

(I.2.6) (i) $F(G)$ is the direct product of all the groups $O_p(G)$ such that p divides $|G|$.

(ii) Let $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$ be a chief series for G .
Then

$$F(G) = \prod_{1 \leq i \leq n} C_G(G_i/G_{i-1}).$$

Proof (i) Let p and q be distinct primes dividing $|G|$.

Since $O_p(G)$ and $O_q(G)$ are both normal, we have

$$[O_p(G), O_q(G)] \leq O_p(G) \cap O_q(G) = 1.$$

Thus the product of the $O_p(G)$ is direct and contained in $F(G)$.

On the other hand, if P is a Sylow p -subgroup of $F(G)$ for some prime p , then P is normal, and hence characteristic in $F(G)$, and so normal in G . Thus $P \leq O_p(G)$, and (i) is proved.

(ii) [17, III, 4.3].

A vital property of $F(G)$ which we will use repeatedly is the following.

(I.2.7) $C_G(F(G)) \leq F(G)$.

Note that this result is not necessarily true for non-soluble G .

Proof Let $C = C_G(F(G))$ and assume that $F(G)C > F(G)$.

Let $A/F(G)$ be a chief factor of G with $F(G)C \triangleright A > F(G)$.

Since G is soluble, $A/F(G)$ is abelian, and so $A' \leq F(G)$. We

denote the i^{th} term in the upper central series of a group X

by $K_i(X)$. Since $F(G)$ is nilpotent, so is $A/A \cap C \cong F(G)/F(G) \cap A \cap C$

and thus $K_n(A/A \cap C) = 1$ for some n .

(I.2.6) (i) $F(G)$ is the direct product of all the groups $O_p(G)$ such that p divides $|G|$.

(ii) Let $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$ be a chief series for G .
Then

$$F(G) = \bigcap_{1 \leq i \leq n} C_G(G_i/G_{i-1}).$$

Proof (i) Let p and q be distinct primes dividing $|G|$.

Since $O_p(G)$ and $O_q(G)$ are both normal, we have

$$[O_p(G), O_q(G)] \leq O_p(G) \cap O_q(G) = 1.$$

Thus the product of the $O_p(G)$ is direct and contained in $F(G)$.

On the other hand, if P is a Sylow p -subgroup of $F(G)$ for some prime p , then P is normal, and hence characteristic in $F(G)$, and so normal in G . Thus $P \leq O_p(G)$, and (i) is proved.

(ii) [12, III, 4.3].

A vital property of $F(G)$ which we will use repeatedly is the following.

(I.2.7) $C_G(F(G)) \leq F(G)$.

Note that this result is not necessarily true for non-soluble G .

Proof Let $C = C_G(F(G))$ and assume that $F(G)C > F(G)$.

Let $A/F(G)$ be a chief factor of G with $F(G)C \triangleright A > F(G)$. Since G is soluble, $A/F(G)$ is abelian, and so $A' \leq F(G)$. We denote the i^{th} term in the upper central series of a group X by $K_i(X)$. Since $F(G)$ is nilpotent, so is $A/A \cap C \cong F(G)/F(G) \cap A \cap C$ and thus $K_n(A/A \cap C) = 1$ for some n .

(I.2.6) (i) $F(G)$ is the direct product of all the groups $O_p(G)$ such that p divides $|G|$.

(ii) Let $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G$ be a chief series for G .
Then

$$F(G) = \bigcap_{1 \leq i \leq n} C_G(G_i/G_{i-1}).$$

Proof (i) Let p and q be distinct primes dividing $|G|$.

Since $O_p(G)$ and $O_q(G)$ are both normal, we have

$$[O_p(G), O_q(G)] \leq O_p(G) \cap O_q(G) = 1.$$

Thus the product of the $O_p(G)$ is direct and contained in $F(G)$.

On the other hand, if P is a Sylow p -subgroup of $F(G)$ for some prime p , then P is normal, and hence characteristic in $F(G)$, and so normal in G . Thus $P \leq O_p(G)$, and (i) is proved.

(ii) [17, III, 4.3].

A vital property of $F(G)$ which we will use repeatedly is the following.

(I.2.7) $C_G(F(G)) \leq F(G)$.

Note that this result is not necessarily true for non-soluble G .

Proof Let $C = C_G(F(G))$ and assume that $F(G)C > F(G)$.

Let $A/F(G)$ be a chief factor of G with $F(G)C \triangleright A > F(G)$. Since G is soluble, $A/F(G)$ is abelian, and so $A' \leq F(G)$. We denote the i^{th} term in the upper central series of a group X by $K_i(X)$. Since $F(G)$ is nilpotent, so is $A/A \cap C \cong F(G)/F(G) \cap A \cap C$ and thus $K_n(A/A \cap C) = 1$ for some n .

Now

$K_{n+1}(A) \leq C \cap A' \leq C \cap F(G) = C_{F(G)}(F(G)) = Z(F(G)) \leq Z(A)$,
the last inequality holding because $A \leq CF(G)$. Thus $K_{n+2}(A) = 1$,
showing that A is nilpotent. But A is also normal in G ,
giving us the contradiction $A \leq F(G)$. Therefore (I.2.7) holds.

In the final result of this section we consider the
relationship between $F(G)$ and $\phi(G)$.

(I.2.8) Let $F = F(G)$ and $\phi = \phi(G)$.

(i) $\phi \leq F$.

(ii) $F(G/\phi) = F/\phi$.

(iii) F/ϕ is the direct product of the elementary abelian
 p -groups $O_p(G)\phi/\phi$. Each $O_p(G)\phi/\phi$ is completely reducible
when regarded as a G -module over the field of p elements.

(iv) $C_G(F/\phi) = F$.

Note: It is explained in (I.5.5) how $O_p(G)\phi/\phi$ (for example)
may be regarded as a G -module, if this is not already familiar.

Proof (i) This is immediate from (I.2.2).

(ii) [17, III.4.2(c)].

(iii) The first statement follows from (I.2.3), (I.2.5), and
(I.2.6(i)); and the second from [17, III.4.4].

(iv) By (iii), the group F/ϕ is abelian, and so $F \leq C_G(F/\phi)$.

Now let $x \in C_G(F/\phi)$. Then $x\phi \in C_{G/\phi}(F/\phi)$. But $F/\phi = F(G/\phi)$
by (ii), so

$C_{G/\phi}(F/\phi) = C_{G/\phi}(F(G/\phi)) \leq F(G/\phi) = F/\phi$,
using (I.2.7) applied to G/ϕ . Thus $x\phi \in F/\phi$, and so $x \in F$, as
required.

I.3. NILPOTENT LENGTH AND DERIVED LENGTH

Let G be a soluble group. Here we list the basic properties of the nilpotent length $l(G)$ and the derived length $d(G)$ of G .

(I.3.1) Suppose that $H \leq G$ and $N \triangleleft G$.

(i) $l(G/N) \leq l(G)$ and $d(G/N) \leq d(G)$.

(ii) $l(H) \leq l(G)$ and $d(H) \leq d(G)$.

(iii) $l(G) \leq l(G/N) + l(N)$ and $d(G) \leq d(G/N) + d(N)$.

Proof All these results are straightforward and easy from the definitions.

Note: We will use (I.3.1) without reference.

(I.3.2) (i) Let G_1, \dots, G_n be soluble groups. Then

$l(G_1 \times \dots \times G_n) = \max_{1 \leq i \leq n} l(G_i)$ and $d(G_1 \times \dots \times G_n) = \max_{1 \leq i \leq n} d(G_i)$.

(ii) Let N_1, \dots, N_n be normal subgroups of a soluble group

G . Then

$l(G/N_1 \cap \dots \cap N_n) = \max_{1 \leq i \leq n} l(G/N_i)$ and

$d(G/N_1 \cap \dots \cap N_n) = \max_{1 \leq i \leq n} d(G/N_i)$.

Proof (i) Straightforward.

(ii) Define a map $\theta: G/N_1 \cap \dots \cap N_n \rightarrow G/N_1 \times \dots \times G/N_n$ by $(N_1 \cap \dots \cap N_n)g \mapsto (N_1g, \dots, N_ng)$ ($g \in G$). It is easy to check that θ is a well-defined, injective homomorphism. Now

applying (i) gives us the result.

$$(I.3.3) \quad l(G) = l(G/\mathcal{Z}(G)).$$

Proof Immediate from (I.2.8(ii)).

I.4. INJECTORS AND PROJECTORS

The study of injectors and projectors is of fundamental importance in the theory of finite soluble groups. We refer the reader to [10] for a general account. We will content ourselves here with a very brief summary of the concepts and basic results together with some characterisations of nilpotent injectors which will need later.

(I.4.1) DEFINITIONS. (i) A class of groups is a collection \underline{X} of groups with the following property: if G is any group in \underline{X} , then \underline{X} contains all groups isomorphic to G .

Note: We will always distinguish classes of groups from other objects by double underlining.

(ii) Let G be a group and let \underline{X} be a class. We say that a subgroup H of G is \underline{X} -maximal in G if $H \in \underline{X}$ and if whenever we have $H < K \leq G$, then K is not in \underline{X} .

(iii) Let G be a group and let $H \leq G$. Suppose that \underline{X} is a class. Then H is an \underline{X} -projector of G if HN/N is \underline{X} -maximal in G/N for all $N \triangleleft G$.

We denote the class of all nilpotent groups by \underline{N} . Now \underline{N} -projectors are also known as Carter subgroups, and we will use this latter term here.

(iv) Let G be a group, let \underline{X} be a class and suppose that $H \leq G$. Then H is an \underline{X} -injector of G if $H \cap K$ is \underline{X} -maximal in K for all subnormal subgroups K of G . (A subgroup N of a group G is subnormal if there exists a chain of subgroups

$N = M_0 \triangleleft M_1 \triangleleft \dots \triangleleft M_n = G$ such that $M_{i-1} \triangleleft M_i$ for $1 \leq i \leq n$.)

(I.4.2) EXAMPLE. Let G be the symmetric group on 4 symbols. We aim to show that G possesses \underline{N} -injectors, and that they are in fact the three Sylow 2-subgroups of G .

Firstly, there is no nilpotent subgroup of G whose order is divisible by both 2 and 3, for such a group would contain an element of order 6, and G does not contain such an element. Next, we note that if H is a nilpotent injector of G , then putting $K = G$ in the definition tells us that H is \underline{N} -maximal in G . Since we also know that H is either a 2-group or a 3-group, H is either a Sylow 2-subgroup or a Sylow 3-subgroup. We need to eliminate the possibility that H is a Sylow 3-subgroup, so suppose for a contradiction that it is. Let $K = \langle (12)(34), (13)(24) \rangle$, a normal subgroup of G of order 4. Then $H \cap K = 1$ is not \underline{N} -maximal in K .

Thus we have shown that the only possibility for H is a Sylow 2-subgroup. It remains to check that a Sylow 2-subgroup is in fact a nilpotent injector. Since the only subnormal subgroups of G are subgroups of K , the alternating group on 4 symbols of order 12, and G itself, this is easily verified.

It can also be shown that the Sylow 2-groups of G are also the Carter subgroups of G . Of course, \underline{N} -injectors and Carter subgroups do not normally coincide.

We note then, that for the particular case where G is the symmetric group on 4 symbols, and \underline{X} is the class of nilpotent groups, G possesses a unique conjugacy class of \underline{X} -injectors and of \underline{X} -projectors. We now wish to make vastly more general

statements along these lines. We need firstly some definitions of particular sorts of classes.

(I.4.3) DEFINITIONS. (i) A class \underline{X} of groups is called a saturated formation if

- (a) \underline{X} is nonempty;
- (b) If $G \in \underline{X}$ and $N \trianglelefteq G$, then $G/N \in \underline{X}$;
- (c) If G is a group with normal subgroups N_1, \dots, N_n such that $G/N_i \in \underline{X}$ for $1 \leq i \leq n$, and $\bigcap_{1 \leq i \leq n} N_i = 1$, then $G \in \underline{X}$;
- (d) If G is a group with a normal subgroup N such that $N \trianglelefteq \emptyset(G)$ and $G/N \in \underline{X}$, then $G \in \underline{X}$.

(ii) A class of groups \underline{X} is called a Fitting class if

- (a) \underline{X} is nonempty;
- (b) If $G \in \underline{X}$ and $N \trianglelefteq G$, then $N \in \underline{X}$;
- (c) If $G = N_1 N_2$ where N_1 and N_2 are normal subgroups of G , and are both members of \underline{X} , then $G \in \underline{X}$.

(I.4.4) REMARK. The class \underline{N} is both a saturated formation and a Fitting class. That \underline{N} is a saturated formation follows from (I.3.1), (I.3.2(ii)), and (I.3.3); that \underline{N} is a Fitting class follows from (I.3.1) and [17, III.4.1].

We now come to the two basic and important results concerning injectors and projectors in finite soluble groups.

(I.4.5) Let G be a soluble group and let \underline{X} be a class of groups.

- (i) If \underline{X} is a saturated formation, then G possesses a unique

conjugacy class of X -projectors.

(ii) If X is a Fitting class, then G possesses a unique conjugacy class of X -injectors.

Proof [9, Satz 2.1], and [7, Satz 1].

Note (I.4.5(i)) holds for more general classes than saturated formations: namely, it holds for Schunck classes. This is proved in [21].

By (I.4.4) and (I.4.5), therefore, every soluble group G possesses a unique conjugacy class of Carter subgroups and a unique conjugacy class of nilpotent injectors. It is natural to ask how the structure of G is related to the structure of its nilpotent injectors and Carter subgroups. It is the main aim of this work to prove results of this type for nilpotent injectors.

We state one more general theorem before concentrating our attention on nilpotent injectors.

(I.4.6) Let G be a soluble group and let X be a class of groups. If X is a saturated formation (respectively Fitting class), and L is an X -projector (respectively X -injector) of G , and $L \leq H \leq G$, then L is an X -projector (respectively X -injector) of H .

Proof [9, Hilfsatz 2.1], and [7, Satz 2].

The next result gives two characterisations of nilpotent

injectors.

(I.4.7) Let G be a soluble group and let E be a subgroup of G .

(i) The following are equivalent.

(a) E is a nilpotent injector of G .

(b) $F(G) \leq E$, and E is N -maximal in G .

(c) For each prime p , the Sylow p -subgroup of E is also a Sylow p -subgroup of $C_G(F(G)_p)$, (where $F(G)_p$ is the Hall p' -subgroup of $F(G)$).

(ii) Further, if for each prime p we choose any Sylow p -subgroup M_p of $C_G(F(G)_p)$, then $[M_p, M_q] = 1$ whenever $p \neq q$, and the (direct) product of the M_p is a nilpotent injector of G .

Proof The statement of this result appears as [17, VI.7.18]. A proof can be found in [19].

Finally in this section, we have an easy result based on the so-called Frattini argument.

(I.4.8) Let E be a nilpotent injector of G and suppose that $E \leq N \triangleleft G$. Then $G = N_G(E)N$.

Proof Let $g \in G$. Then E and E^g are both contained in N , and by (I.4.6) are nilpotent injectors of N . Thus, by (I.4.5) they are conjugate in N , so that

$$E^x = E^g$$

for some $x \in N$. But now $gx^{-1} \in N_G(E)$, and so $g \in N_G(E)N$, and we are done.

1.5. THE MAIN THEOREMS

We now state the three main theorems of this thesis.

THEOREM A. Let p and q be distinct primes. Let K be a soluble p' -group, and let P be a p -group acting on K . Let V be an irreducible $\mathbb{F}_q KP$ -module faithful for KP . Put $d = d(K)$. Then

$$|V|/|P|^2 \geq \begin{cases} 4 \cdot 3^{d-4} & \text{if } d \geq 4 \\ 3 & \text{if } d = 3. \end{cases}$$

THEOREM B. Let p be a prime. Let K be a soluble p' -group and let P be a p -group acting on K . Let V be a nonzero $\mathbb{F}_p KP$ -module faithful for K . Let $l = l(K)$ and $d = d(V)$. Then

- (i) $\text{codim}[V, P] \geq 3^{l(1-3)} \geq 1$, and
- (ii) $\text{codim}[V, P] \geq [3^{l(d-4)}] \geq 1d$.

THEOREM C. Let G be a soluble group. Let E be a nilpotent injector of G . We put

$m = m(E)$ and $m_1 = \max\{m(P); P \in \text{Syl}_p(G) \text{ for some prime } p\}$,
 $d = d(E)$ and $d_1 = \max\{d(P); P \in \text{Syl}_p(G) \text{ for some prime } p\}$.

Then

- (i) $l(G) \leq 4m_1$;
- (ii) $l(G) \leq 5m + 3$;
- (iii) $d(G) \leq 4m_1 + d_1^2$;
- (iv) $d(G) \leq 5m + 2 + d + d^2$.

Theorem C is a fairly easy consequence of Theorem B; we will deduce C from B in this section. Likewise, B follows quite quickly from A. It is the proof of A that occupies the bulk of this work. We will leave further discussion of A and B until the end of Chapter two when we will have covered some necessary representation theory. Before proving that B implies C, we discuss the motivation for C.

Firstly, as promised in the last section, these results provide a link between the structure of a soluble group and the structure of its nilpotent injectors. Further motivation comes from papers of Dade and Hawkes.

In [5], Dade proves the following theorem:

Theorem. Let G be a soluble group and let n be the composition length of a Carter subgroup. Then

$$l(G) \leq 10(2^n - 1) - 4n.$$

Since nilpotent injectors are natural duals to Carter subgroups, the question arises as to whether a similar result holds with Carter subgroups replaced by nilpotent injectors. In fact the 'strict' dual of this theorem is very easy. In (I.5.6(iii)) we will show that if n is the composition length of a nilpotent injector E of G , then

$$l(G) \leq 4 + 2\log_3(n/2).$$

This result is proved without use of Theorem B.

Now $m(E) \leq n$ trivially, and in general $m(E)$ may be much less than n . Thus a bound for $l(G)$ in terms of $m(E)$ is a more satisfactory dual to Dade's theorem. This is what Theorem C(ii) achieves.

Secondly, in [15], Hawkes shows that, in the notation

of Theorem C,

$$l(G) \leq 2m_1^2 + 4m_1 + 1.$$

Hawkes' bound is based on a similar representation theorem to Theorem B (Theorem A(ii) of [15]), but one which only holds when $|K|$ is odd and p is at least 5. Because of this, a quadratic rather than a linear bound is obtained. So a second motivation was to improve Hawkes' bound to a linear one, as in C(i).

Although the intention of this work was to find bounds for $l(G)$, it was realised that with some modification, the representation theorems A and B would hold with $l(G)$ replaced by $d(G)$. Parts (iii) and (iv) of Theorem C are group-theoretic consequences.

(I.5.1) EXAMPLE. Let p be a prime. We aim to show that there are 2-generator finite p -groups of arbitrary derived length. We remove our overall hypothesis that all groups are finite in this example.

Let F be a 2-generator free group, generated by a and b , say. Let n be any natural number. We first show that the n^{th} derived group $F^{(n)}$ of F is nontrivial. In fact, we prove by induction on n the following statement. (*) Let i and j be nonzero integers. Then there exists a nonempty word (and hence a nontrivial element) in $F^{(n)}$ of reduced form $a^i \dots b^j$.

Clearly $[a^i, b^{-j}]$ satisfies (*) for $n=1$, so assume that $n > 1$ and that the result is true for smaller values of n . Then since $i, 2i, j$, and $2j$ are nonzero integers, there exist nonempty words in $F^{(n-1)}$ of reduced form $x = a^i \dots b^{2j}$ and $y = a^{2i} \dots b^j$. It is easily checked that $[x, y^{-1}]$ is the required element of $F^{(n)}$, and so (*) is established.

of Theorem C,

$$l(G) \leq 2m_1^2 + 4m_1 + 1.$$

Hawkes' bound is based on a similar representation theorem to Theorem B (Theorem A(ii) of [15]), but one which only holds when $|K|$ is odd and p is at least 5. Because of this, a quadratic rather than a linear bound is obtained. So a second motivation was to improve Hawkes' bound to a linear one, as in C(i).

Although the intention of this work was to find bounds for $l(G)$, it was realised that with some modification, the representation theorems A and B would hold with $l(G)$ replaced by $d(G)$. Parts (iii) and (iv) of Theorem C are group-theoretic consequences.

(I.5.1) EXAMPLE. Let p be a prime. We aim to show that there are 2-generator finite p -groups of arbitrary derived length. We remove our overall hypothesis that all groups are finite in this example.

Let F be a 2-generator free group, generated by a and b , say. Let n be any natural number. We first show that the n^{th} derived group $F^{(n)}$ of F is nontrivial. In fact, we prove by induction on n the following statement. (*) Let i and j be nonzero integers. Then there exists a nonempty word (and hence a nontrivial element) in $F^{(n)}$ of reduced form $a^i \dots b^j$.

Clearly $[a^i, b^{-j}]$ satisfies (*) for $n=1$, so assume that $n > 1$ and that the result is true for smaller values of n . Then since $i, 2i, j$, and $2j$ are nonzero integers, there exist nonempty words in $F^{(n-1)}$ of reduced form $x = a^i \dots b^{2j}$ and $y = a^{2i} \dots b^j$. It is easily checked that $[x, y^{-1}]$ is the required element of $F^{(n)}$, and so (*) is established.

Now assume for a contradiction that all 2-generator p -groups have derived length at most d (say). It is well known [20, 9.11] that a free group is residually a finite p -group. This means, in particular, that there exist normal subgroups N_i ($i \in I$) of F such that each F/N_i is a finite p -group, and $\bigcap_{i \in I} N_i = 1$. By our assumption, therefore, we have $d(F/N_i) \leq d$. It now follows (using an analogous result to (I.3.2(ii))) that $d(F) \leq d$, whence $F^{(d)} = 1$, contradicting (*).

Thus there are finite 2-generator p -groups of arbitrary derived length.

We see therefore, by (I.5.1), that there is no hope of bounding $d(G)$ in terms of m or m_1 alone if m and m_1 are at least two. (If either $m = 1$ or $m_1 = 1$, then the Fitting group is cyclic and G is metabelian.) The appearance of the quadratic terms in (iii) and (iv) seems suspicious, however. It would be nice to have a linear bound here.

A question that may have arisen in the reader's mind is: why choose $m(E)$ rather than some other invariant of E ? We offer the following example by way of an answer.

