PROBLEMS IN GROUP THEORY

W.B.Stewart



ABSTRACT

Using combinatorial and character-theoretic methods the following theorems are proved.

Theorem I Let G be a finite simple group containing two non-conjugate subgroups A, B such that:

(i) if $a \in A$, $a \neq 1$, then $C_G(a) = A$; if $b \in B$, $b \neq 1$, then $C_G(b) = B$;

(ii) $| N_G(A)/A | = 2$, $| N_G(B)/B | = 2$.

Then G is isomorphic to some PSL $(2,2^{\alpha})$.

Theorem II Let G be a finite simple group containing a subgroup A such that:

(i) if $a \in A$, $a \neq 1$, then $C_G(a) = A$;

(ii) $| N_G(A)/A | = 2$;

(iii) 3 divides $|A|$.

Then G is isomorphic to some PSL $(2,q)$.

A C K N O W L E D G E M E N T S

I am grateful to my Supervisor, Professor G.Higman, who suggested this problem, for his advice and encouragement in the preparation of this thesis. I would also like to thank the Carnegie Trust for the Universities of Scotland, by whom I was supported in 1963-65.

1.5.67. W.B. Stewart.

Table of Contents

			page
Chapter	1.	Introduction	1
Chapter	2.	Notation, Definitions and Known Results	4
Chapter	3.	Preliminary Lemmas	24
Chapter	4.	Dihedral Normalisers	71
Chapter	5.	The Main Theorem	82
Chapter	6.	Structure of the Sylow 2-subgroup of G	88
Chapter	7.	The Value of L, and the character table of G	117
Chapter	8.	The Case $L = 2$	124
Chapter	9.	The Case $L = 0$	129
Chapter	10.	Conclusion	141

Bibliography.

CHAPTER 1

Introduction

The main purpose of this thesis is to prove a generalisation of the following theorem.

Theorem of Feit and Thompson (9)[1] Let G be a non-cyclic simple finite group which contains a self-centralising subgroup of order 3. Then G is isomorphic to PSL (2,5) of to PSL (2,7).

To this end we consider, in Chapter 4, the character tables of a finite simple group G which contains a subgroup A such that:

(i) if $a \in A$, $a \neq 1$ then $C_G(a) = A$;

and (ii) $| N_G(A)/A | = 2$

By induction from $N_G(A)$ a fragment of the character table of G is constructed; and in fact all other irreducible characters of G vanish on $A - \{1\}$. Then by the usual character theoretic method certain of the multiplicative constants of the class algebra of G may be evaluated. Using the known structure of the finite groups

$$< x,y \mid x^2 = y^2 = (xy)^n = 1 > \approx D_{2n}$$

$$< x,y \mid x^2 = y^3 = (xy)^3 = 1 > \approx A_4$$

$$< x,y \mid x^2 = y^3 = (xy)^4 = 1 > \approx S_4$$

$$< x,y \mid x^2 = y^3 = (xy)^5 = 1 > \approx A_5$$

---

1. References of this form are to item 9 in the Bibliography.

group theoretical properties of G are found; and formulae relating the order of G to that of A, and to the order of the centraliser of an involution, are established. From these formulae the following theorem is proved. (cf. 2).

Theorem I. Let G be a finite simple group containing two non-conjugate subgroups A,B with the following properties:

(i) if $a \in A$, $a \neq 1$ then $C_G(a) = A$; if $b \in B$, $b \neq 1$ then $C_G(b) = B$;

(ii) $|\ N_G(A)/A\ | = 2, \quad |\ N_G(B)/B\ | = 2.$

Then $G \approx PSL\ (2,2^{\alpha})$ for some $\alpha \geq 2$.

The main theorem, which is a generalisation of the above Theorem of Feit and Thompson is:

Theorem II. Let G be a finite simple group containing a subgroup A such that:

(i) if $a \in A$, $a \neq 1$, then $C_G(a) = A$;

(ii) $|\ N_G(A)/A\ | = 2$;

(iii) 3 divides $|A|$.

Then $G \approx PSL\ (2,q)$ for some q.

