CHARACTER DEGREES AND A CLASS OF FINITE PERMUTATION GROUPS

KEVIN THACKER

A dissertation for the degree of Doctor of Philosophy submitted to the University of Warwick and consisting of research conducted at the Mathematics Institute.

September, 1979.

SUMMARY

Let f.c.d.(G) denote the set of the degrees of the faithful irreducible complex characters of a finite group G. (Of course f.c.d.(G) may be empty). Chapter 1 is concerned mainly with the structure of those groups G satisfying the condition that $|\text{f.c.d.}(G)| = 1$, groups which are labelled "high-fidelity" groups, By means of the regular wreath product construction it is shown that the class of high-fidelity groups is "large" in the sense that every group is isomorphic to both a subgroup and a factor group of some high-fidelity group.

Use is made of some of D.S. Passman's results classifying soluble half-transitive groups of automorphisms in describing the structure of a special class of high-fidelity groups, namely those which are soluble with a complemented unique minimal normal subgroup. The same situation minus the condition that the unique minimal normal subgroup is complemented is studied in Chapter 2. There arises naturally a generalisation of half-transitive group action in which, instead of being identical, the orbit sizes are the same up to multiplication by powers of some prime. Such an action is called "q'-halftransitive", where q is the prime concerned.

The results of Chapters 3 and 4 produce a classification, similar to Passman's classification mentioned above, of the possibilities for a finite soluble group G which acts q'-halftransitively on the non-trivial elements of a faithful irreducible G-module over the field of q elements. Many of Passman's techniques are used and, apart from one infinite family of groups and a small number of exceptions in the case q = 3, the possibilities for G turn out to be just those on Passman's list.

Finally, in Chapter 5, an upper bound of 6 is obtained on the nilpotent length of a soluble high-fidelity group with a unique minimal normal subgroup.

CONTENTS

		PAGE
INTRODUCTION.		1
CONVENTIONS, TERMINOLOGY, AND NOTATION.		3
BASIC RESULTS.		7
CHAPTER 1.	HIGH-FIDELITY AND PRIMITIVE SOLUBLE GROUPS.	11
CHAPTER 2.	SOLUBLE HIGH-FIDELITY GROUPS WITH A UNIQUE MINIMAL NORMAL SUBGROUP.	48
CHAPTER 3.	SOLUBLE q'-HALFTRANSITIVE GROUPS OF LINEAR TRANSFORMATIONS OF A GF(q)-VECTOR SPACE. I	72
CHAPTER 4.	SOLUBLE q'-HALFTRANSITIVE GROUPS OF LINEAR TRANSFORMATIONS OF A GF(q)-VECTOR SPACE. II	106
CHAPTER 5.	BOUNDING THE NILPOTENT LENGTH OF A SOLUBLE HIGH-FIDELITY GROUP WITH A UNIQUE MINIMAL NORMAL SUBGROUP.	167
REFERENCES.		170

ACKNOWLEDGEMENTS

I am extremely grateful to my supervisor, Dr. T.O. Hawkes, for all his valuable help and advice throughout the preparation of this thesis.

I gratefully acknowledge the financial support of a grant from the Science Research Council during the period in which this research was conducted.

INTRODUCTION

The greater part of this thesis (Chapters 3 and 4) is concerned with the orbit sizes of the action of a finite soluble group G on the elements of a faithful irreducible G-module over a finite field. This study grew quite naturally out of a consideration of some questions in the character theory of finite groups, and the arrangement of material in this thesis is designed to reflect this. Our starting point, then, must be within the theory of group characters.

There are many results connecting the structure of a finite group G to the set c.d.(G) of the degrees of the irreducible complex characters of G. For example, it is a well known fact that $|\text{c.d.}(G)| = 1$ if and only if G is abelian. Several more results of this type are recorded by I.M. Isaacs in Chapter 12 of [8]. If $|\text{c.d.}(G)| = 2$ then ([8] Corollary 12.6) the group G is metabelian. A result due to S.C. Garrison, which appears as Corollary 12.21 of [8], establishes that if G is soluble then the nilpotent length of G is at most $|\text{c.d.}(G)|$.

What connections, if any, can be established between the structure of a finite group G and the various subsets of c.d.(G)? We may conveniently denote the set of the degrees of the faithful irreducible complex characters of a finite group G by f.c.d.(G) (which may, of course, be empty).

Chapter 1 is concerned mainly with those groups G satisfying the condition that $|\text{f.c.d.}(G)| = 1$, groups which I shall call "high-fidelity" groups. Although it is demonstrated that such a condition imposes no obvious restrictions on the structure of an arbitrary group, attention is drawn to the action of a high-fidelity group G on the set of non-trivial irreducible characters of its minimal normal subgroups. In particular,

it is shown that this action is half-transitive (that is, with all orbits of the same size) when G is soluble with a complemented unique minimal normal subgroup (a primitive soluble group), and in this special case the classification of soluble half-transitive groups of automorphisms by D.S. Passman in [10] (with Isaacs), [11], [12], [13] enables us to give a virtually complete description of the group structure. In Chapter 2 we investigate what can be said in the same situation minus the condition that the unique minimal normal subgroup is complemented. It turns out that half-transitivity must be replaced by a slightly weaker condition in which the orbit sizes are all the same up to multiplication by powers of some prime q; I call such an action "q'-halftransitive".

Chapters 3 and 4 are both concerned with obtaining a classification, similar to Passman's classification mentioned above, of the possibilities for a soluble group G such that, for some prime q, G acts q'-half-transitively on the non-trivial elements of a faithful irreducible G-module over the field of q elements. The case in which G has a non-cyclic abelian normal subgroup is handled in Chapter 3, the opposite case in Chapter 4. Many of Passman's results and techniques are employed in both these chapters, but especially in Chapter 4, the scheme of which mimics that of [13]. Besides a small number of exceptions for q = 3, the final list of possibilities differs from Passman's list in the half- transitive case only by the addition of an infinite family of groups, each of which is a semi-direct product of the form NH where N is a member of an infinite family on Passman's list and H is a cyclic q-group.

In the short Chapter 5 the classification obtained in Chapters 3 and 4 is used in conjunction with Passman's classification and the main theorem of Chapter 2 to derive an upper bound of 6 on the nilpotent length of a soluble high-fidelity group with a unique minimal normal subgroup.

CONVENTIONS, TERMINOLOGY, AND NOTATION.

We adopt the convention that throughout this thesis all groups considered are finite. Homomorphisms of abstract groups will usually be written exponentially: thus g^{α} denotes the image of the group element g under the homomorphism α. However, following established usage, representations and characters will be written on the left (as will factor sets of projective representations and certain other maps). The term "module" will be understood to refer to a right module except when otherwise indicated.

If π is a set of primes, then a positive integer n is said to be a π-<u>number</u> if the only primes dividing n are in π. Thus 1 is a π-number for all sets of primes π. We shall use π' to denote the set of primes not in π, and normally a set {p} consisting of a single prime will be written simply as p. For any positive integer n and set of primes π we can express n as a product ab where a is a π-number and b is a π'-number, called, respectively, the π-<u>part</u> and the π'-<u>part</u> of n.

If G is a group and π a set of primes then G is said to be a π-<u>group</u> if the order of G is a π-number. A π-subgroup, H, of G is said to be a <u>Hall</u> π-<u>subgroup</u> of G if the order of H and the index of H in G are co-prime.

Let G be a soluble group. The <u>nilpotent length</u> of G, written n(G), is defined to be the smallest number of factors in a normal series of G with each factor nilpotent if G is non-trivial, zero otherwise.

A class $\mathfrak{F}$ of groups is said to be a <u>formation</u> when, for all groups G, we have (i) $G \in \mathfrak{F}$ implies that all epimorphic images of G are in $\mathfrak{F}$, and (ii) if N_1, N_2 are two normal subgroups of G such that the factor group $G/N_i \in \mathfrak{F}$ for i = 1,2, then $G/(N_1 \cap N_2) \in \mathfrak{F}$.

There follows a survey of notation used, which is, as far as possible, consistent with that of Huppert in [6] and with that of Isaacs in [8].

1	identity group element, trivial group
$Z(G)$	centre of the group G
$F(G)$	Fitting subgroup of G
$\Phi(G)$	Frattini subgroup of G
G'	derived group of G
$\langle g_1,\ldots,g_n\rangle$	subgroup generated by group elements $g_1,\ldots,g_n$
$\Omega_i(G)$	subgroup of p-group G equal to $\langle g \in G : g^{p^i} = 1\rangle$
$O_\pi(G)$	largest normal π-subgroup of G
$soc(G)$	socle of G
$C_G(H)$	centraliser in G of H
$N_G(H)$	normaliser in G of H
$Aut(G)$	automorphism group of G
$\ker\alpha$	kernel of the group homomorphism α
$[g,h]$	the commutator $g^{-1}h^{-1}gh$
$G^{\#}$	set of non-trivial elements of G
$i(G)$	set of non-central involutions of G
$n(G)$	nilpotent length of G
$\lvert G\rvert$	order of G
$\lvert G : H\rvert$	index of H in G
$\lvert g\rvert$	order of a group element g
$\pi(G)$	set of primes dividing $\lvert G\rvert$
$\lvert G\rvert_\pi$	the π-part of $\lvert G\rvert$
G_x	stabiliser in G of x
x^G	orbit of x under G
$H \leqslant G$	H is a subgroup of G

$H < G$	H is a proper subgroup of G
$H \lhd G$	H is a normal subgroup of G
H char G	H is a characteristic subgroup of G
Irr(G)	set of all irreducible complex characters of G
Firr(G)	$\{\chi \in \mathrm{Irr}(G) : \chi \text{ is faithful}\}$
$\hat{G}$	group of linear complex characters of G
$\ker\chi$	kernel of character χ
ker(G on V)	kernel of the action of G on module V
$\mathrm{Hom}_G(U,V)$	group of G-homomorphisms from U to V
χ^G, V^G	induced character, module
χ_H, V_H	restriction to H of character χ, module V
θ^g	conjugate character
G_θ	$\{g \in G : \theta^g = \theta\}$
$\mathrm{Irr}(G\|\theta)$	$\{\chi \in \mathrm{Irr}(G) : \chi_N = e\theta$ some integer e$\}$ where $N \lhd G$ and $\theta \in \mathrm{Irr}(N)$ such that $G_\theta = G$
B(N)	see page 33
$[\chi, \psi]$	$1/\|G\|(\sum_{g \in G} \chi(g)\psi(g^{-1}))$ for characters χ, ψ of G
$\dim_K V$	dimension of V over field K
KG	group algebra of G over field K
J(KG)	Jacobson radical of KG
S(KG)	socle of KG
$H^2(G,\mathbb{C}^\times)$	second cohomology group of G
$Z^2(G,\mathbb{C}^\times)$	group of 2-cocycles (factor sets) of G
$B^2(G,\mathbb{C}^\times)$	group of 2-coboundaries of G
$GF(p^n)$	field of p^n elements
$GL(n,p^m)$	general linear group of degree n over $GF(p^m)$
$SL(n,p^m)$	special linear group of degree n over $GF(p^m)$
$Sp(2n,p^m)$	symplectic group of degree 2n over $GF(p^m)$

S_n	symmetric group of degree n
C_n	cyclic group of order n
D_8	dihedral group of order 8
Q_8	quaternion group of order 8
$\mathcal{T}(q^n)$	see Definition 1.14
$\mathcal{T}_o(q^n)$	see Definition 1.15
$\mathcal{T}_k(q^n)$	see page 27
$\mathcal{T}_o(q^n : q^m)$	see Definition 3.1
$G_1 \times G_2$	direct product of groups G_1, G_2
$G_1 \underset{r}{\sim} G_2$	regular wreath product of G_1 with G_2
$G_1 \curlyvee G_2$	central product of groups G_1, G_2
$E(p,m)$	see page 107

BASIC RESULTS.

Listed below are those results from group theory and representation theory which are assumed. Some of these basic results are used in the course of proofs in this thesis without an explicit reference.

THEOREM. Orbit-stabiliser Theorem. (Huppert [6] I Satz 5.10 a).) *If* G *is a group of permutations on a set* X, *then for each* $x \in X$ *the size of the* G-*orbit containing* x *is precisely the index in* G *of the stabiliser of* x; *that is,* $|x^G| = |G : G_x|$ *for all* $x \in X$.

THEOREM. (Huppert [6] III Satz 4.2 b).) *Let* G *be a soluble group, and let* F *denote the Fitting subgroup of* G. *Then* $C_G(F) \leqslant F$.

THEOREM. (Huppert [6] I Satz 4.6.) *Let* G *be a cyclic group of order* n. *Then* Aut(G) *is isomorphic to the multiplicative group of equivalence classes mod* n *of integers prime to* n. *In particular,* Aut(G) *is abelian, and if* G *is a* 2-*group then so is* Aut(G).

THEOREM. (Huppert [6] V Satz 8.15.) *Let* G *be a group, and let* A *be a subgroup of* Aut(G) *such that* A *acts semi-regularly on the non-trivial elements of* G. *Then for all odd primes* p *the Sylow* p-*subgroups of* A *are cyclic, and the Sylow* 2-*subgroups of* A *are cyclic or generalised quaternion.*

THEOREM. (Gorenstein [4] Chapter 6, Theorem 4.1.) *Let* G *be a soluble group and* π *a set of primes. Then*

(i) G *contains a Hall* π-*subgroup ;*

(ii) *any two Hall* π-*subgroups are conjugate in* G ;

(iii) *any* π-*subgroup of* G *is contained in a Hall* π-*subgroup.*

THEOREM. (Gorenstein [4] Chapter 5, Corollary 3.3.) Let p be a prime, and let P be a p-group. Assume that A is a subgroup of Aut(P) and that there exist normal A-invariant subgroups P_i of P for $0 \leqslant i \leqslant n$ such that

$$1 = P_o \leqslant P_1 \leqslant \ldots \leqslant P_{n-1} \leqslant P_n = P,$$

and such that A centralises P_{i+1}/P_i for $0 \leqslant i \leqslant n-1$. (A is said to stabilise the normal series $1 \leqslant P_1 \leqslant \ldots \leqslant P_{n-1} \leqslant P$.) Then A is a p-group.

For each non-negative integer r let $\mathcal{N}^r$ denote the class of soluble groups with nilpotent length at most r. From the definition of nilpotent length, $\mathcal{N}^o$ consists of the trivial group, and $\mathcal{N}^1$ is the class of all nilpotent groups. If $\mathcal{F}(p) = \mathcal{N}^o$ for all primes p then $\mathcal{N}^1$ is locally defined by $\mathcal{F}(p)$; that is $\mathcal{N}^1$ is precisely the class of those groups G such that for all primes p, if H/N is a chief factor of G with $p \mid |H/N|$ then $G/C_G(H/N) \in \mathcal{F}(p)$. (See Huppert [6] VI Beispiel 7.6a).). In general it is easily verified that, provided $\mathcal{N}^{r-1}$ is a formation, $\mathcal{N}^r$ is locally defined by $\mathcal{F}(p) = \mathcal{N}^{r-1}$ for all primes p, whereupon an easy induction argument together with [6] VI Hauptsatz 7.5 yields the following result.

THEOREM. For each non-negative integer r the class $\mathcal{N}^r$ is a formation.

THEOREM. (Gorenstein [4] Chapter 3 Theorem 2.3.) If an abelian group G has an irreducible representation with kernel K then G/K is cyclic. In particular, a non-cyclic abelian group does not possess a faithful irreducible representation.

THEOREM. (Huppert [6] V Satz 5.17.) Let G be a group, p a prime, and let P be a normal p-subgroup of G. If X is an irreducible representation of G over a field of characteristic p, then P is contained in the kernel of X.

Let G be a group, and let χ, ψ be complex characters of G. Then $[\chi,\psi]$ is defined by

$$[\chi,\psi] = 1/|G|(\sum_{g\in G} \chi(g)\psi(g^{-1})).$$

If χ (ψ) is irreducible then $[\chi,\psi]$ is precisely the multiplicity of χ (ψ) as an irreducible constituent of ψ (χ) (see Isaacs [8] Corollary 2.17 and preceding discussion).

THEOREM. Frobenius Reciprocity. (Isaacs [8] Lemma 5.2.) Let G be a group and let H be a subgroup of G. If χ is a complex character of G, and if θ is a complex character of H, then

$$[\chi_H, \theta] = [\chi, \theta^G] .$$

THEOREM. Clifford's Theorem. (Huppert [6] V Hauptsatz 17.3.) Let G be a group, K a field, and V an irreducible KG-module. Assume that N is a normal subgroup of G.

(i) If W is an irreducible KN-submodule of V then $V = \sum_{g\in G} Wg$. Each Wg is an irreducible KN-module and V_N is completely reducible.

(ii) Let $W_1, \ldots, W_n$ be a complete set of isomorphism types of irreducible KN-submodules of V. For $1 \leq i \leq n$ define V_i to be the sum of all KN-submodules of V isomorphic to W_i. (The V_i are called the homogeneous components of V_N). Then

$$V_N = V_1 \oplus \ldots \oplus V_n ,$$

and G permutes the V_i transitively by right multiplication.

(iii) For $1 \leq i \leq n$ define $A_i = \{g\in G : V_i g = V_i\}$. Then A_i is a subgroup of G, and V_i is an irreducible KA_i-module. Moreover, $V \cong V_i^G$ and $n = |G : A_i|$

(iv) If $i \in \{1, \ldots, n\}$, then let θ_i denote the character of W_i. Assume that χ is the character of V. Then there exists an integer e such that

$$\chi_N = e\sum_{i=1}^{n} \theta_i .$$

THEOREM. Schur's Lemma (Gorenstein [4] Chapter 3. Theorem 5.2.) *If* G *is a group*, K *a field, and* V *an irreudicble* KG-*module, then* $\mathrm{Hom}_G(V,V)$ *is a division ring.*

THEOREM. (Herstein [5] Theorem 7.c.) *A finite division ring is necessarily a commutative field.*

CHAPTER 1

HIGH-FIDELITY AND PRIMITIVE SOLUBLE GROUPS.

In this chapter the notion of a high-fidelity group is introduced (see Definition 1.2 below), and some special cases of such groups are considered. In particular, it is shown that there is a close connection between primitive soluble high-fidelity groups and soluble half-transitive groups of automorphisms (Theorem 1.18), allowing the use of D. Passman's classification of the latter groups (stated below as Theorem 1.16) in obtaining information about the former. The fact that the class of all high-fidelity groups is "large" (in the sense that every group appears as both a subgroup, and as a factor group, of some high-fidelity group) is demonstrated by Theorem 1.25, in which it is shown that if H is any group and C any non-trivial cyclic group, then the regular wreath product $C \underset{r}{\sim} H$ is a high-fidelity group. The final results of the chapter are all concerned with a particular subset of the set of all irreducible complex characters of a soluble group. This subset has the property that if all the characters in it share a common degree then (Theorem 1.32) the structure of the group concerned is restricted by the results on primitive soluble high-fidelity groups.

We follow [8] in using Irr(G) to denote the set of all irreducible complex characters of a group G. It will be convenient to fix a label for the set of faithful irreducible complex characters of a group.

NOTATION. Let G be a group. Then Firr(G) denotes the set

$$\{\chi \in \mathrm{Irr}(G) : \chi \text{ is faithful}\} .$$

For an arbitrary group G the set Firr(G) may be empty. A solution

to the problem of deciding exactly when Firr(G) is non-empty was first given in a paper by K. Shoda ([15]) with acknowledgement to Y. Akizuki. The statement of this result (Theorem 1.21) requires a preliminary discussion of the structure of the socle of a group, and so, since such a discussion would be out of place here, for now we merely record an almost trivial result giving a condition on a group G that guarantees $\mathrm{Firr}(G) \neq \emptyset$, and also a necessary and sufficient condition that $\mathrm{Firr}(G) \neq \emptyset$ for a p-group G.

LEMMA 1.1 ([8] Theorem 2.32) (i) *If* G *is a group with a unique minimal normal subgroup then* $\mathrm{Firr}(G) \neq \emptyset$.

(ii) *If* G *is a* p-*group then* $\mathrm{Firr}(G) \neq \emptyset$ *if and only if* Z(G), *the centre of* G, *is cyclic.*

NOTE. Lemma 1.1 (i) is not included in the statement of [8] Theorem 2.32, but the proof of [8] Theorem 2.32(b) includes an easy and obvious proof of the result.

DEFINITION 1.2. Let G be a group. We call G a *high-fidelity group* if $\mathrm{Firr}(G) \neq \emptyset$, and for all elements χ, ψ, of Firr(G) we have $\chi(1) = \psi(1)$.

Obviously all cyclic groups are high-fidelity groups. A result by Shoda ([16]) gives us some more examples.

THEOREM 1.3 (Shoda [16], Satz 12) *Let* G *be a metabelian group such that* $\mathrm{Firr}(G) \neq \emptyset$, *and let* A *be a maximal abelian subgroup of* G *such that* G', *the derived group of* G, *is a subgroup of* A. *Then for all* $\chi \in \mathrm{Firr}(G)$ *we have* $\chi(1) = |G : A|$. *In particular,* G *is a high-fidelity group.*

As an immediate consequence of our next result, which is well known and concerns the irreducible characters of Frobenius groups, we have further examples of high-fidelity groups.

LEMMA 1.4. ([8] Theorem 6.34(b)) Let G be a Frobenius group with Frobenius kernel R, say. If $\chi \in \mathrm{Irr}(G)$ such that $R \not\leq \ker\chi$, then there exists $\phi \in \mathrm{Irr}(R)$ such that $\phi^G = \chi$.

THEOREM 1.5. Let G be a Frobenius group with abelian Frobenius kernel R, say, such that $\mathrm{Firr}(G) \neq \emptyset$. Then $\chi(1) = |G : R|$ for all $\chi \in \mathrm{Firr}(G)$. In particular G is a high-fidelity group.

Proof. Let $\chi \in \mathrm{Firr}(G)$. Then by Lemma 1.4 there exists $\phi \in \mathrm{Irr}(R)$ such that $\chi = \phi^G$. Since R is abelian we have $\phi(1) = 1$, whereupon $\chi(1) = \phi^G(1) = |G : R|\phi(1) = |G : R|$.

Q.E.D.

Let p be a prime and let P be a class 2 p-group (that is, $P' \leq Z(P)$) such that $Z(P)$ is cyclic. Write $Z = Z(P)$. By Lemma 1.1 we have $\mathrm{Firr}(P) \neq \emptyset$, and, since P/Z is abelian, Theorem 1.3 implies that P is a high-fidelity group. In Chapter 2 we shall require more information concerning the characters in $\mathrm{Firr}(P)$. Specifically we shall need to make use of the fact that if $\chi \in \mathrm{Firr}(P)$ and if λ is an irreducible constituent of χ_Z, then χ and λ are fully ramified with respect to P/Z; that is $\chi(1)^2 = |P : Z|$ or, equivalently, χ is the unique irreducible constituent of λ^P. This fact is exactly the content of [9] Proposition 4.1 which is proved using the properties of group characters. We shall give an alternative proof, independent of character theory, which is based on showing that if A is a maximal normal abelian subgroup of P then $|A : Z| = |P : A|$, and then appealing to Theorem 1.3. (We remark that [16] Satz 12 is proved in terms of group representations and omits all mention of group characters.)

In order to prove the result mentioned above concerning maximal normal abelian subgroups of class 2 p-groups, we shall use a very slightly modified version of [2] Proposition 3, namely Lemma 1.6 below.

DEFINITION. Let G be an abelian group, and let H be a cyclic group. A map $\delta : G \times G \to H$ is a <u>pairing</u> of G to H if, for all elements g_1, g_2, g_3, of G, we have

$$\delta(g_1, g_2g_3) = (\delta(g_1, g_2))(\delta(g_1, g_3)),$$

and,

$$\delta(g_1g_2, g_3) = (\delta(g_1, g_3))(\delta(g_2, g_3)).$$

If, in addition, $\delta(g,g) = 1$ for all $g \in G$ then the pairing δ is said to be <u>skew</u>, and if $\delta(h,g) = 1$ for all $g \in G$ implies that $h = 1$, then we say that δ is <u>non-singular</u>.

Notice that if δ is a pairing from G to H and if $g \in G$, then $\delta(g,g) = (\delta(g,g))(\delta(1,g)) = (\delta(g,g))(\delta(g,1))$, whereupon $\delta(1,g) = \delta(g,1) = 1$.

Although [2] Proposition 3 is stated in terms of a pairing of an abelian group to a commutative ring, the full ring structure is not used in the proof, and the proof of Lemma 1.6 follows the proof of [2] Proposition 3 closely. Nevertheless, it will be convenient to have the conclusions of Lemma 1.6 tailored to facilitate its application in Theorem 1.7 and so, on balance, it seems worthwhile to give the proof in full.

LEMMA 1.6. <u>Let</u> G <u>be an abelian group, and let</u> H <u>be a cyclic group. Assume that</u> δ <u>is a skew non-singular pairing of</u> G <u>to</u> H. <u>Then there exist subgroups</u> G_1, G_2, <u>of</u> G <u>such that</u>

(i) $G = G_1 \times G_2$, $G_1 \cong G_2$;

(ii) $\delta(x,y) = 1$ <u>for all elements</u> x,y, <u>of</u> G_i $(i = 1,2)$;

(iii) <u>if</u> $g \in G$ <u>such that</u> $\delta(g,x) = 1$ <u>for all</u> $x \in G_i$ <u>then</u> $g \in G_i$ $(i = 1,2)$.

<u>Proof</u>. The proof is by induction on $|G|$. If $|G| = 1$ then there is

nothing to prove. Therefore assume that $|G| > 1$, and that if X is an abelian group with $|X| < |G|$ and if δ' is a skew non-singular pairing of X to a cyclic group, then the conclusions of the lemma hold for X and δ'.

Let n denote the exponent of G and let a_1 be an element of G of order n. Suppose that there exists an integer $m < n$ such that $(\delta(a_1,g))^m = 1$ for all $g \in G$. Then $\delta(a_1^m, g) = 1$ for all $g \in G$, and so, since δ is non-singular, $a_1^m = 1$, contradicting the fact that a_1 has order $n > m$. Consequently there exists $a_2 \in G$ such that $\delta(a_1, a_2)$ has order at least n in H. But $(\delta(a_1, a_2))^n = \delta(a_1^n, a_2) = \delta(1, a_2) = 1$, and hence $\delta(a_1, a_2)$ has order exactly n in H. Obviously a_2 has order n in G.

Write $A_1 = \langle a_1 \rangle$, $A_2 = \langle a_2 \rangle$. We show that $A_1 \cap A_2 = 1$. Clearly $A_1 \cap A_2$ is cyclic, say $A_1 \cap A_2 = \langle a \rangle$. Since $a \in A_2$ and δ is skew we must have $\delta(a, a_2) = 1$. Also $a \in A_1$, whence $a = a_1^k$ for some $k \leqslant n$. Therefore

$$(\delta(a_1, a_2))^k = \delta(a_1^k, a_2) = \delta(a, a_2) = 1.$$

But $\delta(a_1, a_2)$ has order n in H, and therefore $k = n$. Thus $a = a_1^n = 1$, and $A_1 \cap A_2 = 1$.

Write $A = A_1 \times A_2$, and $M = \{g \in G : \delta(g,a) = 1 \text{ for all } a \in A\}$. It is easily checked that the pairing δ restricted to A is a skew non-singular pairing of A to H, whence $A \cap M = 1$. Let β denote the map $a \longmapsto \delta(a, -)$, for all $a \in A$, where the space is to be filled by an element of A. Then β is a homomorphism from A to $\mathrm{Hom}(A,H)$, the group of homomorphisms from A to H. Since δ remains non-singular when restricted to A, it follows that β is a monomorphism. Write $\delta(a_1, a_2) = h$. Then, since H is cyclic, $\langle h \rangle$ is the unique subgroup of H of order n. Let $\rho \in \mathrm{Hom}(A,H)$. Clearly there exist integers t_1, t_2, such that $1 \leqslant t_i \leqslant n$ and

$$a_i^{\rho} = h^{t_i}$$

for $i = 1,2$. If a denotes $a_1^{t_2}a_2^{-t_1}$ then it is easily verified that $a^{\beta} = \rho$. We conclude that β is an isomorphism from A to $\mathrm{Hom}(A,H)$.

Define the map γ by $\gamma : g \mapsto \delta(g, -)$ for all $g \in G$, with the space to be filled by an element of A. Then γ is a homomorphism from G to $\mathrm{Hom}(A,H)$, and the kernel of γ is precisely M. Clearly γ restricted to A is the isomorphism β. It follows that γ is an isomorphism from G/M to $\mathrm{Hom}(A,H)$, and we have

$$|G/M| = |\mathrm{Hom}(A,H)| = |A| .$$

Since $A \cap M = 1$ we deduce that $G = A \times M$.

We have $|M| < |G|$, and, clearly, δ restricted to M is a skew non-singular pairing of M to H. Therefore we can apply induction to obtain subgroups M_1, M_2, of M such that

(i) $M = M_1 \times M_2$, $M_1 \cong M_2$;

(ii) $\delta(x,y) = 1$ for all elements x,y, of M_i $(i = 1,2)$;

(iii) if $g \in M$ such that $\delta(g,x) = 1$ for all $x \in M_i$ then $g \in M_i$ $(i = 1,2)$.

Writing $G_i = A_i \times M_i$ for $i = 1,2$, properties (i), (ii), (iii) in the statement of the lemma follow easily, and hence the lemma is proved by induction.

Q.E.D.

THEOREM 1.7. <u>Let</u> p <u>be a prime and let</u> P <u>be a class</u> 2 p-<u>group with cyclic centre,</u> Z <u>say. Then there exist two maximal normal abelian subgroups,</u> A_1, A_2, <u>of</u> P <u>such that</u> $P/Z = A_1/Z \times A_2/Z$, <u>and</u> $A_1/Z \cong A_2/Z$.

<u>Proof</u>. Define a map $\delta : P/Z \times P/Z \to P'$ by $\delta(xZ, yZ) = [x,y]$ for all elements x,y, of P, where $[x,y]$ denotes the commutator $x^{-1}y^{-1}xy$. We shall show that δ is a skew non-singular pairing of the abelian group P/Z to a cyclic group P'.

Since P is class 2 we have $P' \leqslant Z$. Therefore P/Z is abelian, and, since Z is cyclic, so is P'. If a, b, c, are elements of P then the fact

that P is class 2 implies that $[ab,c] = [a,c][b,c]$, and $[a,bc] = [a,b][a,c]$. We check that δ is well-defined. If $xZ = x'Z$ and $yZ = y'Z$, then there exist elements z_1, z_2, of Z such that $x' = xz_1$ and $y' = yz_2$, and we have

$$[x', y'] = [xz_1, yz_2] = [x,y][x,z_2][z_1,y][z_1,z_2] = [x,y] .$$

It follows that δ is well-defined. That δ is a skew pairing is obvious. Suppose that $xZ \in P/Z$ such that $\delta(xZ, yZ) = 1$ for all $yZ \in P/Z$. Then $[x,y] = 1$ for all $y \in P$, which yields $x \in Z$, and we deduce that δ is non-singular.

By Lemma 1.6 there exist subgroups A_1/Z, A_2/Z, of P/Z such that

(i) $P/Z = A_1/Z \times A_2/Z$, $A_1/Z \cong A_2/Z$;

(ii) $\delta(xZ, yZ) = 1$ for all elements xZ, yZ, of A_i/Z $(i = 1,2)$;

(iii) if $xZ \in P/Z$ such that $\delta(xZ, yZ) = 1$ for all $yZ \in A_i/Z$ then $xZ \in A_i/Z$ $(i = 1,2)$.

Let $i \in \{1,2\}$, and let x,y, be elements of A_i. From (ii) we have $[x,y] = \delta(xZ, yZ) = 1$, and it follows that A_i is abelian. Clearly $A_i \triangleleft G$, and A_i is a maximal normal abelian subgroup of P since, if $x \in C_P(A_i)$, then $\delta(xZ, yZ) = [x,y] = 1$ for all $y \in A_i$, whereupon, by (iii), $x \in A_i$.

Q.E.D.

Let G be a group, and N a normal subgroup of G. If $g \in G$ and $\theta \in \mathrm{Irr}(N)$ then θ^g denotes the irreducible character of N defined by $\theta^g(x) = \theta(gxg^{-1})$ for all $x \in N$. The characters θ and θ^g are said to be <u>conjugate</u> in G. The stabiliser in G of θ, that is the set of all elements g of G such that $\theta^g = \theta$, is a subgroup of G and is denoted by G_θ. If $G_\theta = G$, we say that θ is <u>invariant</u> in G, and in this case the set $\{\chi \in \mathrm{Irr}(G) : [\chi_N, \theta] \neq 0\}$ is denoted by $\mathrm{Irr}(G|\theta)$.

We are now in a position to give the alternative proof of

[9] Proposition 4.1 mentioned earlier.

THEOREM 1.8. *Let* p *be a prime and let* P *be a class* 2 p-*group with cyclic centre*, Z *say. Then* $\chi(1)^2 = |P : Z|$ *for all* $\chi \in \mathrm{Firr}(P)$. *Also if* $\lambda \in \mathrm{Firr}(Z)$ *then* $\mathrm{Irr}(P|\lambda) = \{\psi\}$ *for some* $\psi \in \mathrm{Firr}(P)$.

Proof. Since P is class 2 it follows that P is metabelian, and $\mathrm{Firr}(P) \neq \emptyset$ by Lemma 1.1. Let $\chi \in \mathrm{Firr}(P)$. If A is any maximal normal abelian subgroup of P then $A \geqslant Z \geqslant P'$, and hence, by Theorem 1.3, we have $\chi(1) = |P : A|$. Therefore all maximal normal abelian subgroups of P have the same index in P, and by Theorem 1.7 this index is precisely $|P : Z|^{\frac{1}{2}}$. We deduce that $\chi(1)^2 = |P : Z|$ for all $\chi \in \mathrm{Firr}(P)$.

Now let $\lambda \in \mathrm{Firr}(Z)$, and let ψ be an irreducible constituent of λ^P. By Frobenius reciprocity we have $[\psi_Z, \lambda]$, the multiplicity of λ as an irreducible constituent of ψ_Z, is precisely $[\psi, \lambda^P]$, the multiplicity of ψ as an irreducible constituent of λ^P. Obviously $\psi \in \mathrm{Firr}(P)$ and $\psi_Z = \psi(1)\lambda$. Hence $[\psi, \lambda^P] = \psi(1)$. Now $|P : Z| = \lambda^P(1)$, and, as shown above, we have $\psi(1)^2 = |P : Z|$. Therefore $\lambda^P = \psi(1)\psi$ and, since $\chi \in \mathrm{Irr}(P|\lambda)$ if and only if $[\chi, \lambda^P] \neq 0$, we have $\mathrm{Irr}(P|\lambda) = \{\psi\}$.

Q.E.D.

We next state Theorem 6.11 of [8] to which we shall need to refer many times.

THEOREM 1.9. ([8] Theorem 6.11). Let G be a group and N a normal subgroup of G. Assume that $\theta \in \mathrm{Irr}(N)$, and write

$$X = \{\psi \in \mathrm{Irr}(G_\theta) : [\psi_N, \theta] \neq 0\} = \mathrm{Irr}(G_\theta|\theta)$$

and

$$Y = \{\chi \in \mathrm{Irr}(G) : [\chi_N, \theta] \neq 0\} .$$

Then

(i) ψ^G is irreducible for all $\psi \in X$;

(ii) the map $\psi \mapsto \psi^G$ is a bijection from X to Y ;

(iii) if $\psi^G = \chi$, with $\psi \in X$, then ψ is the unique irreducible constituent of χ_{G_θ} which lies in X ;

(iv) if $\psi^G = \chi$, with $\psi \in X$, then $[\psi_N, \theta] = [\chi_N, \theta]$.

If G is a group and N a normal subgroup of G, then we shall often identify the sets Irr(G/N) and $\{\chi \in \mathrm{Irr}(G) : N \leqslant \ker\chi\}$; for, if $\chi \in \mathrm{Irr}(G)$ with $N \leqslant \ker\chi$ then, by defining $\chi(gN) = \chi(g)$ for all $g \in G$, we have $\chi \in \mathrm{Irr}(G/N)$, and each element of Irr(G/N) arises in this way from some $\chi \in \mathrm{Irr}(G)$ with $N \leqslant \ker\chi$. (See, for example, [8] Lemma 2.22)

LEMMA 1.10. <u>Let</u> G <u>be a group and</u> N <u>a normal subgroup of</u> G. <u>Assume that</u> $\theta \in \mathrm{Irr}(N)$, <u>and let</u> K <u>denote</u> $\ker\theta$. <u>Then</u> $K \lhd G_\theta$, <u>and when</u> θ <u>is considered</u>, <u>in the natural way, as an element of both</u> Irr(N/K) <u>and</u> Irr(N), <u>we may identify the two sets</u> $\mathrm{Irr}(G_\theta|\theta)$ <u>and</u> $\mathrm{Irr}(G_\theta/K|\theta)$. <u>In addition, if</u> $\theta(1) = 1$ <u>then</u>

$$G_\theta = \{g \in G : [g,x] \in K \text{ for all } x \in N\} ,$$

<u>and</u> $N/K \leqslant Z(G_\theta/K)$.

<u>Proof</u>. It is easily verified that $K \lhd G_\theta$. Let $\psi \in \mathrm{Irr}(G_\theta|\theta)$. Since $\psi_N = e\theta$ for some integer e we must have $K \leqslant \ker\psi$. It follows immediately that the two sets $\mathrm{Irr}(G_\theta|\theta)$ and $\mathrm{Irr}(G_\theta/K|\theta)$ may be identified.

Now assume that $\theta(1) = 1$. Then

$$\begin{aligned}
G_\theta &= \{g \in G : \theta^g = \theta\} = \{g \in G : \theta^{g^{-1}} = \theta\} \\
&= \{g \in G : \theta(g^{-1}xg) = \theta(x) \text{ for all } x \in N\} \\
&= \{g \in G : \theta(g^{-1}x^{-1}g) = \theta(x^{-1}) \text{ for all } x \in N\} \\
&= \{g \in G : \theta(g^{-1}x^{-1}g)(\theta(x^{-1}))^{-1} = 1 \text{ for all } x \in N\} \\
&= \{g \in G : \theta([g,x]) = 1 \text{ for all } x \in N\} \\
&= \{g \in G : [g,x] \in K \text{ for all } x \in N\} .
\end{aligned}$$

It is an immediate consequence of the above that if $\theta(1) = 1$ then $N/K \leqslant Z(G_\theta/K)$.

Q.E.D.

All the examples of high-fidelity groups we have met so far have the property that the common degree of the faithful irreducible characters has coincided with the index of an abelian normal subgroup. As we shall see later, it is easy to find high-fidelity groups of composite order which do not have this property, and the following example is of a high-fidelity p-group which also lacks this property.

EXAMPLE. Let p be a prime, and let A be an elementary abelian p-group of order p^3. Let G be a Sylow p-subgroup of Aut(A), and write P = AG, the natural semi-direct product of A with G. We shall show not only that $\mathrm{Firr}(P) \neq \emptyset$ and $\chi(1) = p^2$ for all $\chi \in \mathrm{Firr}(P)$, but also that P contains no abelian normal subgroup of index p^2.

We have $\mathrm{Aut}(A) \cong GL(3,p)$, whereupon G is isomorphic to a Sylow p-subgroup of GL(3,p). A Sylow p-subgroup of GL(3,p) is isomorphic to the group of all 3×3 upper uni-triangular matrices with entries in GF(p), the field of p elements. If a, b, c, are elements of GF(p) then

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb+\frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

for all $n \geqslant 1$. Consequently it is easy to see that $G \cong D_8$ for $p = 2$, and for $p > 2$ the group G is an extraspecial group of order p^3 and exponent p. It follows that $|P| = p^6$. Clearly A is a maximal normal abelian subgroup of P, and $|Z(P)| = p$. Since Z(P) is cyclic Lemma 1.1 yields $\mathrm{Firr}(P) \neq \emptyset$.

Let $\chi \in \mathrm{Firr}(P)$, and write

$$\chi_A = e\sum_{i=1}^{t} \lambda_i$$

where $\lambda_i \in \mathrm{Irr}(A)$ for $1 \leqslant i \leqslant t$. Since A is abelian, we have $\lambda_i(1) = 1$ for $1 \leqslant i \leqslant t$, and from the fact that χ is faithful we deduce that

$$\bigcap_{i=1}^{t} \ker\lambda_i = \ker\chi_A = 1.$$

By Clifford's Theorem all the λ_i are conjugate in P, and therefore $\ker\lambda_i$ contains no non-trivial normal subgroup of P. Thus $\ker\lambda_i \cap Z(P) = 1$ for $1 \leqslant i \leqslant t$.

Write $\lambda = \lambda_1$ and consider P_λ. Obviously $A \leqslant P_\lambda$, and we see that $P_\lambda = AG_\lambda$, the semi-direct product of A with the stabiliser in G of λ. Since $t = |P : P_\lambda| = |G : G_\lambda|$ we have $t = 1, p, p^2$, or p^3. If $t = 1$ then $G_\lambda = G$, whereupon $\ker\lambda \lhd P$. But, as noted above, $\ker\lambda$ contains no non-trivial normal subgroup of P, and hence in this case $\ker\lambda = 1$, which is clearly impossible since A is not cyclic. Thus $t \neq 1$.

Write $X = \{\mu \in \mathrm{Irr}(A) : \ker\mu \cap Z(P) = 1\}$. It is easily seen that $|X| = p^2(p-1)$. Also $\lambda \in X$, and if μ is conjugate to λ in P then $\mu \in X$. Since $|X| = p^2(p-1) < p^3$, we have $t \neq p^3$. Therefore $t = p$, or p^2. Suppose that $t = p$. Then $|G_\lambda| = p^2$. From the structure of G we see that if $H \leqslant G$ such that $|H| = p^2$ then $Z(G) \leqslant H$. Consequently $Z(G) \leqslant G_\lambda$. Since the λ_i are all conjugate in P it follows that the subgroups P_{λ_i} are all conjugate in P, whereupon the subgroups G_{λ_i} are all conjugate in G. Hence $Z(G) \leqslant G_{\lambda_i}$ for $1 \leqslant i \leqslant t$. By Lemma 1.10 we have $[Z(G), A] \leqslant \ker\lambda_i$ for $1 \leqslant i \leqslant t$, and thus

$$[Z(G), A] \leqslant \bigcap_{i=1}^{t} \ker\lambda_i = 1,$$

a contradiction since $C_P(A) = A$.

Therefore $t = p^2$, and $|G_\lambda| = p$. Now $|A/\ker\lambda| = p$, and so

$|P_\lambda/\ker\lambda| = p^2$. It follows that $P_\lambda/\ker\lambda$ is abelian. By Theorem 1.9 and Lemma 1.10 there exists $\psi \in \mathrm{Irr}(P_\lambda/\ker\lambda|\lambda)$ such that $\psi^P = \chi$. Hence $\chi(1) = \psi^P(1) = \psi(1)\, t = p^2$. Thus $\chi(1) = p^2$ for all $\chi \in \mathrm{Firr}(P)$.

Suppose that $B \triangleleft P$ such that $|P : B| = p^2$. Since P/B is abelian we have $P' \leq B$. Now $P' = [A,G][G,G]$ is abelian of order p^3, but $C_G([A,G]) = A[G,G]$ is non-abelian of order p^4 and so B is non-abelian. Thus P contains no abelian normal subgroup of index p^2. This completes the example.

Let S denote the symmetric group of degree 4. Then S contains a unique minimal normal subgroup, N say. Also $N \cong C_2 \times C_2$, and $C_S(N) = N$. Furthermore, N is complemented in S by a subgroup H of S, and $H \cong S/N \cong S_3$, the symmetric group of degree 3. Lemma 1.1 yields $\mathrm{Firr}(S) \neq \emptyset$. We have

$$\sum_{\theta \in \mathrm{Irr}(S)} \theta(1)^2 = |S| = 24$$

and,

$$\sum_{\substack{\theta \in \mathrm{Irr}(S) \\ \theta \notin \mathrm{Firr}(S)}} \theta(1)^2 = |S/N| = 6.$$

Therefore

$$\sum_{\theta \in \mathrm{Firr}(S)} \theta(1)^2 = 24 - 6 = 18.$$

Since $\theta(1)|24$ for all $\theta \in \mathrm{Irr}(S)$ and $\theta(1) > 1$ for all $\theta \in \mathrm{Firr}(S)$, we deduce that S has exactly 2 faithful irreducible characters, both of degree 3. Hence S is a high-fidelity group.

The symmetric group of degree 4 is an example of a primitive soluble group. A group G is said to be <u>primitive</u> if G has a faithful primitive permutation representation. It is well known (see, for example, [6] II

Satz 3.2 & Satz 3.3) that a soluble group G is primitive if and only if G contains a self-centralising minimal normal subgroup, or equivalently, if and only if F(G), the Fitting subgroup of G, is the unique minimal normal subgroup of G. The structure of such groups is particularly easy to analyse for, if G is a primitive soluble group with unique minimal normal subgroup N, then N is an elementary abelian q-group for some prime q, and N is complemented in G by a subgroup, H say. Considered additively, N is an irreducible GF(q)H-module (where GF(q)H denotes the group algebra of H over the field GF(q)), which is faithful for H.

If A is an abelian group then $\hat{A}$ denotes the group of all irreducible complex characters of A. As shown in [6] V 6.4, we have $A \cong \hat{A}$.

LEMMA 1.11. <u>Let</u> A <u>be an abelian group and assume that</u> G <u>is a subgroup of</u> Aut(A). <u>For</u> $\lambda \in \hat{A}$, $\alpha \in G$, <u>define</u> λ^{α} <u>by</u> $\lambda^{\alpha}(a) = \lambda(a^{\alpha^{-1}})$ <u>for all</u> $a \in A$. <u>Then, with this definition,</u> G <u>may be regarded as a subgroup of</u> Aut($\hat{A}$). <u>If</u> A <u>is an elementary abelian</u> q-<u>group then, with this definition, considered additively, both</u> A <u>and</u> $\hat{A}$ <u>are</u> GF(q)G-<u>modules, and if</u> A <u>is irreducible, so is</u> $\hat{A}$.

<u>Proof</u>. Clearly if $\alpha \in G$, then $\lambda \mapsto \lambda^{\alpha}$ for all $\lambda \in \hat{A}$ is an automorphism of $\hat{A}$. As is easily checked, the map $\tau : A \to \hat{\hat{A}}$ defined by

$$(a^{\tau})(\lambda) = \lambda(a)$$

for all $a \in A$, $\lambda \in \hat{A}$, is an isomorphism. Moreover if G acts on $\hat{\hat{A}}$ in the obvious way tnen $(a^{\tau})^{\alpha} = (a^{\alpha})^{\tau}$ for all $a \in A$, $\alpha \in G$. Consequently

$$C_G(\hat{A}) \leqslant C_G(\hat{\hat{A}}) = C_G(A) = 1.$$

If $\lambda \in \hat{A}$ and α, β, are elements of G then

$$\lambda^{\alpha\beta}(a) = \lambda(a^{(\alpha\beta)^{-1}}) = \lambda(a^{\beta^{-1}\alpha^{-1}}) = \lambda^{\alpha}(a^{\beta^{-1}}) = (\lambda^{\alpha})^{\beta}(a)$$

for all $a \in A$, whereupon $\lambda^{\alpha\beta} = (\lambda^{\alpha})^{\beta}$. Thus G may be regarded as a subgroup of Aut($\hat{A}$), and it follows immediately that if A is an elementary abelian

q-group then both A and $\hat{A}$ are GF(q)G-modules. If M is a non-trivial proper G-invariant subgroup of $\hat{A}$ then it is easily verified that $M^{\perp} = \{\mu \in \hat{\hat{A}}: \mu(m) = 1$ for all $m \in M\}$ is a non-trivial proper G-invariant subgroup of $\hat{\hat{A}}$. Since the map τ defined above is a G-isomorphism it follows that $(M^{\perp})^{\tau^{-1}}$ is a proper G-invariant subgroup of A, proving the statement about irreducibility.

Q.E.D.

Let G be a group such that $G = G_1 \times G_2$, the direct product of groups G_1, G_2. If $\phi \in \mathrm{Irr}(G_1)$ and $\theta \in \mathrm{Irr}(G_2)$ then, following [8] , we define $\chi = \phi \times \theta$ by $\chi(g_1 g_2) = \phi(g_1)\theta(g_2)$ for all $g_i \in G_i$, $i = 1,2$.

THEOREM 1.12. ([8] Theorem 4.21) <u>Let</u> $G = G_1 \times G_2$ <u>be the direct product of groups</u> G_1, G_2. <u>Then</u> $\mathrm{Irr}(G) = \{\phi \times \theta: \phi \in \mathrm{Irr}(G_1), \theta \in \mathrm{Irr}(G_2)\}$.

In the terminology of the theory of permutation groups, a group G of permutations on a set X with $|X| > 1$ is said to act <u>half-transitively</u> on X if all G-orbits in X have the same size. Clearly, by the orbit-stabiliser theorem, to say that G acts half-transitively on X is equivalent to saying that $|G_x| = |G_y|$ for all elements x, y, of X. In the case in which $|G_x| = 1$ for all $x \in X$ we say that G acts <u>semi-regularly</u> on X, and if G acts both semi-regularly and transitively on X then G is said to act <u>regularly</u> on X. The group G is said to act <u>3/2-transitively</u> on X if G acts transitively on X and, for some $x \in X$, the group G_x acts half-transitively on $X \setminus \{x\}$.

LEMMA 1.13. <u>Let</u> G <u>be a group with a unique minimal normal subgroup</u> N. <u>Assume that</u> N <u>is abelian and that</u> N <u>is complemented in</u> G <u>by a subgroup</u> H, <u>say. Then</u> G <u>is a high-fidelity group if and only if</u> H, <u>regarded as a group of permutations on</u> $\hat{N}$, <u>acts half-transitively on</u> $(\hat{N})^{\#}$ <u>with each stabiliser abelian. Moreover, if</u> G <u>is a high-fidelity group and</u> $\chi \in \mathrm{Firr}(G)$ <u>then</u> $\chi(1) = |G : G_\lambda|$ <u>for all</u> $\lambda \in (\hat{N})^{\#}$, <u>and</u> $(\chi(1), |N|) = 1$.

Proof. The group G has a unique minimal normal subgroup and so, certainly, $\mathrm{Firr}(G) \neq \emptyset$. Let $\chi \in \mathrm{Firr}(G)$ and write

$$\chi_N = e \sum_{i=1}^{t} \lambda_i$$

where $\lambda_i \in \hat{N}$ for $1 \leqslant i \leqslant t$. Since χ is faithful, none of the λ_i is the trivial character. Choose $j \in \{1, \ldots, t\}$ and write $\lambda = \lambda_j$. Obviously $N \leqslant G_\lambda$, and therefore, since N is complemented in G by H, we see that $G_\lambda = NH_\lambda$. Let K denote $\ker\lambda$. Then $K \lhd G_\lambda$. The fact that N is abelian yields $\lambda(1) = 1$, whereupon, by Lemma 1.10, $N/K \leqslant Z(G_\lambda/K)$. Since $H \cap N = 1$ we have $H_\lambda \cong H_\lambda K/K$, and

$$G_\lambda/K = N/K \times H_\lambda K/K. \tag{1}$$

By Theorem 1.9 and Lemma 1.10 the map $\psi \longmapsto \psi^G$ is a bijection from the set $\mathrm{Irr}(G_\lambda/K|\lambda)$ to the set $\{\theta \in \mathrm{Irr}(G) : [\theta_N, \lambda] \neq 0\}$.

Assume that H acts half-transitively on $(\hat{N})^*$ with each stabiliser abelian, and let k denote the common size of all the H-orbits in $(\hat{N})^*$. If χ, λ, t, are as above then we have

$$t = |G : G_\lambda| = |H : H_\lambda| = k,$$

and, since H_λ is abelian, (1) implies that G_λ/K is abelian. There exists $\psi \in \mathrm{Irr}(G_\lambda/K|\lambda)$ such that $\chi = \psi^G$, and hence

$$\chi(1) = \psi^G(1) = \psi(1)|G : G_\lambda| = k.$$

It follows that if H acts half-transitively on $(\hat{N})^*$ with each stabiliser abelian then G is a high-fidelity group.

Now assume that G is a high-fidelity group and let k denote the common degree of all the characters in $\mathrm{Firr}(G)$. Choose $\lambda \in (\hat{N})^*$. We shall show that $|H : H_\lambda| = k$, and that H_λ is abelian. If we write $K = \ker\lambda$ then (1) above holds. Clearly $\psi^G \in \mathrm{Firr}(G)$ for all $\psi \in \mathrm{Irr}(G_\lambda/K|\lambda)$, whereupon

$$\psi^G(1) = \psi(1)|H : H_\lambda| = k \tag{2}$$

for all $\psi \in \mathrm{Irr}(G_\lambda/K|\lambda)$. By Theorem 1.12 we have

$$\mathrm{Irr}(G_\lambda/K) = \{\mu \times \phi : \mu \in \mathrm{Irr}(N/K),\ \phi \in \mathrm{Irr}(H_\lambda K/K)\},$$

and it follows that

$$\mathrm{Irr}(G_\lambda/K|\lambda) = \{\lambda \times \phi:\ \phi \in \mathrm{Irr}(H_\lambda K/K)\}.$$

Therefore, using (2),

$$\phi(1) = \lambda(1)\phi(1) = (\lambda \times \phi)(1) = k/|H : H_\lambda|$$

for all $\phi \in \mathrm{Irr}(H_\lambda K/K)$. Consequently $H_\lambda K/K$ is abelian, and $\phi(1) = 1$ for all $\phi \in \mathrm{Irr}(H_\lambda K/K)$. Thus $|H : H_\lambda| = k$, and $H_\lambda \cong H_\lambda K/K$, an abelian group. We conclude that H acts half-transitively on $(\hat{N})^\#$ with each stabiliser abelian.