(I.5.2) EXAMPLE. Let s be an integer and let p_1, \dots, p_s be distinct primes. Let $G_1 = Z_{p_1}$ and for $2 \leq i \leq s$ define G_i inductively by

$$G_i = G_{i-1} \wr Z_{p_i}.$$

Put $G = G_s$. It is clear from the definition of G_i that it has a normal subgroup of index p_i which is isomorphic

to the direct product of p_i copies of G_{i-1} . It follows that G has a normal series

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_s = G, \quad (*)$$

where H_i is isomorphic to the direct product of $p_h p_{h-1} \dots p_{i+1}$ copies of G_i for $1 \leq i \leq h$.

The following facts about G are easily checked.

- (i) $H_1 = F(G)$ is the unique nilpotent injector of G .
- (ii) $l(G) = d(G) = s$. (In fact the upper Fitting series coincides with (*).)
- (iii) H_i/H_{i-1} is an elementary abelian p_i -group and is isomorphic to a Sylow p_i -subgroup of G .

Thus there are soluble groups of arbitrary nilpotent and derived length which have the property that all their Sylow p -groups and nilpotent injectors are elementary abelian.

We must therefore choose invariants of E (or of the Sylow subgroups) which take large values on large elementary abelian groups. The composition length of E , and the minimal number of generators are two obvious candidates.

The rest of this chapter is devoted to proving that Theorem B implies Theorem C.

In order to do this we need bounds for $d(G)$ and $l(G)$ in terms of the dimension of a faithful, completely reducible representation for G .

(I.5.3) Let G be a soluble group, and let \mathbb{F} be a finite

field. Suppose that V is a completely reducible $\mathbb{F}G$ -module, faithful for G , and put $\dim(V) = n$.

(i) $l(G) \leq 3 + 2\log_3(n/2) \leq 1 + n$.

(ii) $d(G) \leq (5/2)(\log_3(n) + 1) \leq 2 + n$.

Proof The bound $l(G) \leq 3 + 2\log_3(n/2)$ is proved by Hawkes [14]. A very similar bound was proved independently by Frick and Newman [2].

The rest of (i) is easy arithmetic.

(ii) The bound $d(G) \leq (5/2)(\log_3(n) + 1)$ was proved by Dixon [6]. Dixon's bound improves a previous bound of Huppert [15].

Again, the second inequality is easy arithmetic.

We also need bounds for $l_p(G)$ in terms of the derived length of a Sylow p -subgroup of G .

(I.5.4) Let G be a soluble group and let p be a prime. Let $d_p = d(P)$, where P is a Sylow p -subgroup of G . Then

$$l_p(G) \leq d_p.$$

Proof For odd p , this result was proved in the famous paper of Hall and Higman [12]. Then in [2], Berger and Gross showed that $l_2(G) \leq \max(d_2, 2d_2 - 2)$. Finally, in [3], Brjuhanova proved that $l_2(G) \leq d_2$.

(I.5.5) TECHNIQUE. In case the reader is unfamiliar with

the idea of regarding an elementary abelian p -group as a module over the field of p elements, we give a brief account of this method.

Let p be a prime and let V be an elementary abelian p -group. We write V additively. Let \mathbb{F} be the field of p elements. Then $\mathbb{F} \cong \mathbb{Z}/p\mathbb{Z}$ and we can write any element of \mathbb{F} as \bar{n} , the image of some nonnegative $n \in \mathbb{Z}$ under the obvious homomorphism. Then V can be regarded as a vector space over \mathbb{F} by defining multiplication by

$$\bar{n}x = x + \dots + x,$$

where $\bar{n} \in \mathbb{F}$ and $x \in V$, and there are n copies of x on the right hand side of the equation.

Further, if G is a group acting on V , then this action makes V into an $\mathbb{F}G$ -module. (The axioms for V to be a vector space and an $\mathbb{F}G$ -module are all straightforward and easy to check.)

In particular, if G is soluble and H/K is a chief factor of G , then H/K is an elementary abelian p -group and so we can regard H/K as an $\mathbb{F}G$ -module. Note that since H/K is a chief factor, it is irreducible when regarded as a module. Also, we have $\dim_{\mathbb{F}}(H/K) = r_G(H/K)$.

We now derive group-theoretical consequences of (I.5.3), including the 'strict' dual to Dade's theorem of [5].

(I.5.6) Let G be a soluble group and let E be a nilpotent injector of G . Let $n = \nu(E)$ be the composition length of E . Set $F = F(G)$, and $\emptyset = \emptyset(G)$. Then

(i) $l(G) \leq 4 + 2\log_3[2r_G(F/\emptyset)]$;

- (ii) $l(G) \leq 2 + m(F)$;
- (iii) $l(G) \leq 4 + 2\log_3(n/2)$;
- (iv) $d(G/F) \leq 2 + m(F)$.

Proof By (I.2.8(iii)) we can write

$$F/\emptyset \cong_G P_1 \times \dots \times P_n,$$

where each P_i is a chief factor of G . Also, by (I.2.8(iv)) we have

$$F = C_G(F/\emptyset) = \bigcap_{1 \leq i \leq n} C_G(P_i). \quad (*)$$

(i) We regard each P_i as a $G/C_G(P_i)$ -module over the appropriate prime field and deduce from (I.5.3(i)) that

$$l(G/C_G(P_i)) \leq 3 + 2\log_3(\frac{1}{2}r_G(F/\emptyset))$$

since $\dim(P_i) \leq r_G(F/\emptyset)$.

Now (i) follows from (I.5.2(ii)), (*), and the fact that $l(G) = l(G/F) + 1$.

(ii) In an identical way to (i), but using the second inequality of (I.5.3(i)), we obtain

$$l(G) \leq 2 + r_G(F/\emptyset).$$

To prove (ii), therefore, it is sufficient to show that $m(F) \geq r_G(F/\emptyset)$.

Since F is the direct product of the groups $O_p(G)$ for which p divides $|G|$ by (I.2.6(i)), we have

$$\begin{aligned} m(F) &= \max_p m(O_p(G)) \\ &\geq \max_p m(O_p(G)/\emptyset(O_p(G))), \end{aligned}$$

using (I.2.1(ii)). But $O_p(G)/\emptyset(O_p(G))$ is elementary abelian by (I.2.5), so the number of elements required to generate it is equal to its composition length.

Using this together with the fact that $\emptyset(O_p(G)) \leq \emptyset$ by

(I.2.3), we therefore have

$$m(F) \geq \max_p \gamma(O_p(G)\phi/\phi).$$

Finally, since the $O_p(G)\phi/\phi$ are the Sylow p -subgroups of F/ϕ , we must have $\gamma(O_p(G)\phi/\phi) \geq r_G(F/\phi)$ for some p , and so

$$m(F) \geq r_G(F/\phi),$$

which, as we mentioned before, completes the proof of (ii).

(iii) Since $F \leq E$ by (I.4.7(i)), we have

$$r_G(F/\phi) \leq \gamma(F/\phi) \leq \gamma(E) = n,$$

and so (iii) follows from (i).

(iv) This is identical to (i) except that we use (I.5.3(ii)) instead of (I.5.3(i)).

We need an intermediate step before we tackle Theorem C. It is here that we use Theorem B.

(I.5.7) Assume that Theorem B holds. Let D be a soluble group and let p be a prime dividing $|D|$. Assume that $O_p(F(D)) \leq Z(D)$. Let P be a Sylow p -subgroup of D . Then
(i) $l(D) \leq 4m(P)$;
(ii) $d(D/F(D)) \leq 4m(P) + d(P)(l_p(D) - 1)$.

Proof We prove (i) and (ii) together by induction on $|D|$, noting that the conclusions are trivial if $|D| = 1$.

We first use the inductive hypothesis to reduce the situation to a configuration where Theorem B can be applied. Let $F = F(D)$. Suppose firstly that there exists a normal nontrivial subgroup N of D contained in F and with the

property that $F(D/N) = F/N$.

Now PN/N is a Sylow p -subgroup of D/N and we clearly have $m(PN/N) \leq m(P)$ and $d(PN/N) \leq d(P)$. Thus we can apply induction to D/N to deduce that

$$l(D/N) \leq 4m(P) \quad \text{and}$$

$$d(D/N/F(D/N)) \leq 4m(P) + d(P)(l_p(D/N) - 1).$$

But since $F(D/N) = F/N$, and $l_p(D/N) \leq l_p(D)$, we have the desired conclusions. From now on, we assume that there is no such subgroup as N .

In particular, since $F(D/\phi(D)) = F/\phi(D)$ by (I.2.8(ii)), we must have

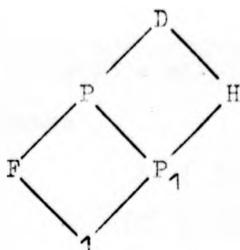
$$\phi(D) = 1. \quad (a)$$

Next put $Q = O_p(F)$. Now Q is certainly a normal subgroup of D contained in F . We wish to show that $F(D/Q) = F/Q$, and to this end we put $F(D/Q) = M/Q$. Since F/Q is nilpotent and normal in D/Q , we clearly have $M \geq F$. Also, by hypothesis,

$$Q \leq Z(D) \cap M \leq Z(M),$$

so $M/Z(M)$ is nilpotent. Thus M is nilpotent; so $M \leq F$, and therefore $M = F$ as required. So now we know that $Q = 1$. Since the group F is nilpotent, it must now be a p -group. From (I.2.8) and (a) it now follows that F is an elementary abelian p -group on which D/F acts faithfully.

By (I.2.4) and (a), the group F has a complement H say, in D . We choose a Sylow p -subgroup P_1 of H . Note that FP_1 is then a Sylow p -subgroup of D , which, without loss of generality, may be taken to be P .



Set $K = O_p(H)$. Roughly speaking, we now apply induction to H/K and Theorem B to the action of $\mathbb{F}_p P_1$ on F to obtain the desired result.

Firstly, since $O_p(H/K) = 1$, we obviously have $O_p(H/K) \leq Z(H/K)$, and since a Sylow p -subgroup of H/K is isomorphic to P_1 we have by induction

$$\left. \begin{aligned} l(H/K) &\leq 4m(P_1), & \text{and} \\ d(H/V/F(H/K)) &\leq 4m(P_1) + d(P_1)(l_p(H/K) - 1) \\ &\leq 4m(P_1) + d(P_1)(l_p(D) - 2). \end{aligned} \right\} \quad (b)$$

(The last inequality holds since $H/K \cong D/O_{p',p,p}(D)$, so that $l_p(H/K) = l_p(D) - 1$.)

Secondly, the $\mathbb{F}_p \mathbb{K} P_1$ -module F satisfies the hypotheses of Theorem B with P_1 in place of P and F in place of V . Thus, using the fact that

$$\text{codim}_{\mathbb{F}_p}([F, P_1]) = m(F/[F, P_1]),$$

we obtain

$$\left. \begin{aligned} l(K) &\leq 3m(F/[F, P_1]), \\ \text{and } d(K) &\leq 4m(F/[F, P_1]). \end{aligned} \right\} \quad (c)$$

Now

$$[F, P_1] = [F, P] \leq [P, P] \leq \mathcal{Z}(P),$$

and $[F, P] \leq P$, so by (I.2.1(ii)), we have

$$m(P) = m(P/[F, P_1]).$$

Since

$$P/[F, P_1] \cong F/[F, P_1] \rtimes P_1,$$

we have

$$m(P) = m(P_1) + m(F/[F, P_1]).$$

Thus (c) becomes

$$\left. \begin{aligned} l(K) &\leq 3m(P) - 3m(P_1), \\ \text{and } d(K) &\leq 4m(P) - 4m(P_1). \end{aligned} \right\} \quad (d)$$

We tackle the final parts of the proofs of (i) and (ii) separately.

$$\begin{aligned} (i) \quad l(D) &= 1 + l(H) \\ &\leq 1 + l(H/K) + l(K) \\ &\leq 1 + 4m(P_1) + 3m(P) - 3m(P_1), \end{aligned}$$

from (b) and (d). Hence

$$l(D) \leq 4m(P) + m(P_1) - m(P) + 1.$$

Finally, we note that since $D \neq 1$, we have $F \neq 1$, and so, since F and P_1 are p -groups, we have $F/[F, P_1] \neq 1$. Thus $m(P) - m(P_1) = m(F/[F, P_1]) \geq 1$. Therefore $l(D) \leq 4m(P)$ and we are finished.

$$\begin{aligned} (ii) \quad d(D/F) &= d(H) \\ &\leq d(H/K/F(H/K)) + d(F(H/K)) + d(K) \\ &\leq 4m(P_1) + d(P_1)(l_p(D) - 2) + d(F(H/K)) \\ &\quad + 4m(P) - 4m(P_1), \end{aligned}$$

using (b) and (d). Now, since $d(P_1) \leq d(P)$, we have

$$d(D/F) \leq 4m(P) + d(P)(l_p(D) - 1) + d(F(H/K)) - d(P).$$

Finally, since $K = O_p(H)$, the group $F(H/K)$ is a p -group and so $d(P) \geq d(F(H/K))$ and the result follows.

This completes the proof of (I.5.7).

Proof of Theorem C

(i) For each prime p dividing $|G|$, we apply (I.5.7(i)) with $D = G/O_p(G)$ to conclude that

$$l(G/O_p(G)) \leq 4m_1.$$

Then, using (I.3.2(ii)) and the fact that the intersection of all the groups $O_p(G)$ is trivial, we have $l(G) \leq 4m_1$ as required.

(iii) For each prime p dividing $|G|$, we apply (I.5.7(ii)) with $D = G/O_p(G)$ to conclude that

$$d[G/O_p(G)/F(G/O_p(G))] \leq 4m_1 + (l_p(G) - 1)d_1.$$

Since $F(G/O_p(G))$ is a p -group, we have $d(F(G/O_p(G))) \leq d_1$, and by (I.5.4) we have $l_p(G) \leq d_1$. Thus

$$\begin{aligned} d(G/O_p(G)) &\leq 4m_1 + l_p(G)d_1 - d_1 + d_1 \\ &\leq 4m_1 + d_1^2, \end{aligned}$$

and then, as in (i), this implies that $d(G) \leq 4m_1 + d_1^2$, as required.

The proofs of (ii) and (iv) are a little more complex. We begin their proofs together.

Let p be a prime dividing the order of G . Let F_p be the Hall p' -subgroup of $F(G)$ and let $F_p = O_p(G)$ (so that $F(G) = F_p \times F_p$). Define C_p and D_p by $C_p = C_G(F_p)$ and $D_p = C_G(F_p)$. Note that since F_p and F_p are normal in G , so are C_p and D_p .

Now let S_p be a Sylow p -subgroup of D_p . By (I.4.7(i)) the group S_p is the Sylow p -subgroup of some nilpotent injector of G , which we can take to be E . Since F_p is a normal p -subgroup of D_p , we have $F_p \leq S_p$. Since E is

nilpotent, $E = S_p \times H_p$, where H_p is a Hall p' -subgroup of E . Therefore H_p centralises F_p and so $H_p \leq C_p$. But we also have $S_p \leq D_p$, so that $E = S_p \times H_p \leq D_p C_p \leq G$. By (I.4.8), therefore,

$$G = N_G(E)C_p D_p. \quad (a)$$

Since D_p is normal in G , we have $F(D_p) \leq F(G)$, and so

$$C_p, (F(D_p)) \leq F_p \cap D_p \leq Z(D_p).$$

Thus we can apply (I.5.7) with D_p in place of D , and S_p in place of P , noting that $m(S_p) \leq m$ and $d(S_p) \leq d$, and also that $l_p(D_p) \leq d(S_p) \leq d$ by (I.5.4), to obtain

$$\left. \begin{aligned} l(D_p) &\leq 4m, \quad \text{and} \\ d(D_p/F(D_p)) &\leq 4m + (d-1)d. \end{aligned} \right\} \quad (b)$$

Next, since E is normal in $N_G(E)$ and E is \underline{N} -maximal in $N_G(E)$ by (I.4.6), we must have $E = F(N_G(E))$ and therefore we may apply (I.5.6(ii),(iv)) to obtain

$$\left. \begin{aligned} l(N_G(E)) &\leq 2 + m, \\ \text{and } d(N_G(E)/F) &\leq 2 + m. \end{aligned} \right\} \quad (c)$$

We complete the proofs of (ii) and (iv) separately.

(ii) From (a),

$$G/C_p = N_G(E)D_p/N_G(E)D_p \cap C_p,$$

so

$$\begin{aligned} l(G/C_p) &\leq l(N_G(E)D_p) \\ &\leq l(N_G(E)) + l(D_p) \\ &\leq 2 + m + 4m = 5m + 2, \end{aligned}$$

using (b) and (c). Now, since

$$\bigcap_p C_p \leq C_G(F(G)) \leq F(G)$$

we have $l(G/F(G)) \leq 5m + 2$ by (I.3.2(ii)) and so

$l(G) \leq 5m + 3$, as required.

(iv) From (a)

$$\begin{aligned} d(G/C_p F) &= d(C_p D_p N_G(E)/C_p F) \\ &\leq d(C_p D_p N_G(E)/C_p D_p F) + d(C_p D_p F/C_p F) \\ &\leq d(N_G(E)) + d(D_p/D_p \cap C_p F) \\ &\leq d(N_G(E)/F) + d(E) + d(D_p/F(D_p)) \\ &\leq 2 + m + d + 4m + d^2 - d \end{aligned}$$

using (b) and (c). Thus, as in (ii), we obtain

$$d(G/F) \leq 5m + 2 + d^2,$$

and since $F \leq E$, we have $d(F) \leq d$, and so $d(G) \leq 5m + 2 + d + d^2$, as required.

This completes the proof of Theorem C.

We conclude this section with an example which shows that, in the notation of Theorem C, we may have $l(G) = 2m$. (Recall that Theorem C (ii) gives the bound $l(G) \leq 5m + 3$.)

(I.5.8) EXAMPLE. Let S denote the symmetric group on $\{1, 2, 3\}$. If H is any group, we can define an action of S on $H \times H \times H$ by $(h_1, h_2, h_3)^s = (h_{1s}, h_{2s}, h_{3s})$, where $h_i \in H$ and $s \in S$. We will denote the semi-direct product $(H \times H \times H)S$ by $H \wr S$. (Note that this is not the regular wreath product which we normally intend by the symbol \wr .) If H is soluble, it is easy to check that if $O^3(H) = H$, $l(H \wr S) = l(H) + l(S) = l(H) + 2$.

Now define G_1 by $G_1 = S$, and for $i > 1$, define G_i

inductively by $G_i = G_{i-1} \sim S$. Let m be any positive integer, and put $G = G_m$. Clearly we have $l(G) = 2m$.

It can be shown that a nilpotent injector of G is a Sylow 3-subgroup of G , which is in fact the successive (regular) wreath product of m copies of Z_3 . That is, if we put $C = Z_3$, and define C_i for $i > 1$ by $C_i = C_{i-1} \sim Z_3$, then a nilpotent injector E of G is isomorphic to C_m . It is easily shown by induction that C_m requires exactly m generators. Thus $n(E) = m$.

It seems reasonable to make the conjecture that $l(G) \leq 2m$ always.

I know of no comparable examples for the other parts of Theorem C. Note that in the above example, a Sylow 2-subgroup of G requires $2^m - 1$ generators, giving a much smaller value of $l(G)$ in terms of m than Theorem C(i).

CHAPTER II

STANDARD RESULTS AND METHODS

In this chapter and the next we prepare the ground for the proofs of Theorems A and B. The aims of this chapter are twofold. Firstly, we assemble the standard results that we will need, modified here and there to the uses to which we will put them. (Sections 1-3.) Then, in Section 4 we give an account of a general method of proof of results about the representation theory of soluble groups, and we discuss how it applies in our case.

II.1. GROUP ACTIONS

Throughout this section, G and A will be groups with A acting on G . The notation and conventions that we use here are explained in (I.1).

Our first result is a consequence of the Schur-Zassenhaus theorem [17, I.18.1, I.18.2]. We use it to derive most of the results of this section.

(II.1.1) Let H be an A -invariant subgroup of G and suppose that A and H have coprime orders. Let $g \in G$ and assume that $Hg^a = Hg$ for all $a \in A$. Then there exists x in G such that $Hg = Hx$ and $x^a = x$ for all $a \in A$. (I.e., each coset of H that is fixed by A contains an element that is fixed by A .)

Proof [17, I.18.6].

(II.1.2) DEFINITION. Let

$$1 = G_0 \leq G_1 \leq \dots \leq G_n = G$$

be a normal series for G . We say that A stabilises this series if each G_i is A -invariant and if A acts trivially on each G_i/G_{i-1} ($1 \leq i \leq n$).

(II.1.3) Suppose that A and G have coprime orders, and that A stabilises some normal series of G . Then A centralises G .

Proof Suppose that A stabilises the series

$$1 = G_0 \leq G_1 \leq \dots \leq G_n = G.$$

We proceed by induction on n . For $n = 1$, the result is trivial, so we assume that $n \geq 2$. Now A stabilises the normal series

$$1 = G_1/G_1 \leq G_2/G_1 \leq \dots \leq G_n/G_1 = G/G_1$$

of G/G_1 , and therefore A centralises G/G_1 by induction. Of course, A also centralises G_1 .

Now let $g \in G$ and apply (II.1.1) with G_1 in place of H . This gives us an element $x \in G$ such that $x^a = x$ for all $a \in A$, and such that $G_1 x = G_1 g$, i.e., $g x^{-1} \in G_1$. Therefore, if $a \in A$, we have

$$g^a = g^a (x^{-1})^a x = (g x^{-1})^a x = g x^{-1} x = g,$$

and the proof is complete.

Next, we have two easy consequences of (II.1.3).

(II.1.4) If A and G have coprime orders, then

$$[G, A] = [G, A, A].$$

Proof We set $B = [G, A, A]$, and note that $B \leq [G, A]$ trivially. Since $[G, A] g^a = [G, A] g$ for all $g \in G$, $a \in A$, it follows from (II.1.1) that $G = [G, A] C_G(A)$. Similarly, $[G, A] = B C_{[G, A]}(A)$, whence $G = B C_G(A)$. Now let $g \in G$, $a \in A$, and write $g = bc$ with $b \in B$ and $c \in C_G(A)$. Then $g^a g^{-1} = b^a c^a c^{-1} b^{-1} = b^a b^{-1} \in B$, and so $[G, A] \leq B$.

(II.1.5) Assume that A and G have coprime orders. Let N be a normal, A -invariant subgroup of G which is centralised by A , and such that $C_G(N) \leq N$. Then A centralises G .

Proof Let $g \in G$ and $a \in A$. Then, for all $n \in N$ we have

$$n^{g^a} = (n^a)^{g^a} = n^{g^a} = (n^g)^a = n^g,$$

since $n^g \in N$. Therefore $g^{-1}g^a \in C_G(N) \leq N$, whence $Ng = Ng^a$.