It follows at once that A is cyclic, and that

$$|A| \pm 1 = 2^{\alpha} = q \qquad \text{or} \qquad 2|A| \pm 1 = p^{\alpha} = q.$$

To prove theorem II we first describe the structure of proper

subgroups of order divisible by 3 in a minimal counter example G to the theorem. This is done in Chapter 5. Then in Chapter 6, by a study of 2-subgroups of G normalised by dihedral groups of order 6, it is proved that the Sylow 2-subgroup of G is dihedral or elementary abelian. That simple groups with dihedral Sylow 2-subgroups are no counter examples to the theorem follows from Gorenstein and Walter's classification of such groups (11). That simple groups with abelian Sylow 2-subgroups are no counter examples to the theorem would follow from the (unpublished) work of Walter on such groups. In this case, however, we argue to a contradiction using Suzuki's characterisation of finite simple groups in which the centralisers of involutions are 2-groups (17, 18, 19).

CHAPTER 2

Notation, definitions, and known results

§2A. The following notation, mostly standard, is used.

$\{\cdots \mid \cdots\}$	The set of ... such that ... .
$\langle \ldots \mid \ldots \rangle$	The group generated by ... such that ... .
$\mid X \mid$	The number of elements in the set X.
$X \leqslant Y$	X is a subgroup of Y
$X < Y$	X is a proper subgroup of Y
$X \lhd Y$	X is a normal subgroup of Y
X char Y	X is a characteristic subgroup of Y
$[x,y]$	If $x,y \in G$, a group, $[x,y] = x^{-1}y^{-1}xy$.
X'	The derived group of X : that is, $\langle [x,y] \mid x,y \in X \rangle$
$Z(X)$	The centre of X: that is $\langle y \in X \mid [y,x] = 1$ for all $x \in X \rangle$
$F(X)$	The Fitting subgroup of the group X: that is, the maximal normal nilpotent subgroup of X.
$\Phi(X)$	The Frattini subgroup of the group X: that is, the intersection of all maximal subgroups of X
$[X,Y]$	This is $\langle [x,y] \mid x \in X, y \in Y \rangle$
$C_X(Y)$	The centraliser of Y in X: that is $\{x \in X \mid [x,y] = 1$ for all $y \in Y\}$
$N_X(Y)$	The normaliser of Y in X: that is $\{x \in X \mid x^{-1}yx \in Y$ for all $y \in Y\}$

$\Omega(X) = \Omega_1(X)$	The subgroup of the p-group X generated by the elements of order p.
cl (X)	The class of a nilpotent group X; that is the least integer n such that $< [x_1,\ldots,x_n] \mid x_i \in X > = <1>$
$P \in S_p(G)$	P is a Sylow p-subgroup of the group G.
Aut G	The automorphism group of a group G.
$O_\pi(G)$	The largest normal subgroup of G which is a π-group: here π is a set of primes.
p'	If p is a prime, $p' = \{q \mid q \text{ is a prime, } q \neq p\}$
$O_{p'p}(G)$	The inverse image in G of $O_p(G/O_{p'}(G))$
$\mathcal{N}_G(A)$	The set of subgroups of G which intersect A trivially and are normalised by A.
$\mathcal{N}_G(A;p)$	The p-groups in $\mathcal{N}_G(A)$.
$\#(g^\cdot h^\cdot = a)$	Here a,g,h are fixed elements of a group G. Then this is the number of solutions of the equation $g_1 h_1 = a$, with g_1 a conjugate of g, h_1 a conjugate of h.
$GF(p^n)$	The Galois field with p^n elements.
Z_n	The cyclic group of order n.
D_{2n}	The dihedral group of order 2n.
A_n	The alternating group on n letters.
S_n	The symmetric group on n letters.
PSL (n,q)	The factor group of the group of n by n unimodular matrices over GF (q) by its centre.

Sz(q)	Suzuki's simple group of order $q^2(q^2+1)(q-1)$. See (17).
rad A	If A is a ring with minimum condition, rad A is the sum of all nilpotent left ideals.
m | n	m divides n.

Convention: All groups, unless the contrary is stated, are finite.

Note: Reference to item 5, say, of the Bibliography is made thus: (5) Lemmas and propositions are numbered consecutively, thus: Lemma 3.21. This means lemma 21 of Chapter 3. Reference is made thus: "by 3.21 we have..."