Assume that G is a high-fidelity group, and let $\chi \in \mathrm{Firr}(G)$. Let $\mu \in (\hat{N})^\#$ such that $[\chi_N, \mu] \neq 0$. It is apparent from the proof above that $\chi(1) = |G : G_\mu| = |H : H_\mu|$. If $\lambda \in (\hat{N})^\#$ then, since H acts half-transitively on $(\hat{N})^\#$, we have

$$\chi(1) = |H : H_\mu| = |H : H_\lambda| = |G : G_\lambda|$$

as required. We see that $\chi(1)$ is the common size of all the H-orbits in $(\hat{N})^\#$, and it follows that $\chi(1)\,|\,|(\hat{N})^\#|$. We have $|(\hat{N})^\#| = |N| - 1$, whereupon $\chi(1)\,|\,(|N| - 1)$, and we conclude that $(\chi(1), |N|) = 1$.

Q.E.D.

The situation in which H is a group of automorphisms of a group N, and H acts half-transitively on $N^\#$, has been studied by D. Passman in the series of papers [10] (with I. Isaacs), [11], [12], [13], giving a classification of the possibilities for H if H is soluble. We shall state this classification below after we have described two particular families

of groups that play a special part in Passman's work.

DEFINITION 1.14. If q is a prime and n a positive integer then $\mathcal{T}(q^n)$ denotes the group of automorphisms of the additive group of $GF(q^n)$ consisting of all maps of the form

$$x \longmapsto ax^{\sigma}$$

for all elements x, a, of $GF(q^n)$ such that $a \neq 0$, and for all $\sigma \in Aut(GF(q^n))$, where $Aut(GF(q^n))$ denotes the group of field automorphisms, a cyclic group of order n.

We make a few easily verifiable observations about the group $\mathcal{T}(q^n)$ and its action on the additive group of $GF(q^n)$. The subgroup, A say, of $\mathcal{T}(q^n)$ consisting of all maps of the form

$$x \longmapsto ax$$

for all elements x, a, of $GF(q^n)$ such that $a \neq 0$, is cyclic of order $q^n - 1$ and is normal in $\mathcal{T}(q^n)$. Clearly A acts transitively, in fact regularly, on the non-zero elements of $GF(q^n)$. Also A is complemented in $\mathcal{T}(q^n)$ by a cyclic subgroup of order n consisting of all maps of the form

$$x \longmapsto x^{\sigma}$$

for all $x \in GF(q^n)$, $\sigma \in Aut(GF(q^n))$. Thus $\mathcal{T}(q^n)$ is metacyclic, and $|\mathcal{T}(q^n)| = n(q^n - 1)$. In addition, $\mathcal{T}(q^n)$ acts transitively on the non-zero elements of $GF(q^n)$, and the stabiliser in $\mathcal{T}(q^n)$ of an element of $GF(q^n)^{\#}$ is a cyclic group of order n.

It will be convenient to introduce some notation for certain subgroups of $\mathcal{T}(q^n)$.

NOTATION. Let $k|n$, and let S denote the unique subgroup of $Aut(GF(q^n))$ of order k. Then $\mathcal{T}_k(q^n)$ denotes the subgroup of $\mathcal{T}(q^n)$ consisting of all maps of the form

$$x \longmapsto ax^{\sigma}$$

for all elements x, a, of $GF(q^n)$ such that $a \neq 0$, and for all $\sigma \in S$.

DEFINITION 1.15. Let q be an odd prime, n a positive integer, and let V be a 2-dimensional vector space over the field $GF(q^n)$. Then $\mathcal{T}_o(q^n)$ denotes the group of all transformations of V of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ 0 & \pm a^{-1} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

and

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} 0 & a \\ \pm a^{-1} & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

for all elements x, y, a, of $GF(q^n)$ such that $a \neq 0$.

It is easily checked that $|\mathcal{T}_o(q^n)| = 4(q^n - 1)$. Let b be a generator of the cyclic multiplicative group of $GF(q^n)$, and let c, d, denote the transformations

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

and

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

respectively. If B denotes the subgroup of $\mathcal{T}_o(q^n)$ generated by c, d, then $B \cong C_{q^n-1} \times C_2$, with $B \triangleleft \mathcal{T}_o(q^n)$ and $|\mathcal{T}_o(q^n) : B| = 2$. If e denotes the transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix},$$

and if γ denotes $q^n - 1$, then in terms of generators and relations we have

$$\mathcal{T}_0(q^n) = \langle c, d, e : c^\gamma = d^2 = e^2 = 1, cd = dc, ece = c^{-1}, ede = c^{\gamma/2}d \rangle.$$

For all $v \in V^\#$ the stabiliser in $\mathcal{T}_0(q^n)$ of v is a group of order 2, whereupon each $\mathcal{T}_0(q^n)$-orbit in $V^\#$ has size $2(q^n - 1)$. In particular, $\mathcal{T}_0(q^n)$ does not act transitively on $V^\#$. Clearly we may regard $\mathcal{T}_0(q^n)$ as a group of transformations of a 2n-dimensional vector space V over the field GF(q), acting half-transitively on $V^\#$.

The following theorem, Theorem 1.16, is a statement of Passman's results on half-transitive groups of automorphisms. The individual cases in Theorem 1.16 are not all stated explicitly in Passman's work, but these are easily deduced from the proofs given.

As in [6] I 9.10, we use $G_1 \curlyvee G_2$ to denote a central product of two groups G_1, G_2. In writing $G_1 \curlyvee G_2$ without additional comment there is always a certain amount of ambiguity, but for our purposes the meaning of $G_1 \curlyvee G_2$ will always be obvious.

THEOREM 1.16 (Passman [10] (with Isaacs), [11], [12], [13]). <u>Assume that</u> H <u>is a group of automorphisms of a group</u> N, <u>such that H acts half-transitively but not semi-regularly on</u> $N^\#$. <u>Then</u> N <u>is an elementary abelian q-group for some prime</u> q, <u>and</u> H <u>acts irreducibly on</u> N. <u>If</u> $|N| = q^n$ <u>and</u> H <u>is soluble then either we may identify</u> N <u>with the additive group of</u> $GF(q^n)$ <u>in such a way that</u> $H \leq \mathcal{T}(q^n)$, <u>or</u> $H \cong \mathcal{T}_0(q^{n/2})$ <u>with</u> $|H_x| = 2$ <u>for all</u> $x \in N^\#$ <u>and</u> H <u>does not act transitively on</u> $N^\#$, <u>or one of the following cases must hold.</u>

(a_1) $q^n = 3^2$, $|H| = 24$, $H_x \cong C_3$ <u>for</u> $x \in N^\#$, $H \cong SL(2,3)$;
(a_2) $q^n = 3^2$, $|H| = 48$, $H_x \cong S_3$ <u>for</u> $x \in N^\#$, $H \cong GL(2,3)$;

(b_1) $q^n = 5^2$, $|H| = 48$, $H_x \cong C_2$ <u>for</u> $x \in N^\#$, $F(H) \cong Q_8 \curlyvee C_4$;
(b_2) $q^n = 5^2$, $|H| = 96$, $H_x \cong C_4$ <u>for</u> $x \in N^\#$, $F(H) \cong Q_8 \curlyvee C_4$;

(c_1) $q^n = 7^2$, $|H| = 72$, $H_x \cong C_3$ for $x \in N^\#$, $F(H) \cong Q_8 \times C_3$;
(c_2) $q^n = 7^2$, $|H| = 144$, $H_x \cong C_3$ for $x \in N^\#$, $F(H) \cong Q_8 \times C_3$;

(d_1) $q^n = 11^2$, $|H| = 48$, $H_x \cong C_2$ for $x \in N^\#$, $F(H) \cong Q_8$;
(d_2) $q^n = 11^2$, $|H| = 240$, $H_x \cong C_2$ for $x \in N^\#$, $F(H) \cong Q_8 \times C_5$;

(e_1) $q^n = 17^2$, $|H| = 96$, $H_x \cong C_2$ for $x \in N^\#$, $F(H) \cong Q_8 \curlyvee C_4$;

(f_1) $q^n = 3^4$, $|H| = 32$, $H_x \cong C_2$ for $x \in N^\#$, $F(H) \cong Q_8 \curlyvee D_8$;
(f_2) $q^n = 3^4$, $|H| = 160$, $H_x \cong C_2$ for $x \in N^\#$, $F(H) \cong Q_8 \curlyvee D_8$;
(f_3) $q^n = 3^4$, $|H| = 320$, $H_x \cong C_4$ for $x \in N^\#$, $F(H) \cong Q_8 \curlyvee D_8$;
(f_4) $q^n = 3^4$, $|H| = 640$, $H_x \cong C_8$ for $x \in N^\#$, $F(H) \cong Q_8 \curlyvee D_8$.

Furthermore, if H is imprimitive as a linear group on N then either $H \cong \mathcal{T}_0(q^{n/2})$, or $q^n = 2^6$ and H is isomorphic to the dihedral group of order 18, or case (f_1) above holds.

LEMMA 1.17. ([8] Theorem 6.32 & Corollary 6.33). Let H be a group which acts on $\mathrm{Irr}(N)$ and on the conjugacy classes of N for some group N. Assume that $\lambda(x) = \lambda^h(y)$ for all $\lambda \in \mathrm{Irr}(N)$, $h \in H$, $x \in N$, where if x is an element of the conjugacy class, C, of N then $y \in C^h$. Then for each $h \in H$, the number of elements of $\mathrm{Irr}(N)$ fixed by h is equal to the number of conjugacy classes of N fixed by h. In addition, the number of H-orbits in $\mathrm{Irr}(N)$ is equal to the number of H-orbits in the set of conjugacy classes of N.

We are now in a position to prove that a primitive soluble high-fidelity group is a 3/2-transitive permutation group.

THEOREM 1.18. Assume that G is a primitive soluble group and let N denote the unique minimal normal subgroup of G, complemented in G by a subgroup, H say. Then G is a high-fidelity group if and only if H acts half-transitively on $(\hat{N})^\#$ with each stabiliser abelian. Moreover, if G is a high-

fidelity group then G is a 3/2-transitive permutation group.

Proof. The subgroup N is an elementary abelian q-group for some prime q, and the "if and only if" statement in the theorem follows immediately from Lemma 1.13.

Assume that G is a high-fidelity group. Then, as a group of automorphisms of the group $\hat{N}$, the group H acts half-transitively on $(\hat{N})^{\#}$. We shall show that H acts half-transitively on $N^{\#}$. If H acts semi-regularly on $(\hat{N})^{\#}$ then Lemma 1.17 implies that H acts semi-regularly on $N^{\#}$. If H acts transitively on $(\hat{N})^{\#}$ then the number of H-orbits in $\hat{N}$ is precisely 2, and, by Lemma 1.17, this is the number of H-orbits in N . Thus if H acts transitively on $(\hat{N})^{\#}$ then H acts transitively on $N^{\#}$. Hence we may assume that H acts neither semi-regularly nor transitively on $(\hat{N})^{\#}$.

Let $|N| = q^n$, and let k denote the common order of the subgroups H_λ for all $\lambda \in (\hat{N})^{\#}$. Suppose that there exists $x \in N^{\#}$ such that $|H_x| > k$. In view of Lemma 1.17 it is apparent that H_x is not cyclic. If $H \leqslant \mathcal{T}(q^n)$ then there exists a normal subgroup, A, of H such that A and H/A are both cyclic, and such that A acts semi-regularly on $(\hat{N})^{\#}$. By Lemma 1.17 the subgroup A acts semi-regularly on $N^{\#}$, whence $H_x \cap A = 1$ and $H_x \cong H_xA/A \leqslant H/A$, a contradiction since H/A is cyclic. Hence $H \not\leqslant \mathcal{T}(q^n)$. Suppose that case (c_1) of Theorem 1.16 holds. Then $|H_\lambda| = 3$ for all $\lambda \in (\hat{N})^{\#}$, whereupon $|H_x| > 3$. Also $F(H) \cong Q_8 \times C_3$ and F(H) acts semi-regularly on $(\hat{N})^{\#}$. By Lemma 1.17 the group F(H) acts semi-regularly on $N^{\#}$, whence $H_x \cap F(H) = 1$. But $|H : F(H)| = 3$, giving $|H_x| \leqslant 3$, a contradiction. Therefore case (c_1) does not hold, and so, since we have assumed that H acts neither semi-regularly nor transitively on $(\hat{N})^{\#}$, Theorem 1.16 yields that the only remaining possibilities are $H \cong \mathcal{T}_0(q^{n/2})$ with $|H_\lambda| = 2$ for all $\lambda \in (\hat{N})^{\#}$, or one of the cases (d_1), (e_1), (f_1), must hold.

Hence H contains a central involution, z say, and $|H_\lambda| = 2$ for all $\lambda \in (\hat{N})^{\#}$. If $h \in H_x$ then by Lemma 1.17 there exists $\lambda \in (\hat{N})^{\#}$ such that

$h \in H_x$, whereupon $h^2 = 1$. We deduce that H_x is an elementary abelian 2-group of order at least 4. But, since z acts without fixed points on $(\hat{N})^{\#}$, we have $z \notin H_x$, and it is easily checked that none of the possibilities for H we are considering contain such a subgroup H_x. This contradiction proves that $|H_x| \leq k$ for all $x \in N^{\#}$.

Each H-orbit in $N^{\#}$ has size at least $|H|/k$. If t denotes the number of H-orbits in $(\hat{N})^{\#}$ then, since each H-orbit in $(\hat{N})^{\#}$ has size $|H|/k$, we must have $|(\hat{N})^{\#}| = t(|H|/k)$. By Lemma 1.17 t is precisely the number of H-orbits in $N^{\#}$, and therefore, from the fact that $|(\hat{N})^{\#}| = |N^{\#}|$, we see that each H-orbit in $N^{\#}$ has size precisely $|H|/k$. Thus H acts half-transitively on $N^{\#}$.

We have $G = NH$. Define an action of G on the set of all elements of N by

$$x(yh) = (xy)^h$$

for all elements x, y, of N, and for all $h \in H$. Then G acts as a group of permutations on the elements of N, and G acts transitively since N acts transitively. It is easily verified that $H = G_1$, the stabiliser of $1 \in N$. As shown above H acts half-transitively on $N^{\#}$, whereupon G is a 3/2-transitive permutation group.

Q.E.D.

Thus, in the very special case in which G is a primitive soluble group as well as a high-fidelity group, we have strong restrictions on the structure of G; for example, it is not difficult to show that the nilpotent length of G is at most 4. These restrictions arise because of conditions on the action of G on $\hat{N}$, where N denotes the unique minimal normal subgroup of G.

For an arbitrary group G the <u>socle</u> of G, written soc(G), is defined

to be the product of all minimal normal subgroups of G. Obviously soc(G) char G. We might ask whether, for an arbitrary high-fidelity group G, the conditions on the action of G on Irr(soc(G)) are strong enough to impose correspondingly strong restrictions on the structure of G. This is a question which we shall attempt to answer, necessitating a careful study of the action of a group G on Irr(soc(G)).

Let G be a group. For any field K, a KG-module consisting of a direct sum of irreducible KG-modules which are all mutually G-isomorphic is said to be <u>homogeneous</u>. An abelian minimal normal subgroup of G may be regarded additively in the usual way as an irreducible GF(q)G-module for some prime q. There are certain subgroups of soc(G) which will be of special interest, namely those subgroups formed by taking the product of all abelian minimal normal subgroups of G which lie in the same G-isomorphism class. If M is a subgroup of soc(G) formed in this way then $M \triangleleft G$, and we say that M is a <u>homogeneous subgroup</u> of soc(G). Considered additively, M is a homogeneous GF(q)G-module for some prime q.

NOTATION. If G is a group and N a subgroup of soc(G) then B(N) denotes the set

$$\{ \chi \in \mathrm{Irr}(N) : \ker\chi \text{ contains no non-trivial normal subgroup of } G\}$$

We turn our attention to the homogeneous subgroups of the socle of a group, together with the irreducible characters of such subgroups. It will be convenient to fix some notation which will remain fixed through to the end of the proof of Lemma 1.20.

Let G be a group and M a homogeneous subgroup of soc(G). Assume that

$$M = N_1 \times N_2 \times \ldots \times N_c$$

where N_i is a minimal normal subgroup of G for $1 \leqslant i \leqslant c$, and let $|N_1| = q^r$ for some prime q. In addition let K denote $\mathrm{Hom}_G(N_1, N_1)$. Then K is a

finite dimensional vector space over the field GF(q), say $\dim_{GF(q)}K = a$. We have $|K| = q^a$.

By Schur's Lemma K is a division ring and so, by Wedderburn's well known theorem on finite division rings (see the list of basic results) it follows that K is a field. Additively, N_1 is a vector space over K, and we have

$$r = \dim_{GF(q)}N_1 = (\dim_K N_1)(\dim_{GF(q)}K) = (\dim_K N_1)a,$$

whence $\dim_K N_1 = r/a$.

By Lemma 1.11, if for all $\lambda \in \hat{N}_1$, $\alpha \in K$, we define

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

for all $x \in N_1$, then K becomes a subgroup of $\mathrm{Aut}(\hat{N}_1)$. It is easily verified that, additively, $\hat{N}_1$ is a vector space over the field K. Since $N_1 \cong \hat{N}_1$ we have $\dim_K \hat{N}_1 = \dim_K N_1 = r/a$.

By assumption M is a homogeneous subgroup of soc(G), and therefore if $i \in \{1,\ldots,c\}$ then N_i is G-isomorphic to N_1. Let $\tau_i : N_1 \to N_i$ be a G-isomorphism for $1 \leq i \leq c$. If $\lambda \in \hat{M}$ and if $i \in \{1,\ldots,c\}$ then let λ_i denote the element of $\hat{N}_1$ defined by

$$\lambda_i(x) = \lambda(x^{\tau_i})$$

for all $x \in N_1$.

The results of È.M. Žmud′in [17] provide us with information concerning the subset of $\hat{M}$ denoted by B(M).

LEMMA 1.19. (Žmud′ [17] §§ 2 & 3.). <u>The map</u> $\lambda \mapsto (\lambda_1, \lambda_2, \ldots, \lambda_c)$ <u>is a bijection from</u> $\hat{M}$ <u>to the set of all ordered subsets of</u> $\hat{N}_1$ <u>of size</u> c. <u>We have</u> $\lambda \in B(M)$ <u>if and only if</u> $\lambda_1, \lambda_2, \ldots, \lambda_c$, <u>are linearly independent over</u> K. <u>In particular</u> $B(M) \neq \emptyset$ <u>if and only if</u> $c \leq r/a$.

NOTE 1. In [17] the action of K on $\hat{N}_1$ is not as defined above, but rather is defined by

$$\lambda^{\alpha}(x) = \lambda(x^{\alpha})$$

for all $\lambda \in \hat{N}_1$, $\alpha \in K$, $x \in N_1$. It is trivial to check that this difference does not affect the veracity of Lemma 1.19.

NOTE 2. The results of [17] are proved in rather greater generality than is indicated by Lemma 1.19. In [17] the author is concerned with those characters λ of M such that $\ker\lambda$ contains no non-trivial normal subgroup of G, and $\lambda = \mu_1 + \mu_2 + \ldots + \mu_k$ for some integer k with $\mu_i \in \hat{M}$ $(1 \leq i \leq k)$. Lemma 1.19 is the case $k = 1$.

As an easy consequence of Lemma 1.19 we have the following result.

LEMMA 1.20. <u>If</u> $c = r/a$ <u>and</u> $\lambda \in B(M)$ <u>then</u> $G_\lambda = C_G(M)$.

<u>Proof</u>. Assume that $c = r/a$ and that $\lambda \in B(M)$. Clearly $C_G(M) \leq G_\lambda$. To obtain the opposite inclusion, let $g \in G_\lambda$. If $x \in N_1$ and $i \in \{1,\ldots,c\}$ we have

$$\lambda_i^g(x) = \lambda_i(gxg^{-1}) = \lambda((gxg^{-1})^{\tau i}) = \lambda(g(x^{\tau i})g^{-1}),$$

the last equality being a consequence of the fact that τ_i is a G-isomorphism. Hence

$$\lambda_i^g(x) = \lambda(g(x^{\tau i})g^{-1}) = \lambda^g(x^{\tau i}) = \lambda(x^{\tau i}) = \lambda_i(x),$$

and thus $\lambda_i^g = \lambda_i$.

By Lemma 1.19 the elements $\lambda_1, \lambda_2, \ldots, \lambda_c$, of $\hat{N}_1$ are linearly independent over K, and therefore, since $\dim_K \hat{N}_1 = r/a = c$, we deduce that $\{\lambda_1, \lambda_2, \ldots, \lambda_c\}$ is a K-basis for $\hat{N}_1$. As shown above, we have $\lambda_i^g = \lambda_i$ for $1 \leq i \leq c$, and, obviously, $(\lambda_i^{\alpha})^g = (\lambda_i^g)^{\alpha}$ for all $\alpha \in K$ and $1 \leq i \leq c$.

Consequently $g \in C_G(\hat{N}_1)$, and so, by Lemma 1.11, $g \in C_G(N_1)$. But, since M is homogeneous, we have $C_G(N_1) = C_G(M)$, whereupon $G_\lambda \leqslant C_G(M)$ and the proof is complete.

Q.E.D.

Next we state the result due to Akizuki and Shoda which gives a necessary and sufficient condition that $\mathrm{Firr}(G) \neq \emptyset$ for a group G.

THEOREM 1.21. (Shoda [15]). *Let* G *be a group, and let* $M_1, \ldots, M_s$, *denote the homogeneous subgroups of* soc(G), *with* N_i *a minimal normal subgroup of* G *contained in* M_i *for* $1 \leqslant i \leqslant s$. *If* $i \in \{1, \ldots, s\}$ *let* q_i *be a prime and* r_i *an integer such that* $|N_i| = q_i^{r_i}$, *and assume that* M_i *is a direct product of* c_i G-*isomorphic copies of* N_i. *In addition let the field* $\mathrm{Hom}_G(N_i, N_i)$ *have exactly* $q_i^{a_i}$ *elements. Then* $\mathrm{Firr}(G) \neq \emptyset$ *if and only if* $c_i \leqslant r_i/a_i$ *for* $1 \leqslant i \leqslant s$.

We shall require some facts concerning the structure of group algebras. Let G be a group, and K a field. The group algebra KG is a quasi-Frobenius algebra (see, for example, [1] Chapter VIII §66 Remark 2). We denote the Jacobson radical of KG by J(KG). Since MJ(KG) = 0 for all irreducible KG-modules M, an irreducible KG-module is an irreducible KG/J(KG)-module and vice versa. In what follows we shall make no distinction between an irreducible KG-module and an irreducible KG/J(KG)-module.

The *socle* of KG, denoted by S(KG), is defined to be the sum of all minimal right ideals in KG. It is a fact ([1] Chapter VIII Theorem 58.12) that S(KG) is precisely the sum of all minimal *left* ideals in KG, and thus S(KG) is a two-sided ideal in KG. Clearly S(KG) is completely reducible, both as a right and as a left KG-module.

As in [14] Section 1.8, we may decompose the group algebra KG, considered as a right KG-module, into a direct sum of principal indecomposable submodules, and there exist primitive idempotents $e_1, \ldots, e_n$, such

that

$$KG = e_1KG \oplus \ldots \oplus e_nKG \tag{1}$$

is such a decomposition, where $1 = e_1 + \ldots + e_n$.

LEMMA 1.22. ([14] Theorem 1.8, Exercise 6 of Section 1.8). Let G be a group, K a field, and assume that the group algebra KG has the decomposition (1) above. If $i \in \{1, \ldots, n\}$ then

(i) the principal indecomposable KG-module e_iKG has a unique maximal submodule, namely $e_iJ(KG) = e_iKG \cap J(KG)$;

(ii) the module e_iKG contains a unique irreducible submodule, and this irreducible submodule is G-isomorphic to $e_iKG/e_iJ(KG)$.

Our next result is a statement of the well known structure theorem for a semi-simple algebra of finite dimension over a field.

THEOREM 1.23.([6] V §§3,4.) Let A be a semi-simple algebra of finite dimension over a field K. Then A may be decomposed as a direct sum of minimal right ideals. Let $A = A_1 \oplus \ldots \oplus A_n$ be any such decomposition, and assume that N is an irreducible A-module. In addition, let $\dim_K N = r$, and let $\dim_K(\mathrm{Hom}_A(N, N)) = a$. Then there are exactly r/a of the ideals A_i which are isomorphic to N as right A-modules.

NOTE. The exact formulation of Theorem 1.23 does not appear in [6]. The theorem is a combination of [6] V Hauptsatz 3.3, together with a direct consequence of the results in [6] V Satz 3.8, Satz 4.1, Haupsatz 4.4, Satz 4.5.

THEOREM 1.24. Let G be a group, K a field, and assume that the group algebra KG has the decomposition (1) above. Then

$$S(KG) = e_1S(KG) \oplus \ldots \oplus e_nS(KG),$$

and $e_iS(KG)$ is an irreducible KG-submodule of the principal indecomposable KG-module e_iKG for $1 \leq i \leq n$. Moreover $KG/J(KG)$ and $S(KG)$ are isomorphic KG-modules. If N is an irreducible KG-module with $\dim_K N = r$ and $\dim_K(\mathrm{Hom}_G(N, N)) = a$, then there are exactly r/a of the $e_iS(KG)$ which are G-isomorphic to N.

Proof. Since $1 = e_1 + \ldots + e_n$, the decomposition

$$S(KG) = e_1S(KG) \oplus \ldots \oplus e_nS(KG)$$

is obvious. As remarked above, $S(KG)$ is a two-sided ideal in KG and a completely reducible right KG-module. Consequently, if $i \in \{1, \ldots, n\}$ then $e_iS(KG)$ is a completely reducible KG-submodule of the principal indecomposable KG-module e_iKG. By Lemma 1.22(ii) the module e_iKG contains a unique irreducible submodule, and hence $e_iS(KG)$ is precisely that unique irreducible submodule of e_iKG. Moreover, again by Lemma 1.22(ii), the modules $e_iS(KG)$ and $e_iKG/e_iJ(KG)$ are G-isomorphic.

From Lemma 1.22(i) and the decomposition (1) we see that

$$KG/J(KG) \cong e_1KG/e_1J(KG) \oplus \ldots \oplus e_nKG/e_nJ(KG)$$

as KG-modules. Thus, since $e_iS(KG) \cong e_iKG/e_iJ(KG)$ for $1 \leq i \leq n$, it follows that

$$KG/J(KG) \cong e_1S(KG) \oplus \ldots \oplus e_nS(KG) = S(KG) \qquad (2)$$

as KG-modules.

Let N be an irreducible KG-module with $\dim_K N = r$ and $\dim_K(\mathrm{Hom}_G(N, N)) = a$. Using (2) above and the fact that $KG/J(KG)$ is a semi-simple algebra over K, Theorem 1.23 implies that there are exactly r/a of the modules $e_iS(KG)$ which are G-isomorphic to N.

Q.E.D.

We are at last in a position to show that if H is any group, and C a non-trivial cyclic group, then $C \underset{r}{\sim} H$ is a high-fidelity group. Details of the construction $C \underset{r}{\sim} H$ and its properties may be found in [6] I § 15.

THEOREM 1.25. <u>Assume that</u> H <u>is a group, and that</u> C <u>is a non-trivial cyclic group. Let</u> G <u>denote</u> $C \underset{r}{\sim} H$, <u>the regular wreath product of</u> C <u>with</u> H. <u>Then</u> $\mathrm{Firr}(G) \neq \emptyset$. <u>Furthermore, if</u> $\chi \in \mathrm{Firr}(G)$ <u>then</u> $\chi(1) = |H|$, <u>whereupon</u> G <u>is a high-fidelity group. Any group is isomorphic to a subgroup, and to a factor group, of some high-fidelity group.</u>

<u>Proof</u>. From the nature of the construction $G = C \underset{r}{\sim} H$ we have the following facts. Firstly, $|G| = |C|^{|H|}|H|$. Secondly, G contains a normal subgroup, D say, such that D is isomorphic to a direct product of $|H|$ copies of C. Thirdly, D is complemented in G by a subgroup, X say, such that $X \cong H$. Moreover, the $|X|$ direct factors of D may be labelled D_x as x varies over the elements of X, in such a way that

$$y^{-1}(D_x)y = D_{xy}$$

for all elements x, y, of X. Since $D_x \cong C$, a cyclic group, there exists a generating set $\{d_x\}_{x \in X}$ for D such that

$$y^{-1}d_x y = d_{xy}$$

for all elements x, y, of X. Clearly $C_G(D) = D$, whence $\mathrm{soc}(G) \leqslant D$. Therefore soc(G) is abelian.

Let N be a minimal normal subgroup of G. Since N is abelian, it follows that N is an elementary abelian q-group for some prime q. Let M denote the homogeneous subgroup of soc(G), containing N, and assume that M is a direct product of c G-isomorphic copies of N. In addition, let $|N| = q^r$, and let $|\mathrm{Hom}_G(N, N)| = q^a$. Assume that S denotes the unique

Sylow q-subgroup of D, and write $E = \Omega_1(S)$; that is, E is the subgroup of S generated by all elements of S of order q. Obviously E is an elementary abelian q-group, and $|E| = q^{|X|}$. Furthermore, if α denotes $|C|/q$, and if we write $e_x = d_x^{\alpha}$, then $\{e_x\}_{x \in X}$ is a generating set for E and,

$$y^{-1}e_x y = e_{xy} \tag{1}$$

for all elements x, y, of X. Clearly $E \triangleleft G$, and $M \leqslant E$. In addition, $C_X(E) = 1$.

Regarded additively, with X acting by conjugation, E is a GF(q)X-module with GF(q)-basis $\{e_x\}_{x \in X}$. From the nature of the X-action on the basis $\{e_x\}$, it is apparent that, as GF(q)X-modules, the group algebra GF(q)X and E are isomorphic. Since $D \leqslant C_G(N)$, it follows that N is irreducible as a GF(q)X-module, and that $\mathrm{Hom}_G(N, N) = \mathrm{Hom}_X(N, N)$. Now as a GF(q)X-module, M is the sum of all irreducible GF(q)X-submodules of E which are X-isomorphic to N, and M is a direct sum of c X-isomorphic copies of N. Hence, by Theorem 1.24, we have $c = r/a$. Theorem 1.21 yields $\mathrm{Firr}(G) \neq \emptyset$.

Let $\chi \in \mathrm{Firr}(G)$, and write

$$\chi_D = e \sum_{i=1}^{t} \theta_i$$

where $\theta_i \in \mathrm{Irr}(D)$ for $1 \leqslant i \leqslant t$. Let θ denote θ_1. Since D is abelian we have $\theta(1) = 1$. From the fact that all the θ_i are conjugate in G, and since $\chi \in \mathrm{Firr}(G)$, it follows that $\ker\theta$ contains no non-trivial normal subgroup of G. We shall show that $G_\theta = D$. Clearly $D \leqslant G_\theta$, and, since $G = DX$, we must have $G_\theta = DX_\theta$. Again let N denote a minimal normal subgroup of G, with q, M, c, r, a, E, $\{e_x\}_{x \in X}$, as before. As proved above, $c = r/a$. We show first that $q \nmid |X_\theta|$.

Suppose that $q \mid |X_\theta|$, and let y be an element of X_θ of order q. We have

$$\theta(e_x) = \theta^y(e_x) = \theta(ye_xy^{-1}) = \theta(e_{xy^{-1}}) \qquad (2)$$

for all $x \in X$. Now y^{-1} permutes the elements of the set $\{e_x\}_{x \in X}$ by conjugation in orbits of length $q = |y^{-1}|$, and (2) shows that θ is constant on each orbit. Assume that y^{-1} permutes the elements of $\{e_x\}_{x \in X}$ in exactly k orbits, say $E_1, \ldots, E_k$, and for $1 \leqslant i \leqslant k$, let $e_i \in E_i$. Since $|e_i| = q$ we must have $\theta(e_i)^q = 1$ for $1 \leqslant i \leqslant k$. Write

$$f = \prod_{x \in X} e_x ,$$

and let F denote $\langle f \rangle$. It is easily verified that $F \lhd G$. We have

$$\theta(f) = \theta(\prod_{x \in X} e_x) = \theta(\prod_{i=1}^{k} \prod_{e_x \in E_i} e_x) = \prod_{i=1}^{k} \theta(\prod_{e_x \in E_i} e_x) =$$

$$\prod_{i=1}^{k} \theta(e_i)^{|E_i|} = \prod_{i=1}^{k} \theta(e_i)^q = 1.$$

Hence $F \leqslant \ker\theta$, a contradiction since $\ker\theta$ contains no non-trivial normal subgroup of G. Therefore $q \nmid |X_\theta|$.

Let λ denote θ_M. Then $\lambda \in \mathrm{Irr}(M)$, and, since $\ker\lambda \leqslant \ker\theta$, it follows that $\ker\lambda$ contains no non-trivial normal subgroup of G. Thus $\lambda \in B(M)$. As noted above, we have $c = r/a$, whereupon Lemma 1.20 yields $G_\lambda = C_G(M) = C_G(N)$. Obviously $G_\theta \leqslant G_\lambda$, and we deduce that $X_\theta \leqslant G_\theta \leqslant C_G(N)$. Therefore X_θ centralises each minimal normal subgroup of G. In particular, X_θ centralises each minimal normal subgroup of G contained in E.

As remarked earlier, regarded additively as a GF(q)X-module, E is isomorphic to the group algebra GF(q)X. Clearly the minimal normal subgroups of G contained in E are precisely the irreducible GF(q)X-submodules of E, and, by Theorem 1.24, every irreducible GF(q)X-module is X-isomorphic to some GF(q)X-submodule of E. Consequently X_θ centralises each irreducible GF(q)X-module. Let

$$1 = Q_0 < Q_1 < \ldots < Q_{s-1} < Q_s = E$$

be an X-composition series for E. Then Q_i/Q_{i-1} is an irreducible $GF(q)X$-module for $1 \leqslant i \leqslant s$. Hence X_θ is a q'-group of automorphisms of the q-group E such that X_θ centralises Q_i/Q_{i-1} for $1 \leqslant i \leqslant s$. We deduce that $X_\theta = 1$, and then $G_\theta = DX_\theta = D$.

By Theorem 1.9 we have $\theta^G = \chi$, whence $\chi(1) = \theta^G(1) = \theta(1)|G : D| = |H|$ as required. It follows that G is a high-fidelity group. Since $H \cong X \cong G/D$ it is clear that any group is isomorphic to a subgroup, and to a factor group, of some high-fidelity group.

Q.E.D.

We see from Theorem 1.25 that, if G is an arbitrary group, the conditions $Firr(G) \neq \emptyset$ and all characters in Firr(G) have the same degree do not impose any obvious restrictions on the structure of G apart from those imposed by the condition that $Firr(G) \neq \emptyset$ alone. Later, using a suitable generalisation of the idea of a half-transitive group of permutations on a set, we shall generalise the results obtained earlier in this chapter on primitive soluble high-fidelity groups to soluble high-fidelity groups with a unique minimal normal subgroup. We close this chapter by showing that if G is any soluble group, then there exists a certain non-empty subset of Irr(G), which we shall denote by $Irr^*(G)$, such that the condition that all characters in $Irr^*(G)$ have the same degree imposes strong restrictions on the structure of G.

For any soluble group G, let n(G) denote the nilpotent length of G.

DEFINITION. If G is a soluble group then the subset $Irr^*(G)$ of Irr(G) is defined by

$$Irr^*(G) = \{\chi \in Irr(G) : n(G/\ker\chi) = n(G)\}.$$

Notice that $Firr(G) \subseteq Irr^*(G)$. However, as we shall show, it is an immediate consequence of [8] Theorem 12.14 that, unlike Firr(G), the set

$\mathrm{Irr}^*(G)$ is non-empty for any soluble group G.

LEMMA 1.26. ([8] Theorem 12.24). Let G be a group, $\chi \in \mathrm{Irr}(G)$, and assume that $F/\ker\chi = F(G/\ker\chi)$. If F is not nilpotent then there exists $\psi \in \mathrm{Irr}(G)$ such that $\ker\psi < \ker\chi$.

THEOREM 1.27. Let G be a soluble group. If $\chi \in \mathrm{Irr}(G)$ such that $\ker\chi$ is minimal among the kernels of all irreducible characters of G, then $\chi \in \mathrm{Irr}^*(G)$. In particular $\mathrm{Irr}^*(G) \neq \emptyset$.

Proof. Let $\chi \in \mathrm{Irr}(G)$ such that $\ker\chi$ is minimal. If $F/\ker\chi$ denotes $F(G/\ker\chi)$ then, by Lemma 1.26 and the minimality of $\ker\chi$, it follows that F is nilpotent, whereupon $F = F(G)$. Clearly, then, $n(G/\ker\chi) = n(G)$, giving $\chi \in \mathrm{Irr}^*(G)$ as required.

Q.E.D.

If G is any group then $\Phi(G)$ denotes the Frattini subgroup of G.

LEMMA 1.28. ([6] III Satz 4.5). Let G be a group. Then $F(G)/\Phi(G) = F(G/\Phi(G))$ is a direct product of abelian minimal normal subgroups of $G/\Phi(G)$.

LEMMA 1.29. Let G be a soluble group, and assume that $\chi \in \mathrm{Irr}^*(G)$ such that $\ker\chi$ is maximal among the kernels of characters in $\mathrm{Irr}^*(G)$. Then $G/\ker\chi$ is a primitive soluble group.

Proof. For all subgroups H of G such that $\ker\chi \leqslant H \leqslant G$, let $\overline{H}$ denote the group $H/\ker\chi$. Since $\chi \in \mathrm{Irr}^*(G)$ we have $n(\overline{G}) = n(G)$. Assume that N is a normal subgroup of G such that $\ker\chi \leqslant N$ and $n(G/N) = n(G)$. Theorem 1.27 implies that $\mathrm{Irr}^*(G/N) \neq \emptyset$, and hence there exists $\psi \in \mathrm{Irr}(G)$ such that $N \leqslant \ker\psi$ and $n(G/\ker\psi) = n(G/N) = n(G)$. Thus $\ker\chi \leqslant N \leqslant \ker\psi$, and $\psi \in \mathrm{Irr}^*(G)$. Therefore, by maximality of $\ker\chi$, we must have $\ker\chi = N = \ker\psi$.

Let $M/\ker\chi$ denote $\Phi(\overline{G})$. By Lemma 1.28 we have $F(\overline{G}/\Phi(\overline{G})) = F(\overline{G})/\Phi(\overline{G})$, and consequently $n(G/M) = n(\overline{G}/\Phi(\overline{G})) = n(\overline{G}) = n(G)$. Therefore, as proved above, we must have $M = \ker\chi$, whereupon $\Phi(\overline{G}) = 1$. By Lemma 1.28 the group $F(\overline{G})$ is a direct product of minimal normal subgroups of $\overline{G}$, say $F(\overline{G}) = \overline{N}_1 \times \overline{N}_2 \times \ldots \times \overline{N}_t$ where $\overline{N}_i$ is a minimal normal subgroup of $\overline{G}$ for $1 \leqslant i \leqslant t$. Suppose that $t > 1$. It is a fact that for any natural number n, the class of all soluble groups with nilpotent length at most n is a formation (see the list of basic results), and hence there exists $j \in \{1,\ldots, t\}$ such that $n(\overline{G}/\overline{N}_j) = n(\overline{G})$. Thus $\ker\chi \leqslant N_j$ with $n(G/N_j) = n(\overline{G}/\overline{N}_j) = n(\overline{G}) = n(G)$, and so, as shown above, we must have $\ker\chi = N_j$. Therefore $N/\ker\chi = \overline{N}_j = 1$, a contradiction. We deduce that $t = 1$; that is, $F(\overline{G})$ is a minimal normal subgroup of $\overline{G}$. From the remarks made earlier concerning primitive soluble groups, it follows that $\overline{G} = G/\ker\chi$ is a primitive soluble group.

Q.E.D.

LEMMA 1.30. ([8] Theorem 12.19). *Let* G *be a soluble group such that* $F(G) < G$. *If* $\chi \in \mathrm{Irr}(G)$ *such that* $\ker\chi \not< F(G)$ *then there exists* $\psi \in \mathrm{Irr}(G)$ *such that* $\psi(1) > \chi(1)$ *and* $\ker\psi < \ker\chi$.

LEMMA 1.31. ([8] Lemma 5.11). *If* G *is a group and* $\theta \in \mathrm{Irr}(H)$ *for some subgroup*, H, *of* G *then*

$$\ker(\theta^G) = \bigcap_{g \in G} (\ker\theta)^g.$$

THEOREM 1.32. *Assume that* G *is a soluble group such that all characters in* $\mathrm{Irr}^*(G)$ *have the same degree, and let* $\chi \in \mathrm{Irr}^*(G)$ *such that* $\ker\chi$ *is maximal among the kernels of characters in* $\mathrm{Irr}^*(G)$. *Then* $G/\ker\chi$ *is a primitive soluble high-fidelity group, and* $F(G)/\ker\chi$ *is the unique minimal normal subgroup of* $G/\ker\chi$. *In addition,* $F(G)$ *is abelian.*

Proof. Obviously we may assume that $G > 1$. Lemma 1.29 implies that

$G/\ker\chi$ is a primitive soluble group. If $\zeta \in \mathrm{Firr}(G/\ker\chi)$ then ζ may be regarded as an element of $\mathrm{Irr}(G)$ such that $\ker\zeta = \ker\chi$. Then $n(G/\ker\zeta) = n(G/\ker\chi) = n(G)$, whereupon $\zeta \in \mathrm{Irr}^*(G)$. Since, by assumption, all characters in $\mathrm{Irr}^*(G)$ have the same degree, it follows that all characters in $\mathrm{Firr}(G/\ker\chi)$ have the same degree, and that the common degree of all elements of $\mathrm{Irr}^*(G)$ is precisely the common degree of all elements of $\mathrm{Firr}(G/\ker\chi)$. Thus, in particular, $G/\ker\chi$ is a high-fidelity group.

Assume that G is nilpotent. Then $G/\ker\chi$ is nilpotent. The group $G/\ker\chi$ is primitive, so that $G/\ker\chi = F(G/\ker\chi)$ is the unique minimal normal subgroup of $G/\ker\chi$. Consequently $G/\ker\chi$ is cyclic. It follows that all characters in $\mathrm{Firr}(G/\ker\chi)$ have degree 1, and thus all characters in $\mathrm{Irr}^*(G)$ have degree 1. But G is nilpotent, whereupon $n(G) = 1$, and $\mathrm{Irr}^*(G)$ consists of all non-trivial elements of $\mathrm{Irr}(G)$. Hence all characters in $\mathrm{Irr}(G)$ have degree 1, and we deduce that G is abelian. Thus if G is nilpotent the theorem holds.

Assume now that G is not nilpotent; that is, assume that $F(G) < G$, and let F denote $F(G)$. Let $\zeta \in \mathrm{Irr}^*(G)$, and suppose that $\ker\zeta \not< F$. Then, by Lemma 1.30, there exists $\psi \in \mathrm{Irr}(G)$ such that $\psi(1) > \zeta(1)$ and $\ker\psi < \ker\zeta$. Obviously $\psi \in \mathrm{Irr}^*(G)$, a contradiction since all elements of $\mathrm{Irr}^*(G)$ have the same degree. Consequently $\ker\zeta < F$ for all $\zeta \in \mathrm{Irr}^*(G)$ In particular, $\ker\chi < F$, and therefore $F/\ker\chi$ is the unique minimal normal subgroup of $G/\ker\chi$. It follows that $F/\ker\chi$ is an elementary abelian q-group for some prime q, and by Lemma 1.13 we see that if $\zeta \in \mathrm{Firr}(G/\ker\chi)$ then $q \nmid \zeta(1)$. Hence, if $\psi \in \mathrm{Irr}^*(G)$, then $q \nmid \psi(1)$.

Let Q denote $O_q(G)$, and suppose that Q is non-abelian. Then, $1 < Q' \triangleleft G$, where Q' denotes the derived group of Q. Clearly there exists $\zeta \in \mathrm{Irr}(G)$ such that $Q' \not\leq \ker\zeta$. Let $\psi \in \mathrm{Irr}(G)$ be such that $\ker\psi \leq \ker\zeta$ and $\ker\psi$ is minimal among the kernels of all irreducible characters of G. By

Theorem 1.27 we have $\psi \in \mathrm{Irr}^*(G)$, and obviously $Q' \not\leq \ker\psi$. Write

$$\psi_Q = e \sum_{i=1}^{t} \theta_i ,$$

where $\theta_i \in \mathrm{Irr}(Q)$ for $1 \leq i \leq t$. The θ_i are all conjugate in G, and therefore, since $Q' \triangleleft G$ and $Q' \not\leq \ker\psi$, we must have $Q' \not\leq \ker\theta_1$. Consequently $\theta_1(1) > 1$. Now $\theta_1(1) \mid |Q|$, and Q is a q-group. Hence $q \mid \theta_1(1)$. But $\psi(1) = et\theta_1(1)$, whereupon $q \mid \psi(1)$, a contradiction. We conclude that Q is abelian.

Let P denote the unique Hall q'-subgroup of F, so that $F = Q \times P$, and let R denote $Q \cap \ker\chi$. Then $R \triangleleft Q$ and $\ker\chi = R \times P$. Fix $1 \neq \lambda \in \mathrm{Irr}(Q/R)$, and let 1_P denote the trivial character of P. By Theorem 1.12 we have $\lambda \times 1_P \in \mathrm{Irr}(F)$. Write $\mu = \lambda \times 1_P$. Since $\ker\chi = R \times P \leq \ker\mu$ it follows that μ is a non-trivial element of $\mathrm{Irr}(F/\ker\chi)$. Now $G/\ker\chi$ is a primitive soluble high-fidelity group, and therefore, by Lemma 1.13, if $\zeta \in \mathrm{Firr}(G/\ker\chi)$ then $\zeta(1)$ is precisely the index in $G/\ker\chi$ of the stabiliser in $G/\ker\chi$ of μ. But, as is easily checked, the stabiliser in $G/\ker\chi$ of μ is exactly $G_\mu/\ker\chi$, whence $\zeta(1) = |G : G_\mu|$. Since $\mu = \lambda \times 1_P$ it follows that $G_\mu = G_\lambda$, whereupon $\zeta(1) = |G : G_\lambda|$. If $\psi \in \mathrm{Irr}^*(G)$ then $\psi(1) = \zeta(1)$, and we conclude that $\psi(1) = |G : G_\lambda|$ for all $\psi \in \mathrm{Irr}^*(G)$.

Since $F/\ker\chi$ is a minimal normal subgroup of $G/\ker\chi$ with $F = Q \times P$ and $\ker\chi = R \times P$, clearly Q/R is a chief factor of G. Let $\phi \in \mathrm{Irr}(P)$, and then, by Theorem 1.12, we have $\lambda \times \phi \in \mathrm{Irr}(F)$. Write $\theta = \lambda \times \phi$, and let ξ denote θ^G. By Lemma 1.31 we have

$$\ker\xi = \ker(\theta^G) = \bigcap_{g \in G} (\ker\theta)^g$$

Since $R \triangleleft G$ with $R \leq \ker\theta$, we have $R \leq Q \cap \ker\xi \leq Q$ and $Q \cap \ker\xi \triangleleft G$. Thus $Q \cap \ker\xi = R$, or $Q \cap \ker\xi = Q$. However, $Q \not\leq \ker\theta$, and therefore $Q \cap \ker\xi = R$. We deduce that $\ker\xi \leq R \times P = \ker\chi$, giving $n(G/\ker\xi) =$

$n(G/\ker\chi) = n(G)$.

Let $\xi = \xi_1 + \ldots + \xi_k$, where $\xi_i \in \mathrm{Irr}(G)$ for $1 \leqslant i \leqslant k$. We have

$$\ker\xi = \bigcap_{i=1}^{k} \ker\xi_i,$$

and so, using the formation property again, there exists $j \in \{1,\ldots, k\}$ such that $n(G/\ker\xi_j) = n(G/\ker\xi) = n(G)$. It follows that $\xi_j \in \mathrm{Irr}^*(G)$. Let ψ denote ξ_j, so that $\psi \in \mathrm{Irr}^*(G)$, and write

$$\psi_F = e \sum_{i=1}^{t} \theta_i$$

where $\theta_i \in \mathrm{Irr}(F)$ for $1 \leqslant i \leqslant t$. By Frobenius reciprocity we must have $\theta = \theta_i$ for some $i \in \{1,\ldots, t\}$. Now $\theta = \lambda \times \phi$, and hence $G_\theta \leqslant G_\lambda$. Since $t = |G : G_\theta| \geqslant |G : G_\lambda|$ and $\psi(1) = et\theta(1)$, we have

$$\psi(1) \geqslant e\,|G : G_\lambda|\,\theta(1) = e|G : G_\lambda|\,\phi(1).$$

But $\psi \in \mathrm{Irr}^*(G)$, and hence, as shown above, $\psi(1) = |G : G_\lambda|$. Therefore $e\phi(1) = 1$, whence $\phi(1) = 1$. By varying ϕ over $\mathrm{Irr}(P)$ we see that $\phi(1) = 1$ for all $\phi \in \mathrm{Irr}(P)$. Hence P is abelian, and thus $F = Q \times P$ is abelian.

Q.E.D.

CHAPTER 2

SOLUBLE HIGH-FIDELITY GROUPS WITH A UNIQUE MINIMAL NORMAL SUBGROUP.

In Chapter 1 it was shown that if G is a primitive soluble high-fidelity group then G acts half-transitively on the non-trivial elements of $\hat{N}$, where N denotes the unique minimal normal subgroup of G. In this chapter we consider a slightly larger class of soluble high-fidelity groups, namely soluble high-fidelity groups with a unique minimal normal subgroup. We show that if G is such a group with minimal normal subgroup N then, although G does not necessarily act half-transitively on $(\hat{N})^{\#}$, the action of G on $(\hat{N})^{\#}$ is, in a certain well-defined sense, "almost half-transitive."

EXAMPLE 2.1. We construct a soluble high-fidelity group G of order $2^{14}.3.7$ with a unique minimal normal subgroup N such that G does not act half-transitively on $(\hat{N})^{\#}$.

Let $A_i = \langle a_i \rangle$, $B_i = \langle b_i \rangle$, be cyclic groups of order 4 for $1 \leqslant i \leqslant 3$, and let

$$F = A_1 \times A_2 \times A_3 \times B_1 \times B_2 \times B_3$$

so that F is an abelian group of order 2^{12}. Define $\alpha \in \mathrm{Aut}(F)$ by $a_i^{\alpha} = b_i^3$, $b_i^{\alpha} = a_i$, for $1 \leqslant i \leqslant 3$ extended to the whole of F in the obvious way. If $i \in \{1,2,3\}$ then

$$a_i \xmapsto{\alpha} b_i^3 \xmapsto{\alpha} a_i^3 \xmapsto{\alpha} b_i \xmapsto{\alpha} a_i ,$$

and so $|\alpha| = 4$. Clearly α^2 is the automorphism of F that acts by inverting each element. Next define $\beta \in \mathrm{Aut}(F)$ by $a_i^{\beta} = a_i b_i$, $b_i^{\beta} = a_i b_i^2$, for $1 \leqslant i \leqslant 3$ extended to the whole of F in the obvious way. If $i \in \{1,2,3\}$ then

$$a_i \xmapsto{\beta} a_i b_i \xmapsto{\beta} a_i^2 b_i^3 \xmapsto{\beta} a_i ,$$

and

$$b_i \xmapsto{\beta} a_i b_i^2 \xmapsto{\beta} a_i^3 b_i \xmapsto{\beta} b_i \ ,$$

whereupon $|\beta| = 3$. Also

$$a_i^{(\alpha^3\beta\alpha)} = b_i^{(\beta\alpha)} = (a_i b_i^2)^\alpha = a_i^2 b_i^3 = a_i^{\beta^2} \ ,$$

and

$$b_i^{(\alpha^3\beta\alpha)} = (a_i^3)^{(\beta\alpha)} = (a_i^3 b_i^3)^\alpha = a_i^3 b_i = b_i^{\beta^2} .$$

Consequently $\alpha^3\beta\alpha = \beta^2$.

Define $\gamma \in \mathrm{Aut}(F)$ by $a_1^\gamma = a_2$, $b_1^\gamma = b_2$, $a_2^\gamma = a_1^3 a_2 a_3$, $b_2^\gamma = b_1^3 b_2 b_3$, $a_3^\gamma = a_1 a_2^3$, $b_3^\gamma = b_1 b_2^3$, extended to the whole of F in the obvious way. We have

$$a_1 \xmapsto{\gamma} a_2 \xmapsto{\gamma} a_1^3 a_2 a_3 \xmapsto{\gamma} a_2^3 a_3 \xmapsto{\gamma} a_1^2 a_2^2 a_3^3 \xmapsto{\gamma} a_1 a_2 a_3^2 \xmapsto{\gamma} a_1 a_3 \xmapsto{\gamma} a_1 \ ,$$

and

$$a_3 \xmapsto{\gamma} a_1 a_2^3 \xmapsto{\gamma} a_1 a_3^3 \xmapsto{\gamma} a_1^3 a_2^2 \xmapsto{\gamma} a_1^2 a_2 a_3^2 \xmapsto{\gamma} a_1 a_2 a_3 \xmapsto{\gamma} a_2 a_3 \xmapsto{\gamma} a_3 \ .$$

Similarly $b_1^{\gamma^7} = b_1$, $b_2^{\gamma^7} = b_2$, $b_3^{\gamma^7} = b_3$, and we deduce that $|\gamma| = 7$. It is easily verified that $\alpha\gamma = \gamma\alpha$ and that $\beta\gamma = \gamma\beta$.