Thus A stabilises $1 \leq N \leq G$, and the result follows from (II.1.3).

(II.1.6) Suppose that A and G have coprime orders. Then for each prime p dividing $|G|$, there exists an A -invariant Sylow p -subgroup of G .

Proof [11, 6.2.2].

(II.1.7) Suppose that G is a p -group and that A is a p' -group. If A centralises $G/\Phi(G)$, then A centralises G .

Proof [11, 5.1.4].

II.2. p-GROUPS

Throughout this section, p is a prime and P is a p -group.

(II.2.1) DEFINITIONS. (i) P is called special if either P is elementary abelian, or $\Phi(P) = P' = Z(P)$ is elementary abelian.

(ii) P is extraspecial if P is special, nonabelian, and $Z(P)$ has order p .

Since any p -group of order at most p^2 is abelian, an extraspecial group must have order at least p^3 .

(II.2.2) Up to isomorphism, there are exactly two extraspecial groups of order p^3 . If p is odd, one of them has exponent p , and the other has exponent p^2 . If $p=2$, they are the quaternion group and the dihedral group of order 8, both of exponent 4.

Proof [11, 5.5.1].

(II.2.3) DEFINITIONS. Let G_1, \dots, G_n be groups. For each $i \in \{1, \dots, n\}$, let $A_i \leq Z(G_i)$ be a subgroup of G_i , and assume that all the A_i are isomorphic to one another via isomorphisms

$$\theta_i: A_1 \rightarrow A_i .$$

Then we can form the central product of G_1, \dots, G_n with

respect to A_1, \dots, A_n , denoted by $G_1 \times G_2 \times \dots \times G_n$. In order to do this, we identify the natural images of the A_i in $G_1 \times G_2 \times \dots \times G_n$. That is, we set $N = \{a^{-1}(a\theta_i); a \in A_1, 2 \leq i \leq n\}$. Then $N \leq G_1 \times \dots \times G_n$, and $G_1 \times \dots \times G_n = G_1 \times \dots \times G_n / N$.

(II.2.4) Let P be extraspecial. Then P is the central product of t (say) extraspecial groups of order p^3 , where the centres of these t groups are all identified.

In particular, $|P| = p^{2t+1}$ for some natural number t.

Proof [11, 5.5.2].

(II.2.5) Let C be a 2-group of order at least 16 which is either generalised quaternion, dihedral or semi-dihedral.

Then the following hold.

- (i) $Z(C)$ has order 2.
- (ii) $C/Z(C)$ is dihedral.
- (iii) C has a characteristic, cyclic, self-centralising subgroup of index two.
- (iv) C has no characteristic abelian noncyclic subgroups.

Note Definitions of these types of groups are given in [17, I.14.9]. We only need the properties listed above.

Proof (i) and (ii). [11, 5.4.3(ii)(c)].

(iii) By [17, I.14.9(b)], the group C has a cyclic subgroup

respect to A_1, \dots, A_n , denoted by $G_1 \vee G_2 \vee \dots \vee G_n$. In order to do this, we identify the natural images of the A_i in $G_1 \times G_2 \times \dots \times G_n$. That is, we set $N = \{a^{-1}(a\theta_i); a \in A_1, 2 \leq i \leq n\}$. Then $N \trianglelefteq G_1 \times \dots \times G_n$, and $G_1 \vee \dots \vee G_n = G_1 \times \dots \times G_n / N$.

(II.2.4) Let P be extraspecial. Then P is the central product of t (say) extraspecial groups of order p^3 , where the centres of these t groups are all identified.

In particular, $|P| = p^{2t+1}$ for some natural number t.

Proof [11, 5.5.2].

(II.2.5) Let C be a 2-group of order at least 16 which is either generalised quaternion, dihedral or semi-dihedral. Then the following hold.

- (i) $Z(C)$ has order 2.
- (ii) $C/Z(C)$ is dihedral.
- (iii) C has a characteristic, cyclic, self-centralising subgroup of index two.
- (iv) C has no characteristic abelian noncyclic subgroups.

Note Definitions of these types of groups are given in [17, I.14.9]. We only need the properties listed above.

Proof (i) and (ii). [11, 5.4.3(ii)(c)].

(iii) By [17, I.14.9(b)], the group C has a cyclic subgroup

D , say, of index two. We claim that D is self-centralising and characteristic.

Since D is abelian, we have $C_G(D) \triangleright D$. If equality did not hold, we would have $C_G(D) = G$, and thus $D \leq Z(G)$. But this is not the case, by (i). Therefore $C_G(D) = D$.

Since D is maximal, we have $D \triangleright \phi(G)$, so $D \leq C_G(\phi(G))$. By [11, 5.4.3(ii)(b)], the group $\phi(G)$ has index 4, so $|\phi(G)| \geq 4$, whence $\phi(G) \triangleright Z(G)$. Therefore we must have $D = C_G(\phi(G))$, and since $\phi(G)$ is characteristic, so is D .

(iv) [11, 5.4.3(ii)(e),(f),(g)].

We now come to the famous theorem of P. Hall which gives the structure of p -groups all of whose characteristic abelian subgroups are cyclic. The relevance of this result to us is that in the 'homogeneous' case of Theorems A and B, every normal r -subgroup of KP (for any prime r) will have this property.

(II.2.6) (P. Hall) If P is a nontrivial p -group such that every characteristic abelian subgroup is cyclic, then P satisfies the following hypotheses.

(II.2.7) HYPOTHESES. P is the central product $E \times C$, where E is either trivial, or is an extraspecial p -group, and $C \neq 1$.

Further

- (i) if $p > 2$, then E has exponent p , and C is cyclic;
- (ii) if $p = 2$, then C is either cyclic, or has order at least 16, and is generalised quaternion, dihedral, or semi-dihedral;

(iii) the centre of C contains a unique subgroup of order p : it is this subgroup that is identified with $Z(E)$ (when $E \neq 1$).

Proof Everything in this statement is proved in [11, 5.4.9] except that $C \neq 1$. Put since $P \neq 1$, and $E = E \rtimes Z_p$ (with Z_p identified with $Z(E)$), it is clear that we may always take $C \neq 1$.

Note We will deal with the type of p -group given by Hypotheses (II.2.7) in many places in the sequel. Whenever a central product $E \times C$ is defined (with E extraspecial) we will mean that $Z(E)$ is identified with the unique subgroup of order p in $Z(C)$. (The other possibility for $E \times C$ is $E \times C$.)

Also, we make the convention that $C \neq 1$ whenever $P \neq 1$. This is merely a notational convenience to ensure that $Z(P) = Z(C)$ always.

It is a corollary of (II.2.6) that a p -group which has all normal abelian subgroups cyclic satisfies (II.2.7) with $E = 1$. We need a slight generalisation of this.

(II.2.8) Let $P_1 \cong P_2$ be p -groups. Assume that every normal abelian subgroup of P_2 which is contained in P_1 is cyclic. Then P_1 is either cyclic, or $p=2$, and P_1 is generalised quaternion, dihedral, or semi-dihedral of order at least 16.

Proof [1, 2.2].

The remainder of the work in this section is aimed at finding bounds for the automorphism group of a p -group satisfying Hypotheses (II.2.7).

(II.2.9) DEFINITIONS. Let m be an integer and let \mathbb{F} be a field. Let V be a vector space of dimension m over \mathbb{F} .

(i) A symplectic form on V is a bilinear map $(,)$ from $V \times V$ into \mathbb{F} satisfying

$$(v,v) = 0 \text{ for all } v \in V.$$

(ii) We say that $(,)$ is nonsingular if whenever $(u,v) = 0$ for all $u \in V$, we have $v = 0$.

(iii) If V is endowed with a nonsingular symplectic form then by [17, II.9.6(b)], the integer m is even, say $m = 2n$. We denote by

$$Sp(2n, \mathbb{F})$$

the group of all automorphisms of V leaving $(,)$ invariant. That is,

$$Sp(2n, \mathbb{F}) = \{ \theta \in GL(2n, \mathbb{F}); (v\theta, w\theta) = (v,w) \text{ for all } v, w \in V \}.$$

(II.2.10) Let \mathbb{F} be a finite field of order q . Then

$$|Sp(2n, \mathbb{F})| = q^{n^2} (q^{2n} - 1)(q^{2n-2} - 1) \dots (q^2 - 1).$$

Proof [17, II.9.13(b)].

(II.2.11) Let $P = EYC$ be a p -group satisfying Hypotheses (II.2.7) with C cyclic. Then the following hold.

(i) $|P'| = p$.

(ii) $\bar{P} = P/Z(P) = P/C$ can be regarded as a nonsingular symplectic vector space over \mathbb{F}_p with form given by

$$(Px, Py) = [x, y] \quad (x, y \in P)$$

where P' is identified with \mathbb{F}_p^τ .

(iii) If A is a group acting on P and centralising C , then A leaves invariant the form defined in (ii).

(iv) If A is as in (iii) and $|\bar{P}| = p^{2t}$, then

$$|A/C_A(P)| \mid p^{t^2} (p^{2t} - 1)(p^{2t-1} - 1) \dots (p^2 - 1).$$

Proof (i) and (ii). [12, III.13.7(a), (b)].

(iii) Clear since $P' \leq C$.

(iv) Follows from (iii) and (II.2.10).

II.3. REPRESENTATION THEORY

(II.3.1) DEFINITION. Let \mathbb{F} be a field and let G be a group. Let V be a completely reducible $\mathbb{F}G$ -module. Choose representatives W_1, \dots, W_s for each of the isomorphism classes of irreducible $\mathbb{F}G$ -submodules of V . Then define V_i to be the sum of all submodules of V which are isomorphic to W_i . As V is completely reducible, each V_i is in fact a direct sum of submodules isomorphic to W_i . Further,

$$V = V_1 \oplus \dots \oplus V_s.$$

We call the V_i the homogeneous components of V . If $s = 1$, so that V is a direct sum of pairwise isomorphic irreducible submodules, then V is homogeneous.

We now state the first main theorem of Clifford theory.

(II.3.2) (Clifford) Let \mathbb{F} be a field and let G be a group. Let V be an irreducible $\mathbb{F}G$ -module. Suppose that $N \trianglelefteq G$.

(i) V_N is completely reducible, so that

$V_N = V_1 \oplus \dots \oplus V_s$ where the V_i are the homogeneous components of V_N .

(ii) The submodules V_1, \dots, V_s are transitively permuted by G via the action $V_i \mapsto V_i g$ ($g \in G$). The kernel of this action contains $NC_G(N)$.

(iii) Put $S_i = \{g \in G; V_i g = V_i\}$. Then $V = (V_i)_{S_i}^G$.

Proof [17, V.17.3].

Theorem (II.3.2) is of fundamental importance in the theory of representations of groups and we shall use it repeatedly. It is so well-known that we shall refer to it as "Clifford's theorem" rather than by a number.

(II.3.3) DEFINITIONS. Let A and B be subgroups of a group G . A double coset of A and B in G is a set of the form

$$AgB = \{agb; a \in A, b \in B\},$$

where $g \in G$. It is easy to show that two double cosets AgB and AhB are either identical or disjoint. (See [17, I.2.191].) Thus we can write

$$G = \bigcup_{1 \leq i \leq n} Ag_iB$$

for suitable g_1, \dots, g_n in G , where the double cosets Ag_1B, \dots, Ag_nB are all distinct (and therefore disjoint). We call this a double coset decomposition of G with respect to A and B , and we call g_1, \dots, g_n a set of double coset representatives of A and B in G .

(II.3.4) (Mackey's theorem.) Let A and B be subgroups of the group G . Suppose that U is a $\mathbb{F}A$ -module and put $V = U|_G$. Then

$$V_B = (Ug_1)_{A \cap B} \Big|_B^R \oplus \dots \oplus (Ug_n)_{A \cap B} \Big|_B^B,$$

where g_1, \dots, g_n is any set of double coset representatives for A and B in G .

Proof [17, V.16.9].

We now turn to some more specific results of use to us. Our main aim in the rest of this section is to find information on the dimensions of faithful representations for groups over finite fields, especially for groups which satisfy the Hyptheses (II.2.7).

(II.3.5) Let $P = E \rtimes C$ satisfy Hypotheses (II.2.7) with C cyclic. Let F be a field of characteristic not equal to p , and suppose that F contains a primitive $|C|^{th}$ root of unity.

- (i) F is a splitting field for P .
- (ii) The dimension of any faithful, irreducible FP -module is p^t , where $|P/C| = p^{2t}$.

Proof (i) If $|C| > p$, then the exponent of P is $|C|$, and we have the result by [18, 9.15].

Assume, therefore, that $|C| = p$, so that $P = E$. Now it is well-known that the character values of E are all p^{th} roots of unity. (See [17, V.16.14].) Thus, by [18, 9.9] and [18, 9.14], we have the result.

(ii) It is well-known [17, V.16.1] that the dimension of an absolutely irreducible, faithful representation for E has dimension p^t . From (i), therefore, the dimension of a faithful, irreducible FE -module is p^t . Clearly the dimension of a faithful, irreducible FC -module is 1. The required result now follows from [11, 2.7.1 and 2.7.2].

We are interested in the dimension of a faithful,

irreducible representation of P over a field which may not contain a primitive $|C|^{th}$ root of unity. The next few results deal with this problem.

(II.3.6) Let \mathbb{F} be a finite field of order q , let A be an abelian group, and suppose that V is a faithful, irreducible $\mathbb{F}A$ -module. Then A is cyclic and the dimension of V is f where f is the smallest integer such that $|A| \mid q^f - 1$.

Proof [17, II.3.10].

(II.3.7) HYPOTHESES. Let \mathbb{F} be a finite field of order q , let G be a group, and suppose that V is a faithful, irreducible $\mathbb{F}G$ -module. Suppose that A is a normal, abelian subgroup of G and that V_A is homogeneous.

We let f be the dimension of an irreducible $\mathbb{F}A$ -submodule of V , and let h be the number of irreducible summands in V_A , so that $\dim_{\mathbb{F}}(V) = fh$.

We can regard V as a vector space of dimension h over the field \mathbb{E} of q^f elements. We denote this vector space by V' to distinguish it from V .

Our next result tells us what the action of G on V' looks like.

(II.3.8) Assume Hypotheses (II.3.7). Then

$$(v' + w')g = v'g + w'g$$

$$\text{and } (\lambda v')g = (\lambda \theta_g)v'g$$

where $g \in G$, $v', w' \in V'$, and $\lambda \in \mathbb{E}$; and θ_g is a field automorphism of \mathbb{E} over \mathbb{F} . Further, if $\theta: G \rightarrow \text{Gal}(\mathbb{E}: \mathbb{F})$ is the map taking g to θ_g , then θ is a group homomorphism with kernel $C_G(A)$.

Proof [17, II.3.11].

This result has two consequences of importance to us which we now state. The first will not be used until the next chapter.

(II.3.9) Assume Hypotheses (II.3.7). Then

$$|G/C_G(A)| \mid f.$$

Proof Any finite extension of finite fields is Galois, so $|\text{Gal}(\mathbb{E}: \mathbb{F})| = |\mathbb{E}: \mathbb{F}| = f$, and the result follows from (II.3.8).

The second corollary to (II.3.8) allows us to regard any irreducible representation over a finite field as an absolutely irreducible representation over a suitable field extension.

(II.3.10) Let \mathbb{F} be a finite field and let H be a group.

Let V be a faithful, irreducible $\mathbb{F}H$ -module. Put

$$K = \text{Hom}_{\mathbb{F}H}(V, V).$$

- (i) K is a field.
- (ii) V may be regarded as a faithful, absolutely irreducible \mathbb{H} -module V' (where the two actions of \mathbb{H} on V are identical when V is regarded simply as a set.)

Proof (i) By Schur's lemma, K is a division ring. It is also obvious that K is finite. Thus by Wedderburn's theorem on finite division rings, K is in fact a field.

(ii) Let $A = K^\times$. Then A is cyclic, and by definition of K , the group A centralises \mathbb{H} . Thus $G = \mathbb{H}A$ is a group, and it is clear that G acts on V as a group of linear maps (over \mathbb{F}). Since A is abelian and centralises \mathbb{H} , we have $A \leq Z(G)$, and so $G = C_G(A)$. Now by Clifford's theorem V_A is homogeneous. We thus have the Hypotheses (II.3.7) and so applying (II.3.8), we know that V may be regarded as a $\mathbb{E}G$ -module V' (using again the fact that $G = C_G(A)$), where \mathbb{E} is the field of q^f elements. By (II.3.6), we know f is the smallest positive integer such that $|A| \mid q^f - 1$. Since $|A| = |K| - 1$, we must have $K \cong \mathbb{E}$.

To complete the proof, therefore, we only need to note that V' is an \mathbb{H} -module by restriction to \mathbb{H} , and that V' is absolutely irreducible by [17, V.11.10].

Note The module V' in (II.3.10(ii)) should not be confused with $V \otimes_K \mathbb{E}$.

Finally, we have the promised extension to (II.3.5) for arbitrary finite fields.

(II.3.11) Let P satisfy Hypotheses (II.2.7) with C cyclic.

Let \mathbb{F} be a finite field of order q where $p \nmid q$, and let V be a faithful, irreducible $\mathbb{F}P$ -module.

Define integers s and f by putting $s^2 = |P/C|$ and letting f be the smallest integer such that $|C| \mid q^f - 1$. Then

(i) $|\text{Hom}_{\mathbb{F}P}(V, V)| = q^f$;

(ii) $\dim_{\mathbb{F}}(V) = fs$.

Proof $C = Z(P)$, so we have Hypotheses (II.3.7) with $P = G$ and $C = A$. Using (II.3.8) and (II.3.6), therefore, V may be regarded as an $\mathbb{F}P$ -module where \mathbb{E} has q^f elements. Since $|C| \mid q^f - 1$, the field \mathbb{E} has a primitive $|C|$ th root of unity. Thus $\dim_{\mathbb{F}}(V) = s$ by (II.3.5). This proves (ii).

Since by (II.3.10), V may also be regarded as an absolutely irreducible module for P over $\text{Hom}_{\mathbb{F}P}(V, V)$ (necessarily of dimension s), we must have $|\text{Hom}_{\mathbb{F}P}(V, V)| = q^f$, proving (i).

II.4. THE METHOD OF PROOF OF THEOREMS A AND B

This section is a discussion of a general (and well-known) method of proof of results about the representation theory of soluble groups, and how it applies in our case. We fix the following notation. G is a soluble group, F is a field, and V is an irreducible FG -module. We assume that we wish to prove something about V - call it (*) for now - which we know by an inductive hypothesis to be true for all 'smaller' modules. (The exact meaning of 'smaller' depends on the inductive hypothesis; we just assume here that the inductive step works.) Now Clifford's theorem gives us two possibilities:

- (1) $V = W_S \uparrow^G$ for some $S < G$ and submodule W of V_S ; or
- (2) V_N is homogeneous whenever $N \triangleleft G$.

For obvious reasons, we call (1) 'the induced case', and (2) 'the homogeneous case'. The rest of this section is planned as follows. We consider (1) first and then (2). In each case we discuss the general situation first, i.e., we show how one might go about proving (*), and then specialize to the proofs of Theorems A and B.

(1) The Induced Case.

To tackle (1), we need some information on so-called primitive groups.

(II.4.1) DEFINITIONS. (i) Let $M \leq G$. Then we define the core of M in G , denoted by $\text{Core}_G(M)$, to be the intersection of all conjugates of M in G . Clearly $\text{Core}_G(M)$

II.4. THE METHOD OF PROOF OF THEOREMS A AND B

This section is a discussion of a general (and well-known) method of proof of results about the representation theory of soluble groups, and how it applies in our case. We fix the following notation. G is a soluble group, F is a field, and V is an irreducible FG -module. We assume that we wish to prove something about V - call it (*) for now - which we know by an inductive hypothesis to be true for all 'smaller' modules. (The exact meaning of 'smaller' depends on the inductive hypothesis; we just assume here that the inductive step works.) Now Clifford's theorem gives us two possibilities:

- (1) $V = W_S \uparrow^G$ for some $S < G$ and submodule W of V_S ; or
- (2) V_N is homogeneous whenever $N \triangleleft G$.

For obvious reasons, we call (1) 'the induced case', and (2) 'the homogeneous case'. The rest of this section is planned as follows. We consider (1) first and then (2). In each case we discuss the general situation first, i.e., we show how one might go about proving (*), and then specialize to the proofs of Theorems A and B.

(1) The Induced Case.

To tackle (1), we need some information on so-called primitive groups.

(II.4.1) DEFINITIONS. (i) Let $M \leq G$. Then we define the core of M in G , denoted by $\text{Core}_G(M)$, to be the intersection of all conjugates of M in G . Clearly $\text{Core}_G(M)$

is normal in G , and is in fact the largest normal subgroup of G contained in M .

(ii) A group G is called primitive if there exists a maximal subgroup M of G such that $\text{Core}_G(M) = 1$.

(II.4.2) Let G be a soluble group and let M be a maximal subgroup of G , and set $T = \text{Core}_G(M)$. Note that G/T is primitive. Then G/T has a unique normal minimal subgroup S/T say, and further,

(i) $G = MS$ and $M \cap S = T$, i.e., M complements S/T in G ;

(ii) $C_G(S/T) = S$.

Proof Let S/T be a minimal normal subgroup of G/T .

We show (i), then (ii); then that S/T is unique.

Since T is the largest normal subgroup of G contained in M , we must have $S \not\leq M$, and so $G = MS$ since M is maximal. Now $M \cap S$ is normalised by M and S , and so $M \cap S \leq G$; thus $M \cap S = T$.

Put $C_G(S/T) = C$. Clearly $C \triangleright S$ since S/T is abelian. Now $C \cap M$ is normalised by M and S , so $C \cap M \leq G$, and $C \cap M = T$. But now

$$C = C \cap MS = (C \cap M)S = T \cap S = S,$$

and so $C_G(S/T) = S$.

Finally, note that if S_1/T is another minimal normal subgroup of G/T , then $[S, S_1] \leq S \cap S_1 = T$, so $S_1 \leq C = S$. Thus S/T is the unique minimal normal subgroup of G/T .

Now suppose that $V = W_S |^G$ and choose a maximal subgroup M containing S . Then by the transitivity of

induction $V = W_S |^M |^G$, and putting $U = W |^M$, we have $V = U |^G$.

We note that U is irreducible as an M -module, since if $0 < U_1 < U_M$, then $0 < U_1 |^G < V_G$, contradicting the irreducibility of V_G . We can thus apply the inductive hypothesis to conclude that (*) holds for the FM -module U .