§ 2B. The following known results are required in the proof of theorems of this thesis and are collected here for convenience.

Proposition 2.1 (3) Let H be a group with a fixed point free automorphism σ of order 2. Then H is an abelian group of odd order, and if $h \in H$, $h^{\sigma} = h^{-1}$.

Proposition 2.2. (3 p. 91 and 4) Let H be a group with a fixed point free automorphism of order 3. Then H is nilpotent.

Note: Here and always "fixed point free" means "leaving no element but the identify fixed."

Definition. X is a normal complex of a group H if X is a subset such that $N_H(X) = H$. If $x \in Z(H)$, then $X = \{x\}$ is a normal complex of H.

Proposition 2.3. (13, p. 203, lemma 14.3.1) If two complexes X,Y are normal in P, $P \in S_p(G)$, then they are conjugate in G if and only if they

are conjugate in $N_G(P)$.

In fact a rather stronger result is required.

Definition. Let $W \leqslant H \leqslant G$. W is said to be weakly closed in H, with respect to G, if, whenever $W^g \leqslant H$ for $g \in G$, then $W^g = W$.

Proposition 2.4. (This result is well known.) If W is weakly closed in a Sylow-p-subgroup of G, then, if $g \in G$,

(i) $< W, W^g >$ is a p-group if and only if $W^g = W$;

(ii) W, W^g are conjugate in $< W, W^g >$;

and (iii) normal complexes X, Y of W are conjugate in G if and only if they are conjugate in $N_G(W)$.

Proof: (i) Let W be weakly closed in $P \in S_p(G)$. Then if $< W, W^g >$ is a p-group, $< W, W^g > \leqslant P_1 \in S_p(G)$. So $P_1 = P^h$. But then $W, W^{h^{-1}} \leqslant P$, so $W = W^h$ and $h \in N(W)$. Then $< W, W^{gh^{-1}} > \leqslant P$. Then by weak closure $W^{gh^{-1}} = W$, and so $W^g = W^h = W$ as required.

(ii) Let $H = < W, W^g >$. Let $W \leqslant P_o \in S_p(H)$, $W^g \leqslant P_1 \in S_p(H)$. Then for some $h \in H$, $W^{gh} \leqslant P_o$. Then $W, W^{gh} \leqslant P_o$. As $P_o \leqslant P$ without loss, $W = W^{gh}$. That is W, W^g are conjugate in H.

(iii) Let X,Y be normal complexes of W which are conjugate in G, that is $X = Y^g$ for $g \in G$. Then X is normal in W, and $X = Y^g$ is normal in W^g. Hence X is normal in $H = < W, W^g >$. But $W^g = W^h$ for $h \in H$. Hence $gh^{-1} = n^{-1} \in N(W)$, and so $Y = X^{g^{-1}} = X^{h^{-1}n} = X^n$, $n \in N(W)$ as required. If X,Y are conjugate in N(W) they are at once conjugate in G.

Definition. A group G has a normal p-complement, or is p-nilpotent, if $G = PN$, $N \trianglelefteq G$, $P \cap N = 1$, $P \in S_p(G)$.

Proposition 2.5. (13, p. 203, theorem 14.3.1) (Burnside's transfer theorem.) If a Sylow p-subgroup of G is in the centre of its normaliser then G has a normal p-complement.

Proposition 2.6.(20) (Thompson's transfer theorem). If p is an odd prime, and if $P \in S_p(G)$, then G has a normal p-complement if $N(H)/C(H)$ is a p-group for all H char P.

This is an improvement, for odd p, of

Proposition 2.7. (13, p. 217, theorem 14.4.7) (Frobenius' transfer theorem.) A group G has a normal p-complement if and only if for every $Q \leq P \in S_p(G)$, $N(Q)/C(Q)$ is a p-group.

Proposition 2.8. (1) (Theorem of Brauer-Wielandt) Let T be a four-group of automorphisms of a group H of odd order. Let x_i, $i = 1,2,3$ be the involutions in T. Then

$$|H| \; |C_H(T)|^2 = |C_H(x_1)| \; |C_H(x_2)| \; |C_H(x_3)|,$$

$$\text{and} \quad H = C_H(x_1)\, C_H(x_2)\, C_H(x_3).$$

Proposition 2.9. (23) (A conjugacy theorem for nilpotent Hall subgroups) If a group G has a nilpotent subgroup N whose order and index are coprime then any subgroup N_1 of G such that $|N_1| = |N|$ is conjugate in G to N.