Write $\langle \alpha, \beta, \gamma \rangle = H$, so that $H \leqslant \mathrm{Aut}(F)$. If H_1 denotes $\langle \alpha, \beta \rangle$, and if H_2 denotes $\langle \gamma \rangle$, then $H_1 = \langle \alpha, \beta : \alpha^4 = \beta^3 = 1, \ \alpha^{-1}\beta\alpha = \beta^{-1} \rangle$, and $H_2 \cong C_7$. Moreover $H = H_1 \times H_2$, and we have $|H| = 2^2.3.7 = 84$. Let G denote FH, the natural semi-direct product of F with H. It follows that $|G| = 2^{14}.3.7$, and obviously G is soluble. Write $N = \Omega_1(F) \lhd G$. Then N is an elementary abelian 2-group of order 2^6, and clearly, $\mathrm{soc}(G) \leqslant N$.

Regarded additively, N is a 6-dimensional H-module over the field GF(2). Furthermore, if R denotes $\langle \beta \rangle$ then

$$N = \langle a_1^2, b_1^2 \rangle \oplus \langle a_2^2, b_2^2 \rangle \oplus \langle a_3^2, b_3^2 \rangle \ ,$$

a direct sum of isomorphic irreducible GF(2)R-modules, faithful for R, and

$$N = \langle a_1^2, a_2^2, a_3^2 \rangle \oplus \langle b_1^2, b_2^2, b_3^2 \rangle ,$$

a direct sum of isomorphic irreducible $GF(2)H_2$-modules, faithful for H_2. Clearly, then, N is a faithful irreducible module for the group $R \times H_2 \cong C_{21}$, and it follows that N is the unique minimal normal subgroup of G. It is straightforward to check that $C_G(N) = \langle F, \alpha^2 \rangle$ and that $G/C_G(N) \cong S_3 \times C_7$.

The group G has a unique minimal normal subgroup and so, certainly, $Firr(G) \neq \emptyset$. We shall show that $\chi(1) = 84$ for all $\chi \in Firr(G)$. Let $\chi \in Firr(G)$, and write

$$\chi_F = e \sum_{i=1}^{t} \lambda_i$$

where $\lambda_i \in Irr(F)$ for $1 \leq i \leq t$. Write $\lambda = \lambda_1$. Since F is abelian, we have $\lambda(1) = 1$, and then, by Lemma 1.10, $G_\lambda = \{g \in G : [g,x] \in \ker\lambda$ for all $x \in F\}$. Also, since $G = FH$, we have $G_\lambda = FH_\lambda$. By Clifford's Theorem the λ_i are all conjugate in G, and from the fact that $\chi \in Firr(G)$ we have $\ker\chi_F = \bigcap_{i=1}^{t} \ker\lambda_i = 1$. Consequently $\ker\lambda_i$ contains no non-trivial normal subgroup of G for $1 \leq i \leq t$. In particular $\ker\lambda$ contains no non-trivial normal subgroup of G.

Suppose that $H_\lambda > 1$. Since $|H| = 2^2.3.7$ we must have $2 \mid |H_\lambda|$, or $3 \mid |H_\lambda|$, or $7 \mid |H_\lambda|$. Suppose that $2 \mid |H_\lambda|$. Then H_λ contains an involution of H. From the structure of the group H we see that H contains a unique involution, namely α^2. Hence $\alpha^2 \in H_\lambda$. It follows that $[\alpha^2, x] \in \ker\lambda$ for all $x \in F$. But $x^{\alpha^2} = x^{-1}$ for all $x \in F$, whereupon $x^2 = (x^{-1})^{\alpha^2} x = [\alpha^2, x] \in \ker\lambda$ for all $x \in F$. Thus $\ker\lambda \geq \langle a_1^2, a_2^2, a_3^2, b_1^2, b_2^2, b_3^2 \rangle = N \triangleleft G$, a contradiction. Hence $2 \nmid |H_\lambda|$.

Suppose that $3 \mid |H_\lambda|$. Then H_λ contains a Sylow 3-subgroup of H, but

H contains a unique Sylow 3-subgroup, namely $R = \langle\beta\rangle$. Therefore $[\beta,x] \in \ker\lambda$ for all $x \in F$, and so $[\beta, a_i^3]$, $[\beta, b_i^3]$, are elements of $\ker\lambda$ for all $1 \leqslant i \leqslant 3$. But $[\beta, a_i^3] = a_i^{\beta}a_1^3 = b_i$, and $[\beta, b_i^3] = b_1^{\beta}b_1^3 = a_ib_i$, whereupon $\ker\lambda \geqslant \langle a_1, a_1b_1, a_2, a_2b_2, a_3, a_3b_3\rangle = F \triangleleft G$, a contradiction. Hence $3 \nmid |H_\lambda|$.

Similarly it can be shown that $7 \nmid |H_\lambda|$, and thus we were incorrect in supposing that $H_\lambda > 1$. Consequently $H_\lambda = 1$, giving $G_\lambda = F$. By Theorem 1.9 we have $\lambda^G = \chi$, and hence $\chi(1) = \lambda^G(1) = |G : F|\lambda(1) = 84$. We conclude that $\chi(1) = 84$ for all $\chi \in \mathrm{Firr}(G)$, and, in particular, G is a high-fidelity group.

All that remains to prove is that G does not act half-transitively on $(\hat{N})^{\#}$. Suppose that the action of G on $(\hat{N})^{\#}$ is half-transitive, and write $\overline{G} = G/C_G(N)$. Then $\overline{G} \cong S_3 \times C_7$, and by Lemma 1.11 $\hat{N}$, regarded additively, is an irreducible $GF(2)\overline{G}$-module, faithful for $\overline{G}$. Moreover, since $(\overline{G})_\mu = G_\mu/C_G(N)$, the group $\overline{G}$ acts half-transitively on $(\hat{N})^{\#}$. Obviously the cyclic normal subgroup of $\overline{G}$ of order 21 acts semi-regularly on $(\hat{N})^{\#}$, whereupon $|(\overline{G})_\mu| \leqslant 2$ for all $\mu \in (\hat{N})^{\#}$. Since $|\hat{N}| = 2^6$ and $2 \mid |\overline{G}|$ it follows that $\overline{G}$ does not act semi-regularly on $(\hat{N})^{\#}$, and then, from the fact that $\overline{G}$ acts half-transitively on $(\hat{N})^{\#}$, we must have $|(\overline{G})_\mu| = 2$ for all $\mu \in (\hat{N})^{\#}$. Let I denote the set of involutions of $\overline{G}$. Then

$$(\hat{N})^{\#} = \bigcup_{x \in I} (C_{\hat{N}}(x))^{\#}. \tag{1}$$

From the structure of $\overline{G}$ we have $|I| = 3$, and the elements of I are all mutually conjugate in $\overline{G}$. Hence, if $I = \{x_1, x_2, x_3\}$ then $\dim_{GF(2)}C_{\hat{N}}(x_1) = \dim_{GF(2)}C_{\hat{N}}(x_2) = \dim_{GF(2)}C_{\hat{N}}(x_3) = n$, say. Moreover, if $i,j \in \{1,2,3\}$ such that $i \neq j$, and if $\mu \in (C_{\hat{N}}(x_i))^{\#} \cap (C_{\hat{N}}(x_j))^{\#}$, then $\langle x_i, x_j\rangle \leqslant \overline{G}_\mu$ contradicting $|(\overline{G})_\mu| = 2$. We deduce that the right hand side of (1) is a disjoint union, which gives

$$63 = 2^6 - 1 = |(\hat{N})^{\#}| = 3(2^n - 1),$$

clearly an impossibility. Therefore G does not act half-transitively on $(\hat{N})^{\#}$, and this completes the example.

It is easily seen that in Example 2.1 the group G has precisely 2 orbits in $(\hat{N})^{\#}$; one of size 21 and one of size 42. Thus the sizes of the G-orbits in $(\hat{N})^{\#}$ all have the form 21.(a power of 2). Loosely speaking we might say that G acts on $(\hat{N})^{\#}$ half-transitively up to multiplication by powers of the prime 2. We shall show that something of the sort always occurs whenever G is a soluble high-fidelity group with unique minimal normal subgroup N.

Let G be a group and $\chi \in \mathrm{Irr}(G)$. Following [8] we let $V(\chi)$ denote the <u>vanishing-off</u> subgroup of χ; that is $V(\chi) = \langle g \in G : \chi(g) \neq 0 \rangle$. We have $V(\chi) \triangleleft G$, and $V(\chi)$ may be characterised as the smallest subgroup H of G such that $\chi(g) = 0$ for all $g \in G \backslash H$.

LEMMA 2.2. ([8] Lemma 12.17). <u>Let</u> G <u>be a group,</u> H <u>a subgroup of</u> G, <u>and</u> $\theta \in \mathrm{Irr}(H)$. <u>Assume that</u> $\chi_H = \theta$ <u>for each irreducible constituent</u> , χ, <u>of</u> θ^G. <u>Then</u> $V(\theta) \triangleleft G$.

Let G be a group. If there exists $\chi \in \mathrm{Irr}(G)$ such that $\chi(1)^2 = |G : Z(G)|$ then G is said to be of <u>central type</u>. Our next result is a characterisation of groups of central type due to F. Demeyer and G. Janusz.

LEMMA 2.3. (Demeyer & Janusz [3] Theorem 2). <u>Let</u> G <u>be a group. Then</u> G <u>is of central type if and only if for each prime</u> p <u>a Sylow</u> p-<u>subgroup</u> S_p <u>of</u> G <u>is of central type and</u> $Z(G) \cap S_p = Z(S_p)$.

The following, rather technical lemma is proved in order to handle a particular case in the induction proof of Lemma 2.15.

LEMMA 2.4. <u>Let</u> G <u>be a soluble group,</u> π <u>a set of primes, and let</u> $P = O_\pi(F)$ <u>where</u> F <u>denotes</u> F(G). <u>Assume that</u> P <u>is cyclic and that</u> $P \nleq Z(G)$. <u>In addition assume that</u> $\lambda \in \mathrm{Firr}(P)$ <u>such that</u> $\chi(1) = \psi(1)$ <u>for all elements</u>

χ, ψ, <u>of</u> $\mathrm{Irr}(G|\lambda)$. <u>Then</u> G <u>contains a normal abelian Hall</u> π'-<u>subgroup and</u> $\chi(1)$ <u>is a</u> π-<u>number for all</u> $\chi \in \mathrm{Irr}(G|\lambda)$.

<u>Proof</u>. Since $P = O_\pi(F)$ we have $F = P \times R$ for some normal nilpotent π'-subgroup R of G. By Theorem 1.12 $\mathrm{Irr}(F) = \{\mu \times \zeta : \mu \in \mathrm{Irr}(P), \zeta \in \mathrm{Irr}(R)\}$. Let 1_R denote the identity character of R, and write $\xi = \lambda \times 1_R$. Then ξ is invariant in G and $\xi \in \mathrm{Irr}(F|\lambda)$. Let χ be an irreducible constituent of ξ^G, whence $\chi \in \mathrm{Irr}(G|\lambda)$. Clearly $R \leqslant \ker\chi$, and $P \cap \ker\chi = 1$ since $\lambda \in \mathrm{Firr}(P)$. If $g \in F$ then $g = xy$ for some $x \in P$, $y \in R$, whereupon $\chi(g) = \chi(1).\xi(g) = \chi(1)\lambda(x) \neq 0$. Consequently $F \leqslant V(\chi)$.

Suppose that $V(\chi) > F$. From the fact that $V(\chi) \lhd G$ we may choose $L \lhd G$ such that $F \leqslant L \leqslant V(\chi)$ and L/F is a minimal normal subgroup of G/F. The solubility of G implies that L/F is an elementary abelian q-group for some prime q. If Q denotes a Sylow q-subgroup of L then Q is not normal in L (otherwise $Q \leqslant O_q(G) \leqslant F(G) = F$), and thus $N_G(Q) < G$. Let H be a maximal subgroup of G containing $N_G(Q)$. By the Frattini argument we have $G = L(N_G(Q)) = LH$. Now $L = FQ$, and so, since $Q \leqslant N_G(Q) \leqslant H$, it follows that $G = FH$. By assumption $P \leqslant Z(G)$, whereupon $P \leqslant N_G(Q) \leqslant H$. Moreover $F = RP$, and, as a result, $G = RH$.

Write $\chi_H = \theta$. Since $G = RH$ and $R \leqslant \ker\chi$ it is obvious that $\theta \in \mathrm{Irr}(H)$. By Frobenius reciprocity θ is an irreducible constituent of ψ_H for each irreducible constituent ψ of θ^G. Suppose that ψ is an irreducible constituent of θ^G such that $\psi_H \neq \theta$. Then $\psi(1) \geqslant \theta(1) = \chi(1)$. But $P \leqslant H$ which implies that $\theta \in \mathrm{Irr}(H|\lambda)$, and hence $\psi \in \mathrm{Irr}(G|\lambda)$, contradicting the assumption that all elements of $\mathrm{Irr}(G|\lambda)$ have the same degree. Thus $\psi_H = \theta$ for all irreducible constituents ψ of θ^G, and Lemma 2.2 yields $V(\theta) \lhd G$.

Clearly $V(\theta) \leqslant V(\chi)$. Let $g \in G$ such that $\chi(g) \neq 0$. Since $G = RH$ we can write $g = yh$ for some $y \in R$, $h \in H$. Then, using the fact that $R \leqslant \ker\chi$, we have $0 \neq \chi(g) = \chi(yh) = \chi(h) = \theta(h)$, and we deduce that

$h \in V(\theta)$. Now let $g \in V(\chi)$. From the definition of $V(\chi)$ there exists an integer n and elements g_i of G such that $g = \prod_{i=1}^{n} g_i$ and $\chi(g_i) \neq 0$ for $1 \leq i \leq n$. If $i \in \{1,\ldots, n\}$ then we can write $g_i = y_i h_i$ for some $y_i \in R$, $h_i \in H$. As shown above we must have $h_i \in V(\theta)$ for $1 \leq i \leq n$. Since $g = (y_1h_1)(y_2h_2)\ldots(y_nh_n)$, and in view of the fact that R and $V(\theta)$ are both normal subgroups of G, we can write $g = yh$ for some $y \in R$ and $h \in V(\theta)$. Consequently $V(\chi) \leq R(V(\theta))$. But $R \leq F \leq V(\chi)$, and $V(\theta) \leq V(\chi)$, whereupon $R(V(\theta)) \leq V(\chi)$. We conclude that $V(\chi) = R(V(\theta))$.

Let $g \in V(\chi)$. Then $g = yh$ for some $y \in R$, $h \in V(\theta)$. If $g \in V(\chi) \cap H$ then, since $V(\theta) \leq H$, we must have $y \in R \cap H$. But $R \leq \ker\chi$, and hence $R \cap H \leq \ker\theta \leq V(\theta)$. Therefore $V(\chi) \cap H \leq V(\theta)$. The opposite inclusion is obvious, whence $V(\chi) \cap H = V(\theta)$. We have $Q \leq L \leq V(\chi)$ and $Q \leq H$. As a result $Q \leq V(\chi) \cap H = V(\theta)$, and we see that $Q \leq L \cap V(\theta) \lhd G$. Since Q is a Sylow q-subgroup of L it follows that Q is a Sylow q-subgroup of $L \cap V(\theta)$. By the Frattini argument $G = (L \cap V(\theta))N_G(Q) \leq H$, a contradiction and thus we were incorrect in supposing that $V(\chi) > F$. It follows that $V(\chi) = F$. Since χ was an arbitrary irreducible constituent of ξ^G we must have $V(\chi) = F$ for all irreducible constituents χ of ξ^G.

Assume that χ and ψ are both irreducible constituents of ξ^G. Then $R \leq \ker\chi$, $R \leq \ker\psi$, and $V(\chi) = F = V(\psi)$. Moreover, χ and ψ are both elements of $\mathrm{Irr}(G|\lambda)$, whereupon $\chi(1) = \psi(1)$. Let $g \in G$. If $g \notin F$ then $\chi(g) = \psi(g) = 0$. If $g \in F$ then, since $\chi_F = \chi(1)\xi = \psi(1)\xi = \psi_F$, we have $\chi(g) = \psi(g)$. Hence $\chi(g) = \psi(g)$ for all $g \in G$, and we deduce that $\chi = \psi$. Therefore $\mathrm{Irr}(G|\xi) = \{\chi\}$. Write $\overline{G} = G/R$ and $\overline{F} = F/R$. When ξ and χ are considered, in the usual way, as elements of $\mathrm{Irr}(\overline{F})$ and $\mathrm{Irr}(\overline{G})$ respectively, we have $\mathrm{Irr}(\overline{G}|\xi) = \{\chi\}$. Since $\chi_{\overline{F}} = \chi(1)\xi$, Frobenius reciprocity yields $\xi^{\overline{G}} = \chi(1)\chi$. Thus

$$|\overline{G} : \overline{F}| = \xi^{\overline{G}}(1) = \chi(1)^2. \qquad (1)$$

Obviously $\overline{F} \leqslant Z(\overline{G})$, and since $\chi(1)^2 \leqslant |\overline{G} : Z(\overline{G})|$ we must have $\overline{F} = Z(\overline{G})$. It follows that $\overline{G}$ is a group of central type. Let p be a prime such that $p \mid |\overline{G}|$, and let $\overline{S}$ denote a Sylow p-subgroup of $\overline{G}$. Then $Z(\overline{S}) > 1$, and by Lemma 2.3 $Z(\overline{S}) = \overline{F} \cap \overline{S}$. Consequently $p \mid |\overline{F}|$. Now $\overline{F} = F/R \cong P = O_\pi(F)$, and we deduce that $p \in \pi$. As a result $\overline{G} = G/R$ is a π-group, whereupon R is a normal Hall π'-subgroup of G.

Since $\chi \in \mathrm{Irr}(G|\lambda)$, and since, by (1), $\chi(1)$ is a π-number, it follows that $\psi(1)$ is a π-number for all $\psi \in \mathrm{Irr}(G|\lambda)$. Let $\zeta \in \mathrm{Irr}(R)$, and write $\phi = \lambda \times \zeta$. Then $\phi \in \mathrm{Irr}(F|\lambda)$, and $\phi(1) = \zeta(1)$. Let ψ be an irreducible constituent of ϕ^G, and write

$$\psi_F = e \sum_{i=1}^{t} \phi_i$$

where $\phi_i \in \mathrm{Irr}(F)$ for $1 \leqslant i \leqslant t$. By Frobenius reciprocity $\phi = \phi_j$ for some $j \in \{1, \ldots, t\}$. Hence $\psi(1) = et\phi(1) = et\zeta(1)$, whereupon $\zeta(1) \mid \psi(1)$ Clearly $\psi \in \mathrm{Irr}(G|\lambda)$, and so $\psi(1)$ is a π-number. But R is a π'-group, and $\zeta \in \mathrm{Irr}(R)$, whence in view of the fact that $\zeta(1) \mid |R|$, we have $(\psi(1), \zeta(1)) = 1$. Thus $\zeta(1) = 1$, and so $\zeta(1) = 1$ for all $\zeta \in \mathrm{Irr}(R)$. We conclude that R is abelian, and the proof is complete.

Q.E.D.

LEMMA 2.5. ([5] Chapter 5, Theorem 2.4.) <u>Let</u> p <u>be a prime, and let</u> A <u>be a</u> p'-<u>group of automorphisms of an abelian</u> p-<u>group</u> P. <u>If</u> A <u>centralises</u> $\Omega_1(P)$ <u>then</u> A = 1.

For any group G we denote the set of all primes dividing $|G|$ by $\pi(G)$.

LEMMA 2.6. <u>Let</u> G <u>be a group, and let</u> M <u>be a cyclic subgroup of</u> Z(G). <u>Assume that</u> N <u>is a normal cyclic subgroup of</u> G <u>such that</u> $M \leqslant N$ <u>and</u> $\pi(N) = \pi(M) = \pi$, <u>say. Then</u> $G/C_G(N)$ <u>is a</u> π-<u>group. Moreover, if</u> $\lambda \in \mathrm{Firr}(M)$ <u>and</u> $\mu \in \mathrm{Irr}(N|\lambda)$ <u>then</u> $\mu \in \mathrm{Firr}(N)$ <u>and</u>

$$\{\phi^G ; \phi \in \mathrm{Irr}(C_G(N)|\mu)\} \subseteq \mathrm{Irr}(G|\lambda).$$

<u>Proof</u>. Write $C = C_G(N)$. The group G/C is isomorphic to a subgroup of $\mathrm{Aut}(N)$. Suppose that G/C is not a π-group. Then there exists a prime $q \notin \pi$ and an element a of G/C of order q. Write $A = \langle a \rangle$. Clearly there exists $p \in \pi$ such that A does not centralise the unique Sylow p-subgroup, N_p, of N. But N is cyclic, and thus so is N_p. Hence, since $M \leqslant N$ and $p \mid |M|$, we must have $\Omega_1(N_p) \leqslant M \leqslant Z(G)$, whereupon A centralises $\Omega_1(N_p)$. Therefore, by Lemma 2.5, A centralises N_p, a contradiction. We conclude that G/C is a π-group.

Now let $\lambda \in \mathrm{Firr}(M)$, and let $\mu \in \mathrm{Irr}(N|\lambda)$. Since M and N are both cyclic with $\pi(M) = \pi(N)$, and since $\mu_M = \lambda$, it follows easily that $\mu \in \mathrm{Firr}(N)$. Lemma 1.10 yields

$$G_\mu = \{g \in G : [g,x] \in \ker\mu \text{ for all } x \in N\},$$

and so, from the fact that $\ker\mu = 1$, we see that $G_\mu = C_G(N) = C$. By Theorem 1.9 we have

$$\{\phi^G : \phi \in \mathrm{Irr}(C|\mu)\} = \{\chi \in \mathrm{Irr}(G) : [\chi_N,\mu] \neq 0\}.$$

But if $\chi \in \mathrm{Irr}(G)$ with $[\chi_N,\mu] \neq 0$ then obviously $\chi \in \mathrm{Irr}(G|\lambda)$, and the result follows.

Q.E.D.

We shall require some of the ideas and results in [8] Chapter 11 on projective representations and Schur representation groups, and so we proceed to give a brief summary of the relevant material. (The term "projective representation" will be used here to mean "projective representation over $\mathbb{C}$" where $\mathbb{C}$ denotes the field of complex numbers. We shall use "ordinary representation" in contrast to "projective representation".)

THEOREM 2.7. ([8] Theorem 11.2.) Let G be a group, and let N be a normal subgroup of G. Assume that Y denotes an irreducible representation of N which affords the character θ, and that θ is invariant in G. Then there exists a projective representation X of G such that for all $n \in N$ and $g \in G$ we have

(a) $X(n) = Y(n)$;

(b) $X(ng) = X(n)X(g)$;

(c) $X(gn) = X(g)X(n)$.

Furthermore, if X_o is another projective representation satisfying (a), (b), (c), then $X_o(g) = X_o(g)\mu(g)$ for some function $\mu : G \to \mathbb{C}^\times$ (where $\mathbb{C}^\times$ denotes the multiplicative group of $\mathbb{C}$) which is constant on cosets of N.

We use the standard notation of group cohomology; that is, $H^2(G,\mathbb{C}^\times)$ denotes the second cohomology group of a group G (where $\mathbb{C}^\times$ is a trivial G-module), $Z^2(G,\mathbb{C}^\times)$ denotes the group of 2-cocycles, and $B^2(G,\mathbb{C}^\times)$ denotes the group of 2-coboundaries. We have $H^2(G,\mathbb{C}^\times) = Z^2(G,\mathbb{C}^\times)/B^2(G,\mathbb{C}^\times)$, and we remark that if X is a projective representation of a group G then the factor set of X is an element of $Z^2(G,\mathbb{C}^\times)$.

THEOREM 2.8 ([8] Theorem 11.7). Let G be a group, N a normal subgroup of G, and let $\theta \in \mathrm{Irr}(N)$ such that θ is invariant in G. Assume that Y denotes an irreducible representation of N affording θ, and that X is a projective representation of G satisfying (a), (b), (c), of Theorem 2.7. Let α denote the factor set of X, and define $\beta \in Z^2(G/N,\mathbb{C}^\times)$ by $\beta(gN,hN) = \alpha(g,h)$. Then β is well-defined and $\bar{\beta}$, the image of β under the natural homomorphism $Z^2(G/N,\mathbb{C}^\times) \longrightarrow H^2(G/N,\mathbb{C}^\times)$, depends only on θ.

A central extension (Γ,ρ) of a group G is a group Γ together with a homomorphism ρ from Γ onto G such that $\ker\rho \leqslant Z(\Gamma)$. If (Γ,ρ) is a central extension of a group G, then we say that a projective representation

X of G can be <u>lifted</u> to Γ if there exists an ordinary representation Y of Γ and a function $\mu : \Gamma \longrightarrow \mathbb{C}^{\times}$ such that

$$Y(a) = X(a^{\rho})\mu(a)$$

for all $a \in \Gamma$. If every projective representation of G can be lifted to Γ then (Γ,ρ) is said to have the <u>projective lifting property</u> for G.

THEOREM 2.9.([8] Theorem 11.17.). <u>For any group</u> G <u>there exists a central extension</u> (Γ,ρ) <u>of</u> G <u>which has the projective lifting property for</u> G. <u>Furthermore,</u> (Γ,ρ) <u>can be chosen such that</u> $\ker\rho \cong H^2(G,\mathbb{C}^{\times})$.

If G is a group, and if (Γ,ρ) is a central extension having the projective lifting property for G such that $\ker\rho \cong H^2(G,\mathbb{C}^{\times})$, then Γ is said to be a <u>Schur representation group</u> for G. Theorem 2.9 asserts the existence of a Schur representation group for any group G.

Let G be a group, N a normal subgroup of G, and let $\theta \in \mathrm{Irr}(N)$ such that θ is invariant in G. Under these hypotheses we say that (G,N,θ) is a <u>character triple</u>. There is a very close relationship between a character triple (G,N,θ) and another triple (Γ,A,λ) where Γ denotes a Schur representation group for the group G/N. To describe this relationship we define the (rather complicated) notion of an isomorphism between two character triples. If (G,N,θ) is a character triple then we have been using $\mathrm{Irr}(G|\theta)$ to denote the set of all elements χ of $\mathrm{Irr}(G)$ such that χ_N is a multiple of θ. Now let $\mathrm{Ch}(G|\theta)$ denote the set of all (possibly reducible) characters χ of G such that χ_N is a multiple of θ. We remark that if (G,N,θ) is a character triple, and if H is a subgroup of G containing N, then (H,N,θ) is a character triple, and $\chi_H \in \mathrm{Ch}(H|\theta)$ for all $\chi \in \mathrm{Ch}(G|\theta)$.

DEFINITION. Let (G,N,θ) and (Γ,M,ϕ) be character triples, and let

$\tau : G/N \longrightarrow \Gamma/M$ be an isomorphism. For each subgroup H of G containing N let H^τ denote the subgroup of Γ such that $H^\tau/M = (H/N)^\tau$. Assume that whenever $N \leqslant H \leqslant G$ there exists a map $\sigma_H : Ch(H|\theta) \longrightarrow Ch(H^\tau|\phi)$ such that the following conditions hold for all $N \leqslant K \leqslant H$ and for all elements χ, ψ, of $Ch(H|\theta)$.

(a) $\sigma_H(\chi + \psi) = \sigma_H(\chi) + \sigma_H(\psi)$;

(b) $[\chi,\psi] = [\sigma_H(\chi), \sigma_H(\psi)]$;

(c) $\sigma_K(\chi_K) = (\sigma_H(\chi))_{K^\tau}$;

(d) $\sigma_H(\chi\zeta) = \sigma_H(\chi)\zeta^\tau$ for all $\zeta \in Irr(H/N)$ where ζ^τ denotes the character of $(H/N)^\tau$ defined by $\zeta^\tau(x^\tau) = \zeta(x)$ for all $x \in H/N$.

Let σ denote the union of the maps σ_H. Then (τ, σ) is an <u>isomorphism from</u> (G,N,θ) <u>to</u> (Γ,M,ϕ).

LEMMA 2.10 ([8] Lemma 11.24) <u>Let</u> $(\tau,\sigma) : (G,N,\theta) \longrightarrow (\Gamma,M,\phi)$ <u>be an isomorphism of character triples. Then</u> σ_G <u>is a bijection from</u> $Irr(G|\theta)$ <u>to</u> $Irr(\Gamma|\phi)$. <u>Furthermore,</u> $\chi(1)/\theta(1) = \sigma_G(\chi)(1)/\phi(1)$ <u>for all</u> $\chi \in Irr(G|\theta)$.

NOTE. Lemma 11.24 of [8] says rather more that is stated in Lemma 2.10 above; we have omitted all that is superfluous to our requirements.

THEOREM 2.11. ([8] Theorem 11.28.) <u>Let</u> (G,N,θ) <u>be a character triple and let</u> (Γ,ρ) <u>be a central extension of</u> G/N <u>having the projective lifting property. If</u> $A = \ker\rho$ <u>then</u> (G,N,θ) <u>and</u> (Γ,A,λ) <u>are isomorphic character triples for some</u> $\lambda \in \hat{A}$.

Let (G,N,θ) be a character triple, and let π denote $\pi(N)$. Let Γ be a Schur representation group for G/N. Then, from the definition of a Schur representation group and using Theorem 2.11, there exists a subgroup A of $Z(\Gamma)$ and an element λ of $\hat{A}$ such that $\Gamma/A \cong G/N$, $A \cong H^2(G/N,\mathbb{C}^\times)$, and (G,N,θ) is isomorphic to (Γ,A,λ). We shall show that $A/\ker\lambda$ is a π-group, but we need a preliminary lemma.

LEMMA 2.12. Let (G,N,θ) be a character triple and let $\overline{\beta}$ denote the element of the group $H^2(G/N,\mathbb{C}^\times)$ associated with (G,N,θ) as in Theorem 2.8. If π denotes $\pi(N)$ then $|\overline{\beta}|$ is a π-number.

Proof. Let Y denote an irreducible representation of N affording θ. Since $\overline{\beta}$ is defined in terms of a projective representation X of G satisfying (a), (b), (c), of Theorem 2.7([8] Theorem 11.2), we examine how such a representation X is constructed in the proof of [8] Theorem 11.2. If $g \in G$ and $n \in N$ then write $Y^g(n) = Y(gng^{-1})$. Since Y affords a G-invariant character θ, the representations Y, and Y^g, are similar for all $g \in G$. Choose a transversal T of N in G such that $1 \in T$. For each $t \in T$ choose a non-singular matrix P_t such that $P_t Y P_t^{-1} = Y^t$. Clearly we may take P_1 to be the $k \times k$ identity matrix where $k = \theta(1)$. Since each $g \in G$ is uniquely of the form nt for some $n \in N$, $t \in T$, we can define X on G by $X(g) = Y(n)P_t$, and, as demonstrated in the proof of [8] Theorem 11.2, X is a projective representation of G satisfying (a), (b), (c), of Theorem 2.7.

Assume that a projective representation X of G has been constructed as above. Write $d_t = \det(P_t)$ for each $t \in T$. Then d_t is a non-zero complex number, and, since the field of complex numbers is algebraically closed, we can choose $c_t \in \mathbb{C}$ such that $(c_t)^k = d_t^{-1}$ for each $t \in T$. Write $P_t' = c_t P_t$. Then $\det(P_t') = (c_t)^k d_t = 1$ for all $t \in T$. Clearly $P_t' Y (P_t')^{-1} = Y^t$ for all $t \in T$, and we can construct a new projective representation X' of G as follows. If $g \in G$ with $g = nt$ for $n \in N$, $t \in T$, then we define $X'(g) = Y(n)P_t'$. The fact that X' has been constructed in the same way as X implies that X' satisfies (a), (b), (c), of Theorem 2.7. Let α denote the factor set of X'. Since $\overline{\beta}$ depends only on θ, it follows that α gives rise to $\overline{\beta}$ as described in the statement of Theorem 2.8.

Let g, h, be elements of G. Then $X'(g)X'(h) = X'(gh)\alpha(g,h)$. Write $g = n_1 t_1$, $h = n_2 t_2$, $gh = n_3 t_3$, where $n_i \in N$, $t_i \in T$, for $1 \leq i \leq 3$. We have $X'(g) = Y(n_1)P_{t_1}'$, $X'(h) = Y(n_2)P_{t_2}'$, $X'(gh) = Y(n_3)P_{t_3}'$, and hence

$$Y(n_1)P'_{t_1}Y(n_2)P'_{t_2} = Y(n_3)P'_{t_3}\alpha(g,h).$$

Therefore

$$\det(Y(n_1)P'_{t_1}Y(n_2)P'_{t_2}) = \det(Y(n_3)P'_{t_3}\alpha(g,h)),$$

and since $\det(P'_{t_i}) = 1$ for $1 \leqslant i \leqslant 3$ it follows that

$$\det(Y(n_1))\det(Y(n_2)) = \det(Y(n_3))(\alpha(g,h))^k. \qquad (1)$$

Write $\lambda(n) = \det(Y(n))$ for all $n \in N$. Then clearly λ is a linear complex character of N. Let m denote the order of λ as an element of the group of linear characters of N. Since $m = |N : \ker\lambda|$ we must have $m \mid |N|$. We may rewrite (1) as

$$\lambda(n_1)\lambda(n_2) = \lambda(n_3)(\alpha(g,h))^k.$$

Therefore

$$(\lambda(n_1)\lambda(n_2))^m = (\lambda(n_3)(\alpha(g,h))^k)^m.$$

But $(\lambda(n))^m = \lambda^m(n) = 1$ for all $n \in N$, and so

$$(\alpha(g,h))^{km} = (\lambda(n_3))^m(\alpha(g,h))^{km} = (\lambda(n_3)(\alpha(g,h))^k)^m$$

$$= (\lambda(n_1)\lambda(n_2))^m = (\lambda(n_1))^m(\lambda(n_2))^m = 1.$$

Since g,h were arbitrary elements of G we deduce that $(\alpha(g,h))^{km} = 1$ for all elements g,h, of G. We have $k = \theta(1)$ and $\theta(1) \mid |N|$. As remarked above, $m \mid |N|$, and hence km is a π-number where π denotes $\pi(N)$. If g,h, are elements of G then define $\beta(gN,hN) = \alpha(g,h)$. Since $(\alpha(g,h))^{km} = 1$ for all elements g,h, of G it follows that the order of β in the group $Z^2(G/N,\mathbb{C}^\times)$ divides km, a π-number. Obviously then $|\overline{\beta}|$ is a π-number.

Q.E.D.

LEMMA 2.13. *Let* (G,N,θ) *be a character triple, and let* Γ *denote a Schur representation group for* G/N. *Then there exists a subgroup* A *of* $Z(\Gamma)$ *and an element* λ *of* $\hat{A}$ *such that* $G/N \cong \Gamma/A$, (G,N,θ) *and* (Γ,A,λ) *are isomorphic, and* $A/\ker\lambda$ *is a cyclic* π*-group where* $\pi = \pi(N)$.

Proof. From the definition of a Schur representation group for G/N there exists an epimorphism $\rho : \Gamma \longrightarrow G$ such that $\ker\rho \leq Z(\Gamma)$, and $\ker\rho \cong H^2(G/N, \mathbb{C}^\times)$. Write $A = \ker\rho$. By Theorem 2.11([8] Theorem 11.28) there exists $\lambda \in \hat{A}$ such that (G,N,θ) and (Γ,A,λ) are isomorphic. Now in the proof of [8] Theorem 11.28, the element λ of $\hat{A}$ chosen so that (G,N,θ) and (Γ,A,λ) are isomorphic character triples satisfies $\lambda^\eta = \overline{\beta}^{-1}$ where η is a certain epimorphism from $\hat{A}$ to $H^2(G/N,\mathbb{C}^\times)$ (η is called the *standard map* in [8]), and $\overline{\beta}$ denotes the element of the group $H^2(G/N,\mathbb{C}^\times)$ associated with (G,N,θ) as in the statement of Theorem 2.8. Since $\hat{A} \cong A \cong H^2(G/N,\mathbb{C}^\times)$, it follows that η is an isomorphism, and we deduce that $|\lambda|$, the order of λ in the group $\hat{A}$, is precisely $|\overline{\beta}^{-1}|$. Let π denote $\pi(N)$. By Lemma 2.12 $|\overline{\beta}|$ is a π-number, whereupon $|\lambda| = |\overline{\beta}^{-1}| = |\overline{\beta}|$, a π-number. But $|\lambda| = |A/\ker\lambda|$ and we conclude that $A/\ker\lambda$ is a cyclic π-group.

Q.E.D.

Our next result is the well known characterisation of p-groups in which each abelian characteristic subgroup is cyclic due to P. Hall.

LEMMA 2.14.([6] III Satz 13.10). *Let* p *be a prime, and let* P *denote a* p*-group such that all abelian characteristic subgroups of* P *are cyclic. Then one of the following must hold.*

(i) P *is cyclic* ;

(ii) $P = P_1 \curlyvee P_2$ *where* $1 \neq P_1$ *is extraspecial of exponent* p *and* P_2 *is cyclic* ;

(iii) $p = 2$ *and* P *is generalised quaternion, dihedral, or semi-dihedral with* $|P| \geq 16$;

(iv) $p = 2$ <u>and</u> $P = P_1 \leftthreetimes P_2$ <u>where</u> $1 \neq P_1$ <u>is extraspecial and either</u> P_2 <u>is dihedral semi-dihedral or generalised quaternion, with</u> $|P_2| \geqslant 16$ <u>or</u> P_2 <u>is cyclic.</u>

We are now in a position to prove the key result in our investigation into the structure of soluble high-fidelity groups with a unique minimal normal subgroup. The motivation for Theorem 2.15 below (which is also of some independent interest) is as follows. Let G be a soluble high-fidelity group with a unique minimal normal subgroup, N say. Then N is an elementary abelian q-group for some prime q. Let $1 \neq \lambda \in \hat{N}$, and write $K = \ker\lambda$. Clearly N/K is a group of order q, and by Lemma 1.10 $N/K \leqslant Z(G_\lambda/K)$. By Theorem 1.9 and Lemma 1.10 we have

$$\{\chi \in \mathrm{Irr}(G) : [\chi_N, \lambda] \neq 0\} = \{\phi^G : \phi \in \mathrm{Irr}(G_\lambda/K|\lambda)\}.$$

Let n denote the common degree of all the characters in Firr(G). If $\chi \in \mathrm{Irr}(G)$ such that $[\chi_N, \lambda] \neq 0$ then, obviously, $\chi \in \mathrm{Firr}(G)$, whereupon $\chi(1) = n$. Consequently $\phi^G(1) = n$ for all $\phi \in \mathrm{Irr}(G_\lambda/K|\lambda)$. It follows that N/K is a cyclic subgroup of $Z(G_\lambda/K)$, and $\lambda \in \mathrm{Firr}(N/K)$ such that all the characters in $\mathrm{Irr}(G_\lambda/K|\lambda)$ have the same degree, namely, $n/|G : G_\lambda|$.

It is desirable, therefore, to have information about the following situation: G is a soluble group, M is a cyclic subgroup of Z(G), and $\lambda \in \mathrm{Firr}(M)$ has the property that all characters in $\mathrm{Irr}(G|\lambda)$ share the same degree. The group SL(2,3) gives an easy example of such an arrangement.

EXAMPLE. Let G denote the group SL(2,3), and write M = Z(G). Then $|G| = 24$, and $|M| = 2$. Moreover, M is the unique minimal normal subgroup of G. Let λ denote the unique non-trivial element of Irr(M). Clearly λ is invariant in G, and $\chi \in \mathrm{Irr}(G|\lambda)$ if and only if $\chi \in \mathrm{Firr}(G)$. Let $\chi \in \mathrm{Firr}(G)$. We have $\chi_M = \chi(1)\lambda$. By Frobenius reciprocity the multiplicity of χ as an irreducible constituent of λ^G is exactly $\chi(1)$, and hence

$$\sum_{\chi \in \mathrm{Firr}(G)} \chi(1)^2 = \lambda^G(1) = |G : M| = 12.$$

Since $\chi \in \mathrm{Firr}(G)$ implies that $\chi(1) > 1$, it follows that $\mathrm{Firr}(G)$ consists of three characters each of degree 2. Thus G is a high-fidelity group. In particular, all characters in $\mathrm{Irr}(G|\lambda)$ have degree 2.

THEOREM 2.15. <u>Let</u> G <u>be a soluble group, and let</u> M <u>be a cyclic subgroup of</u> Z(G). <u>Assume that</u> $\lambda \in \mathrm{Firr}(M)$ <u>such that</u> $\chi(1) = \psi(1)$ <u>for all elements</u> χ, ψ, <u>of</u> $\mathrm{Irr}(G|\lambda)$, <u>and write</u> $\pi = \pi(M)$. <u>Then</u> $\chi(1)$ <u>is a</u> π-<u>number for all</u> $\chi \in \mathrm{Irr}(G|\lambda)$, <u>and</u> G <u>contains an abelian Hall</u> π'-<u>subgroup.</u>

<u>Proof</u>. The proof is by induction on $|G : M|$. If $|G : M| = 1$ then G is abelian and the theorem is obviously true. Now assume that G, M, λ, π, are as in the statement of the theorem, and then the induction hypothesis is as follows : whenever X is a soluble group with Y a cyclic subgroup of Z(X) such that $|X : Y| < |G : M|$ and μ is an element of Firr(Y) having the property that $\theta(1) = \phi(1)$ for all elements θ, ϕ, of $\mathrm{Irr}(X|\mu)$, then, writing $\pi_o = \pi(Y)$, it follows that $\theta(1)$ is a π_o-number for all $\theta \in \mathrm{Irr}(X|\mu)$ and that X contains an abelian Hall π_o'-subgroup.

We shall have two cases to consider according to whether or not there exists $p \in \pi$ such that $O_p(G)$ contains a non-cyclic abelian characteristic subgroup. Let η denote the common degree of all the characters in $\mathrm{Irr}(G|\lambda)$.

CASE 1. For all $p \in \pi$ the subgroup $O_p(G)$ contains no non-cyclic abelian characteristic subgroup.

In this case for all $p \in \pi$ the structure of $O_p(G)$ is given by Lemma 2.14. Assume first that $O_p(G)$ satisfies either (i) or (iii) of Lemma 2.14 for all $p \in \pi$. Then either $O_p(G)$ is cyclic, or $p = 2$, $|O_p(G)| \geq 16$, and $O_p(G)$ is dihedral, semidihedral, or generalised quaternion for each $p \in \pi$. Let $p \in \pi$. If $O_p(G)$ is cyclic, then write $N_p = O_p(G)$. If $O_p(G)$

is not cyclic then $p = 2$ and $O_2(G)$ contains a cyclic characteristic subgroup of index 2 which is its own centraliser in $O_2(G)$. In this case let N_2 denote such a cyclic characteristic subgroup. Hence for each $p \in \pi$ N_p is a cyclic characteristic subgroup of $O_p(G)$ which is its own centraliser in $O_p(G)$. Let N denote the product of all the subgroups N_p. Clearly N is a cyclic normal subgroup of G containing M, and $\pi(N) = \pi = \pi(M)$. If C denotes $C_G(N)$ then $C \lhd G$ and, by Lemma 2.6, G/C is a π-group.

Let $\mu \in \mathrm{Irr}(N|\lambda)$. Lemma 2.6 yields $\mu \in \mathrm{Firr}(N)$, and

$$\{\phi^G : \phi \in \mathrm{Irr}(C|\mu)\} \subseteq \mathrm{Irr}(G|\lambda).$$

Thus for all $\phi \in \mathrm{Irr}(C|\mu)$ we have $|G : C|\phi(1) = \phi^G(1) = n$, the common degree of all the characters in $\mathrm{Irr}(G|\lambda)$, whereupon $\phi(1) = n/|G : C|$ for all $\phi \in \mathrm{Irr}(C|\mu)$.

Since $C \lhd G$ we must have $O_p(C) = O_p(G) \cap C$ for all primes p. Now if p is a prime then $O_p(G) \cap C$ is precisely the centraliser in $O_p(G)$ of N. But for each $p \in \pi$ the group N_p is its own centraliser in $O_p(G)$. We deduce that $N_p = O_p(C)$ for all $p \in \pi$, and hence, if F denotes F(C), then $N = O_\pi(F)$. Thus C is a soluble group, π a set of primes, $O_\pi(F) = N \leqslant Z(C)$ where F denotes F(C), and $\mu \in \mathrm{Firr}(N)$ such that all elements of $\mathrm{Irr}(C|\mu)$ have the same degree, namely $n/|G : C|$. Hence, by Lemma 2.4, C contains a normal abelian Hall π'-subgroup, and $n/|G : C|$ is a π-number. But, as remarked above, G/C is a π-group, and it follows that G contains an abelian Hall π'-subgroup and n, the common degree of all characters in $\mathrm{Irr}(G|\lambda)$, is a π-number. We conclude that if $O_p(G)$ satisfies either (i) or (iii) of Lemma 2.14 for all $p \in \pi$ then the theorem holds.

Hence we may assume that there exists $p \in \pi$ such that $O_p(G)$ satisfies either (ii) or (iv) of Lemma 2.14. Write $P = O_p(G)$. Then $P = P_1 \curlyvee P_2$ where $1 \neq P_1$ is extraspecial, and either P_2 is cyclic, or $p = 2$, $|P_2| \geqslant 16$, and P_2 is dihedral, semi-dihedral, or generalised quaternion. Let Q denote

$C_P(\Phi(P))$. Then Q is a characteristic subgroup of P, whereupon $Q \lhd G$. Moreover $Q = P$ if P_2 is cyclic, and $|P : Q| = 2$ if P_2 is dihedral, semi-dihedral, or generalised quaternion with $|P_2| \geqslant 16$. In fact $Q = Q_1 \curlyvee Q_2$ where $Q_1 \cong P_1$ is extraspecial, and Q_2 is cyclic. Clearly Q is a class 2 p-group with cyclic centre.

Write $R = QM$, and let N denote $Z(R)$. Obviously $\pi(R) = \pi(N) = \pi$, and $M \leqslant N < R \lhd G$. Let $C = C_G(N)$, and choose $\mu \in \mathrm{Irr}(N|\lambda)$. Then by Lemma 2.5 it follows that G/C is a π-group, and that $\mu \in \mathrm{Firr}(N)$ with

$$\{\phi^G : \phi \in \mathrm{Irr}(C|\mu)\} \subseteq \mathrm{Irr}(G|\lambda).$$

Consequently all elements of $\mathrm{Irr}(C|\mu)$ have the same degree, namely $n/|G : C|$.

Let L denote the normal Hall p'-subgroup of M. Then, clearly, $R = QM = Q \times L$, and $N = Z(R) = Z(Q) \times L$. If ζ denotes $\mu_{Z(Q)}$ then Theorem 1.8 implies that $\mathrm{Irr}(Q|\zeta) = \{\psi\}$ for some $\psi \in \mathrm{Firr}(Q)$. Let $\xi = \mu_L$. Using Theorem 1.12 and the fact that $\mu = \zeta \times \xi$ it follows easily that $\mathrm{Irr}(R|\mu) = \{\theta\}$ where $\theta = \psi \times \xi$. Now μ is invariant in C, and hence $\theta^g \in \mathrm{Irr}(R|\mu)$ for all $g \in C$. We deduce that θ is invariant in C, whence (C,R,θ) is a character triple. Moreover, $\phi \in \mathrm{Irr}(C|\theta)$ if and only if $\phi \in \mathrm{Irr}(C|\mu)$, and thus all the characters in $\mathrm{Irr}(C|\theta)$ have degree $n/|G : C|$.

Let Γ be a Schur representation group for C/R. Then, by Lemma 2.13, there exists a subgroup A of $Z(\Gamma)$ and an element ζ of $\hat{A}$ such that $C/R \cong \Gamma/A$, (C,R,θ) and (Γ,A,ζ) are isomorphic character triples, and $A/\ker\zeta$ is a π-group. Write $K = \ker\zeta$, $\overline{\Gamma} = \Gamma/K$, and $\overline{A} = A/K$. Then, in the usual way, we consider ζ as an element of $\mathrm{Firr}(\overline{A})$ and identify $\mathrm{Irr}(\Gamma|\zeta)$ with $\mathrm{Irr}(\overline{\Gamma}|\zeta)$. Let $\psi \in \mathrm{Irr}(\overline{\Gamma}|\zeta)$. It follows from Lemma 2.10 that there exists $\phi \in \mathrm{Irr}(C|\theta)$ such that

$$\phi(1)/\theta(1) = \psi(1)/\zeta(1).$$

Since $\zeta(1) = 1$, and since, as proved above, all characters in $\mathrm{Irr}(C|\theta)$

have degree $n/|G : C|$, we see that

$$\psi(1) = n/|G : C|\theta(1)$$

for all $\psi \in \mathrm{Irr}(\overline{\Gamma}|\zeta)$.

Clearly $\overline{\Gamma}$ is soluble. Moreover $\overline{A}$ is a cyclic subgroup of $Z(\overline{\Gamma})$ with $\pi(\overline{A}) \subseteq \pi$, and $\zeta \in \mathrm{Firr}(\overline{A})$ has the property that all characters in $\mathrm{Irr}(\overline{\Gamma}|\zeta)$ have degree $n/|G : C|\theta(1)$. Since $M < R$ we have

$$|\overline{\Gamma} : \overline{A}| = |\Gamma : A| = |C : R| < |C : M| \leqslant |G : M|,$$

and so, writing $\pi_o = \pi(\overline{A})$, the induction hypothesis implies that $n/|G : C|\theta(1)$ is a π_o-number, and that $\overline{\Gamma}$ contains an abelian Hall π_o'-subgroup. But $\pi_o \subseteq \pi$, and therefore $n/|G : C|\theta(1)$ is a π-number. Also any Hall π_o'-subgroup of $\overline{\Gamma}$ must contain a Hall π'-subgroup of $\overline{\Gamma}$, and thus $\overline{\Gamma}$ contains an abelian Hall π'-subgroup.

As remarked above the group G/C is a π-group, whence $|G : C|$ is a π-number. Also R is a π-group, and therefore, since $\theta \in \mathrm{Irr}(R)$, it follows that $\theta(1)$ is a π-number. We deduce that n, the common degree of all elements of $\mathrm{Irr}(G|\lambda)$, is a π-number. Let H be a Hall π'-subgroup of G. Obviously $H \leqslant C$. Since R is a π-group we have $H \cap R = 1$, whereupon $H \cong HR/R$. It is apparent that HR/R is a Hall π'-subgroup of the group $C/R \cong \Gamma/A \cong \overline{\Gamma}/\overline{A}$. Now $\overline{A}$ is a π-group, and, as proved above, $\overline{\Gamma}$ contains an abelian Hall π'-subgroup. Therefore $\overline{\Gamma}/\overline{A}$, and hence C/R, contains an abelian Hall π'-subgroup, and since all Hall π'-subgroups C/R are isomorphic it follows that $HR/R \cong H$ is abelian. This completes Case 1.

CASE 2. There exists $p \in \pi$ such that $O_p(G)$ contains a non-cyclic abelian characteristic subgroup.

Let R_o denote a non-cyclic abelian characteristic subgroup of $O_p(G)$.

Obviously $R_o \lhd G$. Write $R = R_oM$. Then $R \lhd G$, and R is abelian (since R_o is abelian and $M \leqslant Z(G)$). Moreover, R is not cyclic, and $\pi(R) = \pi$. Let $\phi \in \mathrm{Irr}(R|\lambda)$, and write $K = \ker\phi$. Clearly $K \cap M = 1$, whence $M \cong MK/K \leqslant R/K$. it follows that $\pi(R/K) \supseteq \pi(M) = \pi$, and so, since $\pi(R/K) \subseteq \pi(R) = \pi$, we have $\pi(R/K) = \pi$. By Lemma 1.10 $R/K \leqslant Z(G_\phi/K)$, and Theorem 1.9 and Lemma 1.10 together imply that

$$\{\chi \in \mathrm{Irr}(G) : [\chi_R, \phi] \neq 0\} = \{\psi^G : \psi \in \mathrm{Irr}(G_\phi/K|\phi)\} .$$

Obviously if $\chi \in \mathrm{Irr}(G)$ such that $[\chi_R, \phi] \neq 0$ then $\chi \in \mathrm{Irr}(G|\lambda)$, whereupon $\chi(1) = n$. Consequently $\psi(1)|G : G_\phi| = \psi^G(1) = n$ for all $\psi \in \mathrm{Irr}(G_\phi/K|\phi)$, and we deduce that $\psi(1) = n/|G : G_\phi|$ for all $\psi \in \mathrm{Irr}(G_\phi/K|\phi)$.

Therefore G_ϕ/K is a soluble group, and R/K is a cyclic subgroup of $Z(G_\phi/K)$ with $\pi(R/K) = \pi$. Moreover, $\phi \in \mathrm{Firr}(R/K)$ such that all elements of $\mathrm{Irr}(G_\phi/K|\phi)$ have degree $n/|G : G_\phi|$. Since R is abelian but not cyclic we must have $M < R$, whereupon

$$|G_\phi/K : R/K| = |G_\phi : R| < |G_\phi : M| \leqslant |G : M| .$$

Therefore the induction hypothesis implies that $n/|G : G_\phi|$ is a π-number, and that G_ϕ/K contains an abelian Hall π'-subgroup.

Let I denote the set $\mathrm{Irr}(R|\lambda)$. Clearly G acts as a group of permutations on I, and the above argument establishes that $n/|G : G_\phi|$ is a π-number for each $\phi \in I$. Thus, writing $m(\phi) = n/|G : G_\phi|$, we have

$$n = m(\phi)|G : G_\phi| , \qquad (1)$$

where $m(\phi)$ is a π-number, for each $\phi \in I$. Let $\phi \in I$. By Frobenius reciprocity the multiplicity of ϕ as an irreducible constituent of λ^R is the multiplicity of λ as an irreducible constituent of ϕ_M. But R is abelian, whereupon $\phi(1) = 1$, and we have $\phi_M = \lambda$. Hence each element of I appears as an irreducible constituent of λ^R with multiplicity 1.