Secondly, we deduce from (II.4.2) that, in the notation of that result, S/T is an irreducible $\mathbb{F}_s G$ -module where s is the prime dividing $|S/T|$. Unfortunately, the field has changed. This is the source of two main problems. Firstly, \mathbb{F} may have been, for example, a splitting field for G ; this is unlikely to be true of \mathbb{F}_s . However, since in both Theorem A and Theorem B, we make no such assumption on \mathbb{F} , this problem does not concern us and so we just ignore it. Secondly, one may want some restriction on the characteristic of \mathbb{F} which no longer holds for \mathbb{F}_s . This problem does not occur in the proof of Theorem A, but it stops us applying this argument in Theorem B.

At any rate, if things work nicely, we know that (*) holds for the G -module S/T and for the M -module U : what this tells us about V , of course, depends on (*). It is time to be more specific.

Let us now assume that we are proving Theorem A. We have $G = KP$, where K is a normal p' -group and P is a p -group. There are two possibilities: $s=p$ and $s \neq p$. The case $s=p$ succumbs to an easy inductive argument in Step 1 of the proof and we will not go into details here. Assume, therefore, that $s \neq p$. Here it will be shown that we can assume that $M \triangleright P$, so that $M = (K \cap M)P$. Let $P^* = C_P(S/T)$ and $j = d(K/C_K(S/T))$. Regarding S/T as an $\mathbb{F}_s KP$ -module

and applying induction gives us

$$|P/P^*|^{2w(j)} \leq |S/T| \quad \text{or } j \leq 2, \quad (a)$$

where $w(3) = 3$ and $w(j) = 4 \cdot 3^{j-4}$ for $j > 4$.

It will then be shown that P^* acts faithfully on U , and that $K \cap M$ induces on U a group of derived length at least $d-1-j$, where $d = d(K)$. We thus obtain

$$|P^*|^{2w(d-1-j)} \leq |U| \quad \text{or } d-1-j \leq 2. \quad (b)$$

Also, since $V = U_M \Big|_M^G$ and $|G:M| = |S/T|$ by (II.4.2(i)) we have

$$|V| = |U| |S/T|. \quad (c)$$

If $j > 2$ and $d-j-1 > 2$, then the required bound follows easily from (a), (b) and (c). If either $j \leq 2$ or $d-j-1 \leq 2$, we need a replacement for the straightforward induction argument. The necessary results are contained in the next chapter. In particular, (III.3.6) will be used instead of (b), and (III.1.7) will be used in place of (a).

Let us now turn our attention briefly to Theorem B. For the sake of simplicity we consider B(ii) only - the derived length case. (The proof of B(i) is very similar.) Again we adopt the notation of (II.4.2) and confine our attention to the case $s \neq p$. Remember that we are trying to prove that

$$\text{codim}([V, P]) \geq 3^{j(d-4)}.$$

With $j = d(K/G_K(S/T))$ as before, we find that

$$\text{codim}([U, P]) \geq 3^{j(d-1-j-4)}.$$

We do not go into details here, but it turns out that what we need to know about the KP -module S/T is that the

number of orbits of P on the vectors of S/T increases with j . This information is supplied by (III.4.6).

(2) The Homogeneous Case.

This case is normally trickier than the induced case, and less progress can be made in the general situation.

Let A be a normal abelian subgroup of G . Then V_A is homogeneous, and using (II.3.6) we find that A is cyclic.

Now let r be any prime dividing the order of G , and suppose that A is a characteristic abelian subgroup of $O_r(G)$. Then $A \neq G$, and so by the above, A is cyclic. Thus each $O_r(G)$ satisfies the hypotheses of (II.2.6) and so we deduce that $O_r(G)$ satisfies Hypotheses (II.2.7) (with r in place of p).

Recall that $C_G(F(G)) = Z(F(G))$ by (I.2.7), so that 'most' of G acts faithfully on $F(G)$. Further, since $F(G)$ is the direct product of the $O_r(G)$, we know what $F(G)$ looks like. Often, one can find a chief factor (or factors) of G lying below $F(G)$ to which an inductive argument can be applied. Similar remarks apply to the change of field as in (1). Again, this is not a problem in Theorem A. It is at this point in the proof of Theorem B, however, that we need Theorem A.

In our case, the required chief factor is supplied by (III.2.5). This gives us a normal subgroup R of KP , contained in $O_r(K)$ for some prime r , with the following properties.

(i) R is either extraspecial, or $r=2$, and P is the central product of an extraspecial 2-group and a cyclic group of order 4.

(ii) $\bar{R} = R/Z(R)$ is a chief factor of KP .

(iii) $d(K/C_K(\bar{R})) \geq d-2$.

We set $|\bar{R}| = s^2$.

Suppose that we are proving Theorem A. When $d \geq 5$, we can apply induction to the $\mathbb{F}_r KP$ -module \bar{R} to obtain

$$|P/C_P(\bar{R})|^{2w(d-2)} \leq |\bar{R}| = s^2. \quad (d)$$

Of course, we want to show that $|P|^{2w(d)} \leq |V|$. Now by (II.3.11) we know that the dimension of V is at least s , and so $|V|$ increases rapidly with s . Using (d) therefore, it follows that $|P/C_P(\bar{R})|^{2w(d)}$ is very small compared to $|V|$ for large values of s .

To find a bound for the 'rest' of $|P|$, i.e., $|C_P(\bar{R})|$, we first show that $C_P(\bar{R}) = C_P(R)$, and then look at V considered as a $C_P(R) \times R$ -module. Results (III.3.5) and (III.3.1) of the next chapter will then imply that

$$|C_P(R)| \leq \frac{1}{2}|V|^{3/2s} \quad (e)$$

(with better bounds in particular cases.) Again, for large s , this gives an excellent bound. In fact, s does not have to be very large: if $s \geq 5$, the required bound for $|P|^{2w(d)}$ follows from (d) and (e). For small values of s , several results from (III.3) provide a more accurate replacement for (d).

When $d \leq 4$, we can no longer apply induction to \bar{R} , but K acts nontrivially on \bar{R} , so we can still find a bound for $|P/C_P(\bar{R})|$ in terms of s , using (III.3.6), which allows us to eliminate large values of s . (In fact

$s \geq 16$.) For smaller values we consider various possibilities for p , q , and s , and using the fact that they are mutually coprime, and that V acts nontrivially on \bar{F} , we obtain more careful replacements for (e) and (d).

Finally, we turn to the homogeneous case of Theorem B, and as before we confine our attention to B(ii). The key lemma is (III.4.2):

Lemma Let P^* be a p -group and F a field of characteristic p , and suppose that V^* is an FP -module. Then

$$\text{codim}([V^*, P^*]) \geq \dim(V^*)/|P^*|. \quad (f)$$

Now applying Theorem A to the KP -module \bar{F} gives us

$$|P/C_p(\bar{F})|^{2w(d-2)} \leq |\bar{F}| \leq s^2$$

for $d \geq 5$, as in the proof of Theorem A (where the bound is obtained by induction). Thus

$$|P/C_p(\bar{F})| \sqrt{w(d-2)} \leq s. \quad (g)$$

We then find a suitable FP -composition factor V^* of V , and using (f) with $P^* = P/C_p(\bar{F})$, together with the fact that $\dim(V^*) \geq s$, we can then deduce the required bound for $\text{codim}[V, P]$ from (g).

$s \geq 16$.) For smaller values we consider various possibilities for p , q , and s , and using the fact that they are mutually coprime, and that K acts nontrivially on \bar{F} , we obtain more careful replacements for (e) and (d).

Finally, we turn to the homogeneous case of Theorem B, and as before we confine our attention to B(ii). The key lemma is (III.4.2):

Lemma Let P^* be a p -group and F a field of characteristic p , and suppose that V^* is an FP -module. Then

$$\text{codim}([V^*, P^*]) \geq \dim(V^*)/|P^*|. \quad (f)$$

Now applying Theorem A to the KP -module \bar{F} gives us

$$|P/C_p(\bar{F})|^{2w(d-2)} \leq |\bar{F}| \leq s^2$$

for $d \geq 5$, as in the proof of Theorem A (where the bound is obtained by induction). Thus

$$|P/C_p(\bar{F})| \sqrt{w(d-2)} \leq s. \quad (g)$$

We then find a suitable FP -composition factor V^* of V , and using (f) with $P^* = P/C_p(\bar{F})$, together with the fact that $\dim(V^*) \geq s$, we can then deduce the required bound for $\text{codim}[V, P]$ from (g).

CHAPTER III

PREPARATIONS FOR THEOREMS A AND B

This chapter contains a large number of lemmas that we need for the proofs of Theorems A and B.

The work necessary for Theorem A is contained in the first three sections. The most important results are (III.2.5) and (III.3.6). The last section contains results specifically for Theorem B.

III.1. ARITHMETIC

At dozens of points during the proof of Theorem A and elsewhere, we will require an estimate for a monomial expression of the form x^b in terms of an exponential expression such as c^x . The following result is designed to deal with these situations.

(III.1.1) Let $b, c,$ and x_0 be positive real numbers with c at least one. Define a function $f: \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = x^b/c^x$.

Suppose that $x_0 \geq 3$ and $f(x_0) \leq 1$. Then $f(x) \leq f(x_0)$ for all $x \geq x_0$.

Proof We let e be the base of natural logarithms and put $\log = \log_e$. Assume that $x \geq x_0$. We have

$$f(x) = e^{b \log(x) - x \log(c)}.$$

We aim to show that $f'(x) \leq 0$ for $x \geq x_0$. Now

$$f'(x) = (b/x - \log(c))f(x) = (b - x \log(c))(f(x)/x),$$

and since x and $f(x)$ are both positive, it suffices to show that $b - x \log(c) \leq 0$. But

$$b - x \log(c) \leq b \log(x_0) - x_0 \log(c)$$

since $\log(x_0) \geq \log(3) > 1$, and because $x \geq x_0$ and $\log(c) \geq 0$. So

$$b - x \log(c) \leq \log(f(x_0)) \leq 0$$

since $f(x_0) \leq 1$. Thus $f(x)$ is decreasing for $x \geq x_0$ and the result follows.

The next result, a corollary of the last, is useful in similar situations when we do not know that $x \geq 3$.

(III.1.2) Let x be an integer. Then $x \leq 3^{3^x}$.

Proof We apply (III.1.1) with $b = 1$, $c = 3^3$, and $x_0 = 3$, to deduce the result when $x \geq 3$. The remaining cases, $x = 1$ and $x = 2$, follow immediately from the fact that $3^3 > 2^2$.

Next, we state without proof an elementary fact from number theory.

(III.1.3) Let p and q be primes, and suppose that d and j are natural numbers such that $p^j = q^d - 1$. Then either

- (i) $q = 2$ and $j = 1$, or
- (ii) $p = 2$ and $d = 1$, or
- (iii) $p^j = 8$ and $q^d = 9$.

We now fix the following hypotheses for the rest of this section.

(III.1.4) HYPOTHESES. Let p and q be distinct primes, and let h and f be natural numbers. Let V be a nonzero vector space of dimension h over the field \mathbb{F} of q^f elements. Let P be a p -group acting faithfully on V , so that $P \leq GL(h, q^f)$.

The aim of the rest of this section is to find bounds for $|P|$ in terms of h , q , and f in this situation. We start with some number theory.

(III.1.5) Let p and q be distinct primes and let r be a power of q . Let v and w be natural numbers.

- (i) Suppose that $p \neq 2$. Let d be the smallest integer such that $p \mid r^d - 1$, and suppose that $p^j \nmid r^d - 1$. If $p^v \mid r^w - 1$, with

$v > 0$, then $dp^{v-j} | w$.

(ii) Suppose that $p = 2$. Define integers a, b, j , and k by $r - 1 = a2^j$ and $r + 1 = b2^k$, where a and b are odd. If $p^v | r^w - 1$, then $v \leq j$ if w is odd, and $2^{1+v-(k+j)} | w$ if w is even.

Proof of (i) Firstly, note that d is the order of $r \pmod{p}$. Since $v > 0$, we have $p | r^w - 1$, so that $r^w \equiv 1 \pmod{p}$. Thus $d | w$. We write $w = dp^k m$ where k and m are natural numbers, and m is coprime to p . Also, since $p^j | r^d - 1$ we can write $r^d = ap^j - 1$, where a is an integer. Now

$$\begin{aligned} r^w - 1 &= r^{dp^k m} - 1 \\ &= (r^{dp^k} - 1)(r^{dp^k(m-1)} + \dots + r^{dp^k} + 1). \end{aligned}$$

Each term in the second bracket is a power of r^d and so is equivalent to $1 \pmod{p}$. Since there are m such terms, and m is not divisible by p , the second bracket is also not divisible by p . Thus

$$p^v | r^{dp^k} - 1 \quad (*)$$

Now we prove by induction on k that $(*)$ implies $v - j \leq k$. This will complete the proof of (i). Note that if $k = 0$, then $v \leq j$ and we are done. So assume that $k > 0$. Then

$$r^{dp^k} - 1 = (r^{dp^{k-1}} - 1)(r^{dp^{k-1}(p-1)} + \dots + r^{dp^{k-1}} + 1).$$

For convenience we let the second bracket equal N . We aim to show that $p^2 \nmid N$, and to this end we calculate $N \pmod{p^2}$. Now

$$r^d = ap^j + 1,$$

so if t is a natural number,

$$r^{dt} \equiv (1 + ap^j)^t \pmod{p^2},$$

and so using the binomial theorem,

$$r^{dt} \equiv 1 + tap^j \pmod{p^2}.$$

Thus

$$N \equiv r^{dp^{k-1}(p-1)} + \dots + r^{dp^{k-1}} + 1 \pmod{p^2}$$

$$\begin{aligned}
&\equiv p - 1 + ap^j(p^{k-1}(p-1) + \dots + p^{k-1}) + 1 \pmod{p^2} \\
&\equiv p + ap^{j+k-1}((p-1) + \dots + 2 + 1) \pmod{p^2} \\
&\equiv p + ap^{j+k-1}p(p-1)/2 \pmod{p^2} \\
&\equiv p + p^2a((p-1)/2)p^{j+k-2} \pmod{p^2} \\
&\equiv p \pmod{p^2},
\end{aligned}$$

since both j and k are at least one.

Hence $p^2 \nmid N$, and so $p^{v-1} \mid r^{dp^{k-1}} - 1$, and by induction we conclude that $v-1-j \leq k-1$, whence $v-j \leq k$ as required.

Proof of (ii) We write $w = m2^c$ where m and c are natural numbers, and m is odd. As in the proof of (i) we obtain

$$2^v \mid r^{2^c} - 1. \quad (**)$$

If w is odd, then $c=0$ and $(**)$ implies that $2^v \mid r-1$, so that $v \leq j$. Now we assume that $c > 1$, i.e., that w is even, and prove by induction on c that $(**)$ implies that $c \leq 1+v-(k+j)$.

If $c=1$, then $2^v \mid r^2 - 1$, and so $v \leq j+k$, and we are finished.

Suppose that $c \geq 2$. Then

$$r^{2^c} - 1 = (r^{2^{c-1}} - 1)(r^{2^{c-1}} + 1).$$

Since $c \geq 2$, the number $r^{2^{c-1}}$ is an odd square and so is equivalent to one (mod 4). Thus $4 \nmid (r^{2^{c-1}} + 1)$ and so $2^{v-1} \mid (r^{2^{c-1}} - 1)$. By induction, therefore, $c-1 \leq 1+v-1-(k+j)$, and we are done.

Assume Hypotheses (III.1.4). Suppose further that V_p is irreducible and that V is not induced from a module for a proper subgroup of P . It will then follow from Clifford's Theorem and (II.2.6(iii)) that P is cyclic or has a cyclic subgroup of index two. It is this situation that we deal with in the next result.

(III.1.6) Assume hypotheses (III.1.4). Suppose that P is cyclic or contains a cyclic subgroup of index two. Let n be the highest power of p dividing f . Then

$$|P| \leq \begin{cases} 2nq^{fh/n} & \text{always} \\ nq^{fh/n} & \text{if } p \neq 2. \end{cases}$$

Proof Choose $T \leq P$ to be cyclic of largest possible order. Thus T has index one or two. We prove by induction on $|V|$ the following statement.

$$(*) \quad |T| \leq nq^{fh/n}; \text{ or } h=1, p=2, \text{ and } |T| \leq 2nq^{fh/n}.$$

It is clear that the required result follows from $(*)$ since $T=P$ if $h=1$.

Firstly, we show that we may assume that V_T is irreducible. If it isn't, since V_T is completely reducible and T has a unique minimal normal subgroup, we can write

$$V_T = V_1 \oplus V_2,$$

where V_1 is faithful for T and $V_2 \neq 0$. Therefore, by induction,

$$|T| \leq 2nq^{fg/n},$$

where $g = \dim(V_1)$. But now

$$\begin{aligned} |T| &\leq (nq^{fh/n})(2q^{(f/n)(g-h)}) \\ &\leq (nq^{fh/n})(2 \cdot 2^{-1}) \\ &= nq^{fh/n}, \end{aligned}$$

and we are done.

From now on we assume that V_T is irreducible. From (II.3.6), applied with $\Lambda = T$, we deduce that

$$|T| \mid q^{fh} - 1.$$

We now consider the cases $p=2$ and $p \neq 2$ separately.

Assume firstly that p is odd. Set $|T| = p^v$, and turn to (III.1.5(i)). With $r = q^h$ and $w = f$ we conclude that $dp^{v-j} \mid f$, where $p^j \parallel q^{dh} - 1$. Thus $p^{v-j} \leq n$, and, since d is coprime to p , we have $d \leq f/n$. Hence

$$|T| = p^v \leq np^j \leq nq^{hd} \leq nq^{fh/n},$$

as required.

Now assume that $p = 2$, set $|T| = 2^v$, and apply (III.1.5(ii)) with $r = q^h$ and $w = f$. If $n = 1$, so that f is odd, we have $v \leq j$, where $2^j \parallel q^h - 1$, and so

$$|T| \leq q^h \leq nq^{fh/n}.$$

So assume that n is at least two, and let m be the highest power of two dividing h . Using a similar argument to that of (III.1.5(ii)) (with $r = q$) we obtain

$$2^v \mid q^{nm} - 1$$

and then

$$2^v \mid (nm/2)(q^2 - 1).$$

Now the highest power of two dividing $(q^2 - 1)$ is a divisor of either $2(q-1)$ or $2(q+1)$, according as q is equivalent to 1 or 3 (mod 4). In any case it is at most $2(q+1)$. So

$$2^v \leq nm(q+1).$$

If $h = 1$, then $m = 1$, and $2^v \leq n(q+1) \leq 2nq \leq 2nq^{fh/n}$, as required.

If $h \geq 2$, then, using $q \geq 3$,

$$\begin{aligned} 2^v &\leq nh(q+1) \\ &\leq nh(4/3)q \\ &\leq 4nq^h(h/3q^{h-1}) \\ &\leq 4nq^h(h/3^h). \end{aligned}$$

Applying (III.1.2), we have $h/3^h \leq 3^{-2/3}h \leq 3^{-(4/3)} < \frac{1}{4}$, so

$|T| = 2^v \leq nq^h \leq nq^{fh/n}$, as required.

The truth of (*) and thus (III.1.6) is now established.

(III.1.7) Assume hypotheses (III.1.4). Then

$$2|P| \leq \begin{cases} |V|^{(5/3)} & \text{always} \\ |V|^{(3/2)} & \text{if } p \neq 2 \\ |V| & \text{if } p \neq 2 \neq q. \end{cases}$$

Proof Note that since $GI(h, q^f) \leq GI(hf, q)$, we may assume that $f = 1$. We prove the result by induction on $|V|$. It is convenient to define the number b by

$$b = \begin{cases} 5/3 & \text{if } p = 2 \\ 3/2 & \text{if } p \neq 2, q = 2 \\ 1 & \text{if } p \neq 2, q \neq 2. \end{cases}$$

We thus need to show that $|P| \leq \frac{1}{2}|V|^b$.

We show firstly that we can assume that V_P is irreducible. Since $p \neq q$, the module V is certainly completely reducible, so we can write $V_P = V_1 \oplus \dots \oplus V_s$, where the V_i are irreducible $\mathbb{F}P$ -modules. If $s > 1$ we can apply induction to each V_i to deduce that

$$|P/K_i| \leq \frac{1}{2}|V_i|^b,$$

where $K_i = \ker(P \text{ on } V_i)$ for $1 \leq i \leq s$. Since the groups K_1, \dots, K_s have trivial intersection we have an injective homomorphism from P into $P/K_1 \times \dots \times P/K_s$ defined by $y \mapsto (K_1 y, \dots, K_s y)$ ($y \in P$). Thus

$$\begin{aligned} |P| &\leq |P/K_1| \dots |P/K_s| \\ &\leq \left(\frac{1}{2}\right)^s |V_1|^b \dots |V_s|^b \\ &\leq \left(\frac{1}{2}\right)^s |V|^b \\ &\leq \left(\frac{1}{2}\right) |V|^b, \end{aligned}$$

and we are done.

So from now on we assume that $s = 1$, i.e., that V is irreducible. The next step is to show that we may assume that all normal abelian subgroups of P are cyclic. So let $A \trianglelefteq P$ and suppose that A is abelian but not cyclic. Now, from (II.3.6) it follows that V_A is not homogeneous, so by Clifford's theorem (II.3.2(iii)), we have

$$V_P = U_S \uparrow^P,$$

where $A \leq S < P$ and U is an irreducible $\mathbb{F}S$ -module. By the transitivity of induction, we can assume that S is maximal in

P , and since P is a p -group, this means that S is normal of index p . Now

$$V = Ux_1 \oplus \dots \oplus Ux_p,$$

where $x_1 = 1, x_2, \dots, x_p$ are a set of coset representatives for S in P . Since $S \trianglelefteq P$, the group S acts on each Ux_i , and we can apply induction to each Ux_i considered as an \mathbb{F}_S -module to obtain

$$2|S/K_i| \leq |Ux_i|^b = |U|^b,$$

where $K_i = \ker(S \text{ on } Ux_i)$. Now V_S is faithful, so the K_i intersect trivially, and so using a similar argument to that of the previous paragraph we obtain

$$|S| \leq \left(\frac{1}{2}\right)^p |V|^b.$$

Thus

$$|P| \leq p \left(\frac{1}{2}\right)^p |V|^b.$$

Evidently this gives us the required bound if $p=2$, and an application of (III.1.1) shows that $p/2^p \leq 3/8$ if $p \geq 3$, and we are done.