Proposition 2.10. (22, p. 82, 28.8) (A theorem of Schur.) Let the left regular and right regular representations of a group G be written

as matrices acting on the group algebra of G (over some field K). Then the space of matrices commuting with the left regular representation of G is spanned over K by the matrices in the right regular representation of G.

Proposition 2.1.(The finite polyhedral groups) (7, Chapter 6).

$$D_{2n} \approx \langle x,y \mid x^2 = y^2 = (xy)^n = 1 \rangle$$
$$A_4 \approx \langle x,y \mid x^2 = y^3 = (xy)^3 = 1 \rangle$$
$$S_4 \approx \langle x,y \mid x^2 = y^3 = (xy)^4 = 1 \rangle$$
$$A_5 \approx \langle x,y \mid x^2 = y^3 = (xy)^5 = 1 \rangle$$

If n is odd then all involutions in D_{2n} are conjugate. Elements of order 4 in S_4 are conjugate to their inverses. A_5 contains A_4's.

Definition. A group G is said to be p-soluble (for some prime p), if G has a normal series

$$1 \leq N_o < P_1 < N_1 < \ldots < P_l \leq N_l = G,$$

where P_i/N_{i-1} is a p-group and N_i/P_i is a p′-group. The least l such that $N_l = G$ (for some such series) is called the p- length of G.

Proposition 2.12. (14) (a) If the Sylow p-subgroup of G is abelian and if G is p-soluble then G is of p-length 1.

(b) If G is p-soluble, $O_{p',p}(G)$ contains the centraliser of $O_{p',p}(G)/O_{p'}(G)$.

Proposition 2.13. (11) (Theorem of Gorenstein and Walter) Let G be a finite simple group with dihedral Sylow 2-subgroup: then $G \approx PSL(2,q)$ for some odd prime power $q \geq 5$, or $G \approx A_7$.

Remark: In A_7 there are two classes of elements of order 3, and some 3-element is centralised by an involution.

Definition. A group is said to be a CIT-group if the centraliser of each involution is a 2-group.

Proposition 2.14. (17, 18, 19) (Theorem of Suzuki.) A simple CIT group is isomorphic to some PSL (2,q), some Sz(q), or to PSL (3,4).

Remark: Of these only the PSL $(2,2^{\alpha})$ have elementary abelian Sylow 2-subgroups of order greater than 4. For if q is an odd prime power the Sylow 2-subgroup of PSL (2,q) is either dihedral or of order 4. The Sylow 2-subgroup of Sz(q) is of class 2. PSL (3,4) certainly contains elements of order 4.

The following two results will not be used in the proof of the main theorem of the thesis: but each would lead to a simplification of the proof given, as will be indicated at an appropriate place.

Proposition 2.15. (Thompson's classification of minimal simple groups.) Let G be a finite non-abelian simple group, such that every proper subgroup of G is soluble. Then G is isomorphic to one of the following groups.

(a) PSL $(2,2^p)$, p a prime

(b) PSL $(2,3^p)$, p a prime

(c) PSL $(2,p)$, p a prime, $p > 3$, $p^2 + 1 \equiv 0 \bmod 5$.

(d) Sz (2^p) , p an odd prime

(e) PSL $(3,3)$.

This result is not yet published, but is available in typescript (21).

Remark: Of the groups in (a) - (e) only those of (d) have order prime to 3; and the Sylow 2-subgroup of Sz (2^p) is not elementary.

Proposition 2.16. (Theorem of Walter, unpublished.) There are no new simple groups with elementary abelian Sylow 2-subgroups unless the Sylow 2-group is of order 8, in which case there may be pseudo-Ree groups. Remark: "New" means not on the list published e.g. by Carter (6) In a pseudo-Ree group the Sylow 3-subgroup is not cyclic.