Therefore, since $\lambda^R(1) = |R : M|$, we have $|I| = |R : M|$.

Suppose that $q|n$ for some prime q such that $q \notin \pi$. Then (1) implies that $q \,|\, |G : G_\phi|$ for each $\phi \in I$; that is, q divides the size of each G-orbit in I. Consequently q divides $|I| = |R : M|$, and hence $q \,|\, |R|$. But, as remarked above, $\pi(R) = \pi$, a contradiction. We deduce that n, the common degree of all characters in $\mathrm{Irr}(G|\lambda)$, is a π-number. Let $\phi \in I$, and let H denote a Hall π'-subgroup of G_ϕ. Using (1) and the fact that n is a π-number we see that $|G : G_\phi|$ is a π-number, and it follows that H is a Hall π'-subgroup of G. Writing $K = \ker\phi \lhd R$, we must have that K is a π-group, and so $H \cap K = 1$. Thus $H \cong HK/K$. Clearly HK/K is a Hall π'-subgroup of G_ϕ/K. As proved above, the group G_ϕ/K contains an abelian Hall π'-subgroup, and so, since all Hall π'-subgroups of G_ϕ/K are isomorphic, we conclude that $HK/K \cong H$ is abelian. This completes Case 2, and hence the lemma is proved by induction.

Q.E.D.

We remark that Theorem 2.15 above may be stated in terms of projective representations, and such a formulation is given below as Theorem 2.16. The proof that the two theorems are equivalent, which would be too much of a digression here, is omitted.

THEOREM 2.16. *Let G be a soluble group, and let α be a (complex) factor set of G. Assume that $\bar{\alpha}$ denotes the image of α under the natural homomorphism $Z^2(G,\mathbb{C}^\times) \longrightarrow H^2(G,\mathbb{C}^\times)$, and let π denote the set of primes dividing $|\bar{\alpha}|$. Assume further that all irreducible projective representations of G with factor set α share the same degree. Then the degree of any irreducible projective representation of G with factor set α is a π-number, and G contains an abelian Hall π'-subgroup.*

Theorem 2.15 may be given yet a third formulation in the language

of the theory of twisted group algebras, but we do not include such a formulation here. Instead we move on to give a definition that generalises the idea of a group acting half-transitively on a set.

DEFINITION. Let G be a group of permutations on a set X, such that $|X| > 1$, and let π be a set of primes. We say that G acts π -halftransitively on X if there exists a π-number b such that $|x^G| = b.s(x)$ for all $x \in X$, where $s(x)$ is a π'-number depending on x, and x^G denotes the G-orbit containing x. In addition, if $b = |G|_\pi$, the π-part of the integer $|G|$, then we say that G acts π-semiregularly on X.

Clearly π-halftransitivity is identical to half-transitivity when $\pi = \pi(G)$, and in this case π-semiregular action is semiregular. Also, by the orbit-stabiliser theorem, it is an easy consequence of the definition that a group G acts π-halftransitively on a set X if and only if there exists a π-number c such that $|G_x| = c.t(x)$ for all $x \in X$, where $t(x)$ is a π'-number depending on x.

THEOREM 2.17. Let G be a soluble group with a unique minimal normal subgroup N, an elementary abelian q-group for some prime q. Assume that G is a high-fidelity group. Then G acts q'-halftransitively on the non-trivial elements of $\hat{N}$, and G_λ contains an abelian Hall q'-subgroup for each $1 \neq \lambda \in \hat{N}$. Writing $\overline{G} = G/C_G(N)$ and regarding $\hat{N}$ additively, $\hat{N}$ is an irreducible $GF(q)\overline{G}$-module, faithful for $\overline{G}$, such that $\overline{G}$ acts q'-half-transitively on $(\hat{N})^*$.

Proof. Let n denote the common degree of all the characters in Firr(G), and let $1 \neq \lambda \in \hat{N}$. Write $K = \ker\lambda$, and then N/K is a cyclic group of order q. By Lemma 1.10 and Theorem 1.9, we have $N/K \leqslant Z(G_\lambda/K)$, and

$$\{\chi \in \mathrm{Irr}(G) = [\chi_N, \lambda] \neq 0\} = \{\phi^G : \phi \in \mathrm{Irr}(G_\lambda/K|\lambda)\} .$$

If $\chi \in \mathrm{Irr}(G)$ such that $[\chi_N, \lambda] \neq 0$ then obviously $\chi \in \mathrm{Firr}(G)$, whereupon $\chi(1) = n$. Hence $\phi^G(1) = n$ for all $\phi \in \mathrm{Irr}(G_\lambda/K|\lambda)$. It follows that N/K is a cyclic subgroup of $Z(G_\lambda/K)$ of order q, and $\lambda \in \mathrm{Firr}(N/K)$ such that all elements of $\mathrm{Irr}(G_\lambda/K|\lambda)$ have the same degree, namely $n/|G : G_\lambda|$. Therefore, by Theorem 2.15, there exists an integer, $\alpha(\lambda)$ say, such that

$$q^{\alpha(\lambda)} = n/|G : G_\lambda| , \tag{1}$$

and G_λ/K contains an abelian Hall q'-subgroup. From (1) we have

$$|G : G_\lambda| = n/q^{\alpha(\lambda)} . \tag{2}$$

Let b denote the q'-part of n, so that $n = b.q^k$ for some integer k and $q \nmid b$. Then (2) implies that there exists an integer $\beta(\lambda)$ $(= k - \alpha(\lambda))$ such that

$$|G : G_\lambda| = b.q^{\beta(\lambda)}.$$

But $|G : G_\lambda|$ is precisely the size of the G-orbit containing λ, and it follows that G acts q'-halftransitively on $(\hat{N})^*$. Again let $\lambda \in (\hat{N})^*$, and let H denote a Hall q'-subgroup of G_λ. Write $K = \ker\lambda$, whereupon K is a q-group. Therefore $H \cap K = 1$, and so $H \cong HK/K$. Clearly HK/K is a Hall q'-subgroup of G_λ/K. As proved above, G_λ/K contains an abelian Hall q'-subgroup, and, since all Hall q'-subgroups of G_λ/K are isomorphic, it follows that $HK/K \cong H$ is abelian.

The last statement in the theorem follows easily from Lemma 1.11 and from the fact that $(\overline{G})_\lambda = G_\lambda/C_G(N)$ for all $\lambda \in \hat{N}$.

Q.E.D.

CHAPTER 3

SOLUBLE q' - HALFTRANSITIVE GROUPS OF LINEAR TRANSFORMATIONS OF A GF(q) - VECTOR SPACE. I

In this chapter and the next we study the following situation: G is a soluble group, q is a prime, V is an irreducible GF(q)G-module, faithful for G, and G acts q'-halftransitively on $V^{\#}$. Our aim will be to obtain a classification of the possibilities for such a group G similar to Passman's classification of soluble half-transitive groups of automorphisms. We will require many of Passman's techniques and results, some of which will be needed in an adapted form. Where clarity or continuity of argument demands it, an adapted proof will be given in full, together with a reference to the original result.

The method I have adopted for solving the classification problem defined above is similar to the way in which Passman attacked the problem of classifying soluble half-transitive groups of automorphisms in the series of papers [10] (with Isaacs), [11], [12], [13]. Essentially Passman split the problem into two cases according to whether the group acting was primitive or imprimitive as a linear group. The problem we are concerned with here will also be split into two cases, although not according to primitivity or imprimitivity. The distinction I shall make is whether or not the group acting contains a non-cyclic abelian normal subgroup. It will be seen that these two cases correspond closely enough to the primitive and imprimitive cases to enable us to use many of Passman's methods.

We first consider the case in which the group acting does contain a non-cyclic abelian normal subgroup, and we begin by describing a family of groups that occur as particular examples of this case.

DEFINITION 3.1. Let q be a prime such that $q > 2$, and let n be a positive integer and m a non-negative integer such that $q^m | n$. Also let V denote

a 2-dimensional vector space over the field $GF(q^n)$. $Aut(GF(q^n))$ is a cyclic group of order n and since $q^m|n$ there exists a unique subgroup of $Aut(GF(q^n))$ of order q^m. Let S denote such a subgroup. Let $\mathcal{T}_o(q^n;\ q^m)$ denote the group of all maps from V to V of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 \\ 0 & \pm a^{-1} \end{pmatrix} \begin{pmatrix} x^\sigma \\ y^\sigma \end{pmatrix}$$

and

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} 0 & a \\ \pm a^{-1} & 0 \end{pmatrix} \begin{pmatrix} x^\sigma \\ y^\sigma \end{pmatrix}$$

for all elements x, y, a of $GF(q^n)$ such that $a \neq 0$, and for all $\sigma \in S$.

THEOREM 3.2. (i) $\mathcal{T}_o(q^n) \triangleleft \mathcal{T}_o(q^n;\ q^m)$ <u>and</u> $|\mathcal{T}_o(q^n;\ q^m)| = 4q^m(q^n-1)$;

(ii) $\mathcal{T}_o(q^n;\ q^m)$ <u>is soluble;</u>

(iii) V <u>is a faithful, irreducible module for</u> $\mathcal{T}_o(q^n;\ q^m)$ <u>of dimension</u> 2n <u>over the field</u> GF(q);

(iv) $\mathcal{T}_o(q^n;\ q^m)$ <u>acts</u> q^1 <u>halftransitively on</u> V^* <u>and for all</u> $v \in V^*$ <u>the stabiliser in</u> $\mathcal{T}_o(q^n;\ q^m)$ <u>of</u> v <u>is cyclic of order</u> $2q^{\alpha(v)}$ <u>for some integer</u> $\alpha(v)$ <u>depending on</u> v.

<u>Proof</u>. It is easily checked that $\mathcal{T}_o(q^n) \triangleleft \mathcal{T}_o(q^n;\ q^m)$ and that $\mathcal{T}_o(q^n)$ is complemented in $\mathcal{T}_o(q^n;\ q^m)$ by the cyclic subgroup consisting of all maps of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x^\sigma \\ y^\sigma \end{pmatrix},$$

for all $\sigma \in S$. Since the order of this subgroup is q^m (the order of S), and since $|\mathcal{T}_o(q^n)|$ is $4(q^n-1)$ it follows that $|\mathcal{T}_o(q^n;\ q^m)|$ is precisely $4q^m(q^n-1)$. The solubility of $\mathcal{T}_o(q^n;\ q^m)$ is obvious since both $\mathcal{T}_o(q^n)$ and $\mathcal{T}_o(q^n;\ q^m)/\mathcal{T}_o(q^n)$ are soluble.

Everything in (iii) is clear from the definitions of $\mathcal{T}_o(q^n;\ q^m)$ and V and so it only remains to prove (iv). Let $v \in V^*$ and let H denote the stabiliser in $\mathcal{T}_o(q^n;\ q^m)$ of v. As we have seen in Chapter 1 the stabiliser in $\mathcal{T}_o(q^n)$ of any element of V^* is a group of order 2. Therefore $|H \cap \mathcal{T}_o(q^n)| = 2$. Since $q \nmid |\mathcal{T}_o(q^n)|$ and $\mathcal{T}_o(q^n)$ has index q^m in $\mathcal{T}_o(q^n;\ q^m)$ it follows that $\mathcal{T}_o(q^n)$ is a normal Hall q'-subgroup of $\mathcal{T}_o(q^n;\ q^m)$, and we deduce that $|H|_{q'} = |H \cap \mathcal{T}_o(q^n)| = 2$. Obviously $H \cap \mathcal{T}_o(q^n) \triangleleft H$, and hence H is a cyclic group of order $2q^\alpha$ for some integer α.

Q.E.D.

It will be convenient to have a description of the group $\mathcal{T}_o(q^n;\ q^m)$ in terms of generators and relations. Let q, n, m, V and S be as above and let b be a generator of the multiplicative group of $GF(q^n)$. In addition, let c, d, e denote the maps

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}, \qquad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix},$$

and

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

respectively for all elements x, y, of $GF(q^n)$. As shown in Chapter 1, we have, writing $\gamma = q^n-1$,

$$\mathcal{T}_o(q^n) = \langle c,\ d,\ e,\ :\ c^\gamma = d^2 = e^2 = 1,\ cd = dc,\ ece = c^{-1},\ ede = c^{\gamma/2}d \rangle.$$

The group S is cyclic of order q^m. Suppose $S = \langle \tau \rangle$ and let $f \in \mathcal{T}_o(q^n;\ q^m)$ denote the map

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x^\tau \\ y^\tau \end{pmatrix}.$$

Clearly f has order q^m and $\mathcal{T}_o(q^n;\ q^m) = \langle c, d, e, f\rangle$. Also it is easily checked that fd = df and fe = ef. Write $k = q^m$. Recall that the subgroup $\mathcal{T}_k(q^n)$ of $\mathcal{T}(q^n)$ is defined to be the subgroup consisting of all maps of the form

$$x \longmapsto ax^{\sigma}$$

for all elements x, a, of $GF(q^n)$ such that $a \neq 0$, and for all $\sigma \in S$. Now it is easily seen that the subgroup $\langle c,f\rangle$ of $\mathcal{T}_o(q^n;\ q^m)$ is isomorphic to the group $\mathcal{T}_k(q^n)$. Hence $\mathcal{T}_o(q^n;\ q^m)$ contains elements c, d, e, and f such that $\mathcal{T}_o(q^n;\ q^m) = \langle c, d, e, f\rangle$, $|c| = \gamma$, $|d| = |e| = 2$, $|f| = k$, $[c, d] = [d, f] = [e,f] = 1$, $ece = c^{-1}$, $ede = c^{\gamma/2}e$ and $\langle c, f\rangle \cong \mathcal{T}_k(q^n)$.

We shall require the next result in the proof of Lemma 3.5 later in this chapter.

LEMMA 3.3. <u>Let</u> G <u>be a</u> 2-<u>group containing three distinct normal subgroups</u> R_1, R_2, R_3, <u>each of order</u> 2. <u>Assume that</u> G/R_i <u>is cyclic or generalised quaternion for</u> i = 1, 2, 3. <u>Then</u> $G \cong C_2 \times C_2$.

<u>Proof</u>. Let $R_1 = \langle a\rangle$, $R_2 = \langle b\rangle$, $R_3 = \langle c\rangle$. Since G/R_i is either cyclic or generalised quaternion, G/R_i has a unique involution for i = 1, 2, 3. But both cR_1 and bR_1 are involutions in G/R_1; hence $cR_1 = bR_1$, giving c = b or c = ba. Now $c \neq b$ since $R_2 \neq R_3$, and so c = ba. Therefore, writing $T = \langle R_1, R_2, R_3\rangle$, we have $T \cong C_2 \times C_2$ and $T \lhd G$.

Suppose that $g \in G\backslash T$. Then gR_i is a non-trivial element of G/R_i for i = 1, 2, 3, and gT is a non-trivial element of G/T, a 2-group. Let 2^e be the order of the element gT in the group G/T. Then $g^{2^e} \in T$ and $g^{2^f} \notin T$ for f < e.

If $g^{2^e} = 1$, then $g^{2^{e-1}}$ is an involution in G, and so $g^{2^{e-1}}R_1$ is an involution in G/R_1. Hence $g^{2^{e-1}}R_1 = bR_1$, giving $g^{2^{e-1}} = b$ or ba, and then $g^{2^{e-1}} \in T$, a contradiction. Therefore $g^{2^e} \neq 1$.

If $g^{2^e} = a$, then $g^{2^{e-1}}R_1$ is an involution in G/R_1 and so, arguing as before, $g^{2^{e-1}} = b$ or ba, again a contradiction. Hence $g^{2^e} \neq a$.

Similarly $g^{2^e} \neq b$ and $g^{2^e} \neq c$. But $T = \{1, a, b, c\}$ and we are forced to conclude that $G \setminus T = \emptyset$. Thus $G = T \cong C_2 \times C_2$.

Q.E.D.

ASSUMPTIONS. From this point up to the end of Theorem 3.9 we work under the assumptions that G is a soluble group, q is a prime and V is an irreducible GF(q)G-module, faithful for G, such that G acts q'-halftransitively on V^*. In addition we assume that G contains a non-cyclic abelian normal subgroup.

LEMMA 3.4. <u>We have</u> $q \neq 2$ <u>and there exists</u> $N \triangleleft G$ <u>such that</u> $N \cong C_2 \times C_2$.

<u>Proof</u>. Since G contains a non-cyclic abelian normal subgroup, G must contain a non-cyclic abelian normal p-subgroup for some prime p. Let M be such a normal p-subgroup of G and restrict V to M. By Clifford's Theorem

$$V_M = V_1 \oplus \ldots \oplus V_t$$

where each V_i is the direct sum of M-isomorphic irreducible GF(q)M-modules, a homogeneous component of V_M. Let W_i be an irreducible direct summand of V_i for $1 \leq i \leq t$, and let R_i denote the kernel of M on W_i.

From the fact that V_i is homogeneous, it follows that R_i is the kernel of M on V_i for $1 \leq i \leq t$. Also $R_i > 1$ for $1 \leq i \leq t$ since M is abelian but not cyclic and, from the faithfulness of V, we have $t > 1$ and $\bigcap_{i=1}^{t} R_i = 1$. Let H_i denote the stabiliser in G of V_i. Then $H_i = \{g \in G: V_i g = V_i\}$ and, by Clifford's Theorem, V_i is an irreducible $GF(q)H_i$-module, G permutes the V_i transitively, $V \cong V_i^G$, and $|G : H_i| = t$ for $1 \leq i \leq t$. If K_i denotes $\ker(H_i \text{ on } V_i)$, then $K_i \cap M = R_i \triangleleft H_i$ for $1 \leq i \leq t$ and $\bigcap_{i=1}^{t} K_i = 1$.

Clearly, if $v \in V_i^*$ for some $i \in \{1, \ldots, t\}$, then $G_v \leq H_i$. We have

$t > 1$, and so let $v_i \in V_i^{\#}$, $v_j \in V_j^{\#}$ where $i \neq j$ and write $v = v_i + v_j$. For $g \in G_v$ obviously $v_i g = v_i$ or v_j and so we have a homomorphism from G_v to the symmetric group on $\{i,j\}$ whose kernel is $G_{v_i} \cap G_{v_j}$. Therefore $|G_v : G_{v_i} \cap G_{v_j}| \leqslant 2$. Since $|G_{v_i}|_{q'} = |G_v|_{q'}$ by q'-halftransitivity, we have

$$|G_{v_i} : G_{v_i} \cap G_{v_j}| = q^{\alpha} \text{ or } 2q^{\alpha} \tag{1}$$

for some integer $\alpha \geqslant 0$. (We allow the case $q = 2$.) Let r be a prime such that $r \neq 2,q$. Then (1) shows that G_{v_j} contains a Sylow r-subgroup of G_{v_i}. Since $O_r(G_{v_i}) \leqslant Q$ for all Sylow r-subgroups, Q, of G_{v_i}, by varying v_j inside V_j we see that

$$O_r(G_{v_i}) \leqslant K_j \tag{2}$$

By letting j vary under the restriction $i \neq j$ we deduce that $O_r(G_{v_i}) \leqslant \bigcap_{j \neq i} K_j$. Now $O_r(K_i)$ char $K_i \lhd G_{v_i}$, and so $O_r(K_i) \lhd G_{v_i}$. Thus $O_r(K_i) \leqslant O_r(G_{v_i})$, whence

$$O_r(K_i) \leqslant \bigcap_{j=1}^{t} K_j = 1.$$

Consequently, for all primes r such that $r \neq 2,q$, we have

$$O_r(K_i) = 1 \tag{3}$$

Since M is a non-trivial normal p-subgroup of G and G has a faithful, irreducible module, V, over $GF(q)$, a field of characteristic q, it follows that $p \neq q$. We have $1 < R_i \leqslant O_p(K_i)$ and therefore, using (3), we see that $p = 2$. Hence $q \neq 2$.

Let $g \in O_2(K_i)$. Since $O_2(K_i)$ char $K_i \lhd G_{v_i}$, we have $O_2(K_i) \lhd G_{v_i}$, and it follows that $O_2(K_i) \leqslant O_2(G_{v_i})$. Therefore $O_2(K_i) \leqslant S$ for all Sylow 2-subgroups S of G_{v_i}. Again let $j \neq i$ and $v_j \in V_j^{\#}$. From (1) we have $|G_{v_i} : G_{v_i} \cap G_{v_j}| = q^{\alpha}$ or $2q^{\alpha}$ for some integer $\alpha \geqslant 0$, and so, if T is a Sylow 2-subgroup of $G_{v_i} \cap G_{v_j}$ and S is a Sylow 2-subgroup of G_{v_i} containing T, then $|S : T| \leqslant 2$, whence $T \lhd S$. Therefore $g^2 \in T \leqslant G_{v_j}$. By varying

v_j inside V_j we see that $g^2 \in K_j$, and by varying j we see that

$$g^2 \in \bigcap_{j=1}^{t} K_j = 1. \tag{4}$$

Hence for all $g \in O_2(K_i)$ we have $g^2 = 1$, and we deduce that $O_2(K_i)$ is an elementary abelian 2-group.

We next show that if $i \in \{1,\ldots, t\}$ and if $v_i \in V_i^{\#}$, then there exists $j \neq i$ and $v_j \in V_j^{\#}$ such that $2 \mid |G_{v_i} : G_{v_i} \cap G_{v_j}|$. Suppose, on the contrary, that for all $j \neq i$ and for all $v_j \in V_j^{\#}$ we have $2 \nmid |G_{v_i} : G_{v_i} \cap G_{v_j}|$. Then for all $j \neq i$ and for all $v_j \in V_j^{\#}$ the subgroup G_{v_j} contains a Sylow 2-subgroup of G_{v_i}. Now $R_i \lhd G_{v_i}$ and R_i is a 2-group. Hence $R_i \leqslant O_2(G_{v_i})$, and so R_i is contained in each Sylow 2-subgroup of G_{v_i}. Therefore R_i is a subgroup of G_{v_j} for all $v_j \in V_j^{\#}$ and for all $j \neq i$, giving that $R_i \leqslant K_j$ for all $j \neq i$. But $R_i \leqslant K_i$ and hence $R_i \leqslant \bigcap_{j=1}^{t} K_j = 1$, a contradiction. We conclude that for any $v_i \in V_i^{\#}$ there exists $j \neq i$ and $v_j \in V_j^{\#}$ such that $2 \mid |G_{v_i} : G_{v_i} \cap G_{v_j}|$.

Suppose that $t \geqslant 3$ and choose $i \in \{1,\ldots, t\}$. Pick $v_i \in V_i^{\#}$ and then, in view of the previous paragraph, we may choose $j \in \{1,\ldots, t\}$ and $v_j \in V_j^{\#}$ such that $j \neq i$ and $2 \mid |G_{v_i} : G_{v_i} \cap G_{v_j}|$. Since $t \geqslant 3$ there exists $k \in \{1,\ldots, t\}$ such that $k \neq i$ and $k \neq j$. Let $v_k \in V_k^{\#}$ and write $v = v_i + v_j + v_k$. Using a similar argument to the one used earlier, there is a homomorphism from G_v to the symmetric group on $\{i, j, k\}$ whose kernel is $G_{v_i} \cap G_{v_j} \cap G_{v_k}$. Therefore $|G_v : G_{v_i} \cap G_{v_j} \cap G_{v_k}| = 1,2,3$ or 6 and then since $|G_v|_{q'} = |G_{v_i}|_{q'}$ and $q \neq 2$, it follows that $|G_{v_i} : G_{v_i} \cap G_{v_j} \cap G_{v_k}| = d$ or $2d$ for some odd integer d. But $|G_{v_i} : G_{v_i} \cap G_{v_j} \cap G_{v_k}| = |G_{v_i} : G_{v_i} \cap G_{v_j}| \cdot |G_{v_i} \cap G_{v_j} : G_{v_i} \cap G_{v_j} \cap G_{v_k}|$ and $2 \mid |G_{v_i} : G_{v_i} \cap G_{v_j}|$. Therefore $2 \nmid |G_{v_i} \cap G_{v_j} : G_{v_i} \cap G_{v_j} \cap G_{v_k}|$, and hence G_{v_k} contains a Sylow 2-subgroup of $G_{v_i} \cap G_{v_j}$. Since $O_2(G_{v_i} \cap G_{v_j})$ is contained in each Sylow 2-subgroup of $G_{v_i} \cap G_{v_j}$, by varying v_k inside V_k we see that

$$O_2(G_{v_i} \cap G_{v_j}) \leqslant K_k . \tag{5}$$

By varying k subject to the condition $i \neq k \neq j$ we have

$$O_2(G_{v_i} \cap G_{v_j}) \leqslant \bigcap_{i \neq k \neq j} K_k.$$

Since $O_2(K_i \cap K_j)$ char $K_i \cap K_j \triangleleft G_{v_i} \cap G_{v_j}$, it follows that $O_2(K_i \cap K_j) \triangleleft G_{v_i} \cap G_{v_j}$ and so $O_2(K_i \cap K_j) \leqslant O_2(G_{v_i} \cap G_{v_j})$. Therefore

$$O_2(K_i \cap K_j) \leqslant \bigcap_{k=1}^{t} K_k = 1.$$

Now $R_i \cap R_j \leqslant O_2(K_i \cap K_j) = 1$, and in consequence $R_i \cong R_iR_j/R_j \leqslant M/R_j$, a cyclic group. Hence R_i is cyclic. But $R_i \leqslant O_2(K_i)$, and $O_2(K_i)$ is an elementary abelian 2-group as proved earlier. Therefore $|R_i| = 2$. The group M is a non-cyclic abelian 2-group and M/R_i is cyclic. Hence $M \cong C_{2e} \times C_2$ for some integer $e \geqslant 1$.

On the other hand, if $t = 2$, we have $R_1 \cap R_2 = 1$, giving $R_1 \cong R_1R_2/R_2 \leqslant M/R_2$, a cyclic group. It follows that R_1 is cyclic and, since $R_1 \leqslant O_2(K_1)$, an elementary abelian 2-group, we must have $|R_1| = 2$. Then, as above, $M \cong C_{2e} \times C_2$ for some integer $e \geqslant 1$.

Thus we have shown that, for $t \geqslant 3$ or for $t = 2$, $M \cong C_{2e} \times C_2$ for some $e \geqslant 1$. Writing $N = \Omega_1(M)$, we have $N \triangleleft G$ and $N \cong C_2 \times C_2$.

Q.E.D.

NOTATION. Let N denote a normal subgroup of G such that $N \cong C_2 \times C_2$. (The existence of such a subgroup N is guaranteed by Lemma 3.4) By Clifford's Theorem we have

$$V_N = V_1 \oplus \ldots \oplus V_t$$

where the V_i are the homogeneous components of V_N. To continue fixing our notation, let H_i denote the stabiliser in G of V_i, R_i the kernel of N on V_i, and K_i the kernel of H_i on V_i (whence $R_i = K_i \cap N$) for $1 \leqslant i \leqslant t$. By Clifford's Theorem, V_i is an irreducible $GF(q)H_i$-module. Furthermore

$|G : H_i| = t$ and all the H_i are conjugate in G. Clearly $|R_i| = 2$ for $1 \leq i \leq t$ and $\bigcap_{i=1}^{t} K_i = 1$. Let L denote $C_G(N)$. Obviously $L \leq H_i$ for $1 \leq i \leq t$ and G/L is isomorphic to a subgroup of $\mathrm{Aut}(N) \cong S_3$.

LEMMA 3.5. <u>If</u> t <u>is defined as above, then</u> t = 2.

<u>Proof.</u> Clearly $t > 1$. There are exactly three non-equivalent, non-trivial irreducible representations of N over the field GF(q), and so t = 2 or t = 3. Hence the lemma will be proved if we show that t = 3 is impossible. So suppose, if possible, that t = 3. Then R_1, R_2, R_3 are the three distinct subgroups of N of order 2.

Let $v_1 \in V_1^{\#}$ and suppose that $O_2(G_{v_1}) \leq K_j$ for some $j \neq 1$. Then $R_1 \leq O_2(G_{v_1}) \leq K_j$. But $R_j \leq K_j$ and therefore $\langle R_1, R_j \rangle = N \leq K_j$, clearly an impossibility. Thus, if j = 2 or j = 3, then $O_2(G_{v_1}) \not\leq K_j$. Exactly as in Lemma 3.4(1), for $j \neq 1$ and $v_j \in V_j^{\#}$, we have $|G_{v_1} : G_{v_1} \cap G_{v_j}| = q^{\alpha}$ or $2q^{\alpha}$ for some $\alpha \geq 0$. If for all $v_j \in V_j^{\#}$ we have $2 \nmid |G_{v_1} : G_{v_1} \cap G_{v_j}|$, then it is easily seen that $O_2(G_{v_1}) \leq K_j$, a contradiction. Therefore there exist $v_2 \in V_2^{\#}$, $v_3 \in V_3^{\#}$ such that $|G_{v_1} : G_{v_1} \cap G_{v_2}| = 2q^{\beta}$ and $|G_{v_1} : G_{v_1} \cap G_{v_3}| = 2q^{\gamma}$ for some $\beta, \gamma \geq 0$.

Exactly as in Lemma 3.4(5) we have $O_2(G_{v_1} \cap G_{v_2}) \leq K_3$ and $O_2(G_{v_1} \cap G_{v_3}) \leq K_2$. Write $M = O_2(G_{v_1})$. Then $M \cap G_{v_2} \leq O_2(G_{v_1} \cap G_{v_2}) \leq K_3$. Similarly $M \cap G_{v_3} \leq K_2$. Since $M \cap G_{v_2} \leq K_3 \leq G_{v_3}$, it follows that $M \cap G_{v_2} \cap G_{v_3} = M \cap G_{v_2}$, and similarly, $M \cap G_{v_2} \cap G_{v_3} = M \cap G_{v_3} \leq K_2$. Therefore

$$M \cap G_{v_3} = M \cap G_{v_2} \leq K_2 \cap K_3. \tag{6}$$

Write $K = O_2(K_1) = M \cap K_1$ and consider $K \cap G_{v_2}$. Clearly $K \cap G_{v_2} \leq M \cap G_{v_2}$, whereupon $K \cap G_{v_2} \leq K_2 \cap K_3$. But $K \leq K_1$, and hence $K \cap G_{v_2} \leq K_1 \cap K_2 \cap K_3 = 1$. Let T be a Sylow 2-subgroup of $G_{v_1} \cap G_{v_2}$, and let S be a Sylow 2-subgroup of G_{v_1} such that $S \geq T$. Since $|G_{v_1} : G_{v_1} \cap G_{v_2}| = 2q^{\beta}$, we have $|S : T| = 2$, whence $T \lhd S$. Also $K \leq M = O_2(G_{v_1})$ and it

follows that $K \leqslant S$. Now $K \cap T \leqslant K \cap G_{v_2} = 1$, giving

$$2 = |S/T| \geqslant |KT/T| = |K/K \cap T| = |K|.$$

Therefore, since $R_1 \leqslant K$ and $|R_1| = 2$, we have $K = R_1$. For any prime r with $r \neq 2, q$, we have $O_r(K_1) = 1$ by Lemma 3.4 (1). Consider $O_q(K_1)$. Since $C_G(N) = L \leqslant H_1 \leqslant G$ and $|G/L| \,\big|\, |S_3| = 6$, and using the fact the $|G : H_1| = t = 3$, we see that $|H_1 : L| \leqslant 2$. Now $q > 2$, and so $O_q(K_1) \leqslant L$. Clearly $L \leqslant N_G(K_1)$ and therefore, since $O_q(K_1)$ char K_1, we must have $O_q(K_1) \lhd L$. Hence $O_q(K_1) \leqslant O_q(L)$. But $O_q(L)$ char $L \lhd G$, giving $O_q(L) \lhd G$. We conclude that $O_q(K_1) \leqslant O_q(L) \leqslant O_q(G) = 1$, and it follows that $F(K_1) = O_2(K_1) = R_1$. Since G is soluble, so is K_1, and hence $C_{K_1}(F(K_1)) = F(K_1)$. Therefore $K_1 = R_1 \cong C_2$. Similarly $K_2 = R_2$ and $K_3 = R_3$.

From (6)

$$M \cap G_{v_2} \leqslant K_2 \cap K_3 = R_2 \cap R_3 = 1.$$

With T and S as above, we have $M \leqslant S$, and, since $M \cap T \leqslant M \cap G_{v_2} = 1$, it follows that

$$2 = |S/T| \geqslant |MT/T| = |M/M \cap T| = |M|.$$

Hence

$$M = O_2(G_{v_1}) = R_1 \tag{7}$$

for all $v_1 \in V_1^{\#}$. Similarly $O_2(G_{v_2}) = R_2$ for all $v_2 \in V_2^{\#}$ and $O_2(G_{v_3}) = R_3$ for all $v_3 \in V_3^{\#}$.

Write $L_2 = O_2(L)$. Then, clearly, $L_2 \lhd G$ and $O_2(L/R_i) = L_2/R_i$ for $i = 1, 2, 3$. If $v_i \in V_i^{\#}$, then $G_{v_i} \cap L_2 \lhd G_{v_i}$ and hence $G_{v_i} \cap L_2 \leqslant O_2(G_{v_i}) = R_i$ for $i = 1, 2, 3$. It follows that V_i is a faithful module for the 2-group L_2/R_i, and L_2/R_i acts semi-regularly on $V_i^{\#}$ for $i = 1, 2, 3$. The structure of a group that acts semi-regularly as a group of automorphisms

is well-known. In particular, a 2-group that acts semi-regularly as a group of automorphisms is either cyclic or generalised quaternion. Hence L_2 is a 2-group containing three distinct normal subgroups, R_1, R_2, R_3, each of order 2 such that L_2/R_i is cyclic or generalised quaternion for $i = 1, 2, 3$. Therefore $L_2 \cong C_2 \times C_2$ by Lemma 3.3, giving $L_2 = N$. If r is a prime such that $r \neq 2,q$, and if $v_1 \in V_1^{\#}$, then $O_r(G_{v_1}) \leqslant K_2$ by Lemma 3.4(2). But $|K_2| = 2$, and so $O_r(G_{v_1}) = 1$ for all $v_1 \in V_1^{\#}$. If L_r denotes $O_r(L)$, we have $G_{v_1} \cap L_r \triangleleft G_{v_1}$, and it follows that $G_{v_1} \cap L_r \leqslant O_r(G_{v_1}) = 1$ for all $v_1 \in V_1^{\#}$. Hence L_r acts semi-regularly on $V_1^{\#}$. Since, for any prime $r \neq 2$, an r-group that acts semi-regularly as a group of automorphisms is cyclic, we conclude that L_r is cyclic for all primes r such that $r \neq 2, q$. Clearly $O_q(L) \leqslant O_q(G) = 1$, and hence $F(L) = N \times A$ where A is a cyclic group of odd order.

Now $N \leqslant F(L)$, and so $C_G(F(L)) \leqslant C_G(N) = L$. Therefore $C_G(F(L)) = C_L(F(L)) = F(L)$. It follows that $H_1/F(L)$ is isomorphic to a subgroup of $H_1/C_{H_1}(N) \times H_1/C_{H_1}(A)$, which is clearly abelian because $C_{H_1}(N) = L$, $|H_1/L| \leqslant 2$, and because A is cyclic. Hence $H_1/F(L)$ is abelian. Let $v_1 \in V_1^{\#}$. Since $G_{v_1} \cap F(L) = R_1$, we have $G_{v_1}/R_1 \cong G_{v_1}F(L)/F(L) \leqslant H_1/F(L)$, an abelian group. Thus G_{v_1} is nilpotent, and hence $4 \nmid |G_{v_1}|$ by (7). Therefore, by q'-halftransitivity, $4 \nmid |G_v|$ for all $v \in V^{\#}$.

We next show that N is a Sylow 2-subgroup of L. Let Q be a Sylow 2-subgroup of L, and let $v_1 \in V_1^{\#}$. As we have proved above, $4 \nmid |G_{v_1}|$, whence $4 \nmid |Q_{v_1}|$, and therefore $Q_{v_1} = R_1$. It follows that Q/R_1 is a 2-group that acts faithfully on V_1 and semi-regularly on $V_1^{\#}$, and we deduce that Q/R_1 is either cyclic or generalised quaternion. Similarly Q/R_2 and Q/R_3 are cyclic or generalised quaternion. Thus, by Lemma 3.3, we have $Q \cong C_2 \times C_2$ and so $Q = N$.

We have already shown that $|H_1/L| \leqslant 2$. Suppose that $|H_1/L| = 2$ and let P be a Sylow 2-subgroup of H_1. Then $|P| = 8$ and $C_2 \times C_2 \cong N \leqslant P$.

Now P is non-abelian (since otherwise $P \leqslant C_G(N) = L$, contradicting the fact that N is a Sylow 2-subgroup of L), and therefore P is isomorphic to the dihedral group of order 8. The kernel of H_1 on V_1 is exactly R_1, and so V_1 is a faithful module for $P/R_1 \cong C_2 \times C_2$. Then it is obvious that there exists $v_1 \in V_1^{\#}$ such that $4 \mid |P_{v_1}|$, whence $4 \mid |G_{v_1}|$, which, as we have seen, is impossible. Therefore $|H_1/L| \neq 2$. The only remaining possibility is $|H_1/L| = 1$, so suppose this is the case. We have $H_1 = H_2 = H_3 = L \lhd G$. If $v_1 \in V_1^{\#}$, $v_2 \in V_2^{\#}$, then, clearly, $G_{v_1+v_2} = G_{v_1} \cap G_{v_2}$. By q'-halftransitivity $|G_{v_1}|_{q'} = |G_{v_1+v_2}|_{q'}$, and hence $|G_{v_1} : G_{v_1} \cap G_{v_2}| = q^{\alpha}$ for some $\alpha \geqslant 0$. But, by varying v_2 inside V_2, we see that G_{v_2} contains a Sylow 2-subgroup of G_{v_1} for all $v_2 \in V_2^{\#}$. Therefore $R_1 = O_2(G_{v_1}) \leqslant K_2 = R_2$, a contradiction. Hence $|H_1/L| \neq 1$, and our assumption that $t = 3$ must be false.

Q.E.D.

NOTATION. In view of Lemma 3.5 we have $|G : H_1| = |G : H_2| = 2$. Hence $H_i \lhd G$ for $i = 1, 2$. But H_1 is conjugate to H_2 in G and therefore $H_1 = H_2 = H$, say.

Before proceeding with our analysis of the structure of G, we state, without proof and combined into a single lemma, two results concerning soluble transitive linear groups. The first result, Lemma 3.6(i), is Hilfssatz 3 of [7] and the second, Lemma 3.6 (ii), is Hilfssatz 4 of [7].

LEMMA 3.6 (Huppert [7]). <u>Let</u> A <u>be a group and let</u> p <u>be a prime. Assume that</u> W <u>is a</u> $GF(p)A$-<u>module, faithful for</u> A, <u>and</u> A <u>acts transitively on</u> $W^{\#}$. <u>Then</u>

(i) A <u>is primitive as a linear group on</u> W;

(ii) <u>if</u> A <u>contains a normal subgroup,</u> Q, <u>such that</u> Q <u>is isomorphic to the quaternion group of order</u> 8, <u>then</u> W_Q <u>is irreducible.</u>

LEMMA 3.7. <u>For</u> $i = 1, 2$, <u>we have</u> $K_i = R_i$ <u>and</u> H/K_i <u>acts transitively on</u> $V_i^{\#}$.

Proof. Let $v_2 \in V_2^{\#}$ and suppose that $R_1 \leqslant G_{v_2}$. Now $|R_1| = 2$ and $R_1 \cap K_2 = 1$ (since $K_1 \cap K_2 = 1$), and therefore $|R_1K_2/K_2| = 2$. It follows that R_1K_2/K_2 is central in H/K_2. Since V_2 is an irreducible $GF(q)H/K_2$-module, faithful for H/K_2, the non-trivial element of R_1K_2/K_2 acts like scalar multiplication by -1 on V_2 and thus acts fixed-point-freely on $V_2^{\#}$. But $G_{v_2} \geqslant K_2$ and $G_{v_2} \geqslant R_1$. Hence R_1K_2/K_2 is contained in the stabiliser in H/K_2 of v_2, a contradiction. Therefore we have shown that $R_1 \cap G_{v_2} = 1$ for all $v_2 \in V_2^{\#}$, and, using the same argument with the subscripts 1 and 2 interchanged, we deduce that

$$R_i \cap G_{v_j} = 1 \tag{8}$$

for $i, j \in \{1, 2\}$ such that $i \neq j$ and for all $v_j \in V_j^{\#}$.

If $v_1 \in V_1^{\#}$, $v_2 \in V_2^{\#}$, then, by Lemma 3.4(1), we have $|G_{v_1} : G_{v_1} \cap G_{v_2}| = q^{\alpha}$ or $2q^{\alpha}$ for some $\alpha \geqslant 0$. However, if $2 \nmid |G_{v_1} : G_{v_1} \cap G_{v_2}|$, then G_{v_2} contains a Sylow 2-subgroup of G_{v_1}, and hence contains $O_2(G_{v_1})$. But then $R_1 \leqslant O_2(G_{v_1}) \leqslant G_{v_2}$, contradicting (8), and we conclude that $|G_{v_1} : G_{v_1} \cap G_{v_2}| = 2q^{\alpha}$. By q'-halftransitivity, $|G_{v_1}|_{q'} = |G_{v_1+v_2}|_{q'}$, and hence $2 \mid |G_{v_1+v_2} : G_{v_1} \cap G_{v_2}|$. As before, the existence of a homomorphism from $G_{v_1+v_2}$ to the symmetric group on $\{1, 2\}$ with kernel $G_{v_1} \cap G_{v_2}$ implies that $|G_{v_1+v_2} : G_{v_1} \cap G_{v_2}| \leqslant 2$, and therefore we have shown that

$$|G_{v_1+v_2} : G_{v_1} \cap G_{v_2}| = 2 \tag{9}$$

for all $v_1 \in V_1^{\#}$, $v_2 \in V_2^{\#}$.

Let $v_1 \in V_1^{\#}$, $v_2 \in V_2^{\#}$ and let $g \in G \backslash H$. We have $H_{v_1+v_2} = G_{v_1+v_2} \cap H = G_{v_1} \cap G_{v_2}$, and hence, from (9), there exists $x \in G_{v_1+v_2}$ such that $x \notin H$. Clearly $x = hg$ for some $h \in H$, and, since $V_1g = V_2$, $V_2g = V_1$, we must have $v_1(hg) = v_1x = v_2$ and $v_2(hg) = v_2x = v_1$. Let $v_2g^{-1} = v \in V_1^{\#}$, and then $vg = v_2 = v_1(hg) = (v_1h)g$, giving $v_1h = v$. By keeping v_2 fixed and varying

v_1 inside $V_1^{\#}$, we see that for all $v_1 \in V_1^{\#}$ there exists $h \in H$ such that $v_1 h = v$. Thus H acts transitively on $V_1^{\#}$, and so, since $K_1 = \ker(H \text{ on } V_1)$, the group H/K_1 acts transitively on $V_1^{\#}$. Similarly H/K_2 acts transitively on $V_2^{\#}$.

By the remark immediately following (4) in Lemma 3.4, the group $O_2(K_1)$ is an elementary abelian 2-group. Also, since $K_1 \cap K_2 = 1$, we have $O_2(K_1) \cong O_2(K_1)K_2/K_2 \triangleleft H/K_2$. Now V_2 is a $GF(q)H/K_2$-module, faithful for H/K_2, and H/K_2 acts transitively on $V_2^{\#}$. Therefore, by Lemma 3.6(i), H/K_2 is primitive as a linear group. In particular, each abelian normal subgroup of H/K_2 is cyclic and hence $|O_2(K_1)| \leq 2$. Since $R_1 \leq O_2(K_1)$, it follows that $R_1 = O_2(K_1)$. From Lemma 3.4(3) we have $O_r(K_1) = 1$ for all primes r such that $r \neq 2,q$. Clearly $O_q(K_1)$ char $K_1 \triangleleft H$, and hence $O_q(K_1) \leq O_q(H)$. Since $H \triangleleft G$, it follows that $O_q(H) \leq O_q(G) = 1$, and we deduce that $O_q(K_1) = 1$. Therefore $F(K_1) = O_2(K_1) = R_1$. But $|R_1| = 2$, and so, since $C_{K_1}(F(K_1)) = F(K_1)$, we have $K_1 = F(K_1) = R_1$. Similarly $K_2 = R_2$.

Q.E.D.

Before proceeding to state and prove the main theorem of this chapter, we describe, and fix a symbol to represent a particular soluble group of order 96.

DEFINITION 3.8. Let $A = GL(2,3)$. Then, writing $Z = Z(A)$, we have $|Z| = 2$, and there exist subgroups B, Y of A such that $B = SL(2,3)$, $Y \cong C_2$ and $A = BY$. Let X be any group of order 2. We may define a group, which we denote by Δ, as follows:

$$\Delta = \langle A, X : [B,X] = 1, [Y, X] = Z \rangle.$$

If we write $E = B \times X$, then $E \cong SL(2,3) \times C_2$ and $\Delta = EY$ where Y acts non-trivially on both $O_2(E)/Z(E)$ and $Z(E)$. Clearly Δ is soluble and $|\Delta| = 96$.

THEOREM 3.9. Let G be a soluble group, q a prime and V an irreducible $GF(q)G$-module, faithful for G. Assume that G acts q'-halftransitively on $V^{\#}$ and that G contains a non-cyclic abelian normal subgroup. Then $q \neq 2$, the dimension of V over $GF(q)$ is $2n$ for some integer n, and either $G \cong \mathcal{T}_0(q^n : q^m)$ for some m such that $q^m | n$, or $n = 2$, $q = 3$ and G satisfies one of the following:

(i) $G \cong Q_8 \curlyvee D_8$;

(ii) $G \cong SL(2,3) \curlyvee D_8$;

(iii) $G \cong \Delta$;

(iv) $G \cong GL(2,3) \curlyvee D_8$.

Proof. By Lemmas 3.4, 3.5, and 3.7 we have $q \neq 2$ and there exists $N \lhd G$ such that $N \cong C_2 \times C_2$ and

$$V_N = V_1 \oplus V_2$$

where V_i is a homogeneous component of V_N for $i = 1, 2$. Therefore, writing $n = \dim_{GF(q)} V_2$, we have $\dim_{GF(q)} V = 2n$ as required. If H is the stabiliser in G of V_1 then H is also the stabiliser in G of V_2 and, by the above-mentioned lemmas, if K_i denotes $\ker(H \text{ on } V_i)$ and R_i denotes $\ker(N \text{ on } V_i)$, then $K_i = R_i \cong C_2$ for $i = 1, 2$. Moreover H/K_i acts transitively on $V_i^{\#}$ for $i = 1, 2$.

Assume that H/K_1 acts regularly on $V_1^{\#}$. Then $|H/K_1| = |V_1^{\#}| = q^n - 1$. Since $|K_1| = |G : H| = 2$, it follows that $q \nmid |G|$. Therefore G acts half-transitively on $V^{\#}$ and we can apply Theorem 1.16. If $v \in V_1^{\#}$ then $G_v = K_1 > 1$, and hence G does not act semi-regularly on $V^{\#}$. Also G is imprimitive as a linear group on V since $C_2 \times C_2 \cong N \lhd G$, and therefore by Theorem 1.16 we have either $G \cong \mathcal{T}_0(q^n)$, or $n = 2$, $q = 3$, and $G \cong Q_8 \curlyvee D_8$, or $n = 3$, $q = 2$, and G is isomorphic to the dihedral group of order 18. But we have shown that $q \neq 2$, and hence, if H/K_1 acts regularly on $V_1^{\#}$, then either $G \cong \mathcal{T}_0(q^n) = \mathcal{T}_0(q^n : 1)$, or $n = 2$, $q = 3$, and $G \cong Q_8 \curlyvee D_8$

(case (i) in the statement of the theorem).

Therefore we may assume that H/K_1 acts transitively but not regularly on $V_1^{\#}$. Hence, by Theorem 1.16, one of the following two cases must hold.

CASE 1. We may identify V_1 with the additive group of $GF(q^n)$ in such a way that $H/K_1 \leqslant \mathcal{T}(q^n)$.

CASE 2. One of the cases (a_1), (a_2), (b_1), (b_2), (c_2), (d_2), (f_2), (f_3), (f_4), of Theorem 1.16 holds for the group H/K_1 and the module V_1.

We show that Case 1 leads to the conclusion that $G \cong \mathcal{T}_0(q^n : q^m)$ for some integer m such that $q^m | n$, and that Case 2 leads to the conclusion that $n = 2$, $q = 3$, and G satisfies (ii), (iii), or (iv) in the statement of the theorem.

CASE 1. With suitable identification $H/K_1 \leqslant \mathcal{T}(q^n)$.

Let $v_1 \in V_1^{\#}$. Then H_{v_1}/K_1 is cyclic, and therefore H_{v_1} is central-by-cyclic, whereupon H_{v_1} is abelian. Now $H_{v_1} = G_{v_1}$ and, by Lemma 3.4(2), $O_r(G_{v_1}) \leqslant K_2 \cong C_2$ for all primes r such that $r \neq 2, q$, whence $O_r(G_{v_1}) = 1$ for all such primes r. Since G_{v_1} is abelian we conclude that $r \nmid |G_{v_1}|$ for all primes r such that $r \neq 2, q$, and since H/K_1 acts transitively on $V_1^{\#}$ there exist integers m, β, such that $|G_{v_1}| = 2^\beta q^m$ for all $v_1 \in V_1^{\#}$. By q'-halftransitivity, if $v \in V^{\#}$ then $|G_v| = 2^\beta q^{m(v)}$ for some integer m(v) depending on v. Let $v_2 \in V_2^{\#}$ and let $g \in G \backslash H$. Since $V_1 g = V_2$ it follows that G_{v_2} is conjugate in G to G_{v_1} for some $v_1 \in V_1^{\#}$, and hence G_{v_2} is an abelian group of order $2^\beta q^m$. Also, since $K_1^g = K_2$, the group G_{v_2}/K_2 is isomorphic to G_{v_1}/K_1, a cyclic group.

Since $\mathcal{T}(q^n)$ is metacyclic we have H/K_1 is metacyclic. Clearly $O_q(H/K_1)$ is trivial, and it follows that H/K_1 contains a normal Hall

q'-subgroup, R/K_1 say. Obviously R is a normal Hall q'-subgroup of H. As shown above, if $v_1 \in V_1^{\#}$ then $|H_{v_1}| = 2^{\beta}q^m$, and hence, by the transitivity of H on $V_1^{\#}$, we have $|H| = 2^{\beta}q^m(q^n-1)$. Thus $|R| = 2^{\beta}(q^n-1)$. Let $v_1 \in V_1^{\#}$. Clearly $|H_{v_1} \cap R| = |R_{v_1}| = 2^{\beta}$ and therefore $|R : R_{v_1}| = q^n - 1$, whereupon R acts transitively on $V_1^{\#}$. Hence R/K_1 acts transitively on $V_1^{\#}$.

We claim that $\beta = 1$. We have $\beta \geqslant 1$ and so, in order to obtain a contradiction, suppose that $\beta > 1$. Let I denote the set of non-central involutions of R/K_1. We show that $|I| \geqslant q^{n/2} + 1$, using a very slightly adapted version of the proof of [12] Lemma 1.2. Since $v_1 \in V_1^{\#}$ implies that $|R_{v_1}/K_1| = 2^{\beta-1}$, and since $\beta > 1$ by assumption, we have

$$V_1^{\#} = \bigcup_{x \in I} (C_{V_1}(x))^{\#} .$$

Also, if $v_1 \in V_1^{\#}$, then $R_{v_1}/K_1 \leqslant G_{v_1}/K_1$, a cyclic group. Hence R_{v_1}/K_1 is cyclic and, in particular, R_{v_1}/K_1 contains a unique element of I. Therefore the above union is disjoint. Let $k = \max(\dim(C_{V_1}(x)))$ as x varies over I, and suppose first that $k \leqslant n/2$. Then

$$q^n - 1 = |V_1^{\#}| \leqslant |I|(q^{n/2} - 1),$$

giving $q^{n/2} + 1 \leqslant |I|$ as required. Now suppose $k > n/2$ and let $k = \dim C_{V_1}(x_o)$ for some $x_o \in I$. If $x \neq x_o$ then $C_{V_1}(x) \cap C_{V_1}(x_o) = \langle 0 \rangle$ and so $\dim C_{V_1}(x) \leqslant n-k$. Thus

$$q^n - 1 \leqslant q^k - 1 + (|I| - 1)(q^{n-k} - 1)$$

and, since $n/2 < k < n$, we obtain $q^{n/2} < q^k \leqslant |I| - 1$ as required.

Let $x \in I$ and fix $v_2 \in V_2^{\#}$. Since x is a non-central involution in R/K_1, we may choose $v_1 \in V_1^{\#}$ such that $x \in R_{v_1}/K_1$. The group G_{v_2} is abelian and hence contains a unique Sylow 2-subgroup, S say. Clearly S/K_2 is cyclic of order $2^{\beta-1}$. Since $\beta > 1$ we have $4 \mid |G_v|$ for all $v \in V^{\#}$ and, by Lemma 3.7(8), we have $|G_{v_1+v_2} : G_{v_1} \cap G_{v_2}| = 2$. Therefore $2 \mid |G_{v_1} \cap G_{v_2}|$.