So now we assume that all abelian normal subgroups of P are cyclic. By (II.2.6(iii)), therefore, P is itself either cyclic, generalized quaternion, dihedral, or semi-dihedral, and in particular, by (II.2.5(iii)), P has a cyclic subgroup of index one or two. Thus we can apply (III.1.6) to V , and remembering that $f=1$ we obtain

$$\begin{aligned} |P| &\leq \sqrt{2q^h} = 2|V| \\ &\quad \wedge q^h = |V| \text{ if } p \neq 2. \end{aligned}$$

Assume that $p=2$. If $|V| > 8$, we have $2|P| \leq 4|V| \leq |V|^{5/3}$. But if $|V| < 8$, then $|V| = 3, 5, \text{ or } 7$, and it is easy to check that $|P| \leq \frac{1}{2}|V|^{5/3}$ in these cases.

Assume that $q=2$. If $|V| > 4$, we have $2|P| \leq 2|V| \leq |V|^{3/2}$. If $|V| < 4$, then $|V| = 2$, so $P=1$, and $2|P| \leq |V|^{3/2}$.

Finally, assume that both p and q are odd. Now P is

cyclic, and $|P| \mid q^h - 1$. By (III.1.3), since both p and q are odd, we cannot have $|P| = q^h - 1$. Thus $2|P| \leq q^h = v$. This completes the proof of (III.1.7).

III.2. GROUP THEORY

The main aim of this section is to prove (III.2.5). This result will give us a chief factor of K to which we can apply induction in the homogeneous case of Theorem A. Of great importance in this situation is the result of P. Hall which we stated as (II.2.6) and which we restate here for convenience.

(THEOREM II.2.6) If R is a nontrivial r -group such that every characteristic abelian subgroup is cyclic, then R satisfies the following hypotheses.

(HYPOTHESES II.2.7) R is the central product $E \times C$, where $E = 1$ or is an extraspecial r -group, and $C \neq 1$. Further

- (i) If $r > 2$, then E has exponent r , and C is cyclic;
- (ii) If $r = 2$, then C is either cyclic, or has order at least 16, and is generalised quaternion, dihedral, or semi-dihedral;
- (iii) The centre of C contains a unique subgroup of order r : it is this subgroup that is identified with $Z(E)$ in R (when $E \neq 1$).

Our first result gives us some useful characteristic subgroups of groups satisfying Hypotheses (II.2.7).

(III.2.2) Let R satisfy Hypotheses (II.2.7). Then

- (i) $Z(R) = Z(C)$ ($= C$ if C is abelian);
- (ii) If r is odd, then E is characteristic in R ;
- (iii) Let $r = 2$, and assume that C is cyclic and that $E \neq R$. If Z denotes the unique subgroup of order 4 in C , then EZ is characteristic in R ;
- (iv) If $r = 2$ and C is noncyclic, then C contains a cyclic subgroup, D say, of index two, and ED is characteristic in R .

Proof (i) Since C centralises E , we have $Z(C) \leq Z(R)$. Also, $Z(R) \leq C_R(E) \leq C$, so $Z(R) \leq C_C(R) \leq Z(C)$.

(ii) Let U be the subgroup of R generated by all elements of order r . Clearly U is characteristic in R . We claim that $U = E$.

Since E has exponent r , we certainly have $U \geq E$. Now let $y \in R \setminus E$. Then $y = ec$ with $e \in E$ and $c \in C$. So $y^r = e^r c^r = c^r$. If $c^r = 1$, then c is in the unique subgroup of C of order r , and according to (II.2.5(iii)), is in E . Thus $y^r \neq 1$, and so $U = E$.

(iii) Since $E \neq R$, we have $|C| \geq 4$, and therefore C contains a unique cyclic subgroup Z of order 4. Now, as in (ii), EZ is the subgroup generated by all elements of order at most 4.

(iv) By (II.2.5(iii)), the group C has a characteristic cyclic subgroup of index two. Define a subgroup S of R by

$$S/Z(R) = Z(R/Z(R)).$$

Now

$$R/Z(R) = E/Z(R) \times C/Z(R) = E/Z(E) \times C/Z(C),$$

so

$$\begin{aligned} S/Z(R) &= Z(E/Z(E)) \times Z(C/Z(C)) \\ &= E/Z(R) \times Y/Z(R), \end{aligned}$$

where $Y/Z(C) = Z(C/Z(C))$. Since $C/Z(C)$ is dihedral by (II.2.5(ii)), it has centre of order two by (II.2.5(i)); thus Y has order 4.

We now claim that $C_R(Y) = E \vee D$. Certainly, $E \leq C_R(Y)$. Now $D \leq C$, so D intersects $Z(C)$ nontrivially. But $Z(C) = 2$, and so $D \geq Z(C)$. By a similar argument applied to $C/Z(C)$, we obtain $D \geq Y$. Now D is cyclic, so $D \leq C_C(Y) \leq C_R(Y)$. Thus $E \vee D \leq C_R(Y)$. If equality did not hold we would have $C_R(Y) = R$, but this

would imply that $Y \leq Z(C)$, a contradiction. Therefore $C_R(Y) = E \cap D$.

Finally, we note that since $Y = Z(S)$, and S is characteristic in R , we have that Y and hence $C_R(Y)$ is characteristic in R .

(III.2.3) Let R be an r -group which satisfies the Hypotheses (II.2.7), with C cyclic. Then any automorphism of R which centralises both R/C and C is inner.

Proof Let $\theta \in \text{Aut}(R)$, and suppose that θ centralises R/C and C . Now R/C is elementary abelian, of order r^n say, so we can choose generators Cx_1, \dots, Cx_n for R/C with $x_i \in E$. Since θ centralises C , once we know the action of θ on x_1, \dots, x_n , we will have determined θ .

Since θ centralises R/C , we have, for $1 \leq i \leq n$, that $x_i \theta = x_i z_i$ for suitable $z_i \in C$. The x_i are in E , so they have order r or 4 . If x_i has order r , then $x_i z_i$ has order r also, and so

$$1 = (x_i z_i)^r = x_i^r z_i^r = z_i^r.$$

On the other hand, if x_i has order 4 , then x_i^2 and $x_i^2 z_i^2$ are both elements of C of order 2 . But there is only one element of C of order 2 , so $x_i^2 z_i^2 = x_i^2$, whence $z_i^r = 1$ again.

Therefore there are at most r choices for each $x_i \theta$ and therefore at most r^n possibilities for θ .

But $C = Z(R) = C_R(R)$; so R has $|R/C| = r^n$ inner automorphisms, and hence θ must be one of these.

The following result, together with the last, constitute a generalisation of [11, 5.4.6].

would imply that $Y \leq Z(C)$, a contradiction. Therefore $C_R(Y) = E \cap D$.

Finally, we note that since $Y = Z(S)$, and S is characteristic in R , we have that Y and hence $C_R(Y)$ is characteristic in R .

(III.2.3) Let R be an r -group which satisfies the Hypotheses (II.2.7), with C cyclic. Then any automorphism of R which centralises both R/C and C is inner.

Proof Let $\theta \in \text{Aut}(R)$, and suppose that θ centralises R/C and C . Now R/C is elementary abelian, of order r^n say, so we can choose generators Cx_1, \dots, Cx_n for R/C with $x_i \in E$. Since θ centralises C , once we know the action of θ on x_1, \dots, x_n , we will have determined θ .

Since θ centralises R/C , we have, for $1 \leq i \leq n$, that $x_i \theta = x_i z_i$ for suitable $z_i \in C$. The x_i are in E , so they have order r or 4 . If x_i has order r , then $x_i z_i$ has order r also, and so

$$1 = (x_i z_i)^r = x_i^r z_i^r = z_i^r.$$

On the other hand, if x_i has order 4 , then x_i^2 and $x_i^2 z_i^2$ are both elements of C of order 2 . But there is only one element of C of order 2 , so $x_i^2 z_i^2 = x_i^2$, whence $z_i^r = 1$ again.

Therefore there are at most r choices for each $x_i \theta$ and therefore at most r^n possibilities for θ .

But $C = Z(R) = C_R(R)$; so R has $|R/C| = r^n$ inner automorphisms, and hence θ must be one of these.

The following result, together with the last, constitute a generalisation of [11, 5.4.6].

(III.2.4) Let R be as in the previous result, and suppose that R is a normal subgroup of a group H . Then

$$C_H(R/C) \cap C_H(C) = C_H(R)R.$$

Proof Since both $C_H(R)$ and R centralise both R/C and C , the inclusion

$$C_H(R/C) \cap C_H(C) \supseteq C_H(R)R$$

is clear.

Now let $x \in C_H(R/C) \cap C_H(C)$. By (III.2.3), the element x acts on R as an inner automorphism. Thus there exists $y \in R$ such that $xy^{-1} \in C_H(R)$. Then $x \in C_H(R)R$, as required.

We now come to the main result of this section, on which the proof of the homogeneous case of Theorem A depends.

(III.2.5) Let $K \trianglelefteq G$ be groups where $d(K) = d \geq 3$. Assume that any normal abelian subgroup of G contained in K is cyclic. Then there exists a normal subgroup R of G , contained in K , with the following properties.

- (i) R is either extraspecial or the central product of an extraspecial 2-group with a cyclic group of order 4.
- (ii) $\bar{R} = R/Z(R)$ is a chief factor of G .
- (iii) $d(K/C_K(\bar{R})) \geq d - 2$.

A few comments on the proof are in order. Since $C_K(F(K))$ is contained in $F(K)$, it is in fact contained in the centre of $F(K)$, and so is abelian. Thus K induces on $F(K)$ a group of automorphisms of derived length at least $d - 1$. Thus for some prime r dividing $|F(K)|$, we have $d(K/C_K(O_r(K))) \geq d - 1$. Suppose for the moment that $r > 2$. Then by the condition on normal

(III.2.4) Let R be as in the previous result, and suppose that R is a normal subgroup of a group H . Then

$$C_H(R/C) \cap C_H(C) = C_H(R)R.$$

Proof Since both $C_H(R)$ and R centralise both R/C and C , the inclusion

$$C_H(R/C) \cap C_H(C) \supseteq C_H(R)R$$

is clear.

Now let $x \in C_H(R/C) \cap C_H(C)$. By (III.2.3), the element x acts on R as an inner automorphism. Thus there exists $y \in R$ such that $xy^{-1} \in C_H(R)$. Then $x \in C_H(R)R$, as required.

We now come to the main result of this section, on which the proof of the homogeneous case of Theorem A depends.

(III.2.5) Let $K \triangleleft G$ be groups where $d(F) = d \geq 3$. Assume that any normal abelian subgroup of G contained in K is cyclic. Then there exists a normal subgroup R of G , contained in K , with the following properties.

- (i) R is either extraspecial or the central product of an extraspecial 2-group with a cyclic group of order 4.
- (ii) $\bar{R} = R/Z(R)$ is a chief factor of G .
- (iii) $d(K/C_K(\bar{R})) \geq d - 2$.

A few comments on the proof are in order. Since $C_K(F(K))$ is contained in $F(K)$, it is in fact contained in the centre of $F(K)$, and so is abelian. Thus K induces on $F(K)$ a group of automorphisms of derived length at least $d - 1$. Thus for some prime r dividing $|F(K)|$, we have $d(K/C_K(O_p(K))) \geq d - 1$. Suppose for the moment that $r > 2$. Then by the condition on normal

abelian subgroups of G , we know that $O_r(K)$ is the central product of an extraspecial group E and a cyclic group, both of which are characteristic in $O_r(K)$. It follows that $d(K/C_K(E)) \geq d-1$. Let $Z(E) < M \leq E$, where $M \in G$. When $r > 2$, it is easily shown that M is extraspecial and it follows that $M/Z(E)$ is complemented in $E/Z(E)$ by $C_E(M)/Z(E)$. Thus $E/Z(E)$ is completely reducible as a G -module, and it is now easy to find $R \leq E$ with the required properties.

If $r=2$, however, the above argument goes wrong in several places, and it is this that makes the proof complicated. The key step is to replace $F(K)$ by a subgroup (I , below) which still contains its centraliser, but which has a 'nicer' Sylow 2-subgroup.

Proof of (III.2.5)

Step 1. There exists a normal subgroup I of G , contained in K with the following properties.

- (i) I is the direct product of r -groups $E_r \times D_r$, for various primes r , where each $E_r \times D_r$ satisfies Hypotheses (II.2.7) with $E_r \times D_r$ in place of R , with $E_r = E$, and $D_r = C$. Further, D_r is cyclic.
- (ii) If 2 divides $|I|$, then either 4 divides $|D_2|$; or $|D_2| = 2$, and any normal subgroup of G contained in E_2 is either trivial, extraspecial, or equal to $Z(E_2) = D_2$.
- (iii) $C_K(I) \leq I$.

Let r be a prime dividing $|F(K)|$. Characteristic abelian subgroups of $O_r(K)$ are normal abelian subgroups of G , since $O_r(K)$ is characteristic in K , and are therefore cyclic by hypothesis. If r is odd, then by (II.2.6),

$$O_r(K) = E_r \times D_r$$

where $E_r = 1$, or is extraspecial of exponent r , and D_r is a non-

trivial cyclic group.

If $r=2$, then (II.2.6(ii)) tells us that

$$O_2(K) = B \vee C,$$

where B is trivial or extraspecial, where $C \neq 1$, and C is either cyclic or generalized quaternion, dihedral, or semi-dihedral of order at least 16.

We now wish to define E_2 and D_2 satisfying (i) and (ii) of Step 1, and such that $C_{O_2(K)}(E_2 \vee D_2) \leq E_2 \vee D_2$.

If C is cyclic of order at least 4; or if $|C| = 2$, and any normal subgroup of G contained in B is trivial, extraspecial or equal to $Z(B)$, we put $E_2 = B$, $D_2 = C$, and we are done.

Next, suppose that $|C| = 2$, so that $O_2(K) = B$, but that B contains a subgroup M which is normal in G , but neither 1, $Z(B)$, nor extraspecial. Now since $M \triangleleft G$, characteristic abelian subgroups of M are cyclic by hypothesis, and so we deduce from (II.2.6), together with the fact that M has exponent 4, that $Z(M)$ is cyclic of order 4. Since M is normal in G , so is $Z(M)$, and therefore so is $C_B(Z(M))$. Since the automorphism group of $Z(M)$ has order 2, and since $Z(M) > Z(B)$, the group $C_B(Z(M))$ has index two in B , and thus has the wrong order to be an extraspecial group, by (II.2.4). Hence, by the argument just applied to M , we must have

$$C_B(Z(M)) = E_2 \vee D_2,$$

where E_2 is extraspecial and D_2 is cyclic of order 4. It only remains to check that $C_B(E_2 \vee D_2) \leq E_2 \vee D_2$. Let $x \in C_B(E_2 \vee D_2)$. Now $Z(M) \leq C_B(Z(M))$, so x centralises $Z(M)$, whence $x \in C_B(Z(M))$ as required.

Finally, we need to deal with the case that C is non-cyclic. In this case we have by (III.2.2(iv)) a characteristic subgroup $B \vee D$ of index two in $B \vee C$, where D is cyclic. Since $|C| \geq 16$, we must have $|D| \geq 8$. It is easily checked that

$C_{B \vee C}(B \vee D) \trianglelefteq B \vee D$, so with $E_2 = B$ and $D_2 = D$, we are done.

Now let I be the direct product of all the $E_r \vee D_r$, and note that I is a normal subgroup of G of index either one or two in $F(K)$. Step 1 will be complete once we have shown (iii).

Now $C_K(I)/C_V(F(K))$ stabilises the series $1 \trianglelefteq E_2 \vee D_2 \trianglelefteq O_2(K)$, and thus by (II.1.3) it is a 2-group.

Secondly

$$C_K(F(K)) = Z(F(K)) \trianglelefteq I,$$

so

$$C_K(F(K)) \trianglelefteq Z(C_K(I)),$$

whence $C_K(I)/Z(C_K(I))$ is a 2-group, and therefore $C_K(I)$ is nilpotent. Since it is also normal in K we have

$$C_K(I) \trianglelefteq F(K)$$

and using the fact that $C_{O_2(K)}(E_2 \vee D_2) \trianglelefteq I$, we find that

$$C_K(I) \trianglelefteq I,$$

and so Step 1 is finished.

Step 2. There exists a normal subgroup S of G with $d(K/C_K(S)) \geq d-1$, and such that one of the following holds.

- (i) S is an extraspecial group of exponent r , where r is an odd prime.
- (ii) S is an extraspecial 2-group and any normal subgroup of G contained in S is either 1, $Z(S)$, or extraspecial.
- (iii) S is the central product of an extraspecial 2-group with a cyclic group of order 4.

We have $C_K(I) \trianglelefteq I$, and so $C_K(I)$ is the centre of I and is, in particular, abelian. Thus $K/C_K(I)$ has derived length at least $d-1$. Since I is the direct product of the $E_r \vee D_r$, we have, for some r , that $d(K/C_K(E_r \vee D_r)) \geq d-1$.

We consider three cases.

Suppose firstly that r is odd. Then by (III.2.2(i),(ii)), both E_r and D_r are characteristic in $E_r \vee D_r$, and so

$$C_K(D_r) \cap C_K(E_r) = C_K(E_r \vee D_r).$$

Now $K/C_K(D_r)$ is abelian since D_r is cyclic, and $d-1 \geq 2$ by hypothesis. Hence, using (I.3.2(ii)), we have $d(K/C_K(E_r)) \geq d-1$, and we can put $S = E_r$ to complete Step 2 in this case.

Secondly, suppose that $r=2$, and that D_2 has order 2.

Then by part (ii) of Step 1, putting $S = E_2$ does the trick.

Finally, suppose that $r=2$ and that D_2 has order at least 4. Then by (III.2.2(iii)) the group $E_2 \vee D_2$ contains a characteristic subgroup $E_2 \vee Z$, where Z is cyclic of order 4. We put $S = E_2 \vee Z$. As in the r odd case, it is easy to show that $d(K/C_K(S)) \geq d-1$.

This completes the proof of Step 2.

Step 3. $\bar{S} = S/Z(S)$ is completely reducible as a G -module.

We denote images modulo $Z(S)$ by bars. Let M be any normal subgroup of G lying between $Z(S)$ and S . To prove Step 3, it is sufficient to find a G -module which complements \bar{M} in \bar{S} .

Since M is normal in G , it follows by the usual argument based on (II.2.6) together with the fact that the exponent of S is either r or 4, that $M = AT$, where A is extraspecial, of exponent r if $r > 2$, and T is cyclic of order r or 4. Now $Z(S) \leq Z(M) = T$, and since by choice of S the group T can only have order 4 when $Z(S)$ also has order 4, we have $T = Z(S)$.

Now set $C = C_S(M)$. Since S and M are normal in G , so is C . By (III.2.4), applied with $H=S$ and $R=M$, we have

$$\begin{aligned} MC &= C_S(M/Z(M)) \cap C_S(Z(M)) \\ &= S \cap S = S. \end{aligned}$$

Also, $M \cap C = C_M(M) = Z(M) = Z(S)$. Thus \bar{C} is the required complement to \bar{M} , and so Step 3 is proved.

Step 4. $d(K/C_K(\bar{S})) \geq d-2$.

Let $X = C_K(\bar{S})/C_K(S)$. We aim to show that X is abelian. In view of the fact that $d(K/C_K(S)) \geq d-1$, this will prove Step 4.

Assume firstly that S is extraspecial, i.e., that S satisfies either (i) or (ii) of Step 2. Now $Z(S) = \phi(S)$. If $x \in X$ is an element of r' order, then since x centralises $S/\phi(S)$, it centralises S by (I.1.7), so $x = 1$. Thus X is an r -group. Since the automorphism group of $Z(S)$ is of order $r-1$, the group X centralises $Z(S)$. Now let $x, y \in X$, and $s \in S$. Since X centralises \bar{S} , we have

$$\begin{aligned} s^x &= sz_1, \\ s^y &= sz_2, \end{aligned}$$

for suitable z_1, z_2 in $Z(S)$. Because X centralises $Z(S)$, we have

$$\begin{aligned} s^{x^{-1}} &= sz_1^{-1} \\ s^{y^{-1}} &= sz_2^{-1}. \end{aligned}$$

A trivial calculation shows that $[x, y] = 1$, so that X is abelian.

Secondly, suppose that S satisfies (iii) of Step 2, so that $Z(S)$ has order 4. Let $x, y \in X$ and $s \in S$. We have $s^x = sz_1$ and $s^y = sz_2$ for suitable z_1, z_2 as before. Now, if s has order 2, so does sz_1 , and so

$$1 = (sz_1)^2 = s^2 z_1^2 = z_1^2,$$

while if s has order 4, we find that s^2 and $s^2 z_1^2$ are both of order two in $Z(S)$, and are therefore equal. Thus $z_1^2 = 1$. Similarly, of course, z_2 has order one or two, and so it follows that x and y both act trivially on z_1 and z_2 . Now the argument goes as in the previous case.

This completes the proof of Step 4.

Step 5. Conclusion of the proof.

Choose a subgroup R of G of minimal order subject to
(*) $R \triangleleft G$, $Z(S) \leq R \leq S$, and $d(K/C_K(\bar{R})) \geq d-2$.

(This is possible since S satisfies (*).)

By the argument in Step 3, the group R satisfies (i) of the theorem. By the choice of R , it satisfies (iii). Finally, if \bar{R} is not a chief factor of G , by Step 3 we can write $\bar{R} = \bar{R}_1 \circ \bar{R}_2$, where R_1 and R_2 are normal subgroups of G , and both R_1 and R_2 have order strictly less than that of R .

From (1.3.2(ii)) it follows that K must induce a group of automorphisms of derived length at least $d-2$ on either \bar{R}_1 or \bar{R}_2 . But this contradicts the minimality of $|R|$, and so \bar{R} is a chief factor of G , and the proof is complete.

III.3. REPRESENTATION THEORY

We start with a slight generalisation of Maschke's theorem on complete reducibility.

(III.3.1) Let $G = NP$ be a group where $N \triangleleft G$ and P is a complement to N in G . Let \mathbb{F} be a field and let V be an $\mathbb{F}G$ -module. If V_N is completely reducible and the characteristic of \mathbb{F} is coprime to $|P|$, then V_G is completely reducible.