§ 2C. In this paragraph are collected several of the known results in the representation theory of finite groups. These results are found in (13, Chapter 16), and in (8, Chapter 12). Certain of the modular results are taken from (1).

If G is a finite group, and K a field, the group algebra KG may be constructed. It is the set of formal sums $\sum_i k_i g_i$, $k_i \in K$, $g_i \in G$, with addition and multiplication defined by

$$\Sigma k_i g_i + \Sigma l_i g_i = \Sigma (k_i + l_i) g_i ,$$

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

The multiplication is extended linearly to all of KG.

A class U of G is a set, for some fixed $h \in G$,

$U = \{g \mid g = y^{-1}hy \text{ for some } y \in G\}$. Suppose G has classes U_o, $U_1, \cdots, U_{r-1}$. Let a fixed element x_i be chosen in each U_i. Suppose $U_o = \{1\}$. It is clear that

$$| U_i | = | G | / | C_G(x_i) |$$

A representation of G (over K, on V) is a homomorphism

$$M : G \longrightarrow GL(V),$$

where V is an n-dimensional K-vector space, and GL(V) is the group of one to one endomorphisms of V. By means of M, V may be regarded as a KG-module. If a basis of V is chosen then M gives a representation of G in matrices. The dimension of V as K-space is called the degree of M. The character of G afforded by M is the map

$$\chi : G \longrightarrow K$$

defined by $\chi(g) = tr\ (M(G))$

Any vector space isomorphism

$$f : V \longrightarrow W$$

induces an isomorphism

$$F : GL(V) \longrightarrow GL(W)$$

Two representations

$$M : G \longrightarrow GL(V)$$

$$N : G \longrightarrow GL(W)$$

are said to be equivalent if there is a vector space isomorphism

$$f : V \longrightarrow W$$

so that the induced map

$$F : GL(V) \longrightarrow GL(W)$$

makes the following diagram commutative:

$$\begin{array}{ccc} G & \xrightarrow{M} & GL(V) \\ {\scriptstyle 1}\downarrow & & \downarrow{\scriptstyle F} \\ G & \xrightarrow{N} & GL(W) \end{array}$$

A representation M on V is said to be irreducible if V has no proper non-trivial KG-submodule W. Otherwise it is called reducible. If every KG-submodule of G is complemented by a KG-submodule, then the representation M of G on V is said to be completely reducible. If the representation M of G on V is reducible then it induces representations

$$L : G \longrightarrow GL(V/W)$$

$$N : G \longrightarrow GL(W)$$

Then $\chi_M = \chi_L + \chi_N$.

If G has representations

$$M : G \longrightarrow GL(U)$$

$$N : G \longrightarrow GL(V)$$

then $U \otimes_K V$ has an obvious structure as KG-module, and there is a representation

$$M \otimes N : G \longrightarrow GL(U \otimes V)$$

For the associated characters $\chi_{M \otimes N} = \chi_M \chi_N$.

If K = C, the complex numbers, then by a theorem of Mashke every finite dimensional representation of G is completely reducible and

there are but finitely many inequivalent irreducible representations of G, all obtained by reducing the regular representation of G, that is the representation got by taking V = KG, and defining

$$R : G \longrightarrow GL(V) \quad \text{by}$$

$$R(g)\ [\ \Sigma k_i g_i\ ] = \Sigma k_i (g_i g).$$

In fact if G has r classes there are precisely r inequivalent irreducible representations of G, whose characters denote by χ_o, $\chi_1, \cdots,$ χ_{r-1} where χ_o, the principal character, is afforded by the representation

$$I : G \longrightarrow GL(K)$$

by $\quad I(g) =$ identity map on K.

The character of a representation is a class function on G, and determines completely the equivalence classes to which the irreducible constituents of the representation belong. So we construct a character table for G, whose columns are indexed by the classes U_i, and rows indexed by the χ_i. The entry in the (i,j) place is $\chi_i(x_j)$.

The following orthogonality relations are well known

$$\sum_{i=o}^{r-1} \chi_i(x_j)\, \overline{\chi_i(x_k)} = \delta_{jk}\ |\ C(x_j)\ |$$

$$\sum_{j=o}^{r-1} \frac{|\ G\ |}{|\ C(x_j)\ |}\ \chi_i(x_j)\ \overline{\chi_k(x_j)} = \delta_{ik}\ |\ G\ |.$$

Here as in all character sums — denotes complex conjugate.