If S is cyclic, then K_2 is the unique subgroup of S of order 2, whereupon K_2 is the uniqe subgroup of G_{v_2} of order 2. But then $2 \mid |G_{v_1} \cap G_{v_2}|$ implies that $K_2 \leq G_{v_1}$, contradicting Lemma 3.6(8) since $K_2 = R_2$. Hence S is not cyclic and we conclude that $S \cong C_{2^\beta - 1} \times C_2$. Let T denote $\Omega_1(S)$. Then $T \cong C_2 \times C_2$ and T contains all involutions of G_{v_2}. Therefore $K_2 \leq T$. Since $2 \mid |G_{v_1} \cap G_{v_2}|$ we can choose $h \in G_{v_1} \cap G_{v_2}$ such that $|h| = 2$. Obviously $h \in T$. Also $h \in R$ and it follows that $h \in R_{v_1}$. From Lemma 3.7(8) we have $K_1 \cap G_{v_2} = 1$, and therefore $h \notin K_1$. Hence hK_1 is an element of order 2 in R_{v_1}/K_1 and so, since x is also an involution in R_{v_1}/K_1, a cyclic group, we must have $hK_1 = x$. Again by Lemma 3.7(8) we have $K_2 \cap G_{v_1} = 1$, whence $h \notin K_2$. Therefore $h \in T \setminus K_2$. It follows that there are at most 2 possibilities for h and hence there are at most 2 possibilities for $hK_1 = x$. But then $q^{n/2} + 1 \leq |I| \leq 2$, which is clearly impossible. Therefore our assumption that $\beta > 1$ is false and we conclude that $\beta = 1$.

As a consequence we see that $|H| = 2q^m(q^n - 1)$, $|G| = 4q^m(q^n - 1)$, and if $v \in V^\#$, then $|G_v| = 2q^{m(v)}$ for some integer $m(v)$ depending on v. Since $H/K_1 \leq \mathcal{T}(q^n)$ and $|\mathcal{T}(q^n)| = n(q^n - 1)$, we must have $q^m \mid n$. Clearly $|R| = 2(q^n - 1)$ and so R/K_1 acts regularly on $V_1^\#$. Let p be an odd prime. Obviously $O_p(H) = O_p(R) \cong O_p(R)K_1/K_1 = O_p(R/K_1)$. By the structure of groups that act semi-regularly as groups of automorphisms we have $O_p(R/K_1)$ is cyclic. Hence $O_p(H)$ is cyclic for all odd primes p. Write $Q = O_2(H)$. Then, clearly, $Q \lhd G$ and $Q = O_2(R)$. Since Q/K_1 acts semi-regularly on $V_1^\#$, it follows that Q/K_1 is either cyclic or generalised quaternion.

Suppose that Q/K_1 is isomorphic to the quaternion group of order 8. Then, using Lemma 3.6(ii), since R/K_1 acts transitively on $V_1^\#$ and $Q/K_1 \lhd R/K_1$, we deduce that V_1 is an irreducible Q/K_1-module. But, as is well known, Q_8 has, up to equivalence, a unique faithful irreducible representation over $GF(q)$ for any odd prime q, and this representation has degree 2. Thus $2 = \dim V_1 = n$. But then $q^m \mid n$ implies $q^m = 1$, whence $|H/K_1| = q^n - 1$

contradicting our assumption that H/K_1 does not act regularly on V_1^*. Therefore Q/K_1 is not isomorphic to the quaternion group of order 8, and hence Q/K_1 is either cyclic or generalised quaternion of order at least 16.

Clearly N/K_1 is the unique subgroup of Q/K_1 of order 2 and $N \leqslant Z(H)$. Therefore, writing $\overline{G} = G/N$, $\overline{H} = H/N$, etc., we have $F(\overline{H}) = F(H)/N$ and $\overline{Q}$ is either cyclic (if Q/K_1 is) or a dihedral group. We shall show that, in either case, G contains a normal Hall q'-subgroup.

Suppose that $\overline{Q}$ is a dihedral group. Then $\overline{Q}$ contains a characteristic cyclic subgroup of index 2, $\overline{Q}_o$ say. Write $A = \mathrm{Aut}(\overline{Q})$. We have $C_A(\overline{Q}_o) \lhd A$ and $A/C_A(\overline{Q}_o)$ is isomorphic to a subgroup of $\mathrm{Aut}(\overline{Q}_o)$, a 2-group. Now $C_A(\overline{Q}_o)$ is a group of automorphisms of the 2-group $\overline{Q}$ and $C_A(\overline{Q}_o)$ stabilises the normal series $1 \leqslant \overline{Q}_o \leqslant \overline{Q}$. Hence $C_A(\overline{Q}_o)$ is a 2-group and we deduce that A is a 2-group. As shown above, $O_p(H)$ is cyclic for all odd primes p. Also $F(\overline{H}) = F(H)/N$ and therefore, writing $\overline{Y} = O_{2'}(F(\overline{H}))$, we see that $\overline{Y}$ is a cyclic group of odd order and $F(\overline{H}) = \overline{Q} \times \overline{Y}$. Let $\overline{X}$ denote $\overline{Q}_o \times \overline{Y}$. Then, since $\overline{Q}_o$ char $\overline{Q}$, we have $\overline{X}$ char $F(\overline{H})$ char $\overline{H}$, whence $\overline{X}$ char $\overline{H}$. In addition $|F(\overline{H}) : \overline{X}| = 2$ and $\overline{X}$ is cyclic. Clearly $\overline{Y} \lhd \overline{H}$ and hence $C_{\overline{H}}(\overline{Y}) \lhd \overline{H}$. Since $C_{\overline{H}}(F(\overline{H})) \leqslant F(\overline{H})$, it follows that $C_{\overline{H}}(\overline{Y})/Z(F(\overline{H}))$ is isomorphic to a subgroup of $\mathrm{Aut}(\overline{Q}) = A$, a 2-group. Therefore $C_{\overline{H}}(\overline{Y})$ is a normal, nilpotent subgroup of $\overline{H}$, so $C_{\overline{H}}(\overline{Y}) \leqslant F(\overline{H})$ and then, clearly $C_{\overline{H}}(\overline{X}) = \overline{X}$.

Now suppose that $\overline{Q} = O_2(\overline{H})$ is cyclic. As in the previous paragraph, $O_{2'}(F(\overline{H}))$ is cyclic, and therefore $F(\overline{H})$ is cyclic. In this case write $\overline{X} = F(\overline{H})$.

Thus, whether $\overline{Q}$ is cyclic or dihedral, the group $\overline{H}$ contains a characteristic cyclic subgroup, $\overline{X}$, such that $C_{\overline{H}}(\overline{X}) = \overline{X}$. Clearly $\overline{X} \lhd \overline{G}$ and hence, writing $\overline{C} = C_{\overline{G}}(\overline{X})$, we have $\overline{C} \lhd \overline{G}$. Since $\overline{C} \cap \overline{H} = C_{\overline{H}}(\overline{X}) = \overline{X}$, we see that

$$|\overline{C}/\overline{X}| = |\overline{C}\overline{H}/\overline{H}| \leqslant |\overline{G}/\overline{H}| = 2.$$

Obviously $q \nmid |\overline{X}|$ and therefore $q \nmid |\overline{C}|$. The group $\overline{G}/\overline{C}$ is isomorphic to a subgroup of $\mathrm{Aut}(\overline{X})$, an abelian group since $\overline{X}$ is cyclic. Hence $\overline{G}/\overline{C}$ is abelian and we deduce that $\overline{G}$ contains a normal Hall q'-subgroup. Therefore, since $\overline{G} = G/N$ and $|N| = 4$, the group G contains a normal Hall q'-subgroup, M say.

If $v \in V^{\#}$, then $|G_v| = 2q^{m(v)}$. Hence $|M_v| = |G_v \cap M| = 2$ and it follows that M acts half-transitively on $V^{\#}$ with each stabiliser of order 2. Now $C_2 \times C_2 \cong N \triangleleft M$, and therefore M is imprimitive. Hence by Theorem 1.16, we have $M \cong \mathcal{T}_o(q^n)$, or $2n = 4$, $q = 3$ and $M \cong Q_8 \curlyvee D_8$, or $2n = 6$, $q = 2$ and M is isomorphic to the dihedral group of order 18. But we have shown $q \neq 2$, and if $n = 2$, then $q^m | n$ implies $q^m = 1$ giving $|H/K_1| = q^n - 1$ which we have assumed not to be the case. Hence $M \cong \mathcal{T}_o(q^n)$.

Write $\gamma = q^n - 1$. From the structure of $\mathcal{T}_o(q^n)$ we see that there exist elements c_o, d_o, e_o, of M such that

$$M = \langle c_o, d_o, e_o : c_o^{\gamma} = d_o^2 = e_o^2 = [c_o, d_o] = 1,\ e_o c_o e_o = c_o^{-1},\ e_o d_o e_o = c_o^{\gamma/2} d_o \rangle.$$

Clearly $H \cap M = R = \langle c_o, d_o \rangle \cong C_\gamma \times C_2$. Also $N = \langle c_o^{\gamma/2}, d_o \rangle$ and, relabelling if necessary, $K_1 = \langle d_o \rangle$, $K_2 = \langle c_o^{\gamma/2} d_o \rangle$. Hence, writing $C = \langle c_o \rangle$, we have $R = C \times K_1 = C \times K_2$. Let B be a Sylow q-subgroup of G. Then $B \leqslant H$ and $|B| = q^m$. Also $H = RB$. Obviously there exists $v_1 \in V_1^{\#}$ such that $B \leqslant G_{v_1}$ and then $B \cong BK_1/K_1 = G_{v_1}/K_1$, a cyclic group as proved earlier. Hence B is cyclic.

Let T denote $O_{2'}(R) = O_{2'}(C)$. Clearly $T \triangleleft G$. In addition let L denote the unique Sylow 2-subgroup of C. We have $LK_i/K_i = O_2(H/K_i) \triangleleft H/K_i$ for $i = 1,2$ and, since LK_i/K_i is a cyclic 2-group, the group $\mathrm{Aut}(LK_i/K_i)$ is a 2-group. We deduce that, since $q^m = |B| = |BK_i/K_i|$, the group BK_i/K_i centralises LK_i/K_i for $i = 1,2$. Hence $[B,L] \leqslant K_1 \cap K_2 = 1$, whence B centralises L. Since $T \triangleleft G$, and $T \times L = C$, we have $B \leqslant N_G(C)$, and hence $|CB| = (q^n - 1)q^m$ and $H = CB \times K_1 = CB \times K_2$. Therefore $CB \cong H/K_1 \leqslant \mathcal{T}(q^n)$,

and hence $CB \cong \mathcal{T}_k(q^n)$.

From the description of $\mathcal{T}_o(q^n;\ q^m)$ in terms of generators and relations, given at the start of this chapter, there exist elements $c,\ d,\ e,\ f$, of $\mathcal{T}_o(q^n;\ q^m)$ such that $\mathcal{T}_o(q^n;\ q^m) = \langle c,\ d,\ e,\ f\rangle$,

$|c| = \gamma$, $|d| = |e| = 2$, $|f| = k$ $[c,d] = [d,f] = [e,f] = 1$, $ece = c^{-1}$, $ede = c^{\gamma/2}d$,

and $\langle c,f\rangle \cong \mathcal{T}_k(q^n)$. Hence $\langle c,f\rangle \cong CB$ via an isomorphism, ϕ say, which maps the group $\langle c\rangle$ to the group C. Write $c^\phi = c_1 \in C$, and $f^\phi = f_1 \in CB$. Also, let B_1 denote $\langle f_1\rangle$, a cyclic group of order q^m.

Obviously there exist $v_1 \in V_1^\#$, $v_2 \in V_2^\#$, such that both $B_1 \leqslant G_{v_1}$ and $B_1 \leqslant G_{v_2}$. By Lemma 3.7(9), $|G_{v_1+v_2} : G_{v_1} \cap G_{v_2}| = 2$, and, since for all $v \in V^\#$ $|G_v| = 2q^{m(v)}$ for some integer $m(v)$, we see that $B_1 = G_{v_1} \cap G_{v_2}$ $= H_{v_1+v_2} = G_{v_1+v_2} \cap H$. Let $e_1 \in G_{v_1+v_2}$ such that $|e_1| = 2$. Then $e_1 \notin H$. In fact $e_1 \in M \backslash R$. Clearly $G/M = B_1M/M \cong B_1$, a cyclic group, and $C_2 \cong M/R \lhd G/R$. Hence G/R is abelian. Now $G_{v_1+v_2} \cong G_{v_1+v_2}R/R = G/R$, whence $G_{v_1+v_2}$ is abelian and, in particular e_1 centralises $B_1 = \langle f_1\rangle$. Thus, relabelling $d_o = d_1$, we see that G contains elements $c_1,\ d_1,\ e_1,\ f_1$ such that the map ρ given by $c^\rho = c_1$, $d^\rho = d_1$, $e^\rho = e_1$, $f^\rho = f_1$, extends to an isomorphism from $\mathcal{T}_o(q^n;\ q^m)$ to G. This concludes Case 1.

CASE 2. One of the cases (a_1), (a_2), (b_1), (b_2), (c_2), (d_2), (f_2), (f_3), (f_4) of Theorem 1.16 holds for the group H/K_1 and the module V_1.

We first eliminate all possibilities except (a_1) and (a_2). Suppose that H/K_1 is one of the groups described in (b_1), (b_2), (c_2), (d_2), (f_2), (f_3), (f_4). Then we see that $q \nmid |H/K_1|$. Therefore, since $|K_1| = |G : H| = 2$, we have $q \nmid |G|$, whence G acts half-transitively on $V^\#$. Clearly G is imprimitive and does not act semi-regularly on $V^\#$, and hence, by Theorem 1.16, we have three possibilities for G. Either $G \cong \mathcal{T}_o(q^n)$, or $n = 2$, $q = 3$ and $G \cong Q_8 \curlyvee D_8$, or $n = 3$, $q = 2$ and G is isomorphic to the dihedral group of order 18. However, we have shown $q \neq 2$, and if $G \cong Q_8 \curlyvee D_8$, then $|G| = 32$,

giving $|H/K_1| = 8$ which does not occur in the possibilities for H/K_1 we are considering. Hence $G \cong \mathcal{T}_0(q^n)$, and therefore, from the structure of $\mathcal{T}_0(q^n)$, G contains a normal abelian subgroup of index 2. It follows that H/K_1 contains a normal abelian subgroup of index at most 2, and, as is easily checked, this does not occur in cases (b_1), (b_2), (c_2), (d_2), (f_2), (f_3), (f_4), a contradiction.

Hence we have $q = 3$, $n = 2$, and either $H/K_1 \cong SL(2,3)$, (case (a_1)), or $H/K_1 \cong GL(2,3)$, (case(a_2)). Write $H_2 = O_2(H)$. Then $K_i \leqslant H_2$ for $i = 1,2$, and $H_2/K_1 = O_2(H/K_1) \cong Q_8$. Let $g \in G \backslash H$. We have $K_1^g = K_2$, and hence conjugation by g induces an isomorphism from H/K_1 to H/K_2. Thus $H_2/K_2 \cong H_2/K_1 \cong Q_8$. It is easily seen that this implies $H_2 = P \times K_1 = P \times K_2$ for some subgroup, P, of H_2 such that $P \cong Q_8$. Let x,y be two elements of order 4 in P such that $\langle x,y\rangle = P$, and let $C_2 \cong K_1 = \langle z\rangle$. Then, as is easily checked, there are exactly four subgroups of H_2 isomorphic to Q_8, namely $\langle x,y\rangle$, $\langle x,yz\rangle$, $\langle xz, y\rangle$, $\langle xz,yz\rangle$.

Let C be a Sylow 3-subgroup of G. Then $|C| = 3$ and $C \leqslant H$. Also, since there are exactly four subgroups of H_2 isomorphic to Q_8, the group C must normalise one such subgroup, Q say. Clearly $QC \cong SL(2,3)$. Let B denote QC, and then, if $H/K_1 \cong SL(2,3)$, we have $H = B \times K_1 = B \times K_2$ where $B \cong SL(2,3)$, and $Q \lhd H$.

Suppose that $H/K_1 \cong GL(2,3)$. Then there exists $M \lhd H$ such that $M/K_1 \cong SL(2,3)$. Since $M/H_2 = F(H/H_2)$ char $H/H_2 \lhd G/H_2$, we see that $M \lhd G$, and clearly $M = B \times K_1 = B \times K_2$. Let $g \in G$. The group C normalises Q and permutes the other three subgroups of H_2 isomorphic to Q_8 transitively. Write $C = \langle c\rangle$. We have $c \in M \lhd G$, and therefore $gcg^{-1} \in M$. Also $Q \lhd M$, and it follows that $Q^{gcg^{-1}} = Q$, whence

$$Q^{gc} = Q^g. \tag{10}$$

Now $Q^g \cong Q_8$ and since $H_2 = O_2(H) \lhd G$, we have $Q^g \leqslant H_2$. But (10) above

implies that $C = \langle c \rangle$ normalises Q^g, and so $Q^g = Q$. Therefore $Q \lhd G$.

We remark that, replacing M by H, the proof given above that $Q \lhd G$ in the case $H/K_1 \cong GL(2,3)$ shows that $Q \lhd G$ in the case $H/K_1 \cong SL(2,3)$. Hence, in either case, $Q \lhd G$.

Assume that $H/K_1 \cong SL(2,3)$. Then $H = B \times K_1 = B \times K_2$, where $B = QC \cong SL(2,3)$. Write $D = C_G(Q)$. Then $D \lhd G$ and G/D is isomorphic to a subgroup of $Aut(Q) \cong S_4$. We have $|G| = 4.|SL(2,3)| = 96$ and, clearly, $|D \cap H| = 4$. Therefore $|H/H \cap D| = 12$ and $|G/D| = 12$ or 24. Suppose, first, that $|G/D| = 12$. Then $|D| = 8$. Also, since $N \leqslant Z(H)$, we have $C_2 \times C_2 \cong N \leqslant D$, and $D \not\leqslant H$ since $|D \cap H| = 4$. If D is abelian, then $G = \langle H,D \rangle \leqslant C_G(N)$, whence $N \leqslant Z(G)$; clearly an impossibility. Hence D is non-abelian, and we conclude that D is isomorphic to the dihedral group of order 8. Now $G/C_G(D)$ is isomorphic to a subgroup of $Aut(D)$, a 2-group. Hence $C \leqslant C_G(D)$, and therefore $QC = B$ centralises D. Clearly $\langle B,D \rangle = G$, and so, since $B \cap D = Q \cap D = Z(Q) = Z(B)$, we have $G = BD \cong SL(2,3) \curlyvee D_8$, which is case (ii) in the statement of the theorem.

Next suppose that $|G/D| = 24$. Then $|D| = 4$ and $D = N \cong C_2 \times C_2$. Let $v_1 \in V_1^*$, $v_2 \in V_2^*$. From the action of $H/K_i \cong SL(2,3)$ on V_i, we have $|G_{v_i}/K_i| = 3$ for $i = 1,2$. Therefore G_{v_i} is a cyclic group of order 6, and K_i is the unique Sylow 2-subgroup of G_{v_i} for $i = 1,2$. Since $K_1 \cap K_2 = 1$, we have $2 \nmid |G_{v_1} \cap G_{v_2}|$. By Lemma 3.6(9) we see that $|G_{v_1+v_2} : G_{v_1} \cap G_{v_2}| = 2$. Let Y be a Sylow 2-subgroup of $G_{v_1+v_2}$. Then $|Y| = 2$ and, clearly, $Y \cap (G_{v_1} \cap G_{v_2}) = 1$. Since $G_{v_1} \cap G_{v_2} = H_{v_1} \cap H_{v_2} = H_{v_1+v_2} = G_{v_1+v_2} \cap H$, we have $Y \cap H = 1$. Therefore $G = HY$.

By assumption $|G/D| = 24$, and since $C_G(Q) = D = N$, we have $G/N \cong S_4$, the full automorphism group of $Q \cong Q_8$. Clearly, then, Y acts non-trivially by conjugation on $H_2/N = O_2(H)/Z(H)$. Also Y acts non-trivially on $N = Z(H)$. Thus, since $G = HY$ and $H = B \times K_1 = B \times K_2 \cong SL(2,3) \times C_2$, we see easily that G is isomorphic to the group, Δ, defined in Definition 3.8.

This is case (iii) in the statement of the theorem.

We now drop our assumption that $H/K_1 \cong SL(2,3)$ and assume, instead, that $H/K_1 \cong GL(2,3)$. As shown above, we have $Q_8 \cong Q \lhd G$. Also, if B denotes QC, then $B \times K_1 = B \times K_2 = M \lhd G$. Clearly $|G| = 192$. Again let D denote $C_G(Q)$, and again we have $D \lhd G$ with G/D isomorphic to a subgroup of $Aut(Q) \cong S_4$. Also $D \cap H = N$, and hence

$$24 = |H/N| = |H/H \cap D| = |HD/D| \leqslant |G/D|.$$

Therefore $|G/D| = 24$, whence $|D| = 8$, and we see that $D \not\leqslant H$. If D is abelian, then $G = \langle H,D\rangle \leqslant C_G(N)$, giving $N \leqslant Z(G)$ which is clearly impossible. Hence D is non-abelian, and we deduce that D is isomorphic to the dihedral group of order 8. From the action of $H/K_i \cong GL(2,3)$ on V_i, we have $G_{v_i}/K_i \cong S_3$ for all $v_i \in V_i^*$, for $i = 1,2$. Hence, by 3'-halftransitivity, $|G_v|_{3'} = 4$ for all $v \in V^*$. Let R denote $C_G(D)$. Then $R \lhd G$ and G/R is isomorphic to a subgroup of Aut(D), a 2-group.

Let $d \in D \setminus N$ such that $|d| = 2$, and let $v \in V^*$ such that $d \in G_v$. Since $D \cap H = N$, we have $d \notin H$ and $D = \langle N, d\rangle$. Write $v = v_1 + v_2$ where $v_i \in V_i$ for $i = 1,2$. Since $d \notin H$, it follows that $V_1 d = V_2$, $V_2 d = V_1$ and then, from the fact that $d \in G_{v_1+v_2}$, we have $v_1 d = v_2$, $v_2 d = v_1$, and $v_i \in V_i^*$ for $i = 1,2$. Let T be a Sylow 2-subgroup of G_v such that $d \in T$. We have $|T| = 4$, and then, since $|G : H| = 2$, we see that $T \cap H > 1$. Let $T_1 = T \cap H \cong C_2$. We have $T_1 = T \cap H \leqslant G_{v_1+v_2} \cap H = G_{v_1} \cap G_{v_2}$. By Lemma 3.6(8), we see that $K_1 \cap G_{v_2} = K_2 \cap G_{v_1} = 1$, and hence $T_1 \cap N = 1$. Now $B = QC \cong SL(2,3)$, and $M = B \times K_1 = B \times K_2$. Therefore all involutions in M are contained in $N = K_1 \times K_2$, and we deduce that $T_1 \cap M = 1$.

Since G/R is a 2-group, we have $C \leqslant R$. Clearly $T_1 \leqslant C_G(d)$ and so, since $N = Z(H)$ and $T_1 \leqslant H$, we see that $T_1 \leqslant C_G(\langle N,d\rangle) = C_G(D) = R$. Obviously $Q \leqslant R$, and hence $\langle B, T_1\rangle \leqslant R$, giving $|R| \geqslant 48$. Also

$|G/R| \geq |RD/R| = |D/D \cap R| = 4$, and we obtain $|R| = 48$. Thus $R = \langle B, T_1 \rangle \leq H$ and then, since $K_1 \not\leq R$, we have $H = R \times K_1$. Hence $R \cong H/K_1 \cong GL(2,3)$ and, since $R \cap D = Z(R) = Z(D)$, we see easily that $G = RD \cong GL(2,3) \curlyvee D_8$. This is case (iv) in the statement of the theorem.

Q.E.D.

EXAMPLES. We demonstrate that cases (ii), (iii), and (iv) of Theorem 3.9 do occur. That is, we show that if G satisfies (ii), (iii), or (iv) of that theorem, then there exists an irreducible GF(3)G-module, V, faithful for G, such that the dimension of V over GF(3) is 4 and G acts 3'-half-transitively on $V^{\#}$.

Assume that G satisfies (ii), (iii), or (iv) in the statement of Theorem 3.9. Then we see easily that there exists a subgroup, H, of G such that $|G : H| = 2$, and in cases (ii) and (iii) $H \cong SL(2,3) \times C_2$, while in case (iv) $H \cong GL(2,3) \times C_2$. In addition, there exist subgroups K_1, K_2, of H such that $K_1 \neq K_2$, and $C_2 \cong K_i \lhd H$ for $i = 1,2$, and $K_1^g = K_2$ for all $g \in G \backslash H$. Moreover, $H/K_1 \cong H/K_2 \cong SL(2,3)$ in cases (ii) and (iii), and $H/K_1 \cong H/K_2 \cong GL(2,3)$ in case (iv).

Clearly, in all three cases, we may choose V_1, an irreducible $GF(3)H/K_1$-module, faithful for H/K_1, such that V_1 has dimension 2 over GF(3). Let V denote the induced module, V_1^G. Then it is easy to see that V is an irreducible GF(3)G-module, faithful for G, and V has dimension 4 over GF(3). In addition, it is obvious that

$$V_H = V_1 \oplus V_2$$

where V_2 is an irreducible $GF(3)H/K_2$-module, faithful for H/K_2.

Let $v_1 \in V_1^{\#}$, $v_2 \in V_2^{\#}$. In cases (ii) and (iii), the group H_{v_i}/K_i is a cyclic group of order 3, whence H_{v_i} is a cyclic group of order 6, while in case (iv) we have H_{v_i}/K_i is isomorphic to the symmetric group of

degree 3. ($i = 1,2$). Clearly, then, in all three cases H_{v_i} contains a unique Sylow 3-subgroup of G for $i = 1,2$. Let C_1 and C_2 be two Sylow 3-subgroups of G such that $C_1 \neq C_2$, and let $v_i \in V_i^*$ such that $C_i \leq H_{v_i}$ for $i = 1,2$. It follows that $3 \nmid |H_{v_1} \cap H_{v_2}|$.

Now $K_1 \cong K_1K_2/K_2 \triangleleft H/K_2$, and hence the non-trivial element of K_1 acts like multiplication by -1 on V_2. Thus $K_1 \cap H_w = 1$ for all $w \in V_2^*$, and, in particular $K_1 \cap H_{v_2} = 1$. Therefore, in cases (ii) and (iii) we have $H_{v_1} \cap H_{v_2} = 1$, and in case (iv) we have $|H_{v_1} \cap H_{v_2}| \leq 2$.

If $g \in G \setminus H$ then, clearly $V_1 g = V_2$ and $V_2 g = V_1$. Hence $H_{v_i} = G_{v_i}$ for $i = 1,2$. Using the familiar argument we have $|G_{v_1+v_2} : G_{v_1} \cap G_{v_2}| \leq 2$ and we deduce that $|G_{v_1+v_2}| \leq 2$ in cases (ii) and (iii), and $|G_{v_1+v_2}| \leq 4$ in case (iv). It follows that the size of the G-orbit containing v_1+v_2 is at least 96/2 in cases (ii) and (iii), and at least 192/4 in case (iv). Hence, in all three cases, the size of the G-orbit containing v_1+v_2 is divisible by 48. But $|V^*| = 3^4 - 1 = 80$, and so the size of the G-orbit containing v_1+v_2 is exactly 48.

We have $|G_{v_1}| = 6$ (cases (ii) and (iii)) or $|G_{v_1}| = 12$ (case (iv)) and hence, in all cases, the size of the G-orbit containing v_1 is 96/6 = 192/12 = 16, and this orbit is exactly $V_1^* \cup V_2^*$. Now $48 + 16 < 80$ and therefore there exists $u \in V^*$ such that $u \notin V_1^* \cup V_2^*$ and u is not in the G-orbit containing v_1+v_2. We have $u = u_1 + u_2$ for some $u_1 \in V_1^*$, $u_2 \in V_2^*$. Since $K_1 \cap G_{u_2} = 1$, it follows that $|G_{u_1} \cap G_{u_2}| \leq 3$ in cases (ii) and (iii), while in case (iv) we have $|G_{u_1} \cap G_{u_2}| \leq 6$. Therefore, from $|G_{u_1+u_2} : G_{u_1} \cap G_{u_2}| \leq 2$, we deduce that $|G_{u_1+u_2}| \leq 6$ in cases (ii) and (iii), and $|G_{u_1+u_2}| \leq 12$ in case (iv). It follows that, in all three cases, the size of the G-orbit containing $u_1 + u_2 = u$ is at least 96/6 = 192/12 = 16. However, 80 - (48 + 16) = 16 and hence the size of the G-orbit containing u is exactly 16.

Therefore there are exactly three G-orbits in V^*, two of size 16 and

one of size 48. Hence G acts 3'-halftransitively on V^* and we conclude that cases (ii), (iii), and (iv) of Theorem 3.9 do occur.

We close this chapter with a number of results concerning the group GL(2,3) and its representations over the field GF(3), results that we shall require in Chapter 4. It is easily checked that the matrices

$$a = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$$

generate GL(2,3). In terms of generators and relations we have

$$GL(2,3) = \langle a,b,c,d\colon a^4 = b^4 = c^3 = d^2 = 1,\ [a,b] = a^2 = b^2,\ c^{-1}ac = ab,\ c^{-1}bc = a,\ dad = b,\ dbd = a,\ dcd = ac^2 \rangle .$$

Also $|GL(2,3)| = 48$. Moreover $\langle a,b,c\rangle = SL(2,3)$, and $O_2(SL(2,3)) = O_2(GL(2,3)) = F(GL(2,3)) = \langle a,b\rangle \cong Q_8$. Clearly $Z(GL(2,3)) = Z(SL(2,3)) = \langle a^2\rangle$.

NOTATION. For any group G let i(G) denote the set of non-central involutions of G.

LEMMA 3.10. <u>There are exactly eight conjugacy classes of the group</u> GL(2,3), <u>of which, besides the identity class, two consist of elements of order</u> 2, <u>one consists of elements of order</u> 4, <u>two consist of elements of order</u> 8, <u>one consists of elements of order</u> 3 <u>and one consists of elements of order</u> 6. <u>In addition</u> $|i(GL(2,3)| = 12$.

<u>Proof</u>. Write G = GL(2,3). Throughout this proof we shall use the same notation as in the description of GL(2,3) in terms of generators and relations given above. Two classes of G are obvious, namely $K_1 = \{1\}$ and $K_2 = \{a^2\}$. Let K_3 denote the conjugacy class of G containing b. Clearly $\{a,a^3,b,b^3,ab,ab^3\} \subseteq K_3$. It is easily checked that $(cd)^2 = b$, and hence $C_G(b) \gg \langle cd\rangle \cong C_8$. Therefore $|K_3| = |G : C_G(b)| \leq 48/8 = 6$ and it follows that $K_3 = \{a,a^3,b,b^3,ab,ab^3\}$ and $C_G(b) = \langle cd\rangle$.

The group $\langle c\rangle$ is a Sylow 3-subgroup of G and abd is an element of order 2 such that $(abd)c(abd) = c^2$. We see easily that $N_G(\langle c\rangle) = \langle c, abd, a^2\rangle \cong S_3 \times C_2$, and hence G contains exactly 48/12 = 4 Sylow 3-subgroups, each of order 3. Clearly $C_G(c) = \langle c,a^2\rangle \cong C_6$, and we deduce that the set of all elements of G of order 3 forms a conjugacy class, K_4 say, of size 8. Now ca^2 is an element of G of order 6 and $a^2 \in Z(G)$. Obviously $C_G(ca^2) = C_G(c)$, and therefore, if K_5 denotes the conjugacy class containing ca^2, we have $|K_5| = |K_4| = 8$.

Let K_6 denote the conjugacy class of G containing d. If $3 \mid |C_G(d)|$, then d centralises some element of G of order 3, e say, giving $|C_G(e)| \geq |\langle a^2,e,d\rangle| = 12$ which is impossible since, as shown above, the set of elements of G of order 3 forms a conjugacy class K_4 of size 8. Hence $3 \nmid |C_G(d)|$. We have $C_G(d) \cap \langle a,b\rangle = \langle a^2\rangle$ and then, clearly, $C_G(d) = \langle a^2,d\rangle \cong C_2 \times C_2$. Therefore $|K_6| = |G : C_G(d)| = 48/4 = 12$.

Let K_7 denote the conjugacy class containing cd. Now $(cd)^2 = b$, and hence $C_G(cd) \leq C_G(b)$. But, as shown above, $C_G(b) = \langle cd\rangle$ and so, obviously, $C_G(cd) = \langle cd\rangle$. Therefore $|K_7| = |G : C_G(cd)| = 48/8 = 6$. Clearly $(cd)^5$ is an element of G of order 8. Suppose $(cd)^5 \in K_7$. Then there exists $g \in G$ such that $(cd)^g = (cd)^5$, and hence

$$b^g = ((cd)^2)^g = ((cd)^g)^2 = ((cd)^5)^2 = (cd)^2 = b.$$

It follows that $g \in C_G(b) = \langle cd\rangle$ which is clearly impossible. Therefore $(cd)^5 \notin K_7$. Obviously $C_G((cd)^5) = C_G(cd) = \langle cd\rangle$ and so, writing K_8 for the conjugacy class of G containing $(cd)^5$, we have $|K_8| = |K_7| = 6$.

That $K_1, \ldots, K_8$ are all the conjugacy classes of G follows easily from

$$\sum_{i=1}^{8} |K_i| = 1 + 1 + 6 + 8 + 8 + 12 + 6 + 6 = 48 = |G|,$$

and since K_6 is the unique conjugacy class of non-central involutions of G we must have $|i(G)| = |K_6| = 12$.

Q.E.D.

In order to prove Theorem 3.13 below on the representations of GL(2,3) over the field GF(3) we shall require the following two results from the theory of modular representations of finite groups. The first, Theorem 3.11, is the well-known result on the number of inequivalent irreducible modular representations of a group over a splitting field and is proved in [14], Theorem 1.5. The second result, Theorem 3.12, is a characterisation of the splitting fields for a group and is proved in [1], Theorem 70.3.

If g is an element of a group G, then, for any prime p, g is said to be a p'-element of G if $|g|$ is prime to p.

THEOREM 3.11 ([14] Theorem 1.5). Let G be a group and K a splitting field for G such that the characteristic of K is $p > 0$. Then the number of inequivalent irreducible representations of G over K is exactly the number of conjugacy classes of G consisting of p'-elements.

Following [1] Definition 70.2, we say a representation θ of a group G over a field L is realisable in a subfield, K, of L if there exists a representation θ' of G over K such that θ and θ' are equivalent representations of G over L.

THEOREM 3.12 ([1] Theorem 70.3). Let L denote an algebraically closed field. A subfield K of L is a splitting field for a group G if and only if each irreducible representation of G over L is realisable in K.

THEOREM 3.13. *There exist exactly two non-equivalent faithful, irreducible representations of* $GL(2,3)$ *over the field* $GF(3)$, *say* θ_1 *and* θ_2. *Let* W_1 *and* W_2 *be modules for* $GL(2,3)$ *affording* θ_1 *and* θ_2 *respectively and, for* $i = 1,2$, *let* X_i *denote the set* $\{H : H \leq GL(2,3)$ *and* H *is the stabiliser in* $GL(2,3)$ *of some* $w \in W_i\}$. *Then we have*

(i) $\dim_{GF(3)} W_1 = \dim_{GF(3)} W_2 = 2$;

(ii) $GL(2,3)$ *acts transitively on* W_i^* *for* $i = 1,2$;

(iii) *if* $H \in X_i$ *then* $H \cong S_3$ *and* $|X_i| = 4$ *for* $i = 1,2$;

(iv) $X_1 \cap X_2 = \emptyset$;

(v) *if* R *is a Sylow* 3-*subgroup of* $GL(2,3)$ *and* $g \in i(GL(2,3))$ *such that* $\langle R,g\rangle \in X_i$ *then, letting* z *denote the non-trivial element of* $Z(GL(2,3))$, *we have* $S_3 \cong \langle R, gz\rangle \notin X_i$ *for* $i = 1,2$.

Proof. Write $G = GL(2,3)$. Let K denote $GF(3)$ and let L denote an algebraically closed field such that K is a subfield of L. Again we use the same notation as the description of $GL(2,3)$ in terms of generators and relations given above.

For $i = 1,2$ define θ_i as follows.

$$\theta_1(a) = \theta_2(a) = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \ \theta_1(b) = \theta_2(b) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \theta_1(c) = \theta_2(c) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\theta_1(d) = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, \ \theta_2(d) = \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}.$$

It is easily checked that θ_1 and θ_2 extend to the whole of G to give two non-equivalent faithful irreducible representations of G over K.

Now $G/Z(G) \cong S_4$ and it is easily seen that S_4 has two non-equivalent faithful irreducible representations over the field K. Let θ_3 and θ_4 be two such representations for $G/Z(G)$. Clearly we may regard θ_3 and θ_4 as non-equivalent irreducible representations of G over K with $\ker(\theta_3) = \ker(\theta_4) = Z(G)$.

We have $\langle a,b,c\rangle = SL(2,3) \triangleleft GL(2,3)$ and hence, writing $S = \langle a,b,c\rangle$, the group G/S has order 2. Therefore G/S has two non-equivalent irreducible representations over K and it follows that G has two non-equivalent irreducible representations, θ_5, θ_6, over K such that $\ker(\theta_5) = \ker(\theta_6) = S$.

Since K is a subfield of L we see that $\theta_1,\ldots,\theta_6$ are representations of G over L and it is easy to check that $\theta_1,\ldots,\theta_6$ are irreducible and non-equivalent over L. But L is algebraically closed and hence is a splitting field for G. By Lemma 3.10 the group G contains exactly six conjugacy classes of 3'-elements and so, by Theorem 3.11, there exist exactly six non-equivalent irreducible representations of G over L. Hence $\{\theta_1,\ldots,\theta_6\}$ is a complete set of non-equivalent irreducible representations of G over L. Clearly θ_i is realisable in K for $1 \leq i \leq 6$, and therefore, by Theorem 3.12, K is a splitting field for G. We deduce that $\{\theta_1,\ldots,\theta_6\}$ is a complete set of non-equivalent irreducible representations of G over K. In particular, we see that, up to equivalence, G has precisely two faithful, irreducible representations over K, namely θ_1 and θ_2. We remark that the degree of θ_i is 2 for $i = 1,2$.

Let W_1, W_2, X_1, X_2, be defined as in the statement of the theorem. Then (i) is clear since, for $i = 1,2$, $\dim_K W_i$ is precisely the degree of θ_i. Let Q denote the group $\langle a,b\rangle$ and write $a^2 = z$. Then $Q \cong Q_8$ and $Z(G) = Z(Q) = \langle a^2\rangle = \langle z\rangle$. Clearly z acts like scalar multiplication by -1 on W_1 and W_2. Let $i \in \{1,2\}$. Since z is the unique involution in Q, if $w \in W_i^{\#}$ then $G_w \cap Q = 1$. Hence Q acts semi-regularly on $W_i^{\#}$. But $|Q| = 8 = 3^2 - 1 = |W_i^{\#}|$, whence Q acts transitively on $W_i^{\#}$. Thus G acts transitively on $W_i^{\#}$. If $w \in W_i^{\#}$ then $|G_w| = 48/8 = 6$ and, since $G_w \cap Q = 1$, we have $G_w \cong G_wQ/Q = G/Q \cong S_3$. Hence, if $H \in X_i$, then $H \cong S_3$.

Let $H \in X_i$. Since $C_{W_i}(H)$ is a non-trivial, proper subspace of W_i, a 2-dimensional vector space over K, we must have $\dim_K C_{W_i}(H) = 1$. Clearly

$$W_i^{\#} = \bigcup_{H \in X_i} (C_{W_i}(H))^{\#}$$

and it is easily seen that this union is disjoint. Hence

$$8 = |W_i^{\#}| = |X_i|.2$$

and we deduce that $|X_i| = 4$. This completes the proof of (ii) and (iii).

Again let $i \in \{1,2\}$, and let $H_1 \in X_i$. Then there exists $w \in W_i^{\#}$ such that $H_1 = G_w$. If $g \in G$ then $wg \in W_i^{\#}$ and $G_{wg} = (G_w)^g = H_1^g$, whence $H_1^g \in X_i$. On the other hand, if $H_2 \in X_i$ then there exists $u \in W_i^{\#}$ such that $H_2 = G_u$. But G acts transitively on $W_i^{\#}$ and so there exists $g \in G$ such that $wg = u$, giving $H_2 = G_u = G_{wg} = (G_w)^g = H_1^g$. Thus $H_2 \in X_i$ if and only if H_2 is conjugate to H_1 in G, and we deduce that X_i is a complete conjugacy class of subgroups of G for $i = 1,2$. Therefore, to show $X_1 \cap X_2 = \emptyset$, we need only show that there exists $H \in X_1$ such that $H \notin X_2$.

Let $H = \langle c, abd \rangle$. It is easily checked that $H \cong S_3$ and we have

$$\theta_1(c) = \theta_2(c) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \theta_1(abd) = \theta_1(a)\theta_2(b)\theta_1(d) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\theta_2(abd) = \theta_2(a)\theta_2(b)\theta_2(d) = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}.$$

The above matrices show clearly that $C_{W_1}(H) = C_{W_2}(c) \cap C_{W_2}(abd) > \langle 0 \rangle$ and $C_{W_2}(H) = C_{W_2}(c) \cap C_{W_2}(abd) = \langle 0 \rangle$. Thus $H \in X_1$ but $H \notin X_2$ and we have proved (iv).

Assume that $i \in \{1,2\}$. Let R be a Sylow 3-subgroup of G and $g \in i(G)$ such that $\langle R, g \rangle \in X_i$. Writing $\langle R, g \rangle = T_1$, we must have $\langle 0 \rangle \neq C_{W_i}(T_1) = C_{W_i}(R) = C_{W_i}(g)$. Write $T_2 = \langle R, gz \rangle$ and suppose $T_2 \in X_i$. Then $\langle 0 \rangle \neq C_{W_i}(T_2) = C_{W_i}(gz) = C_{W_i}(R) = C_{W_i}(g)$. Hence there exists $w \in W_i^{\#}$ such that $G_w \geq \langle g, gz \rangle$. But then $z \in G_w$, contradicting the fact that z acts <u>like</u> scalar multiplication by -1 on W_i. Therefore $T_2 \notin X_i$ and we have proved (v).

Q.E.D.

The final two results in this chapter give us another characterisation of the group GL(2,3).

LEMMA 3.14. Let $S = SL(2,3)$, and let Q denote $O_2(S)$. Then if x,y, are elements of S such that $\langle x,y\rangle = Q$, there exists $e \in S$ such that $|e| = 3$ and $e^{-1}xe = xy$, $e^{-1}ye = x$.

Proof. Since $S = SL(2,3)$ there exist elements a,b,c of S such that

$$S = \langle a,b,c\colon a^4 = b^4 = c^3 = 1,\ [a,b] = a^2 = b^2,\ c^{-1}ac = ab,\ c^{-1}bc = a\rangle.$$

We have $\langle a,b\rangle = O_2(S) = Q \cong Q_8$. Let X denote the set of ordered pairs $\{s,t\}$ of elements of S such that $\langle s,t\rangle = Q$. Two elements $\{s,t\}$, $\{s',t'\}$, of X are equal if and only if $s = s'$ and $t = t'$. We claim $|X| = 24$. For if $\{s,t\} \in X$ then clearly $|s| = |t| = 4$ and there are exactly six elements of Q of order 4. Hence for any element $\{s,t\}$ of X there are six choices for s. Once s is chosen, $\langle s,t\rangle = Q$ if and only if $t \in Q\backslash\langle s\rangle$, and so there are four choices for t. Therefore there are exactly $6.4 = 24$ possibilities for $\{s,t\}$.

Now $S = SL(2,3) \leqslant GL(2,3)$ and, clearly, for all $g \in GL(2,3)$ the map $\{s,t\} \longmapsto \{s^g, t^g\}$ is a permutation of the set X. Write $GL(2,3) = G$. Let $\{s,t\} \in X$ and suppose $g \in G$ such that g fixes $\{s,t\}$. Then $s = s^g$ and $t = t^g$. But $\langle s,t\rangle = Q$, and hence $g \in C_G(Q) = Z(G)$. Therefore G permutes the elements of X in an orbit of size $|G : Z(G)| = 24 = |X|$, whence G acts transitively on X.

Let x,y be elements of S such that $\langle x,y\rangle = Q$. Then $\{x,y\} \in X$ and so, since $\{a,b\} \in X$ and G acts transitively on X, there exists $g \in G$ such that $x^g = a$, $y^g = b$. Write $e = c^{g^{-1}}$. We have $e \in S$ and $|e| = |c| = 3$. Also

$$x^e = (gag^{-1})^e = (gc^{-1}g^{-1})(gag^{-1})(gcg^{-1}) = g(c^{-1}ac)g^{-1} = (ab)^{g^{-1}} = a^{g^{-1}}b^{g^{-1}} = xy$$

and

$$y^e = (gbg^{-1})^e = (gc^{-1}g^{-1})(gbg^{-1})(gcg^{-1}) = g(c^{-1}bc)g^{-1} = a^{g^{-1}} = x.$$

Q.E.D.

LEMMA 3.15. Let H be a group of order 48 and assume there exists a subgroup, T, of H such that $T \cong SL(2,3)$, and an element h of i(H) such that h acts non-trivially by conjugation on $O_2(T)/Z(T)$. Then $H \cong GL(2,3)$.

Proof. Write $P = O_2(T)$. Then $P \cong Q_8$ and, since h acts non-trivially on $P/Z(P)$, we see easily that there exist elements x,y of P such that $\langle x,y\rangle = P$ and $x^h = y$, $y^h = x$. Now $T \cong SL(2,3)$ and hence, by Lemma 3.14, there exists $e \in T$ such that $|e| = 3$ and $x^e = xy$, $y^e = x$.

We have $heh \in T$. Also

$$x^{heh} = y^{eh} = x^h = y, \text{ and } y^{heh} = x^{eh} = (xy)^h = x^3y.$$

But $x^{xe^2} = y$ and $y^{xe^2} = x^3y$. Therefore $(heh)(xe^2)^{-1}$ centralises both x and y, whence $(heh)(xe^2)^{-1} \in C_T(P) = Z(P) = \langle x^2\rangle$. It follows that $heh = xe^2$ or x^3e^2. However $|heh| = |e| = |xe^2| = 3$, whereas $|x^3e^2| = 6$ and we conclude that $heh = xe^2$.

Since T contains a unique involution, namely $x^2 \in Z(H)$, we must have $h \notin T$, and hence $H = \langle T,h\rangle$. Therefore

$$H = \langle x,y,e,h\colon x^4 = y^4 = e^3 = h^2 = 1,\ [x,y] = x^2 = y^2,\ e^{-1}xe = xy,$$
$$e^{-1}ye = x,\ hxh = y,\ hyh = x,\ heh = xe^2\rangle,$$

and, comparing this with the description of GL(2,3) in terms of generators and relations given earlier, we see that $H \cong GL(2,3)$.

Q.E.D.

CHAPTER 4

SOLUBLE q' - HALFTRANSITIVE GROUPS OF LINEAR TRANSFORMATIONS OF A GF(q) - VECTOR SPACE . II

In this chapter we continue our investigation into the structure of a soluble group G such that, for some prime q, the group G acts q'-halftransitively on the non-trivial elements of V, an irreducible GF(q)G-module, faithful for G. If G contains a non-cyclic abelian normal subgroup, then Theorem 3.7 applies and we know all the possibilities for G. Therefore we now turn our attention to the case in which G contains no non-cyclic abelian normal subgroup. If G acts q'-semiregularly on V^*, then, since G contains no non-trivial normal q-subgroup, the Fitting subgroup of G acts semi-regularly on V^*. In this case the well-known results on semi-regular groups of automorphisms enable us to analyse the structure of G (see Chapter 5), and so we shall normally work under the assumption that G does not act q'-semiregularly.

Although we shall require results from all four of Passman's papers on soluble half-transitive automorphism groups, [10] (with Isaacs), [11], [12], [13], we shall find [13] particularly useful. Not only shall we make frequent references to results in [13] and, as far as possible, adopt notation consistent with that in [13], but we shall also imitate the general scheme of [13], as will be explained.

Let G be a group such that G contains no non-cyclic abelian normal subgroup, and let P be a normal p-subgroup of G for some prime p. Then, clearly, every characteristic abelian subgroup of P is cyclic. Following [13] we call such a group, P, a group of <u>symplectic type</u>. and, by Lemma 2.14, if p is odd then P is a central product of a cyclic p-group with an extra-special p-group of exponent p, and if p = 2, then P is a central product of a 2-group which is cyclic, dihedral, semi-dihedral, or generalised

quaternion, with an extraspecial 2-group.

In line with [13] (p. 671), we make the following definition.

DEFINITION. A group E is said to be <u>of type E(p,m)</u> if p is a prime such that, for odd p, E is an extraspecial group of order p^{2m+1} and exponent p, and, for p = 2, the group E is a central product of a cyclic group of order 2 or 4 with an extraspecial group of order 2^{2m+1}.

Suppose that P is a p-group of symplectic type. As remarked in [13] (p. 671), if p > 2 then $\Omega_1(P)$ is either cyclic (if P is) or of type E(p,m), with $m \neq 0$. If p = 2, then $\Phi(P)$ is cyclic and $\Omega_2(C_P(\Phi(P)))$ is either cyclic (if P is cyclic or if P is dihedral, semi-dihedral, or generalised quaternion of order at least 16) or of type E(2,m) with $m \neq 0$. Thus, with the above exceptions, P contains a characteristic subgroup of type E(p,m) with $m \neq 0$. We state this formally in the following lemma.

LEMMA 4.1. <u>Let</u> G <u>be a group such that</u> G <u>contains no non-cyclic abelian normal subgroup, and let</u> P <u>be a normal</u> p-<u>subgroup of</u> G <u>for some prime</u> p. <u>Then, writing</u> $E = \Omega_1(P)$ <u>for</u> p > 2 <u>and</u> $E = \Omega_2(C_P(\Phi(P))$ <u>for</u> p = 2, <u>we have</u> $E \triangleleft G$ <u>and either</u> E <u>is of type</u> E(p,m) <u>for some</u> $m \neq 0$, <u>or</u> P <u>is cyclic</u>, <u>or</u> p = 2 <u>and</u> P <u>is dihedral, semi-dihedral, or generalised quaternion of order at least</u> 16.

To describe the scheme of this chapter, let G be a soluble group containing no non-cyclic abelian normal subgroup, q a prime, and V an irreducible GF(q)G-module, faithful for G, such that G acts q'-half-transitively but not q'-semiregularly on V^*. The following is a broad outline, indicating the correspondences with [13], of the main steps in the analysis of the structure of G given in the rest of this chapter.

1. A Reduction Lemma (Lemma 4.4) is proved which, loosely speaking, enables us, in deciding which groups of type E(p,m) might occur as normal

subgroups of G, to assume that, if $E \triangleleft G$ such that E is of type E(p,m), then V_E is irreducible. Lemma 4.4 is analogous to, and proved in the same way as, the Reduction Lemma (Lemma 1.8) in [13].

2. Using the techniques of [13] Section 2 and relying on arithmetic considerations to rule out many cases, we prove (Theorem 4.21) that, for p odd, $O_p(G)$ is cyclic, and if $E \triangleleft G$ with E of type E(2,m) for $m \neq 0$, then either m = 1, or q = 3 and $E \cong Q_8 \curlyvee D_8$. This corresponds to Sections 2, 3, 4, and 5 of [13].

3. We consider the restriction of V to a particular cyclic normal subgroup $A = Z(C_F(\Phi(F)))$ of G (where F denotes the Fitting subgroup of G). In the case where V_A is homogeneous as an A-module we are able to deduce all the possibilities for G (Theorem 4.44). The use of Lemma 3.1 of [13] (stated below as Lemma 4.26) is essential at this stage. This corresponds to Section 6 of [13].

4. Finally we investigate the possibility that V_A is not homogeneous and we show that this case does not occur. (Theorem 4.45). The assumption of primitivity in [13] means that there is no corresponding step in [13].

Before proceeding to the statement and proof of the Reduction Lemma, we record two results to which we shall refer several times in the course of this chapter. The first, Lemma 4.2, is merely a statement of some of the information contained in Lemmas 1.4 and 1.5 of [13] , concerning the action of a group, E, of type E(p,m) on a GF(q)E-module. Lemma 4.2(i) is precisely [13] Lemma 1.14(ii) and Lemma 4.2(ii) is precisely [13] Lemma 1.5(i).

LEMMA 4.2 ([13] Lemmas 1.4 & 1.5). <u>Let</u> E <u>be a group of type</u> E(p,m), <u>let</u> q <u>be a prime, and let</u> V <u>be a</u> GF(q)E-<u>module of dimension</u> n <u>over</u> GF(q) <u>such that</u> E' <u>acts semi-regularly on</u> V^*. <u>Then</u>

(i) *if* $e \in E \backslash Z(E)$ *such that* $|e| = p$, *then* $\dim_{GF(q)} C_V(e) = n/p$;

(ii) *there exists* $x \in V^{\#}$ *such that* $E_x = 1$ *with the following exceptions which occur for* $p = 2$: (a) $q^n = 3^2$, $E \cong D_8$; (b) $q^n = 5^2$, $E \cong Q_8 \curlyvee C_4$; (c) $q^n = 3^4$, $E \cong Q_8 \curlyvee D_8$. *In each of these exceptions* $|E_x| = 2$ *for all* $x \in V^{\#}$.

The second result, Lemma 4.3, is a formalisation of an idea already used in Chapter 3.

LEMMA 4.3. *Let* π *be a set of primes and assume that a group* G *acts* π*-halftransitively as a group of permutations on a set* X. *In addition, assume that* G *contains a normal Hall* π*-subgroup,* H. *Then* H *acts half-transitively on* X, *and if* G *does not act* π*-semiregularly on* X, *then* H *does not act semi-regularly*.