Proof It is sufficient to show that any NP -submodule W has a complement. Since V_N is completely reducible, $V = W \oplus U$, where U is an N -submodule. Let $\theta: V \rightarrow W$ be the projection map, which is clearly an N -homomorphism. Define $\psi: V \rightarrow V$ by

$$v\psi = (1/|P|) \sum_{x \in P} vx\theta x^{-1}.$$

Then ψ is a well-defined linear map. In fact, as we now show, it is a G -homomorphism. Let $g \in G$ and write $g = ny$ where $n \in N$ and $y \in P$. Then

$$\begin{aligned} (v\psi)g &= (1/|P|) \sum_{x \in P} vx\theta x^{-1}ny \\ &= (1/|P|) \sum_{x \in P} vx\theta n^x x^{-1}y \\ &= (1/|P|) \sum_{x \in P} vxn^x \theta x^{-1}y, \end{aligned}$$

since $n^x \in N$ and θ is an N -homomorphism. Thus

$$\begin{aligned} (v\psi)g &= (1/|P|) \sum_{x \in P} v\theta(y^{-1}x)\theta(y^{-1}x)^{-1} \\ &= v\psi \end{aligned}$$

since $y^{-1}x$ runs over P as x does. Thus ψ is a G -homomorphism and therefore $V\psi$ is a G -submodule. The proof that $V = W \oplus V\psi$ now runs exactly as in the proof of Maschke's theorem. (See [11, 3.3.1])

$$\theta(x) = \begin{pmatrix} \beta_{11}(x) & \cdots & \beta_{1h}(x) \\ \vdots & \ddots & \vdots \\ \beta_{h1}(x) & \cdots & \beta_{hh}(x) \end{pmatrix}.$$

Now $xy = yx$ for all $y \in N$, so

$$\theta(x)\theta(y) = \theta(y)\theta(x) \quad \text{for all } y \in N.$$

Thus

$$\beta_{ij}(x)\alpha(y) = \alpha(y)\beta_{ij}(x) \quad \text{for all } y \in N, 1 \leq i, j \leq h.$$

Therefore

$$\beta_{ij}(x) \in \text{Hom}_{\mathbb{F}}(W_1, W_1) = \mathbb{E} \quad \text{for all } 1 \leq i, j \leq h.$$

This gives the required homomorphism from P into $GL(h, \mathbb{E})$. It is injective since V is faithful for P .

We now have three results designed to deal with some small cases.

(III.3.3) Let K be a soluble group of derived length at least three. Let V be a faithful, irreducible module for K over some field \mathbb{F} . Then $|V| \geq 9$.

Proof Since K is nonabelian, we must have $\dim(V) \geq 2$, so the only possibilities for $|V|$ if $|V| < 9$ are $|V| = 4$ or $|V| = 8$. Now $GL(2, 2)$ has order 6, and so derived length at most 2. Thus we may suppose that $|V| = 8$, so that $K \leq GL(3, 2)$.

Since V_K is irreducible, and $O_2(K) \triangleleft K$, the group

$O_2(K)$ acts completely reducibly on V , by Clifford's theorem. But the characteristic of F is 2, so $O_2(K) = 1$. By [12, II.6.2], the group $GL(3,2)$ has order $3 \cdot 3 \cdot 7$, and since $O_2(K) = 1$, we know that $|F(K)|$ divides 21. Since $F(K)$ is nilpotent, it follows that $F(K)$ is cyclic. But the automorphism group of a cyclic group is abelian, so $K/C_K(F(K)) = K/F(K)$ is abelian, and $d(K) \leq 2$.

(III.3.4) Let p be an odd prime and let K be a nontrivial p' -group. Suppose that P is a p -group acting on K and that $KP \leq Sp(4,2)$. Assume that KP acts irreducibly on the underlying vector space of dimension 4 over F_2 .

- (i) $|P| \leq 5$.
- (ii) $|P| \leq 3$ if $p \neq 5$.
- (iii) If $d(K) \geq 2$, then $|P| \leq 3$.
- (iv) If $d(K) \geq 3$, then $P = 1$.
- (v) $d(K) \leq 3$.

Proof By (II.2.10), we have $|Sp(4,2)| = 2^4 \cdot 3^2 \cdot 5$. Since KP acts irreducibly on V , we have $O_2(K) = 1$, so that $|F(K)|$ is odd. Thus $|F(K)P|$ divides 45.

Since the automorphism group of any group of order 1, 3, or 9 has order coprime to 5; and since the automorphism group of any group of order 1 or 5 has order coprime to 3, the group P must centralise $F(K)$. By (I.2.7) and (II.1.5), therefore, P centralises K .

Set $F = F(K)$.

- (i) and (ii). Clearly (i) and (ii) hold unless $|P| = 9$.

Assume for a contradiction that $|P| = 9$. Now $K \neq 1$, so $F \neq 1$, and therefore we must have $|F| = 5$. Thus F acts irreducibly on V (since 4 is the smallest integer n such that $5 \mid 2^n - 1$). The dimension of any absolutely irreducible module for F is 4, so, using (II.3.10), we must have $|\text{Hom}_{\mathbb{F}_2 F}(V, V)| = 16$. Now, (III.3.2) applied with F in place of R gives us $P \leq \text{GL}(1, 16)$, so that $|P|$ divides 15, the required contradiction.

(iii) By (i) and (ii), we are done unless $|P| = 5$, so assume that this is the case. As in the previous paragraph, we can apply (III.3.2) (with P in place of R and K in place of F) to conclude that $K \leq \text{GL}(1, 16)$; thus V is abelian, and (iii) is proved.

(iv) By (iii), we are done unless $|P| = 3$. But if $|P| = 3$, then $|F| = 5$. Since the automorphism group of Z_5 is Z_4 , we have $K/C_K(F) = K/F$ abelian, whence $d(K) \leq 2$, proving (iv).

(v) If 5 divides $|F|$, we can apply (III.3.2) again, with $R = O_5(K)$ and $P = O_3(K)$ to deduce that $|O_3(K)| \leq 3$, whence F is cyclic and $d(K) \leq 2$. Also, if $|P| = 3$, then $d(K) \leq 2$. We may therefore assume that $|F| = 9$.

Regarding F as a (faithful) module for K/F over the field of three elements, and using the fact that $\text{GL}(2, 3)$ has order $2^4 \cdot 3$ by [17, II.6.2], we find that $|K/F|$ divides $2^4 \cdot 3$. But since F has order 9, we also know that $|K/F|$ divides $2^4 \cdot 5$. Thus $|K/F|$ divides 2^4 .

Now, if H is any group of order 16, then, since it is nilpotent, it has a normal subgroup N , say, of order 4.

Now H/N and N are both abelian, so $d(H) \leq 2$. Thus $d(Y/F) \leq 2$, and so $d(K) \leq 3$, as required.

(III.3.5) Let p be a prime not equal to 3, and let $K \neq 1$ be a p '-group. Suppose that P is a p -group acting on K and that $KP \leq \text{Sp}(2,3)$. Assume that KP acts irreducibly on the underlying vector space V of dimension 2 over \mathbb{F}_3 .

- (i) $P = 1$.
- (ii) $d(K) \leq 3$.

Proof (i) By (II.2.10), we have $|\text{Sp}(2,3)| = 2^3 \cdot 3$. Since KP acts irreducibly on V , we have $O_3(K) = 1$. Set $F = F(K)$. Now $K \neq 1$, so $F \neq 1$, whence 2 divides $|F|$. But now P must have order coprime to 2 and 3, so $P = 1$.

(ii) If $|F| = 2$, then $K = F$, and $d(K) = 1$. If $|F| = 4$, then K/F is isomorphic to a subgroup of $\text{GL}(2,2)$, and so $d(K/F) \leq 2$ by (III.3.3), and $d(K) \leq 3$. If $|F| = 3$, then $d(F) \leq 2$, and $|K/F|$ divides 3, so K/F is abelian. Thus $d(K) \leq 3$. Since $O_3(K) = 1$, these are the only possibilities for $|F|$, and so we are finished.

We now come to the main result of this section. It will be used in the induced case of Theorem A, where the straightforward induction argument fails. It may be regarded as a "derived length one version" of Theorem A.

(III.3.6) Let q and p be distinct primes. Let K be a soluble p' -group. Let P be a p -group acting on K .

Suppose that V is an irreducible $\mathbb{F}_q KP$ -module faithful for KP . Assume that $K \neq 1$. Then

- (i) $4|P| \leq |V|^{(3/2)}$, and
- (ii) $2|P| \leq |V|$ if p is odd.

Proof The proof is by induction on $|KP|$. We note that if $|P| = 1$, then the fact that $K \neq 1$ forces $|V| \geq 3$, and (i) and (ii) follow. Thus we assume that $P \neq 1$. We prove (i) and (ii) together.

Step 1. The case where V is induced from a module U for a proper subgroup M containing K .

This is similar to the corresponding part of the proof of (III.1.7) (and Step 1 of the proof of Theorem A).

By the transitivity of induction, we may assume that M is maximal in KP . Since P is a p -group and $M \neq K$, we have $M = KP_0$ where P_0 is a normal subgroup of index p in P . We therefore have

$$V_{KP_0} = Ux_1 \oplus \dots \oplus Ux_p$$

for suitable $x_i \in P$. Since the groups $\ker(V$ on $Ux_i)$ are all conjugate to one another and have trivial intersection, it follows that V acts nontrivially on each Ux_i . Induction applied to each Ux_i therefore yields

$$\left. \begin{aligned} 4|P_0/P_i| &\leq |Ux_i|^{(3/2)} = |U|^{(3/2)} \\ 2|P_0/P_i| &\leq |Ux_i| = |U| \text{ if } p \neq 2, \end{aligned} \right\} \quad (a)$$

where $P_i = \ker(P_0$ on $Ux_i)$.

By the same argument as in (III.1.7), we have
 $|P_0| \leq |P_0/P_1| \times \dots \times |P_0/P_p|$, whence

$$4^p |P_0| \leq |U|^{(3/2)p} = |V|^{(3/2)}, \text{ and}$$

$$2^p |P_0| \leq |U|^p = |V|^p \text{ if } p \neq 2.$$

Thus

$$(4^p/p) |P| \leq |V|^{(3/2)}, \text{ and}$$

$$(2^p/p) |P| \leq |V|^{(3/2)} \text{ if } p \neq 2.$$

To complete Step 1, it suffices to show that $4^p/p \geq 4$ and $2^p/p \geq 2$ for all primes p . These two inequalities clearly hold if $p = 2$, and for $p \geq 3$, they follow from (III.1.1).

Step 2. V_γ is homogeneous. Put $C = C_p(K)$. Then C is cyclic or has a cyclic subgroup of index two.

If V_γ is not homogeneous, then by Clifford's theorem, we are in the case dealt with in Step 1. Thus we may assume that V_γ is homogeneous.

Now let A be an abelian subgroup of C which is normal in P . Then $K \rtimes A$ is normal in KP and contains K . Thus by Step 1 and Clifford's theorem, V_A is homogeneous and so A is cyclic. Thus, by (II.2.8) and (II.2.5(ii)), C has a cyclic subgroup of index one or two.

Step 3. V is cyclic.

If possible, choose a nontrivial, proper, characteristic subgroup N of K . By (III.3.1), the module V_{NP} is completely reducible. Thus

$$V_{NP} = V_1 \oplus \dots \oplus V_s$$

for some $s \geq 1$, where each V_i is an irreducible NP-submodule. Since $N \trianglelefteq KP$, the group N acts nontrivially on each V_i , and so we can apply induction to each V_i , and, using a similar argument to Step 1, deduce that

$$4^s |P| \leq |V|^{(3/2)},$$

$$2^s |P| \leq |V| \quad \text{if } p \neq 2,$$

and we are done. Thus we can assume that K is characteristically simple, and therefore elementary abelian. But V is homogeneous by Step 2, so K is in fact cyclic.

Step 4. The case $p > 2$.

We show firstly that it is sufficient to prove (ii), for then (i) follows. For assume that (ii) holds. Since V and P are both nontrivial, we have $|V| \geq 4$. Thus $4|P| \leq 2|V| \leq |V|^{(3/2)}$.

We now show that (ii) holds under the assumption that $p > 2$. Firstly, we define some integers. Let f be the dimension of an irreducible K -submodule, and suppose that V_P has h irreducible summands. Let n be the highest power of p dividing f .

By (II.3.9) applied with KP in place of G and K in place of A , we deduce that $|P/C|$ divides f , whence

$$|P/C| \leq n. \tag{a}$$

Note that if W is an irreducible submodule of V_P , we have $|\text{Hom}_{\mathbb{F}_q}(W, W)| = q^f$ since K is cyclic. Thus, by (III.3.2) applied with K in place of B and C in place

of P , we have

$$C \leq \text{GI}(h, q^f). \quad (b)$$

Thus, by (III.1.6) and Step 2,

$$|C| \leq nq^{hf/n}. \quad (c)$$

The aim now is to derive the required bound of $2|P|/|V| \leq 1$ from (a), (b), and (c), and the fact that $|V| = q^{fh}$. Now

$$2|P|/|V| \leq 2n^2/(q^{(fh/n)(n-1)}), \quad (d)$$

and since $q^{fh/n} \geq 2$, we have

$$2|P|/|V| \leq 4n^2/2^n. \quad (e)$$

Suppose that $n \geq 9$. Then, by (III.1.1) and (e), we have $2|P|/|V| \leq 2 \cdot 9^2/2^9 < 1$, as required.

Suppose that $n = 7$. If $q^{fh/n} \geq 3$, the required bound is immediate from (d). Assume then, that $q^{fh/n} = 2$, so that $q = 2$, $f = 7$, and $h = 1$. But now, from (b), we have $C \leq \text{GI}(1, 2^7)$, and since $p = 7$, we have $C = 1$. Thus $|P| \leq 7$ by (a), and $2|P| \leq 14 < 128 = |V|$.

Suppose that $n = 5$. Here, (d) gives us the required bound unless $h = 1$, $f = 5$, and $q = 2$ or 3 . In both cases, (b) implies that $C = 1$, so that $2|P| \leq 10 < 32 \leq |V|$.

Next, suppose that $n = 3$. Now, (d) does the trick unless $q^{fh/n} \leq 4$. Since $p = 3$, we have $q = 2$ and $fh = 3$ or 6 . If $fh = 3$, we have $f = 3$ and $h = 1$; here (b) implies that $C = 1$, so that $2|P| \leq 6 < 8 = |V|$. If $fh = 6$, we have either $h = 1$ and $f = 6$, or $h = 2$ and $f = 3$; in both cases, (b) implies that $|C| \leq 9$, so that $2|P| \leq 2 \cdot 3 \cdot 9 = 54 < 64 = |V|$.

Remembering that p is odd, the only possibility left for n is $n = 1$. But now $P = C$, and thus $P * P$ is cyclic. By (II.3.6) we have

$$|V||P| \mid q^{fh} - 1,$$

and since $V \neq 1$, we have $|P| \leq \frac{1}{2}q^{fh}$, i.e., $2|P| \leq |V|$, as required.

This completes Step 4.

Step 5. The case $p = 2$.

This is similar to Step 4. We define h , f , and n as before, and deduce from (II.3.9), (II.3.2), and (III.1.6) that

$$|P/C| \leq n, \quad (f)$$

$$C \leq \text{GT}(h, q^f), \quad (g)$$

and

$$|C| \leq 2nq^{fh/n}. \quad (h)$$

Now, using $q^{fh/n} \geq 3$ (since q is odd), we have

$$4|P|/|V|^{(3/2)} \leq 8n^2/(q^{(fh/n)((3/2)n-1)}) \quad (j)$$

$$\leq 24n^2/(3^{(3/2)n}). \quad (k)$$

If $n \geq 4$, then, by (k) and (III.1.1) we have $4|P|/|V|^{(3/2)} \leq 24 \cdot 4^2/3^6 < 1$, as required.

Suppose that $n = 2$. The desired bound follows from (j) unless $f = 2$, $h = 1$, and $q = 3$ or 5 . But q cannot be 3 , since V is a nontrivial odd group, and $|V| \mid q^2 - 1$. Thus $q = 5$. Now (g) implies that $|C| \leq 8$, and so $4|P|/|V|^{(3/2)} \leq 4 \cdot 2 \cdot 8/25^{(3/2)} < 1$.

Finally, suppose that $n = 1$. Recalling that $P = C$ has a cyclic subgroup of index at most two, by Step 2, and using (II.3.6), we find that $|K||P|/2 \leq q^{fh}$. Since $|V| \geq 3$, we have

$$4|P| \leq (8/3)q^{fh} = (8/3)|V|.$$

Now (i) follows unless $|V| < 8$. Since q is odd, V is

one-dimensional. Since P and K are nontrivial, the only possibility is $|V| = 7$ and $|K| = 3$. Now $|P| \leq 2$, and $4|P| \leq 7^{(3/2)}$, as required.

This completes the proof of Step 5 and of (III.3.6).

We conclude this section with a simple corollary of (III.3.6) (which could be proved along the lines of (III.1.7)).

(III.3.7) Assume Hypotheses (III.1.4). Suppose further that $q^f - 1$ is not a power of p . Then

- (i) $4|P| \leq |V|^{(3/2)}$, and
- (ii) $2|P| \leq |V|$ if p is odd.

Proof. As in the proof of (III.1.7), we may assume that V_p is irreducible. Since $q^f - 1$ is not a power of p , there exists a prime r dividing $q^f - 1$, where $r \neq p$.

But now the group $P \times Z_r$ acts naturally and faithfully on V , so with Z_r in place of K , we may apply (III.3.6) to deduce the required result.

III.4. PREPARATIONS FOR THEOREM B

The proof of Theorem B has, unsurprisingly, a lot in common with the proof of Theorem A(ii) of [15], except that we use our Theorem A in place of Theorem A(i) of [15]. We need four lemmas from [15], starting with two simple results on $\text{codim}([V, G])$ (where V is a G -module).

(III.4.1) Let U be a subgroup of a group G . Let F be a field, let U be a FU -module, and let $V = U^G$. Then $\text{codim}([V, G]) \geq \text{codim}([U, U])$.

Proof [15, 2.2(b)].

(III.4.2) Let P be a p -group, let F be a field of characteristic p , and let V be a FP -module. Then $\text{codim}([V, P]) \geq (\dim(V))/|P|$.

Proof [15, 2.4].

Next, we have a well-known result on choosing a 'nice' set of double coset representatives which will be used in the induced case of Theorem B.

(III.4.3) Let $G = NH$ be the semi-direct product of a normal Hall p' -subgroup N with a Sylow p -subgroup H . Let S/T be a normal p' -section of G (that is, $S, T \in G$ and $T \triangleleft S$) which is complemented in G by a subgroup M , and let

P be a p-subgroup of M. Then it is possible to find a set $\{a_1, \dots, a_m\}$ of double coset representatives for M and P in G which satisfy the following conditions.

- (i) $a_1 = 1$.
- (ii) $P \cap M^{a_i} = C_P(a_i)$ for $1 \leq i \leq m$.
- (iii) $\{a_1^T, \dots, a_m^T\}$ is a complete set of distinct representatives for the orbits of P permuting the elements of S/T by conjugation.

Proof [15, 3.1].

In the proof of Theorem B(i) - i.e., the nilpotent length case - we need the following result in place of (III.2.5).

(III.4.4) Let \mathcal{K} be a soluble p' -group, and let P be a p-group acting on \mathcal{K} . Let $l = l(\mathcal{K})$, and assume that for every proper subgroup H of $\mathcal{K}P$ containing P we have $l(H \cap \mathcal{K}) < l$. Then \mathcal{K} contains a characteristic subgroup Q which is a special q -group for some prime q . Further, $Q/\mathcal{O}(Q)$ is a chief factor of $\mathcal{K}P$ and $l(\mathcal{K}/\mathcal{O}_p(\mathcal{K}/\mathcal{O}(Q))) = l-1$.

Proof [15, 5.2].

Note The group Q in (III.4.4) is in fact the penultimate term in the lower nilpotent series of \mathcal{K} , which is defined in an analogous way to the upper nilpotent series we mentioned in (T.1).

Next, we state a lemma of Hall and Higman.

(III.4.5) Let V be an irreducible G -module over a field of characteristic p . Suppose that N is a normal subgroup of G whose index is a power of p . If V_N is homogeneous, then V_N is irreducible.

Proof [12, 2.2.3].

The last result of this section concerns numbers of orbits. It will be used in the induced case of Theorem B. We assume the truth of Theorem A to prove it.

(III.4.6) Assume that Theorem A holds. Let p and q be distinct primes, let V be a soluble p' -group and let P be a p -group acting on V . Suppose that V is an irreducible \mathbb{F}_q^{KP} -module faithful for V . Let $d = d(V)$ and suppose that P has m orbits on V . Then $m \geq 3^{1(d+1)}$.

Proof Assume firstly that $d \geq 5$. Then by Theorem A we have

$$|P|^2 \cdot 4 \cdot 3^{d-4} \leq |V|,$$

whence

$$|V|/|P| \geq \sqrt{4 \cdot 3^{d-4} \cdot |V|}.$$

Now $m \geq |V|/|P|$, and $|V| \geq 9$ by (III.3.3), so $m \geq 6 \cdot 3^{\frac{1}{2}d-2}$,

and since $d \geq 5$, we have $\frac{1}{2}d \geq \frac{1}{2}(d+1) + \frac{1}{2}$, so

$$m \geq 6 \cdot 3^{\frac{1}{2}(d+1) - \frac{1}{2}} \geq (6/3\sqrt{3}) \cdot 3^{\frac{1}{2}(d+1)} \geq 3^{\frac{1}{2}(d+1)},$$

as required.

Next suppose that $d = 4$. As above, we obtain from Theorem A, the inequality $m \geq 2\sqrt{|V|}$. If $|V| > 9$, we have $m > 6$, whence $m \geq 7 > 3^{(5/3)}$, as required. If $|V| \leq 9$, we must have $|V| = 9$ by (III.3.3), and since $d = 4$, we must in fact have $V = \text{GF}(2,3)$, so that $P = 1$. But then $m \geq 9$, and we are done.

If $d = 3$, then Theorem A tells us that $m \geq \sqrt{3|V|}$, and since $|V| \geq 9$, we have $m \geq 3^{1/2} \geq 3^{1/3}$, as required.

Finally, suppose that $d = 1$ or 2 . Here we only need to show that $m \geq 3$. We assume that $m = 2$ and derive a contradiction.

In this case, P has one orbit of length 1 (consisting of the zero in V), and one of length $|V| - 1$. (Note that $V \neq 0$ since $P \neq 1$.) Thus

$$p^t = q^r - 1,$$

where $r = \dim(V)$ and t is some integer.

If $p = 2$, then by (III.1.3), either $q^r = 9$, or $r = 1$. If $q^r = 9$, then $|V|$ divides 48, the order of $\text{GF}(2,3)$, whence K is a 3-group. But K acts completely reducibly on V , so $K = 1$, a contradiction. If $r = 1$, then since $p^t = q - 1 = |\text{GF}(1,q)|$, we again have $K = 1$.