Proof. If $x \in X$ then $|H_x| = |G_x \cap H| = |G_x|_\pi$, since by assumption H is a normal Hall π-subgroup of G. The result then follows easily.

Q.E.D.

LEMMA 4.4. Reduction Lemma. (cf. [13] Lemma 1.8). *Let* G *be a soluble group*, q *a prime*, V *an irreducible* $GF(q)G$*-module, faithful for* G, *such that* G *acts* q'*-halftransitively but not* q'*-semiregularly on* $V^{\#}$. *Assume* $E \lhd G$ *such that* E *is of type* $E(p,m)$ *with* $m \neq 0$. *Then there exists a soluble group* $\overline{G}$ *and an irreducible* $GF(q)\overline{G}$*-module* U, *faithful for* $\overline{G}$, *such that*

(i) $\overline{G}$ *acts* q'*-halftransitively on* $U^{\#}$;

(ii) *there exists* $\overline{E} \lhd \overline{G}$ *such that* $\overline{E} \cong E$ *and* $U_{\overline{E}}$ *is irreducible*;

(iii) *if* $E \not\cong Q_8$ *then* $\overline{G}$ *does not act* q'*-semiregularly on* $U^{\#}$;

(iv) *if* $p > 2$, *or if* $p = 2$ *and* $m \geq 2$, *then either* $q = 3$ *and* $E \cong D_8 \curlyvee Q_8$, *or* $\overline{G}$ *contains no non-cyclic abelian normal subgroup*.

Proof. We construct $\overline{G}$, $\overline{E}$, U exactly as in [13] Lemma 1.8. Let U be an

irreducible constituent of V_E. Since, by Clifford's Theorem, all irreducible constituents of V_E are conjugate in G, we see that U is faithful for E. Let $N = \{g : g \in G, Ug = U\}$. Obviously N is a subgroup of G. Also $E \leqslant N$ and U is an irreducible GF(q)N-module. Let $u \in U^{\#}$ and assume $g \in G_u$. Clearly Ug is an irreducible GF(q)E-module and therefore, since $0 \neq u \in U \cap Ug$, we must have $U = Ug$. Thus $G_u \leqslant N$ for all $u \in U^{\#}$.

Let K denote the kernel of N on U. Then, writing $\overline{G} = N/K$, obviously $\overline{G}$ is soluble, and we see that U is an irreducible $GF(q)\overline{G}$-module, faithful for $\overline{G}$, such that $\overline{G}$ acts q'-halftransitively on $U^{\#}$. Write $\overline{E} = EK/K$. Since E acts faithfully and irreducibly on U, it follows that $E \cong \overline{E} \lhd \overline{G}$ and $U_{\overline{E}}$ is irreducible. Hence we have proved (i) and (ii).

If $\overline{G}$ acts q'-semiregularly on U then the p-group $\overline{E}$ acts semi-regularly on $U^{\#}$. But $\overline{E} \cong E$, a group of type E(p,m) with $m \neq 0$. Hence $E \cong Q_8$. This yields (iii). Finally assume that either $p > 2$ or that $p = 2$ and $m \geqslant 2$. In addition, assume that $\overline{G}$ contains a non-cyclic abelian normal subgroup. Then the structure of $\overline{G}$ is given in Theorem 3.7. If $\overline{G}$ satisfies (iii) of that theorem, that is, if $\overline{G} \cong \Delta$, then $F(\overline{G}) \cong Q_8 \times C_2$ which is clearly impossible. If $\overline{G} \cong \mathcal{T}_0(q^n; q^k)$ for some integers n, k, then $\overline{G}$ contains a normal abelian subgroup of index $2q^k$ and hence cannot possibly contain $\overline{E}$. Therefore $\overline{G}$ satisfies (i), (ii) or (iv) of Theorem 3.7, giving $q = 3$, and we see easily that $\overline{E} \cong E \cong Q_8 \curlyvee D_8$.

Q.E.D.

ASSUMPTIONS. From this point up to the end of Lemma 4.20 we work under the assumptions that G is a soluble group, q is a prime, and V is an n-dimensional irreducible GF(q)G-module, faithful for G, such that G acts q'-halftransitively but not q'-semiregularly on $V^{\#}$. There exists $E \lhd G$ such that E is of type E(p,m) with $m \neq 0$ and V_E is irreducible. In addition we assume that G contains no non-cyclic abelian normal subgroup. We remark that $p \neq q$.

We shall require several of the results of [13] Section 2 in precisely the same form but valid under the weaker assumptions of q'-halftransitivity (instead of half-transitivity) and the absence of non-cyclic abelian normal subgroups of G (instead of primitivity). These results appear below as Lemmas 4.5 - 4.10 corresponding to Lemmas 2.1 - 2.6 respectively in [13]. We shall not give the revised proofs in full since the revisions required are minimal, but we shall always be careful to point out exactly where the proofs need modifying and how these modifications can be made.

Following [13] (pp 677 - 678), we define the <u>type</u> of E as follows.

type I : $p > 2$,

type II : $p = 2$, $|Z(E)| = 2$,

type III : $p = 2$, $|Z(E)| = 4$, $Z(E) \leqslant Z(G)$,

type IV : $p = 2$, $|Z(E)| = 4$, $Z(E) \not\leqslant Z(G)$.

LEMMA 4.5. (cf. [13] Lemma 2.1). <u>Let</u> $s \geqslant 1$ <u>be minimal such that</u> $|Z(E)| \mid q^s - 1$. <u>Let</u> M <u>be any subgroup of</u> G <u>such that</u> $E \leqslant M \leqslant C_G(Z(E))$. <u>Then</u> $M \leqslant GL(p^m, q^s)$ <u>and this representation of</u> M <u>is absolutely irreducible. Furthermore</u> $n = sp^m$ <u>and we have</u>

type I : $s \mid (p-1)$,

type II : $s = 1$,

type III : $s = 1$ or 2,

type IV : $s = 2$ <u>and if</u> $\overline{M}$ <u>is a</u> q'-<u>subgroup of</u> G <u>such that</u> $E \leqslant \overline{M}$ <u>and</u> $\overline{M} \not\leqslant C_G(Z(E))$, <u>then</u> $\overline{M} \leqslant GL(p^{m+1}, q)$ <u>and this is an absolutely irreducible representation.</u>

<u>Proof</u>. An examination of the proof of [13] Lemma 2.1 reveals that the assumption of half-transitivity is not used, and the assumption of primitivity is used only to ensure that $V_{Z(E)}$ is homogeneous as a

We shall require several of the results of [13] Section 2 in precisely the same form but valid under the weaker assumptions of q'-halftransitivity (instead of half-transitivity) and the absence of non-cyclic abelian normal subgroups of G (instead of primitivity). These results appear below as Lemmas 4.5 - 4.10 corresponding to Lemmas 2.1 - 2.6 respectively in [13]. We shall not give the revised proofs in full since the revisions required are minimal, but we shall always be careful to point out exactly where the proofs need modifying and how these modifications can be made.

Following [13] (pp 677 - 678), we define the <u>type</u> of E as follows.

type I : $p > 2$,

type II : $p = 2$, $|Z(E)| = 2$,

type III : $p = 2$, $|Z(E)| = 4$, $Z(E) \leqslant Z(G)$,

type IV : $p = 2$, $|Z(E)| = 4$, $Z(E) \not\leqslant Z(G)$.

LEMMA 4.5. (cf. [13] Lemma 2.1). <u>Let</u> $s > 1$ <u>be minimal such that</u> $|Z(E)| \mid q^s - 1$. <u>Let</u> M <u>be any subgroup of</u> G <u>such that</u> $E \leqslant M \leqslant C_G(Z(E))$. <u>Then</u> $M \leqslant GL(p^m, q^s)$ <u>and this representation of</u> M <u>is absolutely irreducible. Furthermore</u> $n = sp^m$ <u>and we have</u>

type I : $s \mid (p-1)$,

type II : $s = 1$,

type III : $s = 1$ or 2,

type IV : $s = 2$ <u>and if</u> $\overline{M}$ <u>is a</u> q'-<u>subgroup of</u> G <u>such that</u> $E \leqslant \overline{M}$ <u>and</u> $\overline{M} \not\leqslant C_G(Z(E))$, <u>then</u> $\overline{M} \leqslant GL(p^{m+1}, q)$ <u>and this is an absolutely irreducible representation.</u>

<u>Proof</u>. An examination of the proof of [13] Lemma 2.1 reveals that the assumption of half-transitivity is not used, and the assumption of primitivity is used only to ensure that $V_{Z(E)}$ is homogeneous as a

$Z(E)$-module. Therefore we need only show that $V_{Z(E)}$ is homogeneous without recourse to the assumption of primitivity. But this is trivial since $V_{Z(E)} \cong (V_E)_{Z(E)}$ and V_E is irreducible.

Q.E.D.

As individual lemmas in the sequence 2.1 - 2.6 of [13] are established, they are often required in the proofs of subsequent lemmas in the sequence. We adopt the obvious convention that Lemma 4.5 above plays exactly the same part in the proofs of Lemma 4.6 - 4.10 as [13] Lemma 2.1 plays in the proofs of [13] Lemmas 2.2 - 2.6. For example, for the purposes of establishing Lemma 4.7 below, the references to [13] Lemma 2.1 in the proof of [13] Lemma 2.3 are to be taken as references to Lemma 4.5, and so on. Similarly, Lemmas 4.6 - 4.10 play the roles of [13] Lemmas 2.2 - 2.6 respectively.

Lemma 2.2 of [13] is a general result concerning modules for p-groups, and we reproduce it below as Lemma 4.6.

LEMMA 4.6. ([13] Lemma 2.2). <u>Let</u> M <u>be a</u> p-<u>group acting faithfully and absolutely irreducibly on a vector space</u> W <u>over the field</u> F. <u>Let</u> $\dim_F W = k$. <u>Then there exist subgroups</u> N <u>and</u> K <u>of</u> M <u>and an</u> N-<u>subspace</u> U <u>of</u> W <u>such that the representation of</u> M <u>on</u> W <u>is induced from that of</u> N <u>on</u> U. <u>Furthermore</u> $K = \ker(N \text{ on } U)$ <u>and either</u>

(i) $|M : N| = k$, $\dim_F U = 1$ <u>and</u> N/K <u>is cyclic, or</u>

(ii) $|M : N| = k/2$, $\dim_F U = 2$, $p = 2$ <u>and</u> N/K <u>is dihedral, semi-dihedral or generalised quaternion.</u>

LEMMA 4.7.(cf. [13] Lemma 2.3). <u>Let</u> ω <u>denote the exponent of a Sylow</u> p-<u>subgroup of</u> $C_G(Z(E))$. <u>Then for all</u> $x \in V^*$ <u>we have</u>

$$\begin{aligned}
\text{type I} &: |G : G_x|_p \leq p^m . \min\{\omega, |q^s - 1|_p\}, \\
\text{type II} &: |G : G_x|_p \leq p^{m+1} . \min\{\omega, |q^2 - 1|_p\}, \\
\text{type III} &: |G : G_x|_p \leq p^m . \min\{\omega, |q^2 - 1|_p\}, \\
\text{type IV} &: |G : G_x|_p \leq p^{m+1} . \min\{\omega, |q^2 - 1|_p\}.
\end{aligned}$$

Proof. Inspection of the proof of [13] Lemma 2.3 reveals that the assumption of primitivity is not used and the assumption of half-transitivity is used only in that it guarantees that for all $x,y \in V^{\#}$,

$$|G : G_x|_p = |G : G_y|_p.$$

But, clearly, since $p \neq q$, the above equality follows from the weaker assumption of q'-halftransitivity, and hence the proof of [13] Lemma 2.3 is easily modified to give the proof we require.

Q.E.D.

LEMMA 4.8. (cf. [13] Lemma 2.4). Let $A = C_G(E)$. Then A is a normal cyclic subgroup of G which is central in $C_G(Z(E))$ and acts semi-regularly on $V^{\#}$. Assume that, if $p = 2$, then $m \geq 3$. Then there exists $x \in V^{\#}$ such that $G_x \cap AE = 1$ and $|G : G_x|_p \geq |A_p|p^{2m}$ where A_p is the normal Sylow p-subgroup of A. This yields

$$\begin{aligned}
&\text{type I} &&: \omega \geq p^m|A_p| \ , \ |q^s - 1|_p \geq p^{m+1} \ , \\
&\text{type II} &&: \omega \geq p^{m-1}|A_p|, \ |q^2 - 1|_p \geq p^m \ , \\
&\text{type III} &&: \omega \geq p^m|A_p|, \ |q^2 - 1|_p \geq p^{m+2} \ , \\
&\text{type IV} &&: \omega \geq p^{m-1}|A_p|, \ |q^2 - 1|_p \geq p^{m+1} \ .
\end{aligned}$$

Proof. An examination of the proof of [13] Lemma 2.4 reveals that the assumption of primitivity is not used, and the assumption of half-transitivity is used only in that it guarantees that, for all $x,y \in V^{\#}$,

$$|G : G_x|_p = |G : G_y|_p.$$

But the above equality follows from the weaker assumption of q'-half-transitivity, and hence the proof of [13] Lemma 2.4 is easily adapted to provide the proof we require.

Q.E.D.

LEMMA 4.9. (cf. [13] Lemma 2.5). Let $H = C_G(Z(E))$. Then G has the following structure.

(i) G/H is cyclic;

(ii) H/AE acts faithfully on $W = E/Z(E)$ and, as a linear group on W, we have $H/AE \leqslant Sp(2m,p)$;

(iii) AE/A is elementary abelian of order p^{2m};

(iv) A is cyclic.

Proof. We remark that $W = E/Z(E)$ is made into a symplectic space of dimension 2m over $GF(p)$ by means of the non-singular skew-symmetric bilinear form induced on E/Z(E) by the commutator map [,] on E.

Inspection of the proof of [13] Lemma 2.5 reveals that the assumption of half-transitivity is not used, and the assumption of primitivity is only used to ensure that a certain normal 2-subgroup of G, namely $B_2 = O_2(C_H(W))$, is of symplectic type; that is, B_2 contains no non-cyclic, abelian characteristic subgroup. But, clearly, the weaker assumption that G contains no non-cyclic abelian normal subgroup guarantees that B_2 is of symplectic type. Hence the proof of [13] Lemma 2.5 is easily modified to give the proof we require.

Q.E.D.

LEMMA 4.10. (cf. [13] Lemma 2.6). We must have one of the following.

type I : $p = 3$, $m \leqslant 2$,

type II : $p = 2$, $m \leqslant 6$,

type III : $p = 2$, $m \leqslant 3$,

type IV : $p = 2$, $m \leqslant 5$.

Proof. An examination of the proof of [13] Lemma 2.6 reveals that the assumption of primitivity is not used and the assumption of half-transitivity is used only in that it guarantees that, in the case $p = 3$, $m = 1$, the fact that E does not act semi-regularly on V^* implies that $p \mid |G_x|$ for

all $x \in V^{\#}$. But obviously, since $p \neq q$, the weaker assumption of q'-half-transitivity leads to the same conclusion, and hence the proof of [13] Lemma 2.6 is easily adapted to provide the proof we require.

Q.E.D.

The following result will enable us to eliminate many of the remaining cases.

LEMMA 4.11. (i) <u>Assume that if</u> $p = 2$ <u>then we have both</u> $m \geqslant 2$ <u>and either</u> $q \neq 3$ <u>or</u> $E \not\cong Q_8 \curlyvee D_8$. <u>Then</u> $|E| \mid (q^n - 1)$.

(ii) <u>Assume that</u> $q \nmid |Sp(2m,p)|$, <u>and that either</u> $p = 2$ <u>or</u> $q \nmid |G : H|$. <u>Then</u> G <u>acts half-transitively on</u> $V^{\#}$, <u>we must have</u> $p = 2$, <u>and if</u> $m \neq 1$ <u>then</u> $E \cong Q_8 \curlyvee D_8$ <u>with</u> $q \equiv 3$.

<u>Proof</u>. Assume that if $p = 2$ then we have both $m \geqslant 2$ and either $q \neq 3$ or $E \not\cong Q_8 \curlyvee D_8$. Then, by Lemma 4.2(ii), there exists $x \in V^{\#}$ such that $E_x = G_x \cap E = 1$. Therefore $|E| \mid |G : G_x|$, and it follows that $|E|$ divides the size of the G-orbit containing x. Now $(|E|,q) = 1$ and hence, by q'-halftransitivity, $|E|$ divides the size of each of the G-orbits in $V^{\#}$. We conclude that $|E|$ divides $|V^{\#}| = (q^n - 1)$ and thus we have proved (i).

Assume now that $q \nmid |Sp(2m,p)|$ and that either $p = 2$ or $q \nmid |G : H|$. By Lemma 4.9(ii), the group H/AE is isomorphic to a subgroup of Sp(2m,p), and therefore $q \nmid |H/AE|$. Now A is a normal cyclic subgroup of G and hence, since $O_q(G) = 1$, we have $q \nmid |A|$. Clearly $q \nmid |E|$ and it follows that $q \nmid |AE|$, whence $q \nmid |H|$. If $p = 2$ then $|G : H| \leqslant 2$ and so, since $p \neq q$, we must have $q \nmid |G : H|$. On the other hand, if $p \neq 2$ then, by assumption, $q \nmid |G : H|$. Therefore, whether $p = 2$ or $p \neq 2$, we have $q \nmid |G : H|$ and we conclude that $q \nmid |G|$. Thus G acts half-transitively on $V^{\#}$.

Assume that $E \not\cong Q_8$. Then E does not act semi-regularly on $V^{\#}$. Hence G does not act semi-regularly on $V^{\#}$ and the possibilities for G are listed

in Theorem 1.16. Clearly $G \not\leq \mathcal{T}_0(q^{n/2})$ since $\mathcal{T}_0(q^{n/2})$ contains a normal subgroup isomorphic to $C_2 \times C_2$. If $G \leq \mathcal{T}(q^n)$, then G, and hence E, is metacyclic, whence $p = 2$, $m = 1$. In all the remaining possibilities for G in Theorem 1.16, we see that $p = 2$, and either $m = 1$ or $E \cong Q_8 \curlyvee D_8$ and $q = 3$. This completes the proof of (ii).

Q.E.D.

Next we state, without proof, a result concerning the order of the group $Sp(2m,p)$. A proof is given in [6] II 9.13.

LEMMA 4.12. <u>We have</u>

$$|Sp(2m,p)| = (p^{2m} - 1)p^{2m-1}(p^{2m-2} - 1)p^{2m-3}\ldots(p^2 - 1)p.$$

LEMMA 4.13. <u>The case</u> $p = 3$, $m = 1$, <u>does not occur.</u>

<u>Proof</u>. Suppose that $p = 3$, $m = 1$. Then $|E| = 27$ and by Lemma 4.11 (i), we have $27 \mid (q^n - 1)$. If $q = 2$ then by Lemma 4.5, we have $n = 6$, giving $27 \mid 63$, a contradiction. Hence $q \neq 2$. Now $q \neq 3$ and so, since $|Sp(2,3)| = 24$ and $|G : H| \leq 2$, it follows that $q \nmid |Sp(2,3)|$ and $q \nmid |G : H|$. Therefore, by Lemma 4.11(ii), we have $p = 2$, a contradiction. Thus the case $p = 3$, $m = 1$ does not occur.

Q.E.D.

LEMMA 4.14. The case $p = 3$, $m = 2$, does not occur.

<u>Proof</u>. Suppose that $p = 3$, $m = 2$. Then $|E| = 3^5 = 243$ and, by Lemma 4.11(i), we have $243 \mid (q^n - 1)$. If $q = 2$ or $q = 5$, then $s = 2$ and then, by Lemma 4.5, we have $n = 18$. But it is easily checked that $243 \nmid (2^{18} - 1)$ and $243 \nmid (5^{18} - 1)$, and we deduce that $q \neq 2$, $q \neq 5$. Now $q \neq 3$ and so, since $|Sp(4,3)| = 3^4.5.2^7$ and $|G : H| \leq 2$, it follows that $q \nmid |Sp(4,3)|$ and $q \nmid |G : H|$. Therefore, by Lemma 4.11(ii), we have $p = 2$, a contradiction. Thus the case $p = 3$, $m = 2$, does not occur.

Q.E.D.

The following result is included merely to simplify some of the arithmetical checking in Lemmas 4.16 - 4.20.

LEMMA 4.15. Let a, b, k be positive integers such that k is odd. Then $2^b|(k^{2^a}-1)$ if and only if $2^{b-a+1}|(k^2-1)$.

Proof. If t is an even positive integer then, since $k^t-1=(k^{t/2}-1)(k^{t/2}+1)$, we have $4|(k^t-1)$. Therefore $4\nmid(k^t+1)$. We have

$$(k^{2^a}-1)=(k^{2^{a-1}}-1)(k^{2^{a-1}}+1)=(k^{2^{a-2}}-1)(k^{2^{a-2}}+1)(k^{2^{a-1}}+1)=\ldots=$$

$$(k^2-1)(k^2+1)(k^4+1)\ldots(k^{2^{a-1}}+1)$$

and then, since $4\nmid(k^{2^c}+1)$ for $c\geqslant 1$, we see $2^b|(k^{2^a}-1)\Leftrightarrow$ $2^b|(k^2-1)2^{a-1}\Leftrightarrow 2^{b-a+1}|(k^2-1)$.

Q.E.D.

LEMMA 4.16. The case p = 2, m = 6, does not occur.

Proof. Suppose that p = 2, m = 6. By Lemma 4.10 we see that E is type II, whence $|Z(E)|=2$. Therefore s = 1 and hence, by Lemma 4.5, we have $n=2^6=64$. Now $|E|=2^{13}$ and, using Lemma 4.11(i), it follows that $2^{13}|(q^{2^6}-1)$. Lemma 4.15 yields $2^8|(q^2-1)$. It is easily checked that $2^8|(q^2-1)$ implies that $q\neq 3, 5, 7, 11, 13, 17$, or 31, and therefore, since $|Sp(12,2)|=2^{36}.3^8.5^3.7^2.11.13.17.31$, we deduce that $q\nmid|Sp(12,2)|$. Hence, by Lemma 4.11(ii), we have $m\leqslant 2$, a contradiction. Thus the case p = 2, m = 6 does not occur.

Q.E.D.

LEMMA 4.17. The case p = 2, m = 5, does not occur.

Proof. Suppose that p = 2, m = 5. Then s = 1 or 2 depending on whether $|Z(E)|=2$ or 4 and whether $q\equiv 1$ or -1 mod 4. Hence, by Lemma 4.5, we have $n=2^5$ or 2^6 and if $n=2^6$ then $|Z(E)|=4$. Also if $|Z(E)|=2$

then $|E| = 2^{11}$, and if $|Z(E)| = 4$ then $|E| = 2^{12}$. By Lemma 4.11(i) we have $|E|\,|(q^n-1)$.

If $n = 2^5$ then $2^{11}|(q^{2^5}-1)$, and Lemma 4.15 yields $2^7|(q^2-1)$. If $n = 2^6$ then $|Z(E)| = 4$, and it follows that $|E| = 2^{12}$, whence $2^{12}|(q^{2^6}-1)$ and, using Lemma 4.15, we deduce that, again, $2^7|(q^2-1)$. It is easily checked that $2^7|(q^2-1)$ implies that $q \neq 3, 5, 7, 11, 17, 31$, and therefore, since $|Sp(10,2)| = 2^{35}.3^6.5^2.7.11.17.31$, it follows that $q \nmid |Sp(10,2)|$. Hence, by Lemma 4.11(ii), we have $m \leq 2$, a contradiction. Thus the case $p = 2$, $m = 5$, does not occur.

Q.E.D.

LEMMA 4.18. <u>The case</u> $p = 2$, $m = 4$, <u>does not occur</u>.

<u>Proof</u>. Suppose that $p = 2$, $m = 4$. Using the same argument as in the proof of Lemma 4.17, we see that in this case we must have $2^6|(q^2-1)$. It is easily checked that $2^6|(q^2-1)$ implies that $q \neq 3, 5, 7, 17$, and therefore, since $|Sp(8,2)| = 2^{16}.3^5.5^2.7.17$, it follows that $q \nmid |Sp(8,2)|$. Hence, by Lemma 4.11(ii), we have $m \leq 2$, a contradiction. Thus the case $p = 2$, $m = 4$, does not occur.

Q.E.D.

LEMMA 4.19. <u>The case</u> $p = 2$, $m = 3$, <u>does not occur</u>.

<u>Proof</u>. Suppose that $p = 2$, $m = 3$. Again using the argument in the proof of Lemma 4.17, we see that in this case we must have $2^5|(q^2-1)$. It is easily checked that $2^5|(q^2-1)$ implies that $q \neq 3, 5, 7$, and therefore, since $|Sp(6,2)| = 2^9.3^4.5.7$, it follows that $q \nmid |Sp(6,2)|$. Hence, by Lemma 4.11(ii), we have $m \leq 2$, a contradiction. Thus the case $p = 2$, $m = 3$, does not occur.

Q.E.D.

LEMMA 4.20. *If* $p = 2$ *and* $m = 2$, *then* $q = 3$ *and* $E \cong Q_8 \curlyvee D_8$.

Proof. Assume that $p = 2$, $m = 2$, and suppose that either $q \neq 3$ or that $E \not\cong Q_8 \curlyvee D_8$. As before, $s = 1$ or 2 depending on whether $|Z(E)| = 2$ or 4 and whether $q \equiv 1$ or -1 mod4. By Lemma 4.5 we have $n = 2^2$ or 2^3, and if $n = 2^3$ then $|Z(E)| = 4$. Also if $|Z(E)| = 2$ then $|E| = 2^5$, and if $|Z(E)| = 4$ then $|E| = 2^6$. We have assumed that either $q \neq 3$ or $E \not\cong Q_8 \curlyvee D_8$, and therefore, by Lemma 4.11(i), it follows that $|E| \mid (q^n - 1)$.

If $n = 2^2$, then $2^5 \mid (q^{2^2} - 1)$ and Lemma 4.15 yields $2^4 \mid (q^2 - 1)$. If $n = 2^3$, then $|Z(E)| = 4$ and it follows that $|E| = 2^6$, whence $2^6 \mid (q^{2^3} - 1)$ and, using Lemma 4.15, we deduce that again, $2^4 \mid (q^2 - 1)$. It is easily checked that $2^4 \nmid (q^2 - 1)$ for $q = 3$ or 5, and therefore $q \neq 3$ or 5. Since $|Sp(4,2)| = 2^4.3^2.5$ we conclude that $q \nmid |Sp(4,2)|$. Hence, by Lemma 4.11(ii), we have $q = 3$ and $E \cong Q_8 \curlyvee D_8$, a contradiction. Therefore we were incorrect in supposing that either $q \neq 3$ or $E \not\cong Q_8 \curlyvee D_8$ and, as a result, we must have both $q = 3$ and $E \cong Q_8 \curlyvee D_8$.

Q.E.D.

We now drop the assumptions stated immediately after the proof of Lemma 4.4 and we collect together the preceeding results to obtain the following theorem.

THEOREM 4.21. *Let* G *be a soluble group,* q *a prime, and* V *an irreducible* $GF(q)G$*-module, faithful for* G, *such that* G *acts* q'*-halftransitively but not* q'*-semiregularly on* $V^{\#}$. *Assume that* G *contains no non-cyclic abelian normal subgroup. Then for all odd primes* p *we have* $O_p(G)$ *is cyclic, and if* $E \lhd G$ *such that* E *is of type* $E(2,m)$ *with* $m \neq 0$, *then either* $m = 1$ *or* $q = 3$ *and* $E \cong Q_8 \curlyvee D_8$.

Proof. Let p be a prime such that $p > 2$ and write $P = O_p(G)$. Suppose P

is not cyclic. Then by Lemma 4.1 there exists a subgroup, E, of P such that $E \lhd G$ and E is of type $E(p,m)$ with $m \neq 0$. But then, using the Reduction Lemma and Lemmas 4.10, 4.13, 4.14, we have a contradiction. Hence P is cyclic. Now suppose $E \lhd G$ such that E is of type $E(2,m)$ with $m \geqslant 2$. Then, by the Reduction Lemma and Lemmas 4.10, 4.16 - 4.20, we have $q = 3$ and $E \cong Q_8 \curlyvee D_8$.

Q.E.D.

Theorem 4.21 completes Step 2 in the outline of this chapter given earlier. Before proceeding to Step 3 we state and prove two useful lemmas, and, for convenience, record the results from [11] to which we shall need to refer.

LEMMA 4.22. <u>Let</u> G <u>be a group of order</u> 96 <u>such that</u> $F(G) \cong Q_8 \curlyvee C_4$ <u>and</u> $G/F(G) \cong S_3$. <u>Assume that</u> $|Z(G)| = 2$ <u>and that there exists</u> $g \in G \backslash C_G(Z(F(G)))$ <u>such that</u> $g^2 = 1$. <u>Then there exists at least one irreducible</u> $GF(3)G$-<u>module which is faithful for</u> G, <u>and if</u> W <u>is any such</u> $GF(3)G$-<u>module then</u> $\dim_{GF(3)} W = 4$ <u>and there exists</u> $w \in W^{\#}$ <u>such that</u> $4 \mid |G_w|$.

<u>Proof</u>. Write $F = F(G)$, and let $F = QZ$ where $Q \cong Q_8$ and $Z \cong C_4$ such that $|Q \cap Z| = 2$ and $[Q,Z] = 1$. Clearly $Z = Z(F)$. It is easily seen that Q is characteristic in F, and therefore $Q \lhd G$. Let C be a Sylow 3-subgroup of G. Then $|C| = 3$ and C centralises Z. Write $N = C_G(Z)$, and then, since $|Z(G)| = 2 < 4 = |Z|$, we must have $N < G$. Now $FC \leqslant N$ and $|FC| = 3.16 = 48$, giving $|G : FC| = 2$. Therefore $FC = N \lhd G$. If C centralises Q then C centralises $QZ = F$, whence $C \lhd N$ and $C = O_3(N) \leqslant F(N) \leqslant F(G)$, a contradiction. Hence C does not centralise Q and so clearly, $QC \cong SL(2,3)$.

Let $Z = \langle a \rangle$ and write $a^2 = z$. By assumption there exists $g \in G \backslash N$ such that $g^2 = 1$, and we must have $gag = a^{-1}$. Clearly $QC \lhd G$, and therefore, writing $T = \langle QC, g \rangle$, we have $|T| = 48$, and $QC \leqslant T$ with $QC \cong SL(2,3)$.

Let $R = C_G(Q/Z(Q))$. Then $R \lhd G$ and $C \not\leq R$. Therefore R is a normal 2-subgroup of G, and we deduce that $R = F$. Consequently $g \notin R$ and, by Lemma 3.15, it follows that $T \cong GL(2,3)$. Also $|G : T| = 2$, whence $T \lhd G$.

Let U be an irreducible $GF(3)T$-module which is faithful for T (obviously such a module exists since $T \cong GL(2,3)$), and let W be a non-trivial irreducible submodule of the $GF(3)G$-module U^G. The group G has a unique minimal normal subgroup, namely $\langle z \rangle = Z(Q) = Z(T) = Z(G)$. Now z acts like scalar multiplication by -1 on U, and hence acts in exactly the same manner on U^G. Therefore W is faithful for G, and we have demonstrated the existence of an irreducible $GF(3)G$-module which is faithful for G, namely W.

Now assume that W is any irreducible $GF(3)G$-module, faithful for G, and in addition assume that U is an irreducible constituent of W_T. Obviously U is faithful for T, and therefore, by Lemma 3.13(i), we have $\dim_{GF(3)} U = 2$. Let H denote the stabiliser in G of U. Then

$$H = \{h : h \in G,\ U \text{ and } Uh \text{ are } T\text{-isomorphic}\}.$$

Since $T \leq H$ and $|G : T| = 2$, we must have $H = T$ or $H = G$. Suppose $H = G$. Then U and Ua are T-isomorphic as $GF(3)T$-modules. The element g is a non-central involution in T, and therefore there exists $u \in U^{\#}$ such that $g \in T_u$. By Lemma 3.13(ii) we have $T_u \cong S_3$, and hence $T_u = \langle L, g \rangle$ for some Sylow 3-subgroup, L, of G. Since U and Ua are T-isomorphic, it follows that there exists $x \in (Ua)^{\#}$ such that $T_x = T_u$. Consider the element ua of $(Ua)^{\#}$. Clearly

$$T_{ua} = (T_u)^a = \langle L^a, g^a \rangle .$$

Now $L \leq N = C_G(Z)$ and thus $L^a = L$. Also, since $gag = a^{-1}$, we must have $g^a = a^2 g = gz$. Therefore $T_{ua} = \langle L, gz \rangle$. But then x, ua are two elements of $(Ua)^{\#}$ such that $T_x = T_u = \langle L, g \rangle$ and $T_{ua} = \langle L, gz \rangle$, contradicting

Lemma 3.13(v). Hence $H \neq G$ and we conclude that $H = T$.

By Clifford's Theorem we have

$$W_T = U \oplus Ua$$

where U and Ua are not T-isomorphic, and $W \cong U^G$. Thus $\dim_{GF(3)} W = 4$. All that remains to prove is that there exists $w \in W^\#$ such that $4 \mid |G_w|$. Since $F = QZ$ it is easily seen that $|i(F)| = 6$ and that, if $f \in i(F)$, then no Sylow 3-subgroup of G centralises f. Let $f \in i(F)$. Clearly there exists $w \in W^\#$ such that $f \in G_w$, and since Q acts semi-regularly on $W^\#$, we must have $G_w \cap F = F_w = \langle f \rangle$. Now $G_w \cap F \triangleleft G_w$, and therefore, from the fact that no Sylow 3-subgroup of G centralises f, we deduce that $3 \nmid |G_w|$. Write $w = u + v$ with $u \in U$, $v \in Ua$. If $v = 0$ then $G_w = G_u = T_u \cong S_3$, contradicting $3 \nmid |G_w|$. Hence $v \in (Ua)^\#$, and similarly $u \in U^\#$.

Clearly $G_u \cap G_v = T_{u+v} = T \cap G_{u+v}$. Since $|G_{u+v} : G_u \cap G_v| \leq 2$ and $f \in G_{u+v} \setminus (G_{u+v} \cap T)$, it follows that $|G_{u+v} : G_u \cap G_v| = 2$. Hence, if we can show that $2 \mid |G_v \cap G_u|$, then $4 \mid |G_{u+v}|$ and the proof is complete. Suppose that $2 \nmid |G_u \cap G_v|$. Then, since $G_u = T_u$ and $G_v = T_v$, we have $2 \nmid |T_u \cap T_v|$. Recall that $T_u \cong T_v \cong S_3$ and thus, since $3 \nmid |G_{u+v}|$, we see that $3 \nmid |T_u \cap T_v|$, whence $T_u \cap T_v = 1$. Let L be a Sylow 3-subgroup of G such that $L \triangleleft T_u$ and let g_1, g_2, g_3 be the three involutions in T_u, so that $T_u = \langle L, g_i \rangle$ for $i = 1,2,3$. Write

$$X_1 = \{K : K = T_x \text{ for some } x \in U^\#\}, \quad X_2 = \{K : K = T_x \text{ for some } x \in (Ua)^\#\}$$

Then, since U and Ua are not T-isomorphic, by Lemma 3.13(iii) and (iv) we have $|X_1| = |X_2| = 4$, and $X_1 \cap X_2 = \emptyset$. Arguing as above we see that $L \triangleleft T_{ua}$. Since $T_u \cap T_v = 1$, it follows that $T_{ua} \neq T_v$. Also $g_i \notin T_{ua}$ for $i = 1,2,3$. (since if $g_i \in T_{ua}$ then $T_{ua} = \langle L, g_i \rangle = T_u$ contradicting $X_1 \cap X_2 = \emptyset$). If $i \in \{1,2,3\}$ then g_i is a non-central involution of T, and hence there exists $Y_i \in X_2$ such that $g_i \in Y_i$. Suppose that $Y_i = Y_j$ for $i \neq j$. Then

$Y_i \geqslant \langle g_i, g_j \rangle = T_u$, contradicting $X_1 \cap X_2 = \emptyset$. Clearly, then, Y_1, Y_2, Y_3, T_{ua}, and T_v are all distinct elements of X_2, a contradiction since $|X_2| = 4$. Thus we were incorrect in supposing that $2 \nmid |G_v \cap G_u|$, and therefore $4 \mid |G_w|$.

Q.E.D.

LEMMA 4.23. <u>Let</u> G <u>be a group such that</u> $F(G) = Q \times B$ <u>where</u> $Q \cong Q_8$ <u>and</u> B <u>is cyclic of odd order. Assume</u> G <u>is metacyclic. Then there exists</u> $T \lhd G$ <u>such that</u> T <u>and</u> G/T <u>are cyclic,</u> $|F(G) : T| = 2$, <u>and</u> $C_G(T) = T$. <u>In addition</u> $i(G) = \emptyset$.

<u>Proof</u>. Since G is metacyclic there exists $S \lhd G$ such that both S and G/S are cyclic. In particular QS/S is cyclic. Therefore, since $QS/S \cong Q/S \cap Q$ and $Q \cong Q_8$, we have $|S \cap Q| = 4$. Writing $T = (S \cap Q) \times B$, we must have $S \leqslant T$, whence $T \lhd G$ with both T and G/T cyclic. Also

$$|F(G)/T| = |QT/T| = |Q/T \cap Q| = |Q/S \cap Q| = 2.$$

Write $C = C_G(T)$. Then $C \lhd G$ and C stabilises the chain $Q \geqslant T \cap Q \geqslant 1$. Therefore $C/C_C(Q)$ is a 2-group. But, since $F(G) = QT$, we have $C_C(Q) \leqslant C_G(F(G))$. From the fact that G is metacyclic, it follows that G is soluble, and we deduce that

$$C_C(Q) \leqslant C_G(F(G)) = Z(F(G)) \leqslant T.$$

Hence C/T is a 2-group. We have $T \leqslant Z(C)$, and therefore C is a normal nilpotent subgroup of G. Thus $C \leqslant F(G)$ and it follows easily that $C = T$.

Let $g \in G$ such that $g^2 = 1$. Since G/T is cyclic and $|F(G)/T| = 2$, we must have $g \in F(G)$, whence $g \in Z(Q) \leqslant Z(G)$. We conclude that $i(G) = \emptyset$.

Q.E.D.

Lemma 4.24 below is precisely [11] Proposition 3.3 and Lemma 4.25 is

a combination of two results in [11] ; specifically, Lemma 4.25(i) is [11] Proposition 1.2 and Lemma 4.25(ii) is [11] Lemma 1.5. Lemma 4.26 is also a combination of two results in [11], namely [11] Lemmas 1.3 and 1.4, but appears in the form below (without proof) as Lemma 3.1 of [13].

For the purposes of stating Lemmas 4.24 - 4.26 below, we assume that G is a soluble group, q is a prime and V is an irreducible GF(q)G-module, faithful for G, with $\dim_{GF(q)} V = n$.

LEMMA 4.24. ([11] Proposition 3.3). Assume that G acts half-transitively but not semi-regularly on $V^{\#}$. In addition assume that either there exists a normal self-centralising cylic subgroup of G, A say, or that $F(G) = Q \times B$ where B is a cyclic group of odd order, $Q \cong Q_8$ and A denotes $Z(F(G))$. Then V_A is homogeneous.

LEMMA 4.25. ([11] Proposition 1.2 & Lemma 1.5). Assume that p is a prime such that $p \mid |G_x|$ for all $x \in V^{\#}$. Then

(i) if there exists a normal self-centralising cyclic subgroup A of G such that V_A is homogeneous then $G \leq \mathcal{T}(q^n)$;

(ii) if $F(G) = Q \times B = F$, say, where B is a cyclic group of odd order, $Q \cong Q_8$, and $V_{Z(F)}$ is homogeneous, then either $G \leq \mathcal{T}(q^n)$, or $p = 2$, or $p = 3$.

LEMMA 4.26. ([11] Lemmas 1.3 & 1.4). Assume that p is a prime such that $p \mid |G_x|$ for all $x \in V^{\#}$, and that A is a cyclic normal subgroup of G such that V_A is homogeneous. Let r denote the dimension over GF(q) of an irreducible constituent of V_A, and write $n/r = k$. Consider those subgroups, P, of G containing A such that $|P/A| = p$ and $P \cap G_x > 1$, for some $x \in V^{\#}$. If exactly λ_1 of such subgroups are contained in $C_G(A)$, and exactly λ_2 are not then

$$\text{(i)} \quad \frac{q^{kr}-1}{q^r-1} \leq \lambda_1\left\{1 + \frac{q^{r(k-1)}-1}{q^r-1}\right\} + \lambda_2\left\{\frac{q^{rk/p}-1}{q^{r/p}-1}\right\} ;$$

(ii) $q^r + 1 \leqslant 2\lambda_1 + \lambda_2(q^{r/p} + 1)$ <u>for</u> $k = 2$;

(iii) $q^r < 2(\lambda_1 + \lambda_2)$ <u>for</u> $k > 2$.

ASSUMPTIONS. Throughout the rest of this chapter we shall assume that G is a soluble group, q is a prime, and V is an irreducible $GF(q)G$-module, faithful for G, such that G acts q'-halftransitively but not q'-semiregularly on $V^{\#}$. In addition we shall assume that G contains no non-cyclic abelian normal subgroup.

NOTATION. We fix some notation as follows. Let n denote $\dim_{GF(q)}V$. Let F denote $F(G)$, and write $F_2 = O_2(G)$. If B denotes $O_{2'}(F)$, then Theorem 4.21 implies that B is cyclic, and we have $F = F_2 \times B$. Let A denote $Z(C_F(\Phi(F)))$. Clearly A is an abelian normal subgroup of G, and hence, by assumption, A is cyclic. Obviously $B \leqslant A$. Finally, let p be a prime such that $p \neq q$ and $p \mid |G_x|$ for all $x \in V^{\#}$. (The existence of such a prime p is guaranteed by the assumption that G acts q'-halftransitively but not q'-semiregularly on $V^{\#}$.)

As indicated in the outline of this chapter given earlier, we shall have two cases to consider according to whether or not V_A is homogeneous. However, if F_2 is generalised quaternion of order at least 16, or if F_2 is cyclic, dihedral or semi-dihedral, then the following lemma gives the structure of G without having to assume anything about V_A.

LEMMA 4.27. <u>Assume that</u> F_2 <u>is generalised quaternion of order at least</u> 16, <u>or that</u> F_2 <u>is cyclic, dihedral, or semi-dihedral. Then</u> V_A <u>is homogeneous and</u> $G \leqslant \mathcal{T}(q^n)$.

<u>Proof</u>. We see easily that F contains a characteristic cyclic subgroup, A_1 say, such that $A \leqslant A_1$ and $|F : A_1| \leqslant 2$. Write $C = C_G(A_1)$. Now C stabilises the chain $F_2 \geqslant F_2 \cap A_1 \geqslant 1$, and hence $C/C_C(F_2)$ is a 2-group.

But we have

$$C_C(F_2) \leqslant C_G(F) = Z(F) ,$$

and

$$Z(F) \leqslant A \leqslant A_1 \leqslant Z(C) .$$

Therefore $C/Z(C)$ is a 2-group, and it follows that C is a normal nilpotent subgroup of G. Hence $C = C_G(A_1) \leqslant F$, and we see easily that $C_G(A_1) = A_1$.

We have $G/C_G(A_1)$ is a subgroup of $\mathrm{Aut}(A_1)$, an abelian group. Obviously $q \nmid |A_1|$, and therefore G contains a normal Hall q'-subgroup, N say. By Lemma 4.3, the group N acts half-transitively but not semi-regularly on $V^{\#}$, and by Theorem 1.16, we have V_N is irreducible. Also A_1 is a normal cyclic self-centralising subgroup of N, and hence, by Lemma 4.24, we have V_{A_1} is homogeneous. Clearly, then, V_A is homogeneous. In addition, we may apply Lemma 4.25 to obtain $G \leqslant \mathcal{T}(q^n)$.

Q.E.D.

We add to the list of assumptions given above as follows.

ASSUMPTIONS. In view of Lemma 4.27 above, we assume that F_2 is neither generalised quaternion of order greater than or equal to 16, cyclic, dihedral, nor semi-dihedral. By Lemma 4.1, if E denotes $\Omega_2(C_{F_2}(\Phi(F_2)))$ then $E \lhd G$ and E is of type $E(2,m)$ for some $m \neq 0$. Clearly $C_F(\Phi(F)) = AE$. In addition we assume that V_A is homogeneous.

NOTATION. Let H denote $C_G(A)$, and let r denote the dimension over $GF(q)$ of an irreducible constituent of V_A.

Our next two results are both from Section 6 of [13], namely [13] Lemmas 6.2 and 6.3. Although the assumptions of [13] Section 6 are slightly different from the assuptions we are working under (half-transitivity instead of q'-halftransitivity, and primitivity instead of merely the absence of non-cyclic abelian normal subgroups), it is easily

seen that these assumptions play no part in the proofs of [13] Lemmas 6.2 and 6.3. Therefore we refer to [13] Lemmas 6.2 and 6.3 for proofs of Lemmas 4.28 and 4.29 below.

LEMMA 4.28. ([13] Lemma 6.2). We have $O_2(H/AE) = 1$. Also H/AE acts faithfully on $E/Z(E)$ considered as a symplectic space of dimension $2m$ over $GF(2)$, whence $H/AE \leqslant Sp(2m,2)$.

LEMMA 4.29. ([13] Lemma 6.3). We have

(i) $H \leqslant GL(n/r,q^r)$ and r is the least integer such that $|A| \mid q^r - 1$,

(ii) G/H is cyclic of order dividing r,

(iii) $n = 2^m \omega r$ for some integer ω.

LEMMA 4.30. If $m = 1$ then we have one of the following:

(i) G acts half-transitively on $V^{\#}$;

(ii) $G \leqslant \mathcal{T}(q^n)$:

(iii) $q = 3$ and $2 \mid |G_x|$ for all $x \in V^{\#}$.

Proof. Assume that $m = 1$. Then, since we have assumed that E is not dihedral, either $E \cong Q_8$, or $E \cong Q_8 \curlyvee C_4$. Assume that G does not act half-transitively on $V^{\#}$ and that $G \not\leqslant \mathcal{T}(q^n)$. We shall show that if $q = 3$ then $2 \mid |G_x|$ for all $x \in V^{\#}$, and that if $q \neq 3$ then G does not exist.

Assume that $q = 3$. If $E \cong Q_8$ then, clearly, we have $F = E \times B$, where, in the notation introduced earlier, $B = O_{2'}(F)$, a cyclic group of odd order. In this case we have $A = Z(F)$ and, since we have assumed that V_A is homogeneous and that $G \not\leqslant \mathcal{T}(q^n)$, Lemma 4.25(ii) yields $p = 2$ or 3. But $p \neq q$ and $q = 3$, and therefore $2 \mid |G_x|$ for all $x \in V^{\#}$. If $E \cong Q_8 \curlyvee C_4$ then E does not act semi-regularly on $V^{\#}$, and hence there exists $y \in V^{\#}$ such that $E_y > 1$. Therefore, in this case, by q'-halftransitivity, we have $2 \mid |G_x|$ for all $x \in V^{\#}$. Hence if $q = 3$ then $2 \mid |G_x|$ for all $x \in V^{\#}$.

Now suppose, if possible, that $q \neq 3$. Clearly $q \nmid |AE|$, and, by Lemma 4.28, $H/AE \leqslant Sp(2,2) \cong S_3$. Since $q \neq 2,3$, it follows that $q \nmid |H|$. By Lemma 4.29 the group G/H is cyclic, and therefore G contains a normal Hall q'-subgroup, N say. Hence, by Lemma 4.3, the group N acts half-transitively but not semi-regularly on $V^{\#}$, and, by Theorem 1.16, V_N is irreducible. Let t denote the common size of all the N-orbits in $V^{\#}$. We have assumed that G does not act half-transitively on $V^{\#}$, whence $q \mid |G/N|$, and we see easily that there exists a G-orbit in $V^{\#}$ with size at least qt. Thus

$$qt \leqslant |V^{\#}| = q^n - 1 . \qquad (1)$$

As remarked above, either $E \cong Q_8$, or $E \cong Q_8 \curlyvee C_4$. Suppose that $E \cong Q_8$. Then, as also remarked above, $F = F(G) = E \times B$. But $F = F(N)$, and we can apply Theorem 1.16 to obtain the possibilities for N. Clearly $N \not\leqslant \mathcal{T}_0(q^{n/2})$ since $\mathcal{T}_0(q^{n/2})$ contains a normal subgroup isomorphic to $C_2 \times C_2$ whereas $O_2(N) = E \cong Q_8$. Therefore either $N \leqslant \mathcal{T}(q^n)$, or N is one of the cases (c_1), (c_2), (d_1), (d_2). But it is easily checked that if N is one of the cases (c_1), (c_2), (d_1), (d_2), then (1) does not hold, and hence $N \leqslant \mathcal{T}(q^n)$. It follows that N is metacyclic. Now $F(N) = F = E \times B$ where $E \cong Q_8$ and B is cyclic of odd order, and thus, by Lemma 4.23, there exists $T \lhd N$ such that $|F : T| = 2$ and $C_N(T) = T$. By Lemma 4.24 we have V_T is homogeneous. It is easily seen that there exist exactly three cyclic subgroups of G of index 2 in F. We have $|G/N|$ is a power of q where $q \neq 2,3$ and $N_G(T) \geqslant N$. Clearly, then, $N_G(T) = G$ and hence $T \lhd G$. If $C_G(T) = T$ then Lemma 4.25(i) yields $G \leqslant \mathcal{T}(q^n)$, a contradiction. Hence $C_G(T) > T$, and therefore, since $C_G(T) \cap N = C_N(T) = T$, we have

$$1 < C_G(T)/T \cong C_G(T)N/N \leqslant G/N.$$

Thus $q \mid |C_G(T)|$, and we deduce that there exists $g \in C_G(T)$ such that $|g| = q$. Since $G/C_G(E)$ is isomorphic to a subgroup of $Aut(Q_8) \cong S_4$, we have

$|G/C_G(E)| \mid 24$, and it follows that $g \in C_G(E)$. But then $g \in C_G(F) = Z(F) = A$, whence $q \mid |A|$ which is clearly impossible. We conclude that $E \not\cong Q_8$.

Finally suppose that $E \cong Q_8 \curlyvee C_4$. Clearly $N \not\leq \mathcal{T}(q^n)$ since E is not metacyclic. Therefore, by Theorem 1.16, we have $N \cong \mathcal{T}_0(q^{n/2})$ or N is one of the cases (b_1), (b_2), (e_1). But it is easily checked that if N is one of the cases (b_1), (b_2), (e_1) then (1) does not hold, and hence $N \cong \mathcal{T}_0(q^{n/2})$. If $q^{n/2} - 1$ is not a power of 2 then $O_2(\mathcal{T}_0(q^{n/2}))$ is abelian. But $E \leq O_2(N)$, and it follows that $q^{n/2} - 1$ is a power of 2. Thus either $n = 2$ or $q^n = 3^4$. But we have assumed that $q \neq 3$, and hence $n = 2$. We deduce that t, the size of an N-orbit in V^*, is exactly $2(q^{n/2} - 1) = 2(q - 1)$, giving

$$qt = 2q(q - 1) > (q + 1)(q - 1) = q^2 - 1$$

which contradicts (1). Therefore $E \not\cong Q_8 \curlyvee C_4$.

Q.E.D.

ASSUMPTIONS. From this point until the end of Lemma 4.41, we work under the assumption that $m = 1$. In addition we shall assume that G does not act half-transitively on V^*, and that $G \not\leq \mathcal{T}(q^n)$. Then Lemma 4.30 implies that $q = 3$ and $2 \mid |G_x|$ for all $x \in V^*$.

LEMMA 4.31. <u>We must have</u> $3 \mid |H/AE|$.

<u>Proof</u>. Suppose that $3 \nmid |H/AE|$. Then, since $H/AE \leq Sp(2,2) \cong S_3$ and $O_2(H/AE) = 1$ by Lemma 4.28, we must have $H = AE$. Now $3 \nmid |AE|$ and G/H is cyclic. Therefore G contains a normal Hall 3'-subgroup, N say. By Lemma 4.3 the group N acts half-transitively but not semi-regularly on V^*.

Suppose that $N \leq \mathcal{T}(3^n)$. Then N is metacyclic, and hence, since we have assumed that E is not dihedral, $E \cong Q_8$. It follows that $F = F(N) = E \times B$, and thus, by Lemma 4.23, $i(N) = \emptyset$. But $2 \mid |G_x|$ for all $x \in V^*$, and we deduce that $i(N) \neq \emptyset$, a contradiction. Therefore $N \not\leq \mathcal{T}(3^n)$.

Suppose that $N \cong \mathcal{T}_0(3^{n/2})$. If $\mathcal{T}_0(3^{n/2})$ is not a 2-group then $O_2(\mathcal{T}_0(3^{n/2}))$ is abelian. Since $E \leqslant O_2(N)$ we see that N is a 2-group. Therefore A is a 2-group and $G/C_G(A) = G/H = G/AE$ is isomorphic to a subgroup of Aut(A), a 2-group. Thus $3 \nmid |G|$ and it follows that G acts half-transitively on $V^{\#}$, a contradiction. Hence $N \not\cong \mathcal{T}_0(3^{n/2})$.

Using Theorem 1.16 we conclude that n = 2 and N acts transitively on $V^{\#}$. Hence G acts transitively on $V^{\#}$, a contradiction. Therefore we were incorrect in supposing that $3 \nmid |H/AE|$, whence $3 \mid |H/AE|$.

Q.E.D.

NOTATION. Since we have assumed that m = 1 and that E is not dihedral, we must have $E \cong Q_8$, or $E \cong Q_8 \curlyvee C_4$. In either case E contains a characteristic subgroup isomorphic to Q_8. Let Q denote such a subgroup. Then $Q \lhd G$ and $Q \cong Q_8$. Also $Q \leqslant E$ and, clearly, AE = AQ. Let C denote $C_G(Q)$. Obviously $C \lhd G$, and $A \leqslant C$.

LEMMA 4.32. <u>The group</u> C/A <u>is cyclic of order dividing</u> r, <u>and if</u> $2 \mid |H/AE|$ <u>then</u> G = HC <u>and</u> G/A = H/A × C/A.

<u>Proof</u>. We shall show that $H \cap C = A$. We have $H \cap C = C_G(A) \cap C_G(Q) = C_G(AQ)$. Let R denote $C_G(AQ)$. Then, since $|F_2 : F_2 \cap AQ| \leqslant 2$, we see that R stabilises the chain

$$F_2 \geqslant F_2 \cap AQ \geqslant 1,$$

whence $R/C_R(F_2)$ is a 2-group. But

$$C_R(F_2) \leqslant C_G(F) = Z(F) \leqslant A,$$

and $A \leqslant Z(R)$. Hence R/Z(R) is a 2-group, and it follows that R is a normal nilpotent subgroup of G. Therefore $R \leqslant F$, and we see easily that R = A. Thus $H \cap C = C_G(AQ) = R = A$.

We have

$$C/A = C/H \cap C \cong CH/H \leqslant G/H,$$

and, by Lemma 4.29, G/H is cyclic of order dividing r. Hence C/A is cyclic of order dividing r.

Assume that $2 \mid |H/AE|$. By Lemma 4.31 we have $3 \mid |H/AE|$ and, by Lemma 4.28, we have H/AE is isomorphic to a subgroup of S_3. Therefore $|H/AE| = 6$, and it follows that $|H/A| = 24$. Also G/C is isomorphic to a subgroup of $\mathrm{Aut}(Q) \cong S_4$, and hence $|G/C| \leqslant 24$. Thus

$$24 \geqslant |G/C| \geqslant |HC/C| = |H/H \cap C| = |H/A| = 24,$$

whence G = HC. Obviously, then, G/A = H/A × C/A.

Q.E.D.

LEMMA 4.33. <u>We must have</u> $|A| > 2$ <u>and</u> $r \neq 1$.

<u>Proof.</u> Suppose that $|A| = 2$. Then $H = C_G(A) = G$, and clearly $Q = F = F(G)$. Since H/AE = G/Q is isomorphic to a subgroup of S_3 and $3 \mid |G/Q|$, there exists $S \lhd G$ such that $Q \lhd S$ and $|S : Q| = 3$. Clearly $S \cong SL(2,3)$. Now $2 \mid |G_x|$ for all $x \in V^*$, and Q acts semi-regularly on V^*. Hence there exists $g \in i(G)$ such that $g \notin S$. Therefore $|G| = 48$. By Lemma 4.28 the group G/Q acts faithfully on E/Z(E), and it follows that g acts non-trivially on Q/Z(Q). Thus, by Lemma 3.15, we have $G \cong GL(2,3)$, and, by Theorem 3.13, n = 2 and G acts transitively on V^*, a contradiction. We conclude that $|A| \neq 2$, and then, since $|A| \geqslant Z(E) > 1$, and $|A| \mid 3^r - 1$, it follows that $|A| > 2$ and $r \neq 1$.

Q.E.D.

LEMMA 4.34. <u>If</u> n = 4 <u>then</u> $G \cong GL(2,3) \curlyvee C_4$.

<u>Proof</u>. By Lemma 4.29(iii) we have $4 = n = 2\omega r$ for some integer ω, and

hence $r = 1$ or 2. But, by Lemma 4.33, we have $r \neq 1$, whence $r = 2$. Also by Lemma 4.33 we have $|A| > 2$, and therefore, since $|A| \mid 3^2 - 1$, we see that $|A| = 4$ or 8. Thus $E \cong Q_8 \curlyvee C_4$, and $F_2 = F$. Clearly all involutions of AE are contained in E, and therefore Lemma 4.2(ii) implies that there exists $y \in V^*$ such that $G_y \cap AE = (AE)_y = 1$.

By Lemma 4.28 the group H/AE is isomorphic to a subgroup of S_3, and, by Lemma 4.29(ii), the group G/H is cyclic of order dividing $r = 2$. By Lemma 4.26 we have $3 \mid |H/AE|$, and hence $|G/AE| = 3$, 6, or 12. Now $G_y \cong G_yAE/AE \leqslant G/AE$, and therefore, since $2 \mid |G_y|$, we see that $|G_y| = 2^\alpha . 3^\beta$ where $2^\alpha \leqslant |G/AE|_2$ so that $\alpha = 1$ or 2 and $\beta = 0$ or 1. Thus, by 3'-halftransitivity, $|G_x| = 2^\alpha$ or $2^\alpha . 3$ for all $x \in V^*$.

Since G does not act half-transitively on V^*, there exists $v \in V^*$ such that $|G_v| = 2^\alpha$. Hence

$$80 = 3^4 - 1 = |V^*| \geqslant |G : G_v| = |G|/2^\alpha = (|G/AE|/2^\alpha)|AE| =$$

$$(|G/AE|_2/2^\alpha).3.|E|.|AE/E| = 48|AE/E|(|G/AE|_2/2^\alpha).$$

It follows that $|AE/E| = |G/AE|_2/2^\alpha = 1$, and hence $AE = E$, giving $|A| = 4$. Therefore $E = F_2 = F$, whence $O_2(G/E) = 1$. Thus $|G/E| \neq 12$. Since $|G/E|_2 = 2^\alpha$ and $\alpha \geqslant 1$, we see that $2 \mid |G/E|$, and hence $G/E \cong S_3$. Therefore $\alpha = 1$ and $|G_x| = 2$ or 6 for all $x \in V^*$. Also $|G| = 96$.

We have $G_y \cap E = 1$ and $2 \mid |G_y|$. Hence there exists $g \in G \setminus E$ such that $g^2 = 1$. Suppose that $g \notin C_G(A) = H$. Then $|Z(G)| = 2$, and Lemma 4.22 yields that there exists $x \in V^*$ such that $4 \mid |G_x|$, a contradiction. Hence $g \in C_G(A)$, and we see easily that $A = Z(G)$.

Let K be a Sylow 3-subgroup of G. Then $|K| = 3$ and, clearly, $QK \cong SL(2,3)$. Obviously $QK \cap A = Z(QK) = Z(Q)$ and hence $EK = QKA \cong SL(2,3) \curlyvee C_4$. Also $EK \lhd G$. It is easily seen that $QK \lhd G$ and Lemma 4.28 implies that g acts non-trivially on $Q/Z(Q)$. Using Lemma 3.15 and writing $T = \langle QK, g \rangle$, we have $T \cong GL(2,3)$. Then, since $T \cap A = Z(T)$,

it follows that $G = TA \cong GL(2,3) \curlyvee C_4$.

Q.E.D.

EXAMPLE. We show that the case $G \cong GL(2,3) \curlyvee C_4$ does occur. That is, we show that if $G \cong GL(2,3) \curlyvee C_4$ then there exists a 4-dimensional irreducible $GF(3)G$-module, V, such that V is faithful for G and G acts 3'-half-transitively but not 3'-semiregularly on $V^{\#}$.

Assume that $G \cong GL(2,3) \curlyvee C_4$, and let A denote $Z(G) \cong C_4$. There exists $T \triangleleft G$ such that $T \cong GL(2,3)$ and $G = TA$ with $T \cap A = Z(T)$. If F denotes $F(G)$, then $F \cong Q_8 \curlyvee C_4$ and $G/F \cong S_3$. Let W be a 2-dimensional irreducible $GF(3)T$-module, faithful for T, (such a module exists since $T \cong GL(2,3)$), and write $V = W^G$. Clearly $\dim_{GF(3)} V = 4$, and it is easily seen that V is an irreducible $GF(3)G$-module which is faithful for G.

Since $A = Z(G)$ and $G = TA$ we have $V_T = V_1 \oplus V_2$ where V_1 and V_2 are T-isomorphic irreducible $GF(3)T$-modules, both faithful for T. By Lemma 3.13(iii), if $x \in V_i^{\#}$ then $T_x \cong S_3$, and, since obviously $G_x = T_x$, we have $G_x \cong S_3$ $(i = 1,2)$. Let $y \in V_i^{\#}$. Then $G_y \cong S_3$ and the size of the G-orbit containing y is exactly $|G : G_y| = |G|/|G_y| = 96/6 = 16$. This orbit is clearly $V_1^{\#} \cup V_2^{\#}$.

Since V_1 and V_2 are T-isomorphic, there exists $u \in V_2^{\#}$ such that $T_u = T_y$. Using the familiar argument we have $|G_{y+u} : G_y \cap G_u| \leq 2$ and hence $|G_{y+u}| = 6$ or 12. Suppose that $|G_{y+u}| = 12$. Then, since $G_{y+u} \geq T_y$ and $T_y \cap F = 1$, we must have $|G_{y+u} \cap F| = 2$. Obviously $G_{y+u} \cap F \triangleleft G_{y+u}$ and hence there exists an involution in $F \setminus A$ which is centralised by a Sylow 3-subgroup of G. However, from the structure of G it is easily seen that this is impossible, and we conclude that $|G_{y+u}| = 6$. Therefore the size of the G-orbit containing $y + u$ is exactly $96/6 = 16$.

Clearly there exists $y' \in V_1^{\#}$ such that $T_y \cap T_{y'} = 1$. Hence there exists $u' \in V_2^{\#}$ such that $T_y \cap T_{u'} = 1$. Since $|G_{y+u'} : G_y \cap G_{u'}| \leq 2$

we deduce that $|G_{y+u'}| \leqslant 2$, whence the size of the G-orbit containing $y + u'$ is 96 or 48. But $96 > 80 = 3^4 - 1 = |V^{\#}|$, and thus the size of the G-orbit containing $y + u'$ is exactly 48.

We have $48 + 16 + 16 = 80 = |V^{\#}|$, and hence G has exactly three orbits on $V^{\#}$, two of size 16 and one of size 48. Therefore G acts 3'-halftransitively but not 3'-semiregularly on $V^{\#}$.

LEMMA 4.35. <u>If</u> $r = 2$ <u>then</u> $n = 4$ <u>and</u> $G \cong GL(2,3) \curlyvee C_4$.

<u>Proof</u>. Assume that $r = 2$. Then $|A| \mid 3^2 - 1$ and, since $|A| > 2$ by Lemma 4.33, we have $|A| = 4$ or 8, whence $F_2 = F$ and $E \cong Q_8 \curlyvee C_4$. By Lemma 4.29(iii) we have $n = 2^m \omega r$ for some integer ω and therefore, since $m = 1$ and $r = 2$, it follows that $4 \mid n$. If $n = 4$ then $G \cong GL(2,3) \curlyvee C_4$ by Lemma 4.34. Hence, to prove the lemma, it will be sufficient to show that if $n > 4$ then G does not exist.

Suppose that $n > 4$. Since $4 \mid n$ we must have $n \geqslant 8$. By Lemma 4.28 we have $H/AE \leqslant Sp(2,2) \cong S_3$, and by Lemma 4.29 we have G/H is cyclic of order dividing $r = 2$. Also $3 \mid |H/AE|$ by Lemma 4.31 and hence, if K denotes a Sylow 3-subgroup of G, then $|K| = 3$ and $K \leqslant H$. Obviously K centralises A and K acts non-trivially on $Q/Z(Q)$, whence $QK \cong SL(2,3)$. Write $S = QKA = AEK$. We have $K \cong S/AE = O_3(H/AE)$, giving $S \lhd G$. Therefore, since $Q \lhd G$ and $QK \lhd S$, we see easily that $QK \lhd G$. Clearly $|H : S| \leqslant 2$.

Assume that $h \in H \backslash AE$ such that $h^2 = 1$. We must have $H = \langle S, h \rangle$. Write $T = \langle QK, h \rangle$. Then $|T| = 48$ and $QK \leqslant T$ with $QK \cong SL(2,3)$. Using Lemma 4.28 we see that h acts non-trivially on $Q/Z(Q)$, whence, by Lemma 3.15, $T \cong GL(2,3)$. We have $A = Z(H)$ and $H = TA$ with $T \cap A = Z(T)$. Therefore $H \cong GL(2,3) \curlyvee C_4$ or $GL(2,3) \curlyvee C_8$. Also $T \lhd H \lhd G$, and it follows that V_T is completely reducible. Since $soc(T) = Z(Q)$ and $Z(Q)$ acts semi-regularly on $V^{\#}$, we have

$$V_T = V_1 \oplus V_2 \oplus \ldots \oplus V_c$$

where, for $1 \leqslant i \leqslant c$, V_i is an irreducible GF(3)T-module, faithful for T. By Theorem 3.13 we see that $\dim V_i = 2$ for $1 \leqslant i \leqslant c$, and hence $c = n/2$. Clearly, if h is as above, then $\dim C_{V_i}(h) = 1$ for $1 \leqslant i \leqslant n/2$, whence $\dim C_V(h) = n/2$.

Now assume that $h \in AE \setminus A$ such that $h^2 = 1$. Clearly h is an involution in $E \setminus Z(E)$ and hence, by Lemma 4.2(i), $\dim C_V(h) = n/2$.

Thus we have shown that

$$\dim C_V(h) = n/2, \qquad (1).$$

for all $h \in i(H)$. Now if $i(H) \subseteq AE$ then $i(H) \subseteq E \cong Q_8 \rtimes C_4$, whence $|i(H)| = 6$. On the other hand, if $i(H) \not\subseteq AE$, then as demonstrated above, we have $H \cong GL(2,3) \rtimes C_4$ or $GL(2,3) \rtimes C_8$. In this case it is easily checked that $|i(H)| = 18$. Therefore we conclude that

$$|i(H)| \leqslant 18. \qquad (2).$$

Suppose that $2 \mid |H_x|$ for all $x \in V$. Then it follows that

$$V^* = \bigcup_{h \in i(H)} (C_V(h))^*.$$

Therefore, using (1) and (2), we deduce that

$$3^n - 1 \leqslant 18(3^{n/2} - 1),$$

whence $3^{n/2} + 1 \leqslant 18$, contradicting $n \geqslant 8$. Hence there exists $y \in V^*$ such that $2 \nmid |H_y|$. Now $2 \mid |G_y|$ since G does not act 3'-semiregularly. Also $|G/H| \leqslant 2$, and we conclude that $|G_y|_2 = 2$. Thus, by 3'-halftransitivity, we have

$$|G_x| = 2, \text{ or } 6 \qquad (3).$$

for all $x \in V^{\#}$. In addition, since $H = C_G(A)$ and $G_y \cap H = 1$, we have $|G : H| = 2$ and A is not central in G.

Since $|A| \leqslant 8$ and $|F : AE| \leqslant 2$, it follows that $|F| \leqslant 64$. Let $f \in i(E)$. Then $f \in i(H)$ and hence, by (1), $\dim C_V(f) = n/2$. Let $f' \in i(F)$ such that $f' \neq f$. If $x \in C_V(f) \cap C_V(f')$, then $\langle f, f' \rangle \leqslant F_x$, whence $4 \mid |F_x|$ and $4 \mid |G_x|$. Therefore, since $|G_x|_2 = 2$ for all $x \in V^{\#}$, we have $C_V(f)^{\#} \cap C_V(f')^{\#} = \emptyset$, and thus

$$\dim C_V(f') \leqslant n/2 \qquad (4).$$

for all $f' \in i(F)$.

Write $R = C_G(Q/Z(Q))$. Since any Sylow 3-subgroup acts faithfully on $Q/Z(Q)$ we must have $3 \nmid |R|$. Therefore R is a 2-group and $R \leqslant F_2 = F$.

Suppose that $g \in i(G)$ such that $g \notin F$. Then $g \notin R$ and hence, writing $L = \langle QK, g \rangle$, we have $L \cong GL(2,3)$ by Lemma 3.15. Let A_o denote the subgroup of A of order 4. Clearly $A_o \lhd G$, and $E = QA_o$. Let N denote the group $LA_o = LE$. We have $L \cap A_o = Z(L) \cong C_2$, and therefore

$$|N| = |L| . |A_o| / |L \cap A_o| = 48.4/2 = 96.$$

Also

$$N/E = LE/E \cong L/E \cap L = L/Q \cong S_3.$$

Thus, since $F(N) = E$, we have $N/F(N) \cong S_3$.

Suppose that g does not centralise $A_o = Z(F(N))$. Let W be an irreducible submodule of V_N. We have $\mathrm{soc}(N) = Z(Q)$, and $Z(Q)$ acts semi-regularly on $V^{\#}$. Hence W is faithful for N and, by Lemma 4.22, there exists $x \in W^{\#}$ such that $4 \mid |N_x|$. Therefore $4 \mid |G_x|$, contradicting (3) above. Thus g centralises A_o.

Write $A = \langle a \rangle$. Since g centralises A_o, the subgroup of A of order 4, we see that either g centralises A, or $|A| = 8$ and $a^g = a^5$.

Let U be an irreducible constituent of V_A, and let ϕ be the representation of A afforded by U. Then, if $|A| = 8$ and $a^g = a^5$, the A-module Ug affords the representation ϕ' of A where $\phi'(a) = \phi(a^5)$. But the representations ϕ and ϕ' are not equivalent (since dimU = 2 and, as shown in the proof of Lemma 3.10, there is no element of GL(2,3) of order 8 which is conjugate in GL(2,3) to its own fifth power), contradicting the assumption that V_A is homogeneous. We conclude that g centralises A, whence $g \in C_G(A) = H$.

Therefore we have shown that if $g \in i(G)$ then either $g \in i(H)$ or $g \in i(F)$. Hence, using (1) and (4), we have $\dim C_V(g) \leqslant n/2$ for all $g \in i(G)$. Also $i(H) \cap i(F) = i(E)$, whence $|i(H) \cap i(F)| = 6$.
Therefore, using (2) and the fact that $|F| \leqslant 64$, we have

$$|i(G)| = |i(H) \cup i(F)| = |i(H)| + |i(F)| - 6 \leqslant |i(H)| + |F| - 6 \leqslant 76.$$

But, clearly, since $2 \mid |G_x|$ for all $x \in V^{\#}$, we have

$$V^{\#} = \bigcup_{g \in i(G)} (C_V(g))^{\#},$$

and hence

$$3^n - 1 \leqslant 76(3^{n/2} - 1)$$

which yields $3^{n/2} + 1 \leqslant 76$, the final contradiction since $n \geqslant 8$.

Q.E.D.

We break off from this sequence of results classifying the possibilities for G in order to describe, and fix a symbol, Σ, to represent a particular soluble group of order 480. Subsequently we shall show (Lemma 4.41) that Σ occurs as a possibility for G.

Recall that, as noted in Chapter 3, there exist elements a, b, c, d, of GL(2,3) such that

$$GL(2,3) = \langle a,b,c,d: a^4 = b^4 = c^3 = d^2 = 1,\ [a,b] = a^2 = b^2$$
$$c^{-1}ac = ab,\ c^{-1}bc = a,\ dad = b,\ dbd = a,\ dcd = ac^2 \rangle .$$

DEFINITION 4.36. The group $Z(GL(2,3^2))$ is cyclic of order 8, consisting of scalar matrices. Let $z \in Z(GL(2,3^2))$ such that $|z| = 4$. Now $GL(2,3) \leqslant GL(2,3^2)$, and there exists $d \in GL(2,3)$ such that $d^2 = 1$ and $GL(2,3) = \langle SL(2,3),d \rangle$. Write $e = zd$. Then, clearly $|e| = 4$ and $e^2 = z^2 \in Z(GL(2,3))$. We define a subgroup, Σ_1, of $GL(2,3^2)$ by

$$\Sigma_1 = \langle SL(2,3),e \rangle .$$

Obviously $|\Sigma_1| = 48$ and there exist elements a, b, c, of $SL(2,3)$ such that

$$\Sigma_1 = \langle a,b,c,e: a^4 = b^4 = c^3 = e^4 = 1,\ [a,b] = a^2 = b^2 = e^2,$$
$$c^{-1}ac = ab,\ c^{-1}bc = a,\ e^{-1}ae = b,\ e^{-1}be = a,\ e^{-1}ce = ac^2 \rangle .$$

It is easily seen that the dihedral group of order 10 has a faithful, irreducible representation of degree 2 over $GF(3^2)$, and hence there exists a subgroup, D, of $GL(2,3^2)$ such that D is dihedral of order 10. Let S denote the unique Sylow 5-subgroup of D and let f be an involution in D. With z as above and writing $t = zf$, we define a subgroup, Σ_2, of $GL(2,3^2)$ by

$$\Sigma_2 = \langle S,t \rangle .$$

Obviously $|\Sigma_2| = 20$ and, if $S = \langle s \rangle$, then

$$\Sigma_2 = \langle s,t : s^5 = t^4 = 1,\ t^{-1}st = s^{-1} \rangle .$$

Noting that $Z(\Sigma_1) = \langle z^2 \rangle = Z(\Sigma_2)$, we form a central product of the groups Σ_1, Σ_2 in the obvious way and define

$$\Sigma = \Sigma_1 \curlyvee \Sigma_2.$$

We have $|\Sigma| = |\Sigma_1||\Sigma_2|/2 = 480$, and, clearly, Σ is soluble.

LEMMA 4.37. <u>If</u> $r > 2$ <u>then</u>

(i) $2 \mid |G/H|$;

(ii) $r = 4$, $n = 8$;

(iii) $H/AE \cong S_3$, $G/A \cong H/A \times C/A$;

(iv) $|G_x|_{3'} = 2$ for all $x \in V^{\#}$;

(v) G <u>contains no subgroup isomorphic to</u> $C_2 \times C_2 \times C_2$;

(vi) $|A| = 10$ <u>or</u> 20 <u>and if</u> $|A| = 20$ <u>then</u> $|G/H| = 2$.

<u>Proof</u>. Assume that $r > 2$. Recall that $q = 3$ and $2 \mid |G_x|$ for all $x \in V^{\#}$ by Lemma 4.30 since we have assumed that $G \not\leq \mathcal{T}(q^n)$ and that G does not act half-transitively. Since, by assumption, V_A is homogeneous we are in a position to apply Lemma 4.26 with $p = 2$. Let λ_1, λ_2 be defined in the statement of Lemma 4.26. We remark that Lemma 4.29(iii) implies that $k = n/r \geqslant 2$ and therefore either (ii) or (iii) in Lemma 4.26 must hold.

We first obtain an upper bound for λ_1. Clearly λ_1 is at most the number of involutions in the group H/A. Now $C_2 \times C_2 \cong AE/A \lhd H/A$, and by Lemma 4.28, we have $H/AE \leqslant Sp(2,2) \cong S_3$, whence $|H/A| \leqslant 24$. Also by Lemma 4.28 the group H/AE acts faithfully on AE/A and hence, if S/A is a Sylow 2-subgroup of H/S, we see that either $S/A \cong D_8$ or $S/A = AE/A$. Thus S/A contains at most 5 involutions. Clearly H/A has at most 3 Sylow 2-subgroups and any two such subgroups intersect in AE/A, which contains exactly 3 involutions. Hence

$$\lambda_1 \leqslant (\text{number of involutions in } H/A) \leqslant 3(5-3) + 3 = 9. \qquad (1)$$

Suppose that $2 \nmid |G/H|$. Then $\lambda_2 = 0$ and Lemma 4.26(ii) and (iii) both yield

$$3^r < 2.9 = 18,$$

contradicting our assumption that $r > 2$. Therefore $2 \mid |G/H|$, and since, by Lemma 4.29(ii), the group G/H is cyclic of order dividing r, we deduce that $2 \mid r$. Thus $r \geqslant 4$.

We have $|H/A| \leqslant 24$ and G/H is cyclic. Clearly then $\lambda_2 \leqslant 24$. If $k = n/r > 2$ then Lemma 4.26(iii) gives

$$3^r < 2(9 + 24) = 66,$$

contradicting $r \geqslant 4$. Hence $k = 2$, and Lemma 4.26(ii) gives

$$3^r + 1 \leqslant 18 + 24(3^{r/2} + 1),$$

whence $3^{r/2} \leqslant 41/3^{r/2} + 24$, and we deduce that $r \leqslant 4$. Therefore we have $r = 4$ and, since $k = n/r = 2$, it follows that $n = 8$. Hence we have proved (i) and (ii).

We next show that $H/AE \cong S_3$. We have $H/AE \leqslant Sp(2,2) \cong S_3$ and, by Lemma 4.31, we also have $3 \mid |H/AE|$. Hence if we can show $2 \mid |H/AE|$ then it will follow that $H/AE \cong S_3$. Suppose that $2 \nmid |H/AE|$. Then $H/AE \cong C_3$ and AE/A is the unique Sylow 2-subgroup of H/A, whence $\lambda_1 \leqslant 3$. To obtain an upper bound for λ_2 we need to count the involutions of G/A that are not in H/A. The group G/H is cyclic of order 2 or 4, and hence there exists a unique subgroup, N/H say, of G/H such that $|N/H| = 2$. Clearly N/A contains all involutions of G/A. We have $|N/AE| = 6$ and $C_3 \cong H/AE$ acts faithfully on AE/A. If N/AE acts faithfully on AE/A, then, using the same argument used to establish (1) above, we see that the group N/A contains at most 9 involutions, 3 of which are contained in AE/A. Hence, if N/AE acts faithfully on AE/A, we have $\lambda_2 \leqslant 9 - 3 = 6$. On the other hand, if N/AE does not act faithfully on AE/A, then N/A contains a normal Sylow 2-subgroup which has order 8, and we see easily that $\lambda_2 \leqslant 4$. We conclude that in either case $\lambda_2 \leqslant 6$, and by Lemma 4.26(ii) we have

$$3^4 + 1 \leqslant 6 + 6(3^2 + 1),$$

whence $82 \leqslant 66$, a contradiction. Therefore $2 \mid |H/AE|$ and $H/AE \cong S_3$.

By Lemma 4.27 we have $G/A = H/A \times C/A$ where $C = C_G(Q)$, and C/A is cyclic of order dividing $r = 4$. Let $AE \leqslant L \leqslant H$ such that $|L/AE| = 3$. Obviously $L \lhd G$. Let M be the subgroup of G such that $M/A = L/A \times C/A$. Clearly $M \lhd G$ and $|G : M| = 2$. Suppose that $4 \mid |G_x|$ for all $x \in V^{\#}$. Then, since $M_x = G_x \cap M$, we have $2 \mid |M_x|$ for all $x \in V^{\#}$. It is easily seen that V_M is irreducible, and hence we can apply Lemma 4.26 to the group M. Obviously $\lambda_1 \leqslant 3$, $\lambda_2 \leqslant 4$, and since $k = n/r = 2$, Lemma 4.26(ii) gives

$$3^4 + 1 \leqslant 6 + 4(3^2 + 1).$$

Hence $82 \leqslant 46$, a contradiction. Therefore $|G_x|_2 = 2$ for all $x \in V^{\#}$. Since A acts semi-regularly on $V^{\#}$ and since $|G/A| = 3.2^{\alpha}$ for some α, we have $|G_x|_{3'} = |G_x|_2 = 2$ for all $x \in V^{\#}$.

Suppose that $X \leqslant G$ such that $X \cong C_2 \times C_2 \times C_2$. Then, clearly, there exists $y \in V^{\#}$ such that $4 \mid |X_y|$. Hence $4 \mid |G_y|$, a contradiction. Therefore G contains no subgroup isomorphic to $C_2 \times C_2 \times C_2$.

All that remains to prove is that $|A| = 10$ or 20, and that if $|A| = 20$ then $|G/H| = 2$. Let $y \in V^{\#}$. Since $|H/AE|_2 = 2$ and $|G/H| = 2$ or 4 we have

$$|G : G_y|_2 = |G|_2/2 = (|G/H| . |H/AE|_2 . |AE|_2)/2 = |G/H| . |AE|_2 .$$

By $3'$-halftransitivity we have $(|G/H| . |AE|_2)$ divides $|V^{\#}| = 3^8 - 1$, and hence

$$|G/H| . |AE|_2 \leqslant 32. \qquad (2)$$

We have $2 \mid |G/H|$, and hence $|AE|_2 \leqslant 16$. Clearly, then, $|A|_2 \leqslant 4$. Now r is the least integer such that $|A| \mid 3^r - 1$, and we have shown that $r = 4$. Therefore $5 \mid |A|$ and it follows that $|A| = 10$ or 20. If $|A| = 20$ then $|AE|_2 = 16$ and (2) implies that $|G/H| = 2$.

Q.E.D.

LEMMA 4.38. <u>If</u> $r > 2$ <u>then</u> $|A| = 10$.

<u>Proof</u>. Assume that $r > 2$. Then (i) - (vi) of Lemma 4.37 must hold. Write $D = C_G(Q/Z(Q))$. Then $C = C_G(Q) \leqslant D$. Now $G/C \cong H/A$ and, by Lemma 4.28, the group H/AE acts faithfully on $E/Z(E)$ and thus faithfully on $Q/Z(Q)$. Hence we see that

$$D/A = C_G(Q/Z(Q))/A = AE/A \times C/A.$$

We show that the case $|A| = 20$ does not occur. Suppose that $|A| = 20$. Then $E \cong Q_8 \curlyvee C_4$ and, by Lemma 4.37(vi), we have $|G/H| = 2$. Hence $|C/A| = 2$ and it follows that, if R is a Sylow 2-subgroup of C, then $|R| = 8$. By Lemma 4.37(v) we have $R \not\cong C_2 \times C_2 \times C_2$.

Suppose that $R \cong C_4 \times C_2$. Then, since $R \cap A$ is a cyclic group of order 4, there exists an involution, g say, such that $g \in C \setminus A$. Clearly $g \in C_G(E)$. But E contains a subgroup, Y say, such that $Y \cong C_2 \times C_2$, and we see that $\langle Y, g\rangle \cong C_2 \times C_2 \times C_2$, contradicting Lemma 4.37(v). Hence $R \not\cong C_4 \times C_2$.

Suppose that R is cyclic. We have $R \leqslant C = C_G(Q)$ and $R \cap Q = Z(Q)$, whence $QR \cong Q_8 \curlyvee C_8$. We see easily that QR is a Sylow 2-subgroup of D. Also $E \leqslant QR$ and $E \cong Q_8 \curlyvee C_4$. Clearly all involutions of QR are contained in E, and it follows that all involutions of D are contained in $E \leqslant H$. From the definitions of λ_1, λ_2, we see that only those involutions, gA, of the group $G/A = H/A \times C/A$, such that the coset gA contains an involution of G contribute to a count of λ_1 or λ_2. Thus no involution of the group $D/A = AE/A \times C/A$ contributes to a count of λ_2. By Lemma 4.37 (1), the group H/A contains at most 9 involutions. Therefore we see easily that $\lambda_1 \leqslant 9$, $\lambda_2 \leqslant 6$, and Lemma 4.26(ii) yields

$$3^4 + 1 \leqslant 18 + 6(3^2 + 1),$$

giving $82 \leqslant 78$, a contradiction. Hence R is not cyclic.

We deduce that R is a non-abelian group of order 8, so that $R \cong Q_8$ or D_8. Let A_o denote the subgroup of A of order 4. Clearly $A_o \lhd G$, and $QA_o = E$. Since R is non-abelian and $A_o \leqslant R$, we must have $H = C_G(A) = C_G(A_o)$. Suppose that there exists $g \in i(G)$ such that $g \notin H$, $g \notin D$. Let K be a Sylow 3-subgroup of G. Then $|K| = 3$ and it is easily checked that $EK \lhd G$. Clearly $QK \lhd G$ and $QK \cong SL(2,3)$. Writing $T_o = \langle QK, g\rangle$ and $T = \langle EK, g\rangle$, we have $|T_o| = 48$, $|T| = 96$. Now $g \notin D = C_G(Q/Z(Q))$ and so, by Lemma 3.15, it follows that $T_o \cong GL(2,3)$. We have $F(T) = E \cong Q_8 \curlyvee C_4$ and $A_o = Z(E) = Z(F(T))$. Since $g \notin H = C_G(A_o)$ we deduce that $|Z(T)| = 2$ and $g \in T \setminus C_T(Z(F(T)))$. Also

$$T/F(T) = T/E = T_oE/E \cong T_o/E \cap T_o = T_o/Q \cong S_3 .$$

Let W be a non-trivial irreducible submodule of V_T. Since $soc(T) = Z(Q) \leqslant A$ and A acts semi-regularly on $V^{\#}$, we must have that W is faithful for T, whence, by Lemma 4.22, there exists $y \in W^{\#}$ such that $4 \mid |T_y|$. Hence $4 \mid |G_y|$, contradicting Lemma 4.37(iv). We conclude that there exists no $g \in i(G)$ such that $g \notin H$, $g \notin D$. Hence if gA is an involution in the group G/A such that $gA \notin H/A$, $gA \notin D/A$, then the coset gA contains no involution of G and therefore cannot contribute to a count of λ_2. Thus we see easily that $\lambda_2 \leqslant 4$ and, using $\lambda_1 \leqslant 9$, Lemma 4.26(ii) gives a contradiction.

We conclude that $|A| \neq 20$ and so, by Lemma 4.37(vi) we must have $|A| = 10$.

Q.E.D.

LEMMA 4.39. <u>If</u> $r > 2$ <u>then a Sylow</u> 2-<u>subgroup of</u> C <u>is cyclic of order</u> 4 <u>or</u> 8.

<u>Proof</u>. Assume that $r > 2$. Then (i) - (vi) of Lemma 4.37 must hold, and, in addition, $|A| = 10$ by Lemma 4.38. Hence $E = Q \cong Q_8$. Let S denote the unique Sylow 5-subgroup of A. Then $S \lhd G$ and $F = F(G) = Q \times S$. Also

F acts semi-regularly on $V^{\#}$. In deriving $\lambda_1 \leqslant 9$ in Lemma 4.37(1) we allowed the three involutions of the group $AE/A = F/A$ to contribute to a count of λ_1. But, since F acts semi-regularly, this is clearly impossible and we deduce that

$$\lambda_1 \leqslant 6 . \tag{1}$$

Let R be a Sylow 2-subgroup of C. Clearly $C = AR$ and $R \cap A = Z(Q)$. We have

$$R/Z(Q) = R/R \cap A \cong RA/A = C/A,$$

and C/A is a cyclic group of order 2 or 4. Thus R is an abelian group of order 4 or 8 and R/Z(Q) is cyclic.

Suppose that R is not cyclic. Clearly, then, there exists a cylic subgroup, L_o say, of R such that $|L_o| \leqslant 4$ and $R = Z(Q) \times L_o$. We have $G/A = H/A \times C/A$ and $F = Q \times S \leqslant H$. Let D denote the subgroup of G such that $D/A = F/A \times C/A$. Now $Q \cap R = Z(Q)$ and hence $QR = Q \times L_o$. Clearly QR is a Sylow 2-subgroup of D, and therefore any Sylow 2-subgroup of D has the form $Q \times L$, for some cyclic subgroup, L, of C. It follows that all involutions of D are contained in C. Hence if gA is an involution in the group $D/A = F/A \times C/A$ such that $gA \notin C/A$, then the coset gA contains no involution of G and thus cannot contribute to a count of λ_2. Therefore, noting that C/A is cyclic and thus contains a unique involution, we see that λ_2 is at most one more than the number, α say, of involutions of G/A which are in neither H/A, nor D/A. Since $G/A = H/A \times C/A$ and, since, as in Lemma 4.37 (1), the group H/A contains at most 9 involutions, 3 of which are contained in F/A, we see that $\alpha = 6$ and

$$\lambda_2 \leqslant \alpha + 1 = 7. \tag{2}$$

If there is no involution in $H \backslash Z(Q)$ then obviously $\lambda_1 = 0$ and

Lemma 4.26(ii) yields

$$3^4 + 1 \leqslant 7(3^2 + 1),$$

giving $82 \leqslant 70$, a contradiction. Hence there exists $h \in H \backslash Z(Q)$ such that $h^2 = 1$. Clearly C contains exactly 5 Sylow 2-subgroups, and h permutes these subgroups by conjugation. It follows that h normalises some Sylow 2-subgroup, R_o say, of C. As shown above we must have $R_o \cong C_2 \times C_2$ or $C_2 \times C_4$, and hence, writing $Y = \Omega_1(R_o)$, we have $Y \cong C_2 \times C_2$ and h normalises Y. Let $X = \langle Y,h \rangle$. Then $|X| = 8$. If h centralises Y then $X \cong C_2 \times C_2 \times C_2$, contradicting Lemma 4.37(v). Hence h does not centralise Y. Obviously $Z(Q) \leqslant Y$ and h centralises Z(Q). Thus, if $Z(Q) = \langle z \rangle$ and $g \in Y \backslash Z(Q)$, then $hgh = zg$. Therefore $(hg)^2 = hghg = zg.g = z \in A$, whence hgA is an involution in G/A. Since $R_o \cap H = Z(Q)$ we must have $g \notin H$. As a result $hgA \notin H/A$. Also $h \in H \backslash Q$ and thus $hgA \notin D/A$. Therefore the involution hgA is one of those involutions of G/A which contribute to a count of α.

If the coset hgA does not contain an involution of G then hgA cannot contribute to a count of λ_2, whence $\lambda_2 \leqslant 6$. But we have $\lambda_1 \leqslant 6$ from (1), and Lemma 4.26(ii) yields

$$3^4 + 1 \leqslant 12 + 6(3^2 + 1),$$

giving $82 \leqslant 72$, a contradiction. Thus the coset hgA contains an involution of G and so there exists $d \in A$ such that $(hgd)^2 = 1$.

Now $g \notin H = C_G(A)$ and therefore conjugation by g is an automorphism of A of order 2. But a cyclic group of order 10 has a unique automorphism of order 2, namely the automorphism that acts by inverting each element. Hence $gdg = d^{-1}$ and, using the fact that $h \in H = C_G(A)$, we see that

$$(hgd)^2 = hgdhgd = hghdgd = zgdgd = zd^{-1}d = z,$$

Lemma 4.26(ii) yields

$$3^4 + 1 \leqslant 7(3^2 + 1),$$

giving $82 \leqslant 70$, a contradiction. Hence there exists $h \in H \backslash Z(Q)$ such that $h^2 = 1$. Clearly C contains exactly 5 Sylow 2-subgroups, and h permutes these subgroups by conjugation. It follows that h normalises some Sylow 2-subgroup, R_o say, of C. As shown above we must have $R_o \cong C_2 \times C_2$ or $C_2 \times C_4$, and hence, writing $Y = \Omega_1(R_o)$, we have $Y \cong C_2 \times C_2$ and h normalises Y. Let $X = \langle Y, h \rangle$. Then $|X| = 8$. If h centralises Y then $X \cong C_2 \times C_2 \times C_2$, contradicting Lemma 4.37(v). Hence h does not centralise Y. Obviously $Z(Q) \leqslant Y$ and h centralises Z(Q). Thus, if $Z(Q) = \langle z \rangle$ and $g \in Y \backslash Z(Q)$, then $hgh = zg$. Therefore $(hg)^2 = hghg = zg.g = z \in A$, whence hgA is an involution in G/A. Since $R_o \cap H = Z(Q)$ we must have $g \notin H$. As a result $hgA \notin H/A$. Also $h \in H \backslash Q$ and thus $hgA \notin D/A$. Therefore the involution hgA is one of those involutions of G/A which contribute to a count of α.

If the coset hgA does not contain an involution of G then hgA cannot contribute to a count of λ_2, whence $\lambda_2 \leqslant 6$. But we have $\lambda_1 \leqslant 6$ from (1), and Lemma 4.26(ii) yields

$$3^4 + 1 \leqslant 12 + 6(3^2 + 1),$$

giving $82 \leqslant 72$, a contradiction. Thus the coset hgA contains an involution of G and so there exists $d \in A$ such that $(hgd)^2 = 1$.

Now $g \notin H = C_G(A)$ and therefore conjugation by g is an automorphism of A of order 2. But a cyclic group of order 10 has a unique automorphism of order 2, namely the automorphism that acts by inverting each element. Hence $gdg = d^{-1}$ and, using the fact that $h \in H = C_G(A)$, we see that

$$(hgd)^2 = hgdhgd = hghdgd = zgdgd = zd^{-1}d = z,$$

contradicting $(hgd)^2 = 1$. Thus we were incorrect in supposing that a Sylow 2-subgroup of C is not cyclic, and we conclude that any such subgroup is cyclic.

Q.E.D.

LEMMA 4.40. <u>If</u> $r > 2$ <u>then</u> $n = 8$ <u>and</u> $G \cong \Sigma$.

<u>Proof</u>. Assume that $r > 2$. Then (i) - (vi) of Lemma 4.37 must hold and $|A| = 10$ by Lemma 4.39. Again let S denote the unique Sylow 5-subgroup of A. We have $F = Q \times S$ and F acts semi-regularly on V^*. By Lemma 4.37(iv) we have $G/A = H/A \times C/A$, and from Lemma 4.39 (1) we have $\lambda_1 \leqslant 6$. As in Lemma 4.37 (1) we see that the group H/A contains at most 9 involutions, and, since C/A is cyclic, it follows that the group G/A contains at most 10 involutions which are not in H/A. Let gA denote the unique involution in C/A. By Lemma 4.39 a Sylow 2-subgroup of C is cyclic, and hence C contains a unique involution, namely the non-trivial element of Z(Q). Therefore the coset gA does not contain an involution of G and thus cannot contribute to a count of λ_2. Hence $\lambda_2 \leqslant 9$ and, in fact, λ_2 is precisely the number of involutions of the group G/A of the form hgA, where hA is an involution in H/A such that the coset hgA contains an involution of G. That is, λ_2 is precisely the number of involutions, hA, of the group H/A such that the coset hgA contains an involution of G.

Let T denote a Hall 5'-subgroup of H. Since S is a Sylow 5-subgroup of H and $S \leqslant Z(H)$, we must have $H = T \times S$. Obviously $T \lhd G$. We have $AE = F = Q \times S$ and Lemma 4.37(iii) implies that $H/F \cong S_3$. Hence $|H| = 240$ and $|T| = 48$. Let K be a Sylow 3-subgroup of G. Clearly $K \leqslant T$, and $QK \cong SL(2,3)$. Also $|T : QK| = 2$. We show that the group T contains a unique involution, namely the non-trivial element of Z(Q).

Suppose that $h \in T \backslash Z(Q)$ such that $h^2 = 1$. Then $h \in H \backslash F$ and, by Lemma 4.28, we see that h acts non-trivially on $E/Z(E) = Q/Z(Q)$. Since $h \notin QK$

we deduce that $T = \langle QK,h\rangle$ and, by Lemma 3.15, we have $T \cong GL(2,3)$. Write $Z(Q) = \langle z\rangle$. With reference to Lemma 3.10 we see that T contains exactly 12 non-central involutions, say $h = h_1, h_2, \ldots, h_{12}$, where $h_{i+6} = h_i z$ for $1 \leq i \leq 6$. Hence $h_1A, \ldots, h_6A$, are six distinct involutions in H/A, not contained in F/A.

The group C contains exactly 5 Sylow 2-subgroups and obviously h permutes these subgroups by conjugation. Therefore there exists a Sylow 2-subgroup R say, of C, such that h normalises R. By Lemma 4.39 R is cyclic of order 4 or 8. Let R_o denote the subgroup of R of order 4, and let $R_o = \langle g\rangle$. Clearly gA is the unique involution in C/A. Suppose that h centralises R_o. It is easily seen that QK centralises C, and hence $T = \langle QK,h\rangle$ centralises R_oA. If the coset h_igA contains an involution of G for some $i \in \{1,\ldots, 6\}$ then there exists $d \in A$ such that $1 = (h_igd)^2$. In this case then, since $h_i \in T \leq C_G(R_oA)$, we have

$$1 = (h_igd)^2 = h_igdh_igd = h_i^2(gd)^2 = (gd)^2$$

whence gd is an involution in C, contradicting the fact that z is the unique involution in C. Therefore for $1 \leq i \leq 6$ the coset h_igA does not contain an involution of G. It follows that $\lambda_2 \leq 3$ and, using $\lambda_1 \leq 6$, Lemma 4.26(ii) gives a contradiction. We conclude that h does not centralise R_o.

Write $L = TR_o$. Then $|L| = 96$ and it is trivial to check that L satisfies all the conditions of Lemma 4.22. Also $soc(L) = Z(Q)$ and $Z(Q)$ acts semi-regularly on V^*. Thus if W is a non-trivial irreducible submodule of V_L then W is faithful for L and, by Lemma 4.22, there exists $y \in W^*$ such that $4 \mid |L_y|$. Hence $4 \mid |G_y|$, contradicting Lemma 4.37(iv). Therefore we were incorrect in supposing that there exists $h \in T\setminus Z(Q)$ such that $h^2 = 1$ and it follows that z is the unique involution in T, and hence in H.

As a consequence we have $\lambda_1 = 0$. Let P be a Sylow 2-subgroup of T. Then $|P| = 16$. Since Z(Q) is the unique subgroup of order 2 in P and Z(Q) acts semi-regularly on $V^{\#}$, the group P acts semi-regularly on $V^{\#}$, whence P is isomorphic to a generalised quaternion group of order 16. Therefore there exists $e \in P$ such that $e \notin Q$ and $|e| = 4$. We must have $e^2 = z \in Z(Q)$. Clearly $T = \langle QK, e\rangle$ and e acts non-trivially on Q/Z(Q). It follows that there exist elements a, b, of Q such that $a^e = b$, $b^e = a$ and $Q = \langle a,b\rangle$. We have $QK \cong SL(2,3)$ and hence, by Lemma 3.14, there exists $c \in QK$ such that $|c| = 3$ and $a^c = ab$, $b^c = a$. We have

$$a^{e^{-1}ce} = b^{ce} = a^e = b = a^{ac^2},$$

and

$$b^{e^{-1}ce} = a^{ce} = (ab)^e = ba = b^{ac^2}.$$

Therefore $(e^{-1}ce)(ac^2)^{-1} \in C_T(Q) = Z(Q)$, whence $e^{-1}ce = ac^2z$ or ac^2. But $|c| = 3$ and so $|e^{-1}ce| = 3$, whereas $|ac^2z| = 6$, and hence $e^{-1}ce = ac^2$. Thus we can write $T = \langle QK, e\rangle$ in terms of generators and relations as follows.

$$T = \langle a,b,c,e\colon a^4 = b^4 = c^3 = e^4 = 1,\ [a,b] = a^2 = b^2 = e^2,$$
$$c^{-1}ac = ab,\ c^{-1}bc = a,\ e^{-1}ae = b,\ e^{-1}be = a,\ e^{-1}ce = ac^2\rangle.$$

Comparing this with the description of Σ_1 in terms of generators and relations given in Definition 4.36, we see that $T \cong \Sigma_1$.

The group C contains 5 Sylow 2-subgroups and so there exists one such subgroup, R say, such that e normalises R. We have $R \cong C_4$ or C_8. Let R_o denote the subgroup of R of order 4 and write $R_o = \langle t\rangle$. Clearly tA is the unique involution in C/A, and $t^2 = z$. Now $\lambda_1 = 0$ and thus Lemma 4.26(ii) implies that $82 \leqslant 10\lambda_2$, whence $\lambda_2 \geqslant 9$. Since H/A contains at most 9 involutions our remarks at the beginning of this proof on the

size of λ_2 imply that if $h'A$ is any involution in H/A then the coset $h'tA$ contains an involution of G. Hence the coset etA contains an involution and it follows that there exists $d \in A$ such that $(etd)^2 = 1$. Clearly conjugation by t is an automorphism of A of order 2, and therefore conjugation by t inverts each element of A. Hence, using the fact that $e \in H = C_G(A)$, we have

$$1 = (etd)^2 = etdetd = etedtd = etetd^{-1}d = etet .$$

Therefore

$$et = (et)^{-1} = t^{-1}e^{-1} = t^3e^3 = (t\,t^2)(e^2e) = (tz)(ze) = te ,$$

and we conclude that e centralises $\langle t \rangle = R_o$.

Thus conjugation by e is an automorphism of R of order 2 which centralises R_o. Consequently we must have either e centralises R or $|R| = 8$ and, if $R = \langle f \rangle$, then $e^{-1}fe = f^5$. Suppose that $|R| = 8$ and write $R = \langle f \rangle$. Clearly $\langle f^2 \rangle = R_o$. Consider the group $X = \langle aef, f^2 \rangle$. Since $a \in Q$ and $f \in C = C_G(Q)$ we see that a and f commute. Also, as shown above, e centralises $R_o = \langle f^2 \rangle$. Hence the two generators of X commute. Now $e^{-1}fe = f$ or f^5, and in either case it is easily checked that $|aef| = 4$ and $(aef)^2 \neq z = f^4$. It follows that $X \cong C_4 \times C_4$. But then, obviously, there exists $y \in V^{\#}$ such that $4 \mid |X_y|$, whence $4 \mid |G_y|$, contradicting Lemma 4.37(iv). Hence $|R| \neq 8$ and we deduce that $R = R_o = \langle t \rangle$.

Write $S = \langle s \rangle$. We have

$$C = \langle s,t\colon s^5 = t^4 = 1,\ t^{-1}st = s^{-1} \rangle .$$

Comparing this with the description of Σ_2 in terms of generators and relations given in Definition 4.36 we see that $C \cong \Sigma_2$.

It is easily checked that QK centralises C, and hence, since $T = \langle QK, e \rangle$ and e centralises C, it follows that T centralises C. Also $G = HC = TC$

and $T \cap C = Z(Q)$. Hence

$$G = TC \cong \Sigma_1 \curlyvee \Sigma_2 = \Sigma .$$

Q.E.D.

Our next result shows that the case $G \cong \Sigma$ does occur.

LEMMA 4.41. <u>Let</u> $G \cong \Sigma$. <u>Then there exists an irreducible</u> $GF(3)G$-<u>module</u> V, <u>faithful for</u> G, <u>such that</u> $\dim_{GF(3)} V = 8$ <u>and</u> $|G_x|_{3'} = 2$ <u>for all</u> $x \in V^{\#}$.

<u>Proof</u>. Write $L = GF(3^2)$. The groups Σ_1, Σ_2, are both subgroups of $GL(2,3^2)$. Hence, for $i = 1,2$, there exists an $L\Sigma_i$-module U_i such that U_i is faithful for Σ_i and $\dim_L U_i = 2$. Clearly U_i is irreducible for $i = 1,2$. Write $U = U_1 \otimes_L U_2$. Then, since $\Sigma = \Sigma_1 \curlyvee \Sigma_2$, we can make U into an $L\Sigma$-module in the obvious way. It is easily seen that U is irreducible and faithful for Σ. Also $\dim_L U = 4$.

Assume that $G \cong \Sigma$. Then there exists an irreducible LG-module, V say, such that V is faithful for G and $\dim_L V = 4$. Naturally we may regard V as a $GF(3)G$-module, and $\dim_{GF(3)} V = 8$. We shall show $|G_x|_{3'} = 2$ for all $x \in V^{\#}$ in nine steps.

STEP 1: $|i(G)| = 90$.

Since $G \cong \Sigma = \Sigma_1 \curlyvee \Sigma_2$ it follows that there exist subgroups, T, C, of G with the properties that (i) $G = TC$; (ii) $[T,C] = 1$; (iii) $T \cong \Sigma_1$, $C \cong \Sigma_2$; (iv) $|T \cap C| = 2$. Write $T \cap C = \langle z \rangle$. Then z is the unique central involution of G, and z acts like scalar multiplication by -1 on V .

Write $Q = O_2(T)$. From the structure of $T \cong \Sigma_1$ we have $F(T) = O_2(T) = Q \cong Q_8$. Clearly $Z(Q) = \langle z \rangle$. It is easily seen that T contains exactly 3 Sylow 2-subgroups, each a generalised quaternion group of order 16, and any 2 such subgroups intersect in Q. Since a generalised quaternion group of order 16 contains exactly 10 elements of order 4, and Q contains

and $T \cap C = Z(Q)$. Hence

$$G = TC \cong \Sigma_1 \curlyvee \Sigma_2 = \Sigma .$$

Q.E.D.

Our next result shows that the case $G \cong \Sigma$ does occur.

LEMMA 4.41. <u>Let</u> $G \cong \Sigma$. <u>Then there exists an irreducible</u> $GF(3)G$-<u>module</u> V, <u>faithful for</u> G, <u>such that</u> $\dim_{GF(3)} V = 8$ <u>and</u> $|G_x|_{3'} = 2$ <u>for all</u> $x \in V^{\#}$.

<u>Proof</u>. Write $L = GF(3^2)$. The groups Σ_1, Σ_2, are both subgroups of $GL(2,3^2)$. Hence, for $i = 1,2$, there exists an $L\Sigma_i$-module U_i such that U_i is faithful for Σ_i and $\dim_L U_i = 2$. Clearly U_i is irreducible for $i = 1,2$. Write $U = U_1 \otimes_L U_2$. Then, since $\Sigma = \Sigma_1 \curlyvee \Sigma_2$, we can make U into an $L\Sigma$-module in the obvious way. It is easily seen that U is irreducible and faithful for Σ. Also $\dim_L U = 4$.

Assume that $G \cong \Sigma$. Then there exists an irreducible LG-module, V say, such that V is faithful for G and $\dim_L V = 4$. Naturally we may regard V as a $GF(3)G$-module, and $\dim_{GF(3)} V = 8$. We shall show $|G_x|_{3'} = 2$ for all $x \in V^{\#}$ in nine steps.

STEP 1: $|i(G)| = 90$.