If $p > 2$, then since $K \neq 1$, we can apply (III.3.5(ii)) to conclude that $2|P| \leq |V|$. Now $m = 2$, so we must have $2|P| = |V|$. But q and p are distinct primes, so we must have $P = 1$, and $|V| = 2$; thus $K = 1$, the final contradiction.

CHAPTER IV

THE PROOFS OF THEOREMS A AND B

We restate Theorem A. It is useful, for inductive arguments, to add some more details to the statement that appears in Chapter I.

THEOREM A. Let p and q be distinct primes. Let K be a soluble p' -group, and let P be a p -group acting on K . Let V be an irreducible $\mathbb{F}_q KP$ -module faithful for KP . Let $G = KP$ and put $d = d(K)$.

Then $|V|/|F|^2 \geq \max\{4, 4 \cdot 3^{d-4}\}$ unless either

(i) $d \leq 2$, or

(ii) $d = 3$ and $p = 5$, when $|V|/|F|^2 \geq 3$.

(IV.1) EXAMPLES. Before proving Theorem A we discuss briefly some of the examples that make the 'exceptions' (i) and (ii) necessary.

(i) Let E be an extraspecial group of order 32. Let Z be a cyclic group of order 15. Then Z acts faithfully on $E/Z(E)$, and we can form the semi-direct product $G = EZ$. Let V be the (normal) subgroup containing E of index 5 in G , and let P be a Sylow 5-subgroup of G . Then $G = KP$, and $d(K) = 3$.

By (II.3.5), the group E has a faithful, irreducible representation of dimension 4 over the field \mathbb{F}_3 . It is well-known that this representation may be extended to a faithful irreducible representation for G . If V is the vector space of dimension 4 over \mathbb{F}_3 , we now have the hypotheses of Theorem A, with $p = 5$ and $q = 3$.

Further, $d(K) = 3$, and $|V|/|P|^2 = 81/25 < 4$.

There are various other, similar examples where K is extraspecial of order 8, 27, or 32, (so that $d(K) = 2$) and $|V|/|P|^2 < 4$.

(ii) Let \mathbb{F} be the field of 3 elements, and let $\mathbb{E} > \mathbb{F}$ be the field of 3^5 elements.

Let C be the cyclic subgroup of \mathbb{E}^\times of order 56. Let $D = \text{Gal}(\mathbb{E}:\mathbb{F})$, a cyclic group of order 6. Then D acts naturally on \mathbb{E}^\times , and hence on C . Let G be the semi-direct product CD . Let C_7 be the subgroup of C of order 7, and D_3 the subgroup of D of order 3. We claim that $C_7 D_3$ is normal in G . Certainly C_7 is normal in G (since $C_7 = O_7(G)$). Also, D_3 is normalised by D . It therefore suffices to show that D_3 is normalised by C_8 , the subgroup of C of order 8. Now C_8 is normal in G , and so D_3 acts on C_8 . But the automorphism group of C_8 is $\mathbb{Z}_2 \times \mathbb{Z}_2$, so D_3 in fact centralises C_8 , whence D_3 is normalised by C_8 , as required.

Now put $K = C_7 D_3$, and let P be a Sylow 2-subgroup of G . Then G is the semi-direct product of K and P . Using (II.3.8), it is clear that K is nonabelian, so that $d(K) = 2$. Also $|P| = 16$.

Next, we may regard \mathbb{E} as a vector space V of dimension 6 over \mathbb{F} , and we have a natural action of G on V . (Elements of C act according to the multiplication in \mathbb{E} , and D acts naturally on \mathbb{E} because $D = \text{Gal}(\mathbb{E}:\mathbb{F})$.) It is easily checked that this makes V into a faithful, irreducible

KP -module which satisfies the hypotheses of Theorem A.

We have $d(K) = 2$, and $|V|/|P|^2 = 3^6/16^2 < 3$.

There are similar examples to this with different numbers.

Our third example shows that once we have V, K, P, p , and q satisfying the hypotheses of Theorem A with $d(K) = d$ (say) and $|V|/|P|^2 < p^{2/(p-1)}$, we can then construct another example (consisting of module V^* and group V^*P^*) which also satisfies the hypotheses of Theorem A, where $d(P^*) = d$, and $|V^*|/|P^*|^2$ is as small as we like.

Note in particular that in Example (ii) we have $d = 2$, and $|V|/|P|^2 < 3 < p^{2/(p-1)} = 4$, so that there are examples which satisfy the hypotheses of Theorem A with $d(K) = 2$ and $|V|/|P|^2$ arbitrarily small.

(iii) Let V_1, K_1, P_1, p and q satisfy the hypotheses of Theorem A, and suppose that $|V_1|/|P_1|^2 = b_1 < p^{2/(p-1)}$.

Let V_2 be the direct sum of p copies of V_1 . Then V_1 may naturally be regarded as a faithful, irreducible module for the (regular) wreath product $G_2 = K_1 P_1 \wr_{\mathbb{Z}_p}$. Let K_2 be the normal subgroup of G_2 isomorphic to the direct product of p copies of K_1 . Let P_2 be the subgroup $P_1 \wr_{\mathbb{Z}_p}$ of G_2 . Then V_2, K_2, P_2, p and q satisfy the hypotheses of Theorem A, and $d(K_2) = d(K_1)$. Note that $b_2 = |V_2|/|P_2|^2 = |V_1|^p/|P_1|^{2p} \cdot p^2 = (b_1)^p/p^2 = b_1 \cdot (b_1)^{p-1}/p^2$, and since $b_1 < p^{2/(p-1)}$, we have $b_2 < b_1$.

This process may be repeated to obtain modules V_1, V_2, V_3, \dots and groups $K_1 P_1, K_2 P_2, K_3 P_3, \dots$ which

each satisfy the hypotheses of Theorem A. It is easily shown that $b_i = |V_i|/|P_i|^2 \rightarrow 0$ as $i \rightarrow \infty$.

The Proof of Theorem A.

The proof is by induction on $|G|$. Since the theorem is trivial when $d \leq 2$, we assume that $d \geq 3$.

Firstly, we tackle the induced case, in Steps 1 and 2. Here, we assume that there is a normal subgroup N of G , contained in K , and such that V_N is not homogeneous. In this case, Clifford's theorem (II.3.2) tells us that $V = U|G$, where U is a module for a proper subgroup M of G , and N contains M . Further, by the transitivity of induction, we can assume that M is a maximal subgroup of G . This is the situation of Steps 1 and 2.

Step 1. The induced case with $M \gg K$.

It is convenient to define the real number w by

$$w = \begin{cases} 3 & \text{if } d=3 \text{ and } p=5, \\ 4 & \text{if } d=3 \text{ and } p \neq 5, \\ 4.3^{d-4} & \text{if } d \geq 4. \end{cases}$$

We need to show that $w|U|^2 \leq |V|$.

Since M is maximal in KP and P is a p -group, we have $M = KP_0$ where P_0 is a normal subgroup of index p in P . Since $V = U|G$, we therefore have

$$V_{KP_0} = Ux_1 \oplus \dots \oplus Ux_p,$$

for suitable x_1, \dots, x_p in P . We wish to apply induction to the Ux_i : to this end we set $K_i = \ker(K \text{ on } Ux_i)$ and $P_i = \ker(P_0 \text{ on } Ux_i)$. It is easily checked that $K_i = \pi_1^{x_i}$ so the groups K/K_i are all isomorphic to one another.

Also, $\bigcap_{1 \leq i \leq p} K_i = 1$ since V is faithful for K .

Thus, using (I.3.2(ii)), we have

$$d = d(K) = \max_{1 \leq i \leq p} d(K/K_i) = d(K/K_1)$$

for $1 \leq i \leq p$. Induction applied to the Ux_i therefore yields

$$w|P_0/P_i|^2 \leq |Ux_i| = |U|. \quad (a)$$

As in Step 1 of the proof of (III.3.6), we have

$|P_0/P_1| \times \dots \times |P_0/P_p| \geq |P_0|$, so (a) becomes

$$w^p |P_0|^2 \leq |U|^p = |V|,$$

whence

$$(w^{p-1}/p^2) \cdot w |P|^2 \leq |V|. \quad (b)$$

The required bound follows immediately from (b)

as soon as we know that $p^2/w^{p-1} \leq 1$.

If $p=5$ and $d=3$, then $p^2/w^{p-1} \leq 25/3^4 < 1$. Thus we may assume that $w \geq 4$. If $p=2$, then $p^2/w^{p-1} = 4/w \leq 1$, and if $p \geq 3$, we can use (III.1.1) to deduce that

$p^2/w^{p-1} \leq 4p^2/4^p \leq 4 \cdot 3^2/4^3 < 1$. This completes Step 1.

Step 2. The induced case with $M \not\leq K$.

To complete the induced case we assume that $M \not\leq K$. Then $G = MK$ by the maximality of M , and thus $|G| = |M| |K| / |K \cap M|$, whence $|P|$ divides $|M|$. Thus a Sylow p -subgroup of M is also one of G , and so M contains a conjugate of P .

Replacing M by a conjugate if necessary, we can assume that $M \geq P$.

Let $T = \text{Core}_G(M)$ and apply (II.4.2). This tells us that there is a unique minimal normal subgroup S/T say, of G/T ; that M complements S/T in G ; and that $C_G(S/T) = S$. Since M complements S/T in G we have $|G:M| = |S/T|$, and because $M \triangleright P$, we know that $|S/T|$ is coprime to p . Since S/T is a minimal normal subgroup, it is in fact an elementary abelian r -group for some prime r say, where $r \neq p$.

The group K is a Hall p' -subgroup of MP ; thus K^T/T is a Hall p' -subgroup of G/T . Since S/T is a normal p' -subgroup of G/T , we have $S \leq K^T$. Now $(K \cap S)^T = K^T \cap S$ since $T \leq S$, and because $S \leq K^T$, we have $(K \cap S)^T = S$. Now $K \cap S / K \cap T \cong_{\nu_P} (K \cap S)^T / T$ by an isomorphism theorem, and so

$$K \cap S / K \cap T \cong_{\nu_P} S/T.$$

Now we define a normal subgroup P^* of P by

$$P^* = C_P(S/T) = C_P(K \cap S / K \cap T).$$

Next, let j denote the derived length of $K/C_P(S/T)$, the group of automorphisms that K induces on S/T . We regard S/T as an $\mathbb{F}_r K/P$ -module and by induction deduce that

$$|P/P^*|^{2w(j)} \leq |S/T| \quad \text{or} \quad j \leq 2, \quad (c)$$

where $w(j) = \max\{3, 4 \cdot 3^{j-4}\}$ ($j < d$), and $w(d) = w$.

We turn our attention to the M -module U . Since $P \leq M$, we have $M = (K \cap M)P$. We aim to show that P^* acts faithfully on U and that $K \cap M$ induces on U a group of derived length at least $d - 1 - j$.

Firstly, we note that since $C_G(S/T) = S$, we have $C_P(S/T) = C_P(S \cap K / T \cap K) = S \cap K$, so that $S \cap K / T \cap K$ is self-centralising in $K/K \cap T$. Now P^* centralises $S \cap K / T \cap K$ and so by (II.1.5), the group P^* centralises $K/K \cap T$.

Let $g \in K$. Then $(K \cap M)g^a = (K \cap M)g$ for all $a \in P^*$, since

$K \cap M \geq K \cap T$. So we can apply (II.1.1) with K in place of G , $K \cap K$ in place of H , and P^* in place of A to find a set of coset representatives $\{x_1, \dots, x_s\}$ say, for $M \cap K$ in K which are centralised by P^* . Clearly we may assume that $x_1 = 1$. Now x_1, \dots, x_s is also a set of coset representatives for M in G , so

$$V = Ux_1 \oplus \dots \oplus Ux_s,$$

and

$$s = |G:M| = |S/T|.$$

Since P^* centralises $K/K \cap T$, it is easily shown that $(K \cap T)P^* \leq G$. Since $(K \cap T)P^* \leq K$, each of the Ux_i ($1 \leq i \leq s$) is a $(K \cap T)P^*$ -module. Further, since each x_i is centralised by P^* , we have $U \cong_{P^*} Ux_i$ ($1 \leq i \leq s$). Because V is faithful for P^* , it now follows that U is faithful for P^* .

Now, since $K \cap T$ is normal in G , it follows by a similar argument to that used in Step 1 that $K \cap T$ induces on U a group of derived length equal to $d(K \cap T)$. Also,

$$\begin{aligned} d &= d(K) \leq d(K \cap T) + d(K \cap S / K \cap T) + d(K / K \cap S) \\ &\leq d(K \cap T) + 1 + j, \end{aligned}$$

and since $K \cap T \leq K \cap N$, we know that $K \cap N$ induces on U a group of derived length at least $d - 1 - j$.

We can therefore apply induction to the $(K \cap N)P$ -module U to conclude that

$$|P^*|^{2(d-1-j)} \leq |U| \quad \text{or} \quad d-1-j \leq 2 \quad (d)$$

Recall that $s = |S/T| = |G:M|$, so that we have

$$|V| = |U|^s. \quad (e)$$

We now begin the arithmetic, using (c), (d), and (e).

We divide the argument into the four cases given by (c) and (d).

$j > 2, d-1-j > 2$. Here, we have $s \geq 9$ and $|U| \geq 9$ by (III.3.3). From (c), (d), and (e),

$$w(d)|P|^2/|V| \leq (w(d)/w(j) \cdot w(d-1-j)) \cdot s \cdot |U|^{1-s}.$$

Now $w(d)/w(j) \leq 3^{d-j}$ and $w(d-1-j) \geq 4 \cdot 3^{d-j-5}$, so

$$\begin{aligned} w(d)|P|^2/|V| &\leq (3^5/4) \cdot s \cdot |U|^{1-s} \\ &\leq (3^7/4)(s/9^s), \end{aligned}$$

using the fact that $|U| \geq 9$. But now, using (III.1.1), we have $s/9^s \geq 9/9^9$, and so we have $w(d)|P|^2/|V| \leq 1$, as required.

$j > 2, d-1-j \leq 2$. We still have $s \geq 9$, and still obtain a bound for $|P/P^*|$ from (c); but we need a replacement for (d). Recall that $U \geq N$, where N is a normal subgroup of G , contained in K such that V_N is not homogeneous. We thus have $N \neq 1$, and $N \leq V \cap \text{Core}_G(M) = K \cap M$, whence $K \cap M \neq 1$. It now follows that $V \cap M$ acts nontrivially on U , and we can apply (III.3.6) to the U -module U to deduce that

$$\left. \begin{aligned} 4|P^*| &\leq |U|^{(3/2)} \text{ and } \\ 2|P^*| &\leq |U| \text{ if } p \neq 2. \end{aligned} \right\} \quad (f)$$

From (c), (e), and (f),

$$w(d)|P|^2/|V| \leq (w(d)/w(j)) \cdot s \cdot (1/16) \cdot |U|^{3-s}.$$

Because $d-j \leq 3$, we have $w(d)/w(j) \leq 27$, so

$$w(d)|P|^2/|V| \leq (27/16) \cdot s \cdot |U|^{3-s}.$$

Since $K \cap M$ acts nontrivially on U , we must have $|U| \geq 3$.

Thus

$$w(d)|P|^2/|V| \leq (27/16)(s/3^{s-3})$$

$$\leq (3^6/16)(9/3^9)$$

$$= 1/48,$$

using (III.1.1) and the fact that $s \geq 9$.

$j \leq 2, d-1-j \geq 2$. Here $|U| \geq 9$ and (d) gives us a bound for $|P^*|$, but we need a replacement for (c). Now $|P/P^*|$ acts faithfully on the module S/\mathfrak{T} , and so by (III.1.7) we have

$$|P/P^*| \leq 1.s^{(5/3)}. \quad (c')$$

We assume firstly that s is at least 4. From (d), (e), and (c'),

$$w(d)|P|^2/|V| \leq (w(d)/w(d-1-j))|U|^{1-s} \cdot 1.s^{(10/3)}.$$

Since $j \leq 2$, we have $w(d)/w(d-1-j) \leq 27$, and using $|U| \geq 9$ we have

$$w(d)|P|^2/|V| \leq (3^5/4)(s^{31}/9^s),$$

and since $s \geq 4$, we have $s^{31}/9^s \leq 4^{31}/3^8$. Thus

$$w(d)|P|^2/|V| \leq 4^{21}/27, \text{ and we are done, since } 4^{21} < 27.$$

Secondly, suppose that $s = 3$. Now we must have $j \leq 1$, and $|P/P^*| \leq 2$, so

$$\begin{aligned} w(d)|P|^2/|V| &\leq (w(d)/w(d-1-j))|U|^{-2} \cdot 2^2 \\ &\leq 9 \cdot 4/9^2 \\ &< 1. \end{aligned}$$

Finally suppose that $s = 2$. Now $j = 0$ and $P = P^*$, so

$$\begin{aligned} w(d)|P|^2/|V| &\leq (w(d)/w(d-1-j))|U|^{-1} \\ &\leq 3 \cdot 3^{-1} \\ &= 1. \end{aligned}$$

$j \leq 2, d-1-j \leq 2$. Here we know that $|U| \geq 3$ and we have bounds (f) and (g). Also, $d \leq 5$, so $w(d) \leq 12$. We need to

consider several possibilities for s , and start off with the case $s \geq 8$.

Suppose that $s \geq 8$. From (e), (f), and (g),

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 12.4 \cdot s^{3j} \cdot (1/16) \cdot |U|^{3-s} \\ &\leq (12.27/4 \cdot 16) (s^{3j} / 3^s) \\ &\leq (81/16) (8^{3j} / 3^8) \\ &= 2^5 / 3^4 \\ &< 1, \end{aligned}$$

using the fact that $|U| \geq 3$, and (III.1.1).

Suppose that $s = 5$ or 7 . Now $j \leq 1$, so $d \leq 4$, and thus $w(d) \leq 4$. Also, $|P/P^*| \leq 4$. Thus

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot 4^2 \cdot (1/16) \cdot |U|^{-2} \\ &\leq 4/3^2 \\ &< 1. \end{aligned}$$

Suppose that $s = 4$ and $j = 2$. Here, P must act trivially on S/P , so $P = P^*$. Thus

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 12 \cdot (1/16) \cdot |U|^{-1} \\ &< 1. \end{aligned}$$

Suppose that $s = 4$, and $j \leq 1$. Here $|P/P^*| \leq 3$, and $w(d) \leq 4$, so

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot 9 \cdot (1/16) \cdot |U|^{-1} \\ &\leq 4 \cdot 9 / 16 \cdot 3 \\ &< 1. \end{aligned}$$

Suppose that $s = 3$. Here, $|P/P^*| \leq 2$, and $j \leq 1$, so that $w(d) \leq 4$. Thus

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot 4 \cdot (1/16) \\ &= 1. \end{aligned}$$

Finally, suppose that $s = 2$. Now $P = P^*$, and $j = 0$. Further, $p \neq 2$, so from (E), we have $|P^*| \leq |U|$, and

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot 1 \cdot |U|^2 / |V| \\ &= 1. \end{aligned}$$

consider several possibilities for s , and start off with the case $s \geq 8$.

Suppose that $s \geq 8$. From (e), (f), and (g),

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 12 \cdot 4 \cdot s^{31} \cdot (1/16) \cdot |U|^{3-s} \\ &\leq (12 \cdot 27 / 4 \cdot 16) (s^{31} / 3^8) \\ &\leq (81/16) (8^{31} / 3^8) \\ &= 2^5 / 3^4 \\ &< 1, \end{aligned}$$

using the fact that $|U| \geq 3$, and (III.1.1).

Suppose that $s = 5$ or 7 . Now $j \leq 1$, so $d \leq 4$, and thus $w(d) \leq 4$. Also, $|P/P^*| \leq 4$. Thus

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot 4^2 \cdot (1/16) \cdot |U|^{-2} \\ &\leq 4/3^2 \\ &< 1. \end{aligned}$$

Suppose that $s = 4$ and $j = 2$. Here, P must act trivially on S/P , so $P = P^*$. Thus

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 12 \cdot (1/16) \cdot |U|^{-1} \\ &< 1. \end{aligned}$$

Suppose that $s = 4$, and $j \leq 1$. Here $|P/P^*| \leq 3$, and $w(d) \leq 4$, so

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot 9 \cdot (1/16) \cdot |U|^{-1} \\ &\leq 4 \cdot 9 / 16 \cdot 3 \\ &< 1. \end{aligned}$$

Suppose that $s = 3$. Here, $|P/P^*| \leq 2$, and $j \leq 1$, so that $w(d) \leq 4$. Thus

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot 4 \cdot (1/16) \\ &= 1. \end{aligned}$$

Finally, suppose that $s = 2$. Now $P = P^*$, and $j = 0$. Further, $p \neq 2$, so from (e), we have $|P^*| \leq \frac{1}{2}|U|$, and

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot \frac{1}{2} |U|^2 / |V| \\ &= 1. \end{aligned}$$

This completes Step 2 and therefore the induced case. So from now on, we assume that if N is any normal subgroup of G contained in K , then V_N is homogeneous.

Step 3. The homogeneous case.

In particular, we now know that every abelian normal subgroup of G contained in K is cyclic, so we have the hypotheses for (III.2.5). Thus there is a normal subgroup R of G , contained in K , with the following properties.

- (i) R is either extraspecial or the central product of an extraspecial 2-group with a cyclic group of order 4.
- (ii) $\bar{R} = R/Z(R)$ is a chief factor of G .
- (iii) $d(K/C_G(\bar{R})) \geq d-2$.

Next, we show that $C_P(R) = C_P(\bar{R})$. If R is extraspecial, then $Z(R) = \langle R \rangle$, and this follows from (II.1.7). Otherwise, R is a 2-group, and $Z(R)$ is cyclic of order 4. Thus the automorphism group of $Z(R)$ is Z_2 , and so P centralises $Z(R)$. Thus, by (II.1.3), the group $C_P(\bar{R})$ centralises R .