Since $G \cong \Sigma = \Sigma_1 \curlyvee \Sigma_2$ it follows that there exist subgroups, T, C, of G with the properties that (i) $G = TC$; (ii) $[T,C] = 1$; (iii) $T \cong \Sigma_1$, $C \cong \Sigma_2$; (iv) $|T \cap C| = 2$. Write $T \cap C = \langle z \rangle$. Then z is the unique central involution of G, and z acts like scalar multiplication by -1 on V .

Write $Q = O_2(T)$. From the structure of $T \cong \Sigma_1$ we have $F(T) = O_2(T) = Q \cong Q_8$. Clearly $Z(Q) = \langle z \rangle$. It is easily seen that T contains exactly 3 Sylow 2-subgroups, each a generalised quaternion group of order 16, and any 2 such subgroups intersect in Q. Since a generalised quaternion group of order 16 contains exactly 10 elements of order 4, and Q contains

and $T \cap C = Z(Q)$. Hence

$$G = TC \cong \Sigma_1 \curlyvee \Sigma_2 = \Sigma .$$

Q.E.D.

Our next result shows that the case $G \cong \Sigma$ does occur.

LEMMA 4.41. <u>Let</u> $G \cong \Sigma$. <u>Then there exists an irreducible</u> $GF(3)G$-<u>module</u> V, <u>faithful for</u> G, <u>such that</u> $\dim_{GF(3)} V = 8$ <u>and</u> $|G_x|_{3'} = 2$ <u>for all</u> $x \in V^{\#}$.

<u>Proof</u>. Write $L = GF(3^2)$. The groups Σ_1, Σ_2, are both subgroups of $GL(2,3^2)$. Hence, for $i = 1,2$, there exists an $L\Sigma_i$-module U_i such that U_i is faithful for Σ_i and $\dim_L U_i = 2$. Clearly U_i is irreducible for $i = 1,2$. Write $U = U_1 \otimes_L U_2$. Then, since $\Sigma = \Sigma_1 \curlyvee \Sigma_2$, we can make U into an $L\Sigma$-module in the obvious way. It is easily seen that U is irreducible and faithful for Σ. Also $\dim_L U = 4$.

Assume that $G \cong \Sigma$. Then there exists an irreducible LG-module, V say, such that V is faithful for G and $\dim_L V = 4$. Naturally we may regard V as a $GF(3)G$-module, and $\dim_{GF(3)} V = 8$. We shall show $|G_x|_{3'} = 2$ for all $x \in V^{\#}$ in nine steps.

STEP 1: $|i(G)| = 90$.

Since $G \cong \Sigma = \Sigma_1 \curlyvee \Sigma_2$ it follows that there exist subgroups, T, C, of G with the properties that (i) $G = TC$; (ii) $[T,C] = 1$; (iii) $T \cong \Sigma_1$, $C \cong \Sigma_2$; (iv) $|T \cap C| = 2$. Write $T \cap C = \langle z \rangle$. Then z is the unique central involution of G, and z acts like scalar multiplication by -1 on V .

Write $Q = O_2(T)$. From the structure of $T \cong \Sigma_1$ we have $F(T) = O_2(T) = Q \cong Q_8$. Clearly $Z(Q) = \langle z \rangle$. It is easily seen that T contains exactly 3 Sylow 2-subgroups, each a generalised quaternion group of order 16, and any 2 such subgroups intersect in Q. Since a generalised quaternion group of order 16 contains exactly 10 elements of order 4, and Q contains

exactly 6 elements of order 4 we see that T contains exactly $3(10 - 6) + 6 = 18$ elements of order 4. From the structure of $C \cong \Sigma_2$ we see that C contains exactly 5 Sylow 2-subgroups each a cyclic group of order 4. Thus C contains exactly $2.5 = 10$ elements of order 4.

Since neither T nor C contains an involution other than z, it follows that if $g \in i(G)$ then $g = tc$ for some $1 \neq t \in T$, $1 \neq c \in C$. Then $1 = g^2 = t^2c^2$ implies that $t^2 = c^2 = z$. Therefore $g \in i(G)$ if and only if $g = tc$ for some $t \in T$, $c \in C$ such that $|t| = |c| = 4$. We have shown that T contains exactly 18 elements of order 4, and that C contains exactly 10 elements of order 4. Also if $t \in T$, $c \in C$ with $|t| = |c| = 4$ we have $t^3c = tzc = tc^3$, and hence $|i(G)| = 18.10/2 = 90$.

STEP 2: <u>if</u> $x \in V^*$ <u>then</u> $|G_x| = 6, 3, 2,$ <u>or</u> $1,$ <u>and if</u> $g_1, g_2 \in i(G)$ <u>such that</u> $g_1 \neq g_2$ <u>then</u> $x \in (C_V(g_1))^* \cap (C_V(g_2))^*$ <u>implies that</u> $G_x \cong S_3$.

Let S denote $O_5(C)$. Then $S \triangleleft G$ and $F(G) = Q \times S$. Consider $TS = T \times S$. We have $|G : TS| = 2$ and $i(G) \cap TS = \emptyset$. Let $x \in V^*$ and let P be a Sylow 2-subgroup of G_x. Since $i(G) \cap TS = \emptyset$ we must have $P \cap TS = 1$ and hence $|P| \leq 2$. Therefore $|G_x|_2 \leq 2$. We have $|G| = 480 = 2^5.3.5$ and clearly S, a Sylow 5-subgroup of G, acts semi-regularly on V^*. Thus $5 \nmid |G_x|$ and it follows that $|G_x| = 6, 3, 2,$ or 1. Let $g_1, g_2 \in i(G)$ such that $g_1 \neq g_2$ and let $x \in (C_V(g_1))^* \cap (C_V(g_2))^*$. Then $x \in V^*$ and G_x contains two distinct involutions, namely g_1 and g_2. Therefore G_x is a non-abelian group of order 6, whence $G_x \cong S_3$.

STEP 3: <u>if</u> $h \in i(G)$ <u>then</u> $\dim_L C_V(h) = 2$.

Let R denote a Sylow 2-subgroup of QC. Then, clearly, $Q \triangleleft R$ and $R \cong Q_8 \curlyvee C_4$. The group R contains exactly 6 involutions distinct from z. Let $g \in i(G) \cap R$. Considering V as a $GF(3)R$-module, Lemma 4.2(i) implies that $\dim_{GF(3)} C_V(g) = 4$, whence $\dim_L C_V(g) = 2$. Let $h \in i(G)$. If

$x \in (C_V(h))^{\#} \cap (C_V(g))^{\#}$ then, by Step 2, we have $G_x \cong S_3$. But $QC \triangleleft G$ and $3 \nmid |QC|$, and hence, since $\langle g \rangle \leqslant G_x \cap QC$, we see that $1 < (G_x \cap QC) \triangleleft G_x \cong S_3$ and $3 \nmid |G_x \cap QC|$, clearly an impossibility. Thus $(C_V(h))^{\#} \cap (C_V(g))^{\#} = \emptyset$, and we deduce that $\dim_L C_V(h) \leqslant 2$. Now if $h \in i(G)$ then $hz \in i(G)$. Thus we have $\dim_L C_V(h) \leqslant 2$ and $\dim_L C_V(hz) \leqslant 2$. But clearly $V = C_V(h) \oplus C_V(hz)$, and it follows that $\dim_L C_V(h) = \dim_L C_V(hz) = 2$.

STEP 4: G <u>contains exactly</u> 4 <u>Sylow</u> 3-<u>subgroups, say</u> K_1, K_2, K_3, K_4, <u>and for</u> $1 \leqslant i \leqslant 4$ <u>we have</u> $\dim_L C_V(K_i) = 2$.

Since $T \cong \Sigma_1$ there exists a subgroup, M, of T such that $M \cong SL(2,3)$. Obviously $M \triangleleft G$, and all Sylow 3-subgroups of G are contained in M. Thus G contains exactly 4 Sylow 3-subgroups, K_1, K_2, K_3, K_4, say. By Theorem 3.13 any faithful irreducible module for GL(2,3) over the field GF(3) has dimension 2, and thus, any faithful irreducible module for SL(2,3) over GF(3) has dimension 2. Hence, considering V as a GF(3)G-module and writing

$$V_M = W_1 \oplus \ldots \oplus W_\alpha$$

where each W_j is an irreducible GF(3)M-module, we see easily that each W_j is faithful for M, whence $\dim_{GF(3)} W_j = 2$ for $1 \leqslant j \leqslant \alpha$. It follows that $\alpha = 4$. Let $i \in \{1, \ldots, 4\}$. Clearly $\dim_{GF(3)} C_{W_j}(K_i) = 1$ for $1 \leqslant j \leqslant 4$, and therefore $\dim_{GF(3)} C_V(K_i) = 4$. We conclude that $\dim_L C_V(K_i) = 2$.

STEP 5: <u>if</u> $X = \{x : x \in V^{\#}, 3 \mid |G_x|\}$, <u>then</u> $|X| = 4.(3^4 - 1)$.

Clearly

$$X = \bigcup_{i=1}^{4} (C_V(K_i))^{\#} .$$

If $1 \leqslant i \neq j \leqslant 4$, then $x \in (C_V(K_i))^{\#} \cap (C_V(K_j))^{\#}$ implies that $\langle K_i, K_j \rangle \leqslant G_x$, which is clearly impossible since, by Step 2, we have $|G_x| \leqslant 6$. Thus the above union is disjoint and, since $\dim_L C_V(K_i) = 2$ for $1 \leqslant i \leqslant 4$, we must have $|X| = 4(3^4 - 1)$.

STEP 6: $G_x \cong S_3$ <u>for at least one</u> $x \in V^{\#}$.

Suppose that for all $x \in V^{\#}$ we have $G_x \ncong S_3$. Let $x \in V^{\#}$. Since $|G_x| = 6, 3, 2,$ or 1 by Step 2 and $G_x \ncong S_3$, it follows that G_x contains a unique involution. Therefore if $g_1, g_2 \in i(G)$ such that $g_1 \neq g_2$ then, clearly, $(C_V(g_1))^{\#} \cap (C_V(g_2))^{\#} = \emptyset$. By Step 3 we have $\dim_L C_V(h) = 2$ for all $h \in i(G)$, and hence

$$3^8 - 1 = |V^{\#}| \geq \Big|\bigcup_{h \in i(G)} (C_V(h))^{\#}\Big| = |i(G)|(3^4 - 1) = 90(3^4-1),$$

giving $3^4 + 1 \geq 90$, a contradiction. Thus there exists at least one $x \in V^{\#}$ such that $G_x \cong S_3$.

STEP 7: <u>if</u> $x \in V^{\#}$ <u>such that</u> $G_x \cong S_3$ <u>then</u> $\dim_L C_V(G_x) = 1$.

Let $x \in V^{\#}$ such that $G_x \cong S_3$. Then $G_x = \langle K,h \rangle$ for some Sylow 3-subgroup, K, of G and for some $h \in i(G)$. By Steps 3 & 4 we have $\dim_L C_V(h) = \dim_L C_V(K) = 2$, and hence, since $0 \neq x \in C_V(G_x) = C_V(h) \cap C_V(K)$, we must have $\dim_L C_V(G_x) = 1$ or 2. Let W denote $C_V(K)$. Then $\dim_L W = 2$ and, writing $N = N_G(K)$, it follows that W is a module for the group N over the field L. Clearly we have $S \leq N$.

Suppose that $\dim_L C_V(G_x) = 2$. Then $C_V(G_x) = W$ and G_x is a subgroup of the kernel of N on W. But, as shown in Step 2, if $y \in V^{\#}$ then $|G_y| \leq 6$. Therefore, since $|G_x| = 6$, we see that G_x is precisely the kernel of N on W, whence $G_x \triangleleft N$. In particular S normalises G_x. It is easily seen that $C_G(S) = TS$ and, as observed in Step 2, we have $i(G) \cap TS = \emptyset$. Hence $h \notin C_G(S)$. Therefore, since $h \in G_x \cong S_3$, it is obvious that S does not normalise G_x, a contradiction. Thus $\dim_L C_V(G_x) \neq 2$, and we conclude that $\dim_L C_V(G_x) = 1$.

STEP 8: <u>if</u> $x \in X$ <u>then</u> $G_x \cong S_3$.

Let $x \in V^{\#}$ such that $G_x \cong S_3$. Then $G_x = \langle K,h \rangle$ for some Sylow 3-subgroup, K, of G and for some $h \in i(G)$. As in Step 7, writing $W = C_V(K)$

and $N = N_G(K)$ we have that W is a module for the group N of dimension 2 over the field L and $S \leq N$. By Step 7 we have $\dim_L C_V(G_x) = \dim_L C_W(h) = 1$. Since $W = C_W(h) \oplus C_W(hz)$, we must have $\dim_L C_W(hz) = 1$. Write $W_1 = C_W(h)$, $W_2 = C_W(hz)$.

It is easily seen that W contains exactly 10 distinct one-dimensional subspaces, and, clearly, S permutes these subspaces in two orbits of size 5. We claim that the S-orbit containing W_1 does not contain W_2. For, if $(W_1)s = W_2$ for some $s \in S$ and if $w \in W_1^*$, then $ws \in W_2 = C_W(hz)$, whence $(ws)(hz) = ws$. But $S \cong C_5$ and $S \lhd G$. Hence we may write $sh = hs^\alpha$ for some α. Then

$$ws = (ws)hz = whs^\alpha z = ws^\alpha z$$

which yields $w = w(s^{\alpha-1}z)$. Thus $s^{\alpha-1}z \in G_w$. But $1 \neq s^{\alpha-1}z \in F = Q \times S$ and F acts semi-regularly on V^*, a contradiction. We conclude that W_1 and W_2 are in different S-orbits.

We have $C_G(W_1) = G_x$, and $C_G(W_2) = \langle K, hz \rangle \cong S_3$. Therefore, since any one-dimensional subspace of W is either $(W_1)s$ or $(W_2)s$ for some $s \in S$, we must have $G_y \cong S_3$ for all $y \in W^* = C_V(K)^*$. Let $i \in \{1, \ldots, 4\}$. Then the Sylow 3-subgroup K_i of G is conjugate to K, and it follows that there exists $g \in G$ such that $Wg = C_V(K_i)$. Therefore if $x \in (C_V(K_i))^*$ then $x = yg$ for some $y \in W^*$, whence $G_x = (G_y)^g \cong G_y \cong S_3$. To complete this step we merely remark that $X = \bigcup_{i=1}^{4} (C_V(K_i))^*$.

STEP 9: $|G_x|_3 = 2$ <u>for all</u> $x \in V^*$.

By Step 2 we have that if $x \in V^*$ then $|G_x| = 6, 3, 2,$ or 1. Thus we need only show that $2 \mid |G_x|$ for all $x \in V^*$ to establish that $|G_x|_3 = 2$ for all $x \in V^*$. Clearly $2 \mid |G_x|$ for all $x \in V^*$ if and only if

$$V^* = \bigcup_{h \in i(G)} (C_V(h))^*. \qquad (1)$$

Let $x \in V^{\#}$. Step 2 implies that $x \in (C_V(h_1))^{\#} \cap (C_V(h_2))^{\#}$ for distinct elements h_1, h_2 of $i(G)$ if and only if $G_x \cong S_3$. Also, using Step 8, we see that $G_x \cong S_3$ if and only if $x \in X$. Now if $G_x \cong S_3$ then G_x contains exactly 3 elements of $i(G)$, and it follows that x is an element of exactly 3 subsets of $V^{\#}$ of the form $(C_V(h))^{\#}$ for some $h \in i(G)$. By Step 3 we have $\dim_L C_V(h) = 2$ for all $h \in i(G)$, and hence to calculate $|\bigcup_{h \in i(G)} (C_V(h))^{\#}|$ we must subtract 2 from $|i(G)|.(3^4 - 1) = 90(3^4 - 1)$ for each element of X.

By Step 5 we have $|X| = 4(3^4 - 1)$, and hence

$$|\bigcup_{h \in i(G)} (C_V(h))^{\#}| = 90(3^4 - 1) - 2(4.(3^4 - 1)) = 82(3^4 - 1) = 3^8 - 1 = |V^{\#}| .$$

Therefore (1) holds, and the proof is complete.

Q.E.D.

This completes our investigation of the case $m = 1$, and we now drop our assumptions, stated immediately after the proof of Lemma 4.30, that $m = 1$, that G does not act half-transitively on $V^{\#}$, and that $G \not\leq \mathcal{N}(q^n)$. We proceed to examine the case $m = 2$ working under the assumptions stated immediately before and immediately following Lemma 4.27 and using the notation introduced there.

LEMMA 4.42. <u>If</u> $m = 2$ <u>then</u> $q = 3$ <u>and</u> $E \cong Q_8 \curlyvee D_8$, <u>and either</u> G <u>acts half-transitively on</u> $V^{\#}$ <u>or</u>

(i) $H/AE \cong C_3$ <u>or</u> S_3;

(ii) $r = 1, 3,$ <u>or</u> 4 ;

(iii) $4 \mid |G_x|$ <u>for all</u> $x \in V^{\#}$.

<u>Proof</u>. Assume that $m = 2$. Then by Theorem 4.21 we have $q = 3$ and $E \cong Q_8 \curlyvee D_8$. Therefore $4 \nmid |A|$, giving $E = F_2 = O_2(G)$ and $AE = F = F(G)$. Recall that $H = C_G(A)$. Let $\overline{H}$ denote H/AE and let $\overline{R}$ denote $F(\overline{H})$. By

Lemma 4.28 we have that $\overline{H}$, as a linear group on the symplectic space $E/Z(E)$, is a subgroup of $Sp(4,2)$ and $O_2(\overline{H}) = 1$.

By Lemma 4.12 we have $|Sp(4,2)| = 2^4.3^2.5$. Assume that $3 \nmid |\overline{R}|$. Then, since $O_2(\overline{H}) = 1$, we must have $\overline{R} = 1$ or $\overline{R} \cong C_5$. If $\overline{R} = F(\overline{H}) = 1$ then, clearly, $\overline{H} = 1$, whence $H = AE$. If $\overline{R} \cong C_5$ then $|\overline{H}| | 20$. Thus, whether $\overline{R} = 1$ or $\overline{R} \cong C_5$, we must have $3 \nmid |H|$. By Lemma 4.29(ii) the group G/H is cyclic, and hence G contains a normal Hall $3'$-subgroup, N say. By Lemma 4.3 we see that N acts half-transitively but not semi-regularly on $V^{\#}$. Clearly $N \notin \mathcal{T}(3^n)$ since $E \leqslant N$ and E is not metacyclic. Also $N \notin \mathcal{T}_0(3^{n/2})$ since $\mathcal{T}_0(3^{n/2})$ contains an abelian subgroup of index 2 whereas $E \leqslant N$ and a maximal abelian normal subgroup of E has index 4 in E. It follows that N must satisfy one of the cases (f_1), (f_2), (f_3), (f_4), of Theorem 1.16. But in all these cases we have $F(N) \cong Q_8 \curlyvee D_8$, and thus $|A| = 2$ which yields $C_G(A) = H = G = N$. Therefore if $3 \nmid |\overline{R}|$ then G acts half-transitively on $V^{\#}$.

Assume that G does not act half-transitively on $V^{\#}$. Then $3 | |\overline{R}|$. We need some of the facts concerning the group $Sp(4,2)$ and its action on a 4-dimensional symplectic space W given in the discussion immediately following Lemma 4.1 in [13]. Let L be a Sylow 3 subgroup of $Sp(4,2)$. Then, as stated in [13] (and as is easily checked), $L \cong C_3 \times C_3$, and $W = W_1 \oplus W_2$ where W_1 and W_2 are 2-dimensional non-isotropic subspaces normalised by L. Also, as shown in [13], the group $Sp(4,2)$ contains no element of order 15.

Since we have assumed that $3 | |\overline{R}|$, and since $Sp(4,2)$ contains no element of order 15, it follows that $\overline{R}$ is a 3-group. Therefore $\overline{R} \cong C_3$ or $C_3 \times C_3$. We use the argument at the beginning of the proof of [13] Lemma 4.4 to show that $\overline{R} \ncong C_3 \times C_3$. Suppose that $\overline{R} \cong C_3 \times C_3$. Then $\overline{R}$ is a Sylow 3-subgroup of $Sp(4,2)$ and hence, writing $W = E/Z(E)$, we have $W = W_1 \oplus W_2$ where W_1 and W_2 are 2-dimensional non-isotropic subspaces

normalised by $\overline{R}$. Let $E_1/Z(E) = W_1$, $E_2/Z(E) = W_2$. Then, since W_1 and W_2 are non-isotropic, E_1 and E_2 are non-abelian groups of order 8. But E_1 and E_2 both admit automorphisms of order 3, whence $E_1 \cong E_2 \cong Q_8$ and we have

$$E = E_1E_2 \cong Q_8 \curlyvee Q_8 \not\cong Q_8 \curlyvee D_8,$$

contradicting $E \cong Q_8 \curlyvee D_8$. Hence $\overline{R} \not\cong C_3 \times C_3$, and we conclude that $\overline{R} \cong C_3$. Thus $\overline{H} \cong C_3$ or S_3, which proves (i).

The group E does not act semi-regularly on V^*, and so there exists $y \in V^*$ such that $2 \mid |E_y|$. Therefore $2 \mid |G_y|$ and, by 3'-halftransitivity we have $2 \mid |G_x|$ for all $x \in V^*$. By assumption V_A is homogeneous, and hence we can apply Lemma 4.26 with $p = 2$. Note that it is Lemma 4.26(iii) that applies since, by Lemma 4.29(iii), we have $4 = 2^m \geqslant n/r$. Since $|H/A| \leqslant 96$ and G/H is cyclic we must have $\lambda_1 \leqslant 96$, $\lambda_2 \leqslant 96$. Lemma 4.26(iii) yields

$$3^r \leqslant 2(96 + 96) = 384$$

and we deduce that $r \leqslant 5$. But if $r = 5$ then, since $|G/H|$ divides r, we have $\lambda_2 = 0$ and Lemma 4.26(iii) gives a contradiction. Thus $r \leqslant 4$. Now $4 \nmid |A|$ and r is the least integer such that $|A| \mid 3^r - 1$. It follows that $r \neq 2$ and we have proved (ii).

All that remains to prove is that $4 \mid |G_x|$ for all $x \in V^*$. Suppose that there exists $y \in V^*$ such that $4 \nmid |G_y|$. Then, since $2 \mid |G_y|$, we must have $|G_y|_2 = 2$. Therefore, by 3'-halftransitivity, $|G_x|_2 = 2$ for all $x \in V^*$. Let $h \in i(G) \cap E$. By Lemma 4.2(i) we have $\dim C_V(h) = n/2$. Let $g \in i(G)$ such that $g \notin E$, and let $x \in C_V(h) \cap C_V(g)$. Since $h \in E_x$ we have $2 \mid |E_x|$. But $g \in G_x \setminus E_x$ and $g \in i(G)$, whence $2 \mid |G_x/E_x|$ and $4 \mid |G_x|$. Therefore $x = 0$, and we deduce that $C_V(h) \cap C_V(g) = 0$. Hence for all $g \in i(G)$ we

have $\dim C_V(g) \leqslant n/2$. Since $|G_x|_2 = 2$ for all $x \in V^*$ it follows that

$$V^* = \bigcup_{g \in i(G)} C_V(g)^*. \qquad (1)$$

Suppose that $r = 4$. Then $|A| = 10$ and $|H| \leqslant 960$. Since $|G/H| \leqslant r = 4$ we have $|G| \leqslant 3840$. Certainly $|i(G)| \leqslant |G| \leqslant 3840$ and (1) yields

$$3^n - 1 = |V^*| \leqslant 3840(3^{n/2} - 1),$$

giving $3^{n/2} + 1 \leqslant 3840$. But, by Lemma 4.29(iii), we see that $n \geqslant 2^m r = 16$, and we have a contradiction. Hence $r \neq 4$.

Suppose that $r = 3$. Then $|A| = 26$, so let B denote the subgroup of A of order 13. Now $B \leqslant A \leqslant Z(H)$ and so, if T denotes a Hall 13'-subgroup of H, then we have $H = T \times B$. Also $T \leqslant 192$ and $i(G) \subseteq T$. Consequently $|i(G)| \leqslant 192$ and (1) yields

$$3^n - 1 = |V^*| \leqslant 192(3^{n/2} - 1),$$

giving $3^{n/2} + 1 \leqslant 192$. But $n \geqslant 2^m r = 12$, and we have a contradiction. Hence $r \neq 3$.

Therefore $r = 1$, whence $|A| = 2$ and $H = G$. Thus $G/E = H/AE \cong C_3$ or S_3. The group $E \cong Q_8 \curlyvee D_8$ contains exactly 10 non-central involutions and hence, if $2 \nmid |G/E|$, then $i(G) \subseteq E$ which yields $|i(G)| \leqslant 10$. Assume that $2 \mid |G/E|$, and let $S/Z(E)$ be a Sylow 2-subgroup of $G/Z(E)$. Clearly $|S/Z(E)| = 32$, and the group $E/Z(E)$ has index 2 in $S/Z(E)$. Let $sZ(E) \in S/Z(E)$ such that $sZ(E) \notin E/Z(E)$ and $|sZ(E)| = 2$. By Lemma 4.28 the group G/E acts faithfully on $E/Z(E)$, and hence, writing $W = E/Z(E)$, we have $|C_W(sZ(E))| \leqslant 8$. If $tZ(E) \in E/Z(E)$ then $|stZ(E)| = 2$ if and only if $tZ(E) \in C_W(sZ(E))$. Thus the group $S/Z(E)$ contains at most 8 involutions not contained in $E/Z(E)$. Clearly $G/Z(E)$ contains three Sylow 2-subgroups, any two of which intersect in $E/Z(E)$. Hence the group $G/Z(E)$ contains

at most $3.8 = 24$ involutions not contained in $E/Z(E)$, whence G contains at most $2.24 = 48$ involutions not contained in E. It follows that $|i(G)| \leqslant 48 + 10 = 58$. Thus, whether $G/E \cong C_3$ or S_3, we have $|i(G)| \leqslant 58$, and (1) yields

$$3^n - 1 = |V^*| \leqslant 58(3^{n/2} - 1),$$

which implies that $3^{n/2} + 1 \leqslant 58$. Hence $n \leqslant 6$. But $2^m = 4$ divides n, and we conclude that $n = 4$. Since $|G_x|_2 = 2$ for all $x \in V^*$, it follows that $|G|_2/2$ divides the size of each G-orbit in V^*, and thus $|G|_2/2$ divides $|V^*| = 80$. Hence $|G|_2 \leqslant 32$, and therefore E is a Sylow 2-subgroup of G. Let K be a Sylow 3-subgroup of G. Then $G = EK$.

Now E contains exactly 10 non-central involutions, and therefore E contains precisely 5 subgroups isomorphic to $C_2 \times C_2$ containing $Z(E)$. Each of these subgroups is normal in E, and clearly K normalises at least one such subgroup, M say. But then $M \cong C_2 \times C_2$ and $M \lhd G$, contradicting our assumption that G contains no non-cyclic abelian normal subgroup. Hence we were incorrect in supposing that there exists $y \in V^*$ such that $4 \nmid |G_y|$, and we conclude that $4 \mid |G_x|$ for all $x \in V^*$.

Q.E.D.

LEMMA 4.43. <u>If</u> $m = 2$ <u>then</u> G <u>acts half-transitively on</u> V^*.

<u>Proof</u>. Assume that $m = 2$. By Lemma 4.42 we have $q = 3$ and $E \cong Q_8 \curlyvee D_8$. Suppose that G does not act half-transitively on V^*. Then (i), (ii), (iii), of Lemma 4.42 must hold. If $r = 3$ then, since $|G/H| \mid 3$ and $|H/AE|_2 \leqslant 2$, we must have $2 \mid |G_x \cap AE|$ for all $x \in V^*$. In this case, then, $2 \mid |E_x|$ for all $x \in V^*$, and Lemma 4.1(ii) yields $n = 4$, a contradiction since $r = 3$ and $r \mid n$.

Suppose that $r = 4$, and write $L/AE = F(G/AE)$. Since G/H is cyclic of order dividing 4 and $H/AE \cong C_3$ or S_3, we see easily that $|G : L| \leqslant 2$

and L/AE is cyclic of order 3,6, or 12. Clearly either V_L is irreducible, or $V_L = V_1 \oplus V_2$ where V_1 and V_2 are irreducible GF(3)L-modules such that $(V_1)g = V_2$, $(V_2)g = V_1$, for all $g \in G \backslash L$. Let U denote a non-trivial irreducible submodule of V_L. Since $r = 4$ we must have $|A| = 10$ and we see easily that $soc(G) = soc(L) = A$. From the fact that A acts semi-regularly on $V^{\#}$ it follows that U is faithful for L. If $x \in U^{\#}$ then $4 \mid |G_x|$, and hence $2 \mid |G_x \cap L|$. Therefore $2 \mid |L_x|$ for all $x \in U^{\#}$ and, since obviously U_A is homogeneous, we can apply Lemma 4.26 to the group L and the module U. It is easily seen that $\lambda_1 \leq 15$, $\lambda_2 \leq 16$. Now if V_L is irreducible then $\dim U = n$, whence $(\dim U)/r > 2$, and Lemma 4.26(iii) gives a contradiction.

Therefore $V_L = V_1 \oplus V_2$ where V_1 and V_2 are irreducible GF(3)L-modules, faithful for L, such that $(V_1)g = V_2$, $(V_2)g = V_1$, for all $g \in G \backslash L$. If $x \in V_1^{\#}$, then $G_x \leq L$, whence $L_x = G_x$, and L acts 3'-halftransitively but not 3'-semiregularly on $V_1^{\#}$. Clearly $\dim V_1 = n/2$. However, L/AE is cyclic and so L contains a normal Hall 3'-subgroup, N say. By Lemma 4.2 the group N acts half-transitively but not semi-regularly on $V_1^{\#}$, and clearly $N \not\leq \mathcal{T}(3^{n/2})$ and $N \not\leq \mathcal{T}_0(3^{n/4})$. Hence, by Theorem 1.16, we see that N must satisfy one of the cases (f_1), (f_2), (f_3), (f_4) in the statement of that theorem. But then we have $n/2 = 4$, whence $n = 8$, contradicting the fact that $2^m r = 16$ divides n. Therefore $r \neq 4$.

Using Lemma 4.42(ii) we conclude that $r = 1$, which yields $|A| = 2$ and $C_G(A) = H = G$. Thus $G/E = H/AE \cong C_3$ or S_3. Since $4 \mid |G_x|$ for all $x \in V^{\#}$ we see that $2 \mid |E_x|$ for all $x \in V^{\#}$, and therefore, by Lemma 4.1(ii), we have $n = 4$ and $|E_x| = 2$, for all $x \in V^{\#}$. Consequently $G/E \cong S_3$. Let K be a Sylow 3-subgroup of G. As observed in the proof of Lemma 4.42, the group E contains exactly 5 subgroups isomorphic to $C_2 \times C_2$ containing Z(E). Each of these subgroups is normal in E, and, clearly, K normalises at least one such subgroup, M say. Thus $EK \leq N_G(M)$. Let $g \in M \backslash Z(E)$.

Then g is a non-central involution in E, and there exists $y \in V^{\#}$ such that $E_y = \langle g \rangle$. Since $E_y = E \cap G_y \lhd G_y$ it follows that $G_y \leqslant C_G(g)$, and, since $M = \langle Z(E), g \rangle$, we must have $G_y \leqslant C_G(g) \leqslant N_G(M)$. Now $4 \mid |G_y|$, and therefore $2 \mid |G_y : G_y \cap E|$. Hence $G_y \nleqslant EK$. But $|G : EK| = 2$ and we deduce that $N_G(M) \geqslant \langle EK, G_y \rangle = G$, giving $M \lhd G$, the final contradiction since G contains no non-cyclic abelian normal subgroup. Thus G acts half-transitively on $V^{\#}$.

Q.E.D.

The preceeding results are collected together to obtain the following theorem.

THEOREM 4.44. <u>Let</u> G <u>be a soluble group,</u> q <u>a prime, and</u> V <u>an irreducible</u> $GF(q)G$-<u>module, faithful for</u> G, <u>such that</u> $\dim_{GF(q)} V = n$ <u>and</u> G <u>acts</u> q'-<u>halftransitively but not</u> q'-<u>semiregularly on</u> $V^{\#}$. <u>Assume that</u> G <u>contains no non-cyclic abelian normal subgroup, and that if</u> A <u>denotes</u> $Z(C_F(\Phi(F)))$ <u>where</u> $F = F(G)$ <u>then</u> V_A <u>is homogeneous. Then one of the following must hold.</u>

(i) G <u>acts half-transitively on</u> $V^{\#}$;

(ii) $G \leqslant \mathcal{T}(q^n)$;

(iii) $q^n = 3^4$ <u>and</u> $G \cong GL(2,3) \leftthreetimes C_4$;

(iv) $q^n = 3^8$ <u>and</u> $G \cong \Sigma$, <u>where</u> Σ <u>is the group defined in Definition</u> 4.36.

<u>Proof</u>. By Theorem 4.21 we have $O_p(G)$ is cyclic for all odd primes p. Let F_2 denote $O_2(G)$ and write $E = \Omega_2(C_{F_2}(\Phi(F_2)))$. If F_2 is generalised quaternion of order at least 16, or if F_2 is cyclic, dihedral or semi-dihedral, then by Lemma 4.27 we have $G \leqslant \mathcal{T}(q^n)$. Therefore we may assume that F_2 is not cyclic, dihedral, or semi-dihedral, and that F_2 is not a generalised quaternion group of order greater than or equal to 16. Then by Lemma 4.1 the group E is of type $E(2,m)$ for some $m \neq 0$ and by Theorem

4.21 we have $m = 1$ or $m = 2$. If $m = 2$ then, by Lemma 4.43, the group G acts half-transitively on $V^{\#}$, and hence we may assume that $m = 1$. Therefore Lemmas 4.30 - 4.35 and Lemmas 4.37 - 4.40 imply that if G does not act half-transitively on $V^{\#}$, and if $G \not\leq \mathcal{T}(q^n)$, then $q = 3$ and either $n = 4$ and $G \cong GL(2,3) \curlyvee C_4$, or $n = 8$ and $G \cong \Sigma$.

Q.E.D.

This concludes Step 3 in the outline of this chapter given earlier. We now drop the assumptions, stated immediately following the proof of Lemma 4.27, that V_A is homogeneous and that F_2 is neither generalised quaternion of order at least 16, cyclic, dihedral, nor semi-dihedral. We proceed to Step 4, the investigation of the possibility that V_A is not homogeneous, under the assumptions stated immediately preceding Lemma 4.27 and using the notation introduced there.

LEMMA 4.45. <u>The case in which V_A is not homogeneous does not occur</u>.

<u>Proof</u>. Suppose that V_A is not homogeneous. Then, by Lemma 4.27, it follows that F_2 is neither generalised quaternion of order greater than or equal to 16, cyclic, dihedral, nor semi-dihedral. Consequently $q \neq 2$ and Lemma 4.1 yields that, writing $E = \Omega_2(C_{F_2}(\Phi(F)))$, we have E is a group of type $E(2,m)$ with $m \neq 0$.

Let

$$V_A = V_1 \oplus \ldots \oplus V_t$$

where V_i is a homogeneous component of V_A. Since, by assumption, V_A is not homogeneous we have $t > 1$. Let S_i denote the stabiliser in G of V_i for $1 \leq i \leq t$. Then $C_G(A) \leq S_i$ and $|G : S_i| = t$ for $1 \leq i \leq t$. Also the S_i are conjugate in G. Now $G/C_G(A)$ is isomorphic to a subgroup of $Aut(A)$, an abelian group. Thus $S_1 = S_2 = \ldots = S_t = S$, say, and $S \triangleleft G$.

The V_i are permuted by G and if $i \in \{1,\ldots,t\}$ and $g \in G$ then $V_i g = V_i$ if and only if $g \in S$. Hence if $i \in \{1,\ldots,t\}$ and $x \in V_i^{\#}$ then $G_x \leqslant S$, whence $G_x = S_x$. By Clifford's Theroem each V_i is an irreducible GF(q)S-module and, clearly, $(V_i)_A$ is homogeneous for $1 \leqslant i \leqslant t$.

Since $S \lhd G$ we must have $F(S) \leqslant F = F(G)$. From the fact that $C_G(A) \leqslant S$ it follows that $E \leqslant S$, whence $AE \leqslant F(S)$. Now $|F : AE| \leqslant 2$, and from the structure of F_2, a 2-group of symplectic type, we see that $\Phi(C_2(S)) = \Phi(F_2)$ Therefore, writing $L = F(S)$, we have $\Phi(L) = \Phi(F)$, and so

$$C_L(\Phi(L)) = L \cap C_F(\Phi(F)) = L \cap AE = AE.$$

Consequently $Z(C_F\Phi(F)) = A = Z(C_L(\Phi(L)))$. Clearly $soc(S) \leqslant A$, and, since A acts semi-regularly on $V^{\#}$, the module V_i is faithful for S $(1 \leqslant i \leqslant t)$.

We have shown that V_1 is an irreducible GF(q)S-module, faithful for S, and, since $G_x = S_x$ for all $x \in V_1^{\#}$, we see that S acts q'-halftransitively but not q'-semiregularly on $V_1^{\#}$. Obviously S is soluble.

Suppose that S contains a non-cyclic abelian normal subgroup. Then the possibilities for S are given in Theorem 3.9. If S satisfies (iii) in Theorem 3.9 then $\Omega_1(O_2(S)) \cong C_2 \times C_2$ and clearly, $\Omega_1(O_2(S)) \lhd G$, a contradiction. If S satisfies (i), (ii), or (iv) of Theorem 3.9 then we must have $|A| = 2$, giving $A \leqslant Z(G)$ which contradicts our assumption that V_A is not homogeneous. Hence $S \cong \mathcal{T}_o(q^\alpha : q^\beta)$ for some integers α, β, such that $q^\beta | \alpha$. But $O_2(\mathcal{T}_o(q^\alpha : q^\beta))$ is abelian unless $q^\alpha - 1$ is a power of 2, and we have a non-abelian subgroup of $O_2(S)$, namely E. Hence $q^\alpha - 1$ is a power of 2. Therefore either $\alpha = 2$ and $q = 3$, or $\alpha = 1$ and q is a Fermat prime. As a consequence we see that $q \nmid \alpha$, which yields $\beta = 0$ and

$$|S| = |\mathcal{T}_o(q^\alpha : q^\beta)| = |\mathcal{T}_o(q^\alpha)| = 4(q^\alpha - 1).$$

It follows that S is a 2-group, whence A is a 2-group and $G/C_G(A)$ is a 2-group. Since $C_G(A) \leqslant S \leqslant G$ we conclude that G is a 2-group, and G acts half-transitively but not semi-regularly on $V^{\#}$. Also G is imprimitive as a linear group, and hence Theorem 1.16 implies that either $G \cong \mathcal{T}_0(q^{n/2})$, or $G \cong Q_8 \curlyvee D_8$, or $q = 2$ and G is isomorphic to the dihedral group of order 18. But $\mathcal{T}_0(q^{n/2})$ and $Q_8 \curlyvee D_8$ both contain a non-cyclic abelian normal subgroup, and we have $q \neq 2$. Hence we were incorrect in supposing that S contains a non-cyclic abelian normal subgroup, and thus S contains no such subgroup.

We have shown above that $A = Z(C_L(\Phi(L)))$ where L denotes F(S), and we have $(V_1)_A$ is homogeneous. Therefore we can apply Theorem 4.44 to the group S and the module V_1. Suppose that either (iii) or (iv) of that theorem holds. Then $q = 3$ and $A \cong C_4$ or C_{10}. But both C_4 and C_{10} possess a unique (up to equivalence) faithful irreducible representation over GF(3), contradicting our assumption that V_A is not homogeneous. Thus either S acts half-transitively on $V_1^{\#}$, or $S \leqslant \mathcal{T}(q^{\alpha})$ where α denotes $\dim_{GF(q)} V_1$. Let β denote the dimension over GF(q) of an irreducible constituent of $(V_1)_A$.

We proceed to eliminate the possibility that $S \leqslant \mathcal{T}(q^{\alpha})$, so, in order to obtain a contradiction, suppose that $S \leqslant \mathcal{T}(q^{\alpha})$. Then S is metacyclic, whereupon E is metacyclic, and it follows that $E \cong Q_8$. Therefore $L = F = E \times B$ where B is a cyclic group of odd order, and $Z(F) = A$. By Lemma 4.23 we have $i(S) = \emptyset$. We deduce that if $x \in V_1^{\#}$ then $2 \nmid |S_x|$. From the fact that S acts q'-halftransitively but not q'-semiregularly on $V_1^{\#}$ there exists a prime, p say, distinct from q, such that $p \mid |S_x|$ for all $x \in V_1^{\#}$, and we have shown that $p \neq 2$.

By Lemma 4.23 there exists a normal cyclic subgroup T of S such that $|F : T| = 2$ and S/T is cylic. Clearly $A \leqslant T$ and $|T : A| = 2$. Also we have $2^m = 2$, and, by Lemma 4.29(iii), we see that $2 \geqslant \alpha/\beta$. We apply

Lemma 4.26 to the group S, the module V_1, and the restriction of V_1 to A. Since $\alpha/\beta \geqslant 2$ it follows that either Lemma 4.26(ii) or Lemma 4.26(iii) applies. We have $p \neq 2$ and $|T : A| = 2$ where S/T is cyclic. Hence S/A is central-by-cyclic, and we must have S/A abelian with a unique cyclic Sylow p-subgroup. But then either $\lambda_1 = 0$, $\lambda_2 \leqslant 1$, or $\lambda_1 \leqslant 1$, $\lambda_2 = 0$, and both of these cases contradict Lemma 4.26(ii) and (iii). Hence $S \not\leqslant \mathcal{T}(q^\alpha)$.

The only remaining possibility is that S acts half-transitively on $V_1^\#$, so suppose that this is the case. Since S does not act q'-semiregularly on $V_1^\#$ it follows that S does not act semi-regularly on $V_1^\#$. As proved above, $S \not\leqslant \mathcal{T}(q^\alpha)$ and S contains no non-cyclic abelian normal subgroup. Therefore we see that the possibilities for S, q, α are precisely those given in cases (a_1), (a_2), (b_1), (b_2), (c_1), (c_2), (d_1), (d_2), (e_1), (f_2), (f_3), (f_4) in the statement of Theorem 1.16. Obviously cases (a_1), (a_2), are impossible since in these cases $|A| = 2$ and $A \leqslant Z(G)$. It is easily checked that in the remaining cases $q \nmid |S|$ and $q \nmid |\mathrm{Aut}(A)|$. But $C_G(A) \leqslant S \leqslant G$, and $G/C_G(A)$ is isomorphic to a subgroup of Aut(A). Therefore $q \nmid |G|$, and we deduce that G acts half-transitively but not semi-regularly on $V^\#$. Since V_A is not homogeneous G is imprimitive as a linear group, and Theorem 1.16 implies that either $G \cong \mathcal{T}_0(q^{n/2})$, or $G \cong Q_8 \curlyvee D_8$, or $q = 2$ and G is isomorphic to the dihedral group of order 18. But both $\mathcal{T}_0(q^{n/2})$ and $Q_8 \curlyvee D_8$ contain non-cyclic abelian normal subgroups, and we have $q \neq 2$, the final contradiction.

Q.E.D.

With the groups $\mathcal{T}(q^n)$, $\mathcal{T}_0(q^n : q^m)$, Δ, Σ, as defined in Definitions 1.14, 3.1, 3.8, 4.36, respectively we collect together the results of this chapter and Chapter 3 to obtain the following theorem.

THEOREM 4.46. Let G be a soluble group, q a prime, V an irreducible $GF(q)G$-module, faithful for G, such that G acts q'-halftransitively but not q'-semiregularly on $V^{\#}$. Let n denote $\dim_{GF(q)} V$. Then one of the following cases must hold.

(i) G acts half-transitively on $V^{\#}$;

(ii) $G \leq \mathcal{T}(q^n)$;

(iii) $G \cong \mathcal{T}_0(q^{n/2} : q^m)$ for some integer m such that $q^m | n/2$;

(iv) $q^n = 3^4$ and $G \cong SL(2,3) \curlyvee D_8$;

(v) $q^n = 3^4$ and $G \cong \Delta$;

(vi) $q^n = 3^4$ and $G \cong GL(2,3) \curlyvee D_8$;

(vii) $q^n = 3^4$ and $G \cong GL(2,3) \curlyvee C_4$;

(viii) $q^n = 3^8$ and $G \cong \Sigma$.

Proof. Write $A = Z(C_F(\Phi(F)))$ where F denotes $F(G)$. If G contains a non-cyclic abelian normal subgroup then the possibilities for G are given in Theorem 3.9. Notice that if $G \cong Q_8 \curlyvee D_8$ then G acts half-transitively on $V^{\#}$. If G contains no non-cyclic abelian normal subgroup then Lemma 4.45 implies that V_A is homogeneous and the possibilities for G are given in Theorem 4.44.

Q.E.D.

CHAPTER 5

BOUNDING THE NILPOTENT LENGTH OF A SOLUBLE HIGH - FIDELITY GROUP WITH A UNIQUE MINIMAL NORMAL SUBGROUP.

In this chapter we bound the nilpotent length of a soluble group which acts faithfully, irreducibly, and q'-semiregularly as a group of linear transformations of a vector space over the field GF(q) for some prime q. We conclude by using this bound, together with the main results from earlier chapters, to show (Theorem 5.2) that if G is a soluble high-fidelity group with a unique minimal normal subgroup then n(G), the nilpotent length of G, is at most 6.

LEMMA 5.1. *Let* G *be a soluble group,* q *a prime, and let* V *be an irreducible* GF(q)G*-module, faithful for* G, *such that* G *acts* q'*-semiregularly on* $V^{\#}$. *Then* $n(G) \leq 3$.

Proof. Write F = F(G). Since V is a faithful, irreducible G-module over the field of characteristic q we must have $O_q(G) = 1$, whereupon $q \nmid |F|$. The fact that G acts q'-semiregularly on $V^{\#}$ implies that G_v is a q-group for each $v \in V^{\#}$, and therefore F acts semi-regularly on $V^{\#}$. From the structure of groups that act semi-regularly as groups of automorphisms we deduce that if p is an odd prime then $O_p(G)$, the unique Sylow p-subgroup of F, is cyclic, and $O_2(G)$, the unique Sylow 2-subgroup of F, is either cyclic or generalised quaternion.

Let B denote the normal Hall 2'-subgroup of F. Then B is a cyclic group of odd order, and $F = O_2(G) \times B$. If $O_2(G)$ is cyclic then write A = F. If $O_2(G)$ is generalised quaternion of order at least 16 then $O_2(G)$ contains a characteristic cyclic subgroup of index 2, R say. Clearly R is self-centralising in $O_2(G)$. In this case write $A = R \times B$. Thus,

if $O_2(G)$ is generalised quaternion of order at least 16, or if $O_2(G)$ is cyclic, then A is a normal cyclic subgroup of G such that $|F : A| \leqslant 2$ and $C_F(A) = A$.

Assume that $O_2(G)$ is either generalised quaternion of order at least 16, or cyclic, and let A denote the normal cyclic subgroup of G constructed in the previous paragraph. Let N denote $C_G(A)$. Then N stabilises the chain

$$O_2(G) \geqslant O_2(G) \cap A \geqslant 1 ,$$

and so $N/C_N(O_2(G))$ is a 2-group. Also the solubility of G implies that $C_G(F) = Z(F)$, and hence

$$C_N(O_2(G)) \leqslant C_G(F) = Z(F) \leqslant A \leqslant Z(N) \quad .$$

Therefore $N/Z(N)$ is a 2-group, and consequently N is a normal nilpotent subgroup of G. It follows that $N \leqslant F$, whereupon $N = C_G(A) = A$. We conclude that $G/A = G/C_G(A)$ is isomorphic to a subgroup of Aut(A), an abelian group, and then, obviously, $n(G) \leqslant 2$.

Hence we may assume that $O_2(G)$ is isomorphic to the quaternion group of order 8. Write $Q = O_2(G)$, so that $F = Q \times B$ with $Q \cong Q_8$ and B a cyclic group of odd order. As above we have $C_G(F) = Z(F)$, and therefore, writing $Z = Z(F)$, $S = C_G(Q)$, $T = C_G(B)$, we see that the map $\rho : G/Z \longrightarrow G/S \times G/T$ defined by $\rho : gZ \longmapsto (gS, gT)$ for all $g \in G$ is well-defined and is a monomorphism. Thus G/Z is isomorphic to a subgroup of $G/S \times G/T$.

Now B is cyclic, and hence G/T is abelian. Also G/S is isomorphic to a subgroup of $\mathrm{Aut}(Q) \cong S_4$, the symmetric group of degree 4. Clearly $F/Z \cong C_2 \times C_2$, and ρ maps F/Z isomorphically onto the subgroup $FS/S \times 1$ of $G/S \times G/T$ (where 1 denotes the trivial subgroup of G/T). Then, from the structure of the group S_4, it is easily seen that G/F is isomorphic to a subgroup of $S_3 \times E$ for some abelian group E which yields $n(G/F) \leqslant 2$,

and hence $n(G) \leqslant 3$.

Q.E.D.

THEOREM 5.2. Let G be a soluble high-fidelity group with a unique minimal normal subgroup. Then $n(G) \leqslant 6$.

Proof. Let N denote the unique minimal normal subgroup of G. Then N is an elementary abelian q-group for some prime q. Write $R = C_G(N)$. We show first that $n(R) \leqslant 3$. Let $1 \neq \lambda \in \hat{N}$, and then, by Theorem 2.17, the group G_λ contains an abelian Hall q'-subgroup, H say. If Q denotes $O_q(G_\lambda)$ then $H \cap Q = 1$, whence $H \cong HQ/Q$, and clearly, HQ/Q is a Hall q'-subgroup of G_λ/Q. Since $Q = O_q(G_\lambda)$ it follows that the group G_λ/Q contains no non-trivial normal q-subgroup, and so $F(G_\lambda/Q)$ is a normal q'-subgroup of G_λ/Q. Now G is soluble, and hence so is G_λ/Q. Consequently $F(G_\lambda/Q)$ is a subgroup of each Hall q'-subgroup of G_λ/Q, and therefore, in particular, $F(G_\lambda/Q) \leqslant HQ/Q$, an abelian group. As a result $HQ/Q \leqslant C/Q$, where C/Q denotes the centraliser in G_λ/Q of the subgroup $F(G_\lambda/Q)$. But the solubility of G_λ/Q implies that $C/Q \leqslant F(G_\lambda/Q)$, and hence $HQ/Q = F(G_\lambda/Q)$. Thus $HQ \lhd G_\lambda$, and since H is a Hall q'-subgroup of G_λ we deduce that G_λ/HQ is a q-group. It follows easily that $n(G_\lambda) \leqslant 3$, and then, in view of the fact that $R = C_G(N) \leqslant G_\lambda$, we have $n(R) \leqslant 3$.

Let $\overline{G}$ denote G/R. Clearly $\overline{G}$ is soluble. Theorem 2.17 implies that, regarded additively, $\hat{N}$ is an irreducible $GF(q)\overline{G}$-module, faithful for $\overline{G}$, such that $\overline{G}$ acts q'-halftransitively on $(\hat{N})^*$. If $\overline{G}$ acts q'-semiregularly on $(\hat{N})^*$ then $n(\overline{G}) \leqslant 3$ by Lemma 5.2. If $\overline{G}$ does not act q'-semiregularly on $(\hat{N})^*$ then Theorem 4.46 lists the possibilities for $\overline{G}$, and, using Theorem 1.16 for the half-transitive case, it is a simple matter to check that $n(\overline{G}) \leqslant 3$.

We conclude that R is a normal subgroup of G such that both $n(R) \leqslant 3$ and $n(G/R) \leqslant 3$. Hence $n(G) \leqslant 6$ as required.

Q.E.D.

REFERENCES

1. C. Curtis and I. Reiner, Representation theory of finite groups and associative algebras (Wiley-Interscience, New York, 1962).

2. F.R. Demeyer, "Galois theory in separable algebras over commutative rings", Illinois J. Math. 10 (1966) 287-295.

3. ———— and G.J. Janusz, "Finite groups with an irreducible representation of large degree", Math. Z. 108 (1969) 145-153.

4. D. Gorenstein, Finite groups (Harper and Row, New York, 1968).

5. I.N. Herstein, Topics in algebra (Xerox College Publishing, Lexington, Mass., 1964).

6. B. Huppert, Endliche Gruppen I (Springer, Berlin 1967).

7. ————, "Zweifach transitive, auflösbare Permutationsgruppen", Math. Z. 68 (1957) 126-150.

8. I.M. Isaacs, Character theory of finite groups (Academic Press, New York, 1976).

9. ———— and D.S. Passman, "Groups with representations of bounded degree", Canad. J. Math. 16 (1964) 299-309.

10. ————————————, "Half-transitive automorphism groups", Canad. J. Math. 18 (1966) 1243-1250.

11. D.S. Passman, "Solvable half-transitive automorphism groups", J. Algebra 6 (1967) 285-304.

12. ——————, "Solvable 3/2-transitive permutation groups", J. Algebra 7 (1967) 192-207.

13. ——————, "Exceptional 3/2-transitive permutation groups", Pacific J. Math. 29 (1969) 669-713.

14. B.M. Puttaswamaiah and J.D. Dixon, Modular representation theory of finite groups (Academic Press, New York, 1977).

15. K. Shoda, "Bemerkungen über vollständig reduzible Gruppen", J. Fac. Sci. Tokyo (1) II (1931) 203-209.

16. ————, "Über die monomialen Darstellungen einer endlichen Gruppe", Proc. Phys. - Math. Soc. Japan 15 (1933) 251-257.

17. È.M. Žmud', "On isomorphic linear representations of finite groups", (Russian) Mat. Sb. (N.S.) 38 (80) (1956) 417-430.