We now set up some notation that we shall use throughout the rest of the proof. Put $P_1 = C_P(R) = C_P(\bar{R})$. By (II.2.4), the number $|\bar{R}|$ is the square of some prime power, so we can put $s^2 = |\bar{R}|$, where s is a prime power. We let f be the dimension of an irreducible $Z(R)$ -submodule of V , and suppose that V_P has h irreducible summands. By (II.3.11), the dimension of V is sfh . Thus

$$|V| = q^{sfh}. \quad (h)$$

If $W \subseteq V_P$ is irreducible, then (II.3.11) tells us that $|\text{Hom}_{\mathbb{F}_q P}(W, W)| = q^f$. Now, by (III.3.2), applied with P_1 in place of P , we obtain

$$P_1 \in \text{GL}(h, q^f). \quad (j)$$

Since $q^f - 1$ is divisible by $|Z(F)|$, we know that $q^f - 1$ is not a power of p . Thus (III.3.7) tells that

$$\left. \begin{aligned} |P_1| &\leq \frac{1}{2}q^{(3/2)hf} \quad \text{and} \\ |P_1| &\leq \frac{1}{2}q^{hf} \quad \text{if } p \neq 2. \end{aligned} \right\} \quad (k)$$

It is now convenient to consider two cases: $d \geq 5$ and $d < 5$.

$d \geq 5$. Here, we have $d - 2 \geq 3$, and we may therefore apply induction to the $F_{p^d} \mathbb{K}P$ -module \bar{P} to conclude that

$$w(d-2) |P/P_1|^2 \leq s^2. \quad (l)$$

From (h), (k), and (l),

$$\begin{aligned} w(d) |P|^2 / |V| &\leq (w(d)/w(d-2)) \cdot s^2 \cdot (1/16) \cdot q^{(3-s)hf} \\ &\leq (9/16) \cdot s^2 / q^{hf(s-3)}. \end{aligned} \quad (m)$$

Suppose that $s \geq 7$. Using the fact that $q^{fh} \geq 3$ (since $|Z(R)|$ divides $q^f - 1$), we have

$$\begin{aligned} w(d) |P|^2 / |V| &\leq (9/16) \cdot s^2 / 3^{s-3} \\ &\leq 9 \cdot 27 \cdot 49 / 3^7 \\ &< 1, \end{aligned}$$

using (III.1.1).

Suppose that $s = 5$. Now $|Z(R)| = 5$, so $q^{fh} \geq 11$, and the required bound is immediate from (m).

Suppose that $s = 4$. Now (III.3.4(iv),(v)) implies that $P = P_1$ and $d \leq 5$. Thus $w(d) \leq 12$, and since $p \neq 2$, we have $|P_1| \leq \frac{1}{2}q^{hf}$ by (k). So

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 12 \cdot \frac{1}{4} \cdot q^{2hf} / q^{4hf} \\ &\leq 3 / 3^2 \\ &< 1. \end{aligned}$$

Suppose that $s = 3$. By (III.3.5), we have $d \leq 5$, and $P = P_1$, so

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 12 \cdot (1/16) \cdot q^{3hf} / q^{3hf} \\ &= \frac{3}{4}. \end{aligned}$$

We cannot have $s \leq 2$ when $d - 2 \geq 3$, so the case $d \geq 5$ is finished.

$d < 5$. Here, we have $d = 3$ or $d = 4$. We cannot (usefully) apply induction to \bar{P} , but since $d - 2 \geq 1$, we do know that K acts nontrivially on \bar{P} . Thus we can apply (III.3.6) to the $\mathbb{F}_p K P$ -module \bar{P} to deduce that

$$|P/P_1| \leq \begin{cases} \frac{1}{2}s^3, & \text{and} \\ \frac{1}{2}s^2 & \text{if } p \neq 2. \end{cases} \quad (n)$$

Also, we note that $w(d) \leq 4$, so from (h), (k), and (n),

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot (1/16) \cdot s^6 \cdot (1/16) \cdot q^{hf(3-s)} \\ &\leq s^6 / 64 q^{hf(s-3)}. \end{aligned} \quad (p)$$

If $s \geq 10$, the required bound follows from (p), using (III.1.1).

Suppose that $s = 13, 11$, or 7 . Here $q^{fh} \geq 8$, and the required bound is immediate from (p).

Suppose that $s = 9$. If $q^{fh} \geq 5$, then (p) implies that $w(d) |P|^2 / |V| \leq 1$, so we may assume that $q^{fh} \leq 4$. But 3 divides $q^f - 1$, so we must in fact have $q = 2$, $h = 1$, and $f = 2$. Going back to (k), this tells us that $P_1 = 1$. Since $q = 2$, we know that $p \neq 2$, so using (h) and (n),

$$\begin{aligned} w(d) |P|^2 / |V| &\leq 4 \cdot \frac{1}{16} \cdot 9^4 / 4^9 \\ &\leq 1. \end{aligned}$$

Suppose that $s = 8$. We can obtain the required bound from (p) unless $h = 1$, $f = 1$, and $q = 3$. Now (k) implies that $P_1 = 1$; and $p \neq 2$ since 2 divides s . Thus

$$w(d) |P|^2 / |V| \leq 4 \cdot 1 \cdot 8^4 / 3^8$$

$$< 1.$$

Suppose that $s = 5$. If $q^{fh} > 16$, then (p) gives us the required bound, so we can assume that $q = 11$, $h = 1$, and $f = 1$. Now (j) implies that $|E_1| \leq 2$, and so

$$w(d) |P|^2 / |V| \leq 4 \cdot (1/16) \cdot 5^6 \cdot 4 / 11^5$$

$$< 1.$$

Suppose that $s = 4$. If $d = 4$, or $p \neq 5$, then (III.3.4(ii), (iii)) implies that $|P/P_1| \leq 3$; also $p \neq 2$, so

$$w(d) |P|^2 / |V| \leq 4 \cdot 9 \cdot 1 \cdot q^{2hf} / q^{4hf}$$

$$\leq 9 / 3^2$$

$$= 1.$$

If $d = 3$ and $p = 5$, then $w(d) = 3$. By (III.3.4(i)), we have $|P/P_1| \leq 5$. Thus

$$w(d) |P|^2 / |V| \leq 3 \cdot 25 \cdot 1 / q^{2fh},$$

and this gives us the required bound unless $q = 3$, $f = 1$, and $h = 1$. But in this case, (j) implies that $P_1 = 1$, so we have $w(d) |P|^2 / |V| \leq 3 \cdot 25 / 3^4 < 1$.

Suppose that $s = 3$. Now (III.3.5) tells us that $P = P_1$, and

$$w(d) |P|^2 / |V| \leq 4 \cdot (1/16) \cdot q^{3fh} / q^{3fh}$$

$$= 1.$$

Finally, suppose that $s = 2$. Since K acts nontrivially on \bar{K} , and $p \neq 2$, we must have $P = P_1$. Thus

$$w(d) |P|^2 / |V| \leq 4 \cdot 1 \cdot q^{2hf} / q^{2hf}$$

$$= 1.$$

This completes the proof of Theorem A.

For convenience, we restate Theorem B.

THEOREM B. Let p be a prime. Let K be a soluble
 p' -group and let P be a p -group acting on K . Let V be a
nonzero \mathbb{F}_p^{KP} -module faithful for K . Let $l = l(K)$ and
 $d = d(K)$. Then

- (i) $\text{codim}[V, P] \geq 3^{1(1-3)} \geq 1$, and
(ii) $\text{codim}[V, P] \geq [3^{1(d-4)}] \geq 1d$.

The proofs of (i) and (ii) are very similar. We prove (i) in detail, and then go through the proof of (ii) more quickly. The inequalities $3^{1(1-3)} \geq 1$ and $[3^{1(d-4)}] \geq 1d$ are easily checked using (III.1.1), and $\text{codim}[V, P]$ is obviously an integer, so it suffices to prove that $\text{codim}[V, P] \geq 3^{1(1-3)}$ and $\text{codim}[V, P] \geq [3^{1(d-4)}]$.

Proof of (i).

The proof is by induction on $\dim(V) + |KP|$. We may clearly assume that $l \geq 4$.

Step 1. V is irreducible.

Let $Q = I_{l-1}(K)$, the penultimate term in the lower nilpotent series of K . The group Q has the following property (as is easily checked using (I.3.2(ii))): if N is any normal subgroup of K , then $l(K/N) \geq l-1$ if and only if $N \not\leq Q$.

Since V is faithful, $C_V(Q) < V$, and because $Q \trianglelefteq KP$, the vector space $C_V(Q)$ is a KP -module. Thus we can

For convenience, we restate Theorem B.

THEOREM B. Let p be a prime. Let K be a soluble
 p' -group and let P be a p -group acting on K . Let V be a
nonzero \mathbb{F}_p^{KP} -module faithful for K . Let $l = l(K)$ and
 $d = d(K)$. Then

- (i) $\text{codim}[V, P] \geq 3^{1(1-3)} \geq 1$, and
(ii) $\text{codim}[V, P] \geq [3^{1(d-4)}] \geq 1d$.

The proofs of (i) and (ii) are very similar. We prove (i) in detail, and then go through the proof of (ii) more quickly. The inequalities $3^{1(1-3)} \geq 1$ and $[3^{1(d-4)}] \geq 1d$ are easily checked using (III.1.1), and $\text{codim}[V, P]$ is obviously an integer, so it suffices to prove that $\text{codim}[V, P] \geq 3^{1(1-3)}$ and $\text{codim}[V, P] \geq [3^{1(d-4)}]$.

Proof of (i).

The proof is by induction on $\dim(V) + |KP|$. We may clearly assume that $l \geq 4$.

Step 1. V is irreducible.

Let $Q = I_{l-1}(K)$, the penultimate term in the lower nilpotent series of K . The group Q has the following property (as is easily checked using (I.3.2(ii))): if N is any normal subgroup of K , then $l(K/N) \geq l-1$ if and only if $N \not\leq Q$.

Since V is faithful, $C_V(Q) < V$, and because $Q \trianglelefteq KP$, the vector space $C_V(Q)$ is a KP -module. Thus we can

in KP such that $a_1 = 1$ and $M^{B_1} \cap P = C_P(a_1)$. Further, part (iii) of that result tells us that m is the number of orbits of P on the vectors of S/T .

By Mackey's theorem (II.3.4),

$$V_P = U \oplus (Ua_2)_{C_P(a_2)} \Big|_P \oplus \dots \oplus (Ua_m)_{C_P(a_m)} \Big|_P. \quad (a)$$

Set $U_i = (Ua_i)_{C_P(a_i)} \Big|_P$ ($2 \leq i \leq m$). Since a_i is centralised by $C_P(a_i)$, it follows that U is isomorphic to Ua_i as a $C_P(a_i)$ -module. Thus $U_i \cong U_{C_P(a_i)} \Big|_P$, and so by (III.4.1), we have

$$\text{codim}[U_i, P] \geq \text{codim}[U, P].$$

It now follows from (a) that

$$\text{codim}[V, P] \geq m \cdot \text{codim}[U, P]. \quad (b)$$

Let $j = 1(K/K \cap S)$, the nilpotent length of the group that K induces on S/T . As in the proof of Step 3 of Theorem A, the group $K \cap M$ induces on U a group of nilpotent length at least $1 - j - 1$. Therefore, applying induction to the $(K \cap M)P$ -module U gives

$$\text{codim}[U, P] \geq 3^{1-j-1}. \quad (c)$$

Applying (III.4.6) to the KP -module S/T tells us that

$$m \geq 3^{j+1}. \quad (d)$$

From (b), (c), and (d),

$$\text{codim}[V, P] \geq 3^{j(1-3)},$$

as required.

Thus, from now on we can assume that V is not induced from a module for a proper subgroup. In particular, by the usual argument based on Clifford's theorem and (II.3.6), we know that any abelian normal subgroup of KP is cyclic.

Step 3. Q is an extraspecial q -group for some prime q
(with $q \neq p$) and $\bar{Q} = Q/Z(Q)$ is a chief factor of KP such
that $l(K/C_P(\bar{Q})) = 1 - 1$.

If H is a proper subgroup of KP such that $H \triangleright P$
and $l(H \cap K) = 1$, we can apply induction to the H -module
 V to conclude that $\text{codim}[V, P] \geq 3^{1-(1-3)}$, as required.

Thus we can assume that no such H exists, and
(III.4.4) now tells us that Q is a special q -group for
some prime q ; that \bar{Q} is a chief factor of KP ; and that
 $l(V/C_K(\bar{Q})) = 1 - 1$. Since $Z(Q)$ is abelian and normal in
 KP , it is in fact cyclic. Thus Q is either cyclic or
extraspecial. But if Q was cyclic, we would have $1 \leq 2$.
Thus Q is extraspecial, and Step 3 is complete.

Step 4. The final step.

We are now in a position to apply Theorem A to the
 KP -module \bar{Q} . Now $l(V/C_P(\bar{Q})) = 1 - 1$, so $d(V/C_P(\bar{Q})) \geq 1 - 1 \geq 3$.
By Theorem A, therefore,

$$|\bar{Q}|/|P/C_P(\bar{Q})|^2 \geq \max\{3, 4 \cdot 3^{1-5}\}. \quad (e)$$

Now choose a maximal QP -submodule W of V , so that
 $(V/W)_{QP}$ is irreducible. We show next that
 $C_P(\bar{Q}) = \ker(P \text{ on } V/W)$.

Firstly, note that $C_P(\bar{Q}) = C_P(Q)$, by (II.1.7). By
(III.4.5), the vector space V/W is irreducible as a
 Q -module. Since V_Q is homogeneous, V/W is faithful for
 Q . It follows that $\ker(P \text{ on } V/W) \leq C_P(Q)$. Now consider
 V/W as a $Q \times C_P(Q)$ -module. Since $(V/W)_Q$ is irreducible,
so is $(V/W)_{Q \times C_P(Q)}$. By Clifford's theorem, therefore,

$(V/W)_{C_p(Q)}$ is completely reducible. Since $C_p(Q)$ is a p -group, it must in fact act trivially on V/W , so that $C_p(\bar{Q}) = \ker(P \text{ on } V/W)$, as required.

By (II.3.11), we have $\dim(V/W) \geq \sqrt{|\bar{Q}|}$. Thus (e) implies that

$$\dim(V/W)/|P/\ker(P \text{ on } V/W)| \geq \max\{3^{\frac{1}{2}}, 2 \cdot 3^{\frac{1}{2}(1-5)}\}.$$

Applying (III.4.2) to $(V/W)_P$ now gives us

$$\text{codim}[V/W, P] \geq \max\{3^{\frac{1}{2}}, 2 \cdot 3^{\frac{1}{2}(1-5)}\}. \quad (f)$$

Note that when $l=5$, we cannot have equality here, since this would imply that $|\bar{Q}| = 4$, contradicting the fact that $l(K/C_K(\bar{Q})) = l-1 = 4$. Using this fact, it is now easy to show that (f) implies that

$$\text{codim}[V/W, P] \geq 3^{\frac{1}{2}(1-3)},$$

whence $\text{codim}[V, P] \geq 3^{\frac{1}{2}(1-3)}$, completing the proof of (i).

Proof of (ii).

Again, we proceed by induction on $\dim(V) + |KP|$. Here, we may assume that $d \geq 5$. Most of the proof is identical to that of (i), with nilpotent length replaced by derived length, and $3^{\frac{1}{2}(1-3)}$ replaced by $3^{\frac{1}{2}(d-4)}$ in the appropriate places, and we only comment on the more substantial differences here.

Step 1. V is irreducible.

Let Q be the penultimate term in the derived series for K . The proof then goes as before.

$(V/W)_{G_p(Q)}$ is completely reducible. Since $G_p(Q)$ is a p -group, it must in fact act trivially on V/W , so that $G_p(\bar{Q}) = \ker(P \text{ on } V/W)$, as required.

By (II.3.11), we have $\dim(V/W) \geq \sqrt{|\bar{Q}|}$. Thus (e) implies that

$$\dim(V/W)/|\mathbb{P}/\ker(P \text{ on } V/W)| \geq \max\{3^{\frac{1}{2}}, 2 \cdot 3^{\frac{1}{2}(1-5)}\}.$$

Applying (III.4.2) to $(V/W)_{\mathbb{P}}$ now gives us

$$\text{codim}[V/W, \mathbb{P}] \geq \max\{3^{\frac{1}{2}}, 2 \cdot 3^{\frac{1}{2}(1-5)}\}. \quad (f)$$

Note that when $l=5$, we cannot have equality here, since this would imply that $|\bar{Q}| = 4$, contradicting the fact that $l(K/G_K(\bar{Q})) = l - 1 = 4$. Using this fact, it is now easy to show that (f) implies that

$$\text{codim}[V/W, \mathbb{P}] \geq 3^{\frac{1}{2}(1-3)},$$

whence $\text{codim}[V, \mathbb{P}] \geq 3^{\frac{1}{2}(1-3)}$, completing the proof of (i).

Proof of (ii).

Again, we proceed by induction on $\dim(V) + |\mathbb{P}|$. Here, we may assume that $d \geq 5$. Most of the proof is identical to that of (i), with nilpotent length replaced by derived length, and $3^{\frac{1}{2}(1-3)}$ replaced by $3^{\frac{1}{2}(d-4)}$ in the appropriate places, and we only comment on the more substantial differences here.

Step 1. V is irreducible.

Let Q be the penultimate term in the derived series for K . The proof then goes as before.

Step 2. The induced case.

This is almost identical to Step 2 of the proof of (i).

Step 3. There exists a normal subgroup R of KP , contained in K which is either extraspecial or the central product of an extraspecial 2-group and a cyclic group of order 4. Further, $\bar{R} = R/Z(R)$ is a chief factor of KP , and $d(K/C_K(\bar{R})) \geq d-2$.

By Step 2, normal abelian subgroups of KP are cyclic. Thus Step 3 follows from (III.2.5).

Step 4. The final step.

We apply Theorem A to the KP -module \bar{V} to deduce that

$$|\bar{V}|/|P/C_P(\bar{V})|^2 \geq \max\{3, 4 \cdot 3^{d-5}\}. \quad (g)$$

Note that we have $C_P(\bar{V}) = C_P(R)$. If P is extraspecial, this follows from (II.1.7); if not, it follows from (II.1.3) and the fact that P must centralise $Z(R)$. Now we can deduce exactly as in Step 4 of the proof of (i), that

$$\text{codim}[V, P] \geq \max\{3^{\frac{1}{2}}, 2 \cdot 3^{\frac{1}{2}(d-5)}\} \quad (h)$$

whence $\text{codim}[V, P] \geq 3^{\frac{1}{2}(d-4)}$, where we are using the fact that we cannot have equality in (h) when $d=6$.

This completes the proof of (ii) and therefore of Theorem B.

BIBLIOGRAPHY

- 1 T. R. BERGER, 'Hall-Higman type theorems I', *Canad. J. Math.* 26 (1974), 513-531.
- 2 T. R. BERGER & F. GROSS, '2-length and derived length of a Sylow 2-subgroup', *Proc. London Math. Soc.* 34 (1977), 520-534.
- 3 E. G. BRJUNANOVA, 'The relation between 2-length and derived length of a Sylow 2-subgroup of a finite soluble group' (Russian), *Mat. Zametki* 29 (1981), no. 2, 161-170, 316. English translation: *Math. Notes* 29, no. 1-2, 85-90.
- 4 P. CARTER, 'Nilpotent self-normalising subgroups of soluble groups', *Math. Z.* 75 (1961), 133-139.
- 5 E. C. DADE, 'Carter subgroups and Fitting heights of finite soluble groups', *Illinois J. Math.* 13 (1969), 449-513.
- 6 J. D. DIXON, 'The soluble length of a solvable linear group', *Math. Z.* 107 (1968), 151-158.
- 7 B. FISCHER, M. GASCHÜTZ, B. HARTLEY, 'Injektoren endlicher auflösbarer Gruppen', *Math. Z.* 102 (1967), 337-339.
- 8 M. FRICK, H. F. NEWMAN, 'Soluble linear groups',

BIBLIOGRAPHY

- 1 T. R. BERGER, 'Hall-Higman type theorems I', *Canad. J. Math.* 25 (1974), 513-531.
- 2 T. R. BERGER & F. GROSS, '2-length and derived length of a Sylow 2-subgroup', *Proc. London Math. Soc.* 34 (1977), 520-534.
- 3 E. G. BRJUNANOVA, 'The relation between 2-length and derived length of a Sylow 2-subgroup of a finite soluble group' (Russian), *Mat. Zametki* 29 (1981), no. 2, 151-170, 316. English translation: *Math. Notes* 29, no. 1-2, 85-90.
- 4 R. CARTER, 'Nilpotent self-normalising subgroups of soluble groups', *Math. Z.* 75 (1961), 135-139.
- 5 E. C. DADE, 'Carter subgroups and Fitting heights of finite soluble groups', *Illinois J. Math.* 13 (1969), 449-513.
- 6 J. D. DIXON, 'The soluble length of a solvable linear group', *Math. Z.* 107 (1968), 151-158.
- 7 B. FISCHER, W. GASCHÜTZ, B. HARTLEY, 'Injektoren endlicher auflösbarer Gruppen', *Math. Z.* 102 (1967), 337-339.
- 8 M. FRICK, H. F. NEWMAN, 'Soluble linear groups',

Bull. Austral. Math. Soc. 6 (1972), 31-34.

9 W. GASCHÜTZ, 'Zur Theorie der endlichen auflösbaren Gruppen', Math. Z. 80 (1953), 300-305.

10 ———, 'Lectures on subgroups of Sylow type in finite soluble groups', Notes on Pure Mathematics 11, (Australian National University 1979).

11 D. GORENSTEIN, 'Finite groups' (Harper and Row, New York, 1968).

12 P. HALL, G. HIGMAN, 'On the p -length of p -soluble groups and reduction theorems for Burnside's problem', Proc. London Math. Soc. 6 (1955), 1-40.

13 G. H. HARDY, E. M. WRIGHT, 'An introduction to the theory of numbers' (Oxford University Press, London 1975).

14 T. O. HAWKES, 'On the Fitting length of a finite soluble linear group', Pac. J. Math. 44 (1973), 537-540.

15 ———, 'Bounding the nilpotent length of a finite group, I', Proc. London Math. Soc. 33 (1976), 329-360.

16 B. HUPPERT, 'Lineare auflösbare Gruppen', Math. Z. 62 (1957), 479-518.

17 ———, 'Endliche Gruppen, I' (Springer, Berlin, 1967).

18 T. M. ISAACS, 'Character theory of finite groups (Academic Press, New York, San Francisco, London, 1976).

19 F. P. LOCKETT, 'On the theory of Fitting Classes of finite soluble groups', Ph. D. Thesis, Univ. of Warwick, 1971.

20 D. J. S. ROBINSON, 'Finiteness conditions and generalised soluble groups' (Springer-Verlag, Berlin, Heidelberg, New York, 1972).

21 H. SCHULZ, 'H-Untergruppen in endlichen auflösbaren Gruppen', Math. Z. 97 (1967), 326-330.