The numbers $\dfrac{|G|}{|C(x_i)|}\dfrac{\chi_j(x_i)}{\chi_j(1)}$ are algebraic integers.

With respect to the basis

$$[U_i] = \sum_{g \in U_i} g$$

of the centre of the group

algebra of G, called the class algebra of G, the multiplicative

constants are given by

$$[U_i]\,[U_j] = \sum_{k=o}^{r-1} a_{ijk}\ [U_k]$$

where

$$a_{ijk} = \frac{|G|}{|C_G(x_i)|\,|C_g(x_j)|} \sum_{e=o}^{r-1} \frac{\chi_e(x_i)\,\chi_e(x_j)\,\overline{\chi_e(x_k)}}{\chi_e(1)}$$

By inspection

$a_{ijk} = \#\,(x_i^{\bullet}\, x_j^{\bullet} = x_k)$, so that we have the useful

counting formula

<u>Proposition 2.17</u> $\#\,(a^{\bullet}b^{\bullet} = c) = \dfrac{|G|}{|C(a)|\,|C(b)|} \sum_{i=o}^{r-1} \dfrac{\chi_i(a)\chi_i(b)\overline{\chi_i(c)}}{\chi_i(1)}$

As $(\chi_i\chi_j)$ is also a character of G is may be written

$$\chi_i\chi_j = \sum_{k=o}^{r-1} b_{ijk}\,\chi_k.$$

Extending this linearly defines a multiplication on the set of formal

sums $\Sigma a_i \chi_i$, a_i a positive or negative integer, and makes of it a ring, the character ring of G. The elements of this ring are called difference characters of G. A metric can be defined on the ring by

$$(\chi, \phi)_G = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\phi(g)}$$

Then $\chi_0, \chi_1, \cdots \chi_{r-1}$ form an orthonormal basis for the character ring as Z-module. Call the character ring of G, char (G).

Suppose $H \leq G$. Then given a representation

$$M : G \longrightarrow GL(V)$$

we have at once a representation

$$M_H : H \longrightarrow GL(V) \quad \text{by restriction}$$

Given a representation of H

$$N : H \longrightarrow GL(U),$$

we have a representation

$$N^G : G \longrightarrow GL(KG \otimes_{KH} U), \text{ the induced}$$

representation. If χ is the character afforded by M, χ_H is the character afforded by M_H. If ϕ is the character of N, then ϕ^G is the character afforded by N^G.

Now define maps

$\downarrow_H$: char (G) $\longrightarrow$ char (H) , restriction to H,

$\uparrow^G$: char (H) $\longrightarrow$ char (G) , induction to G

by $\downarrow_H(\chi) = \chi_H$ on the basis of char (G),

$\uparrow^G(\phi) = \phi^G$ on the basis of char (H),

and extending linearly. These extensions do not violate the definitions made above for (proper) characters of G, and H.

These maps are transitive in the sense that if

$$H \leqslant L \leqslant G$$

then $((\chi)_L)_H = \chi_H$

and $(\phi^L)^G = \phi^G$

The following is often used

<u>Proposition 2.18</u> (The Frobenius Reciprocity Theorem.) Let $H \leqslant G$. Let $\chi \in$ char (G), $\phi \in$ char (H). Then $(\chi_H, \phi)_H = (\chi, \phi^G)_G$.

In certain circumstances the following result allows induced characters to be readily calculated. But first a

<u>Definition</u>. Let S be a subset of a group G, and let $1 \in S$.

Then S is said to be a TI-set in G if

(a) $S \leqslant N_G(S)$

(b) $S \cap x^{-1}Sx = \{1\}$ for all $x \in G \setminus N_G(S)$.

<u>Proposition 2.19</u> (<u>8</u>, page 275, lemma 38.15). Let S be a TI-set in G. Let $H = N_G(S)$. If $\phi \in$ char (H) vanishes outside S then ϕ and ϕ^G coincide on S- {1}. If also $\phi(1) = 0$ then for each $\psi \in$ char (H), vanishing on $J(S^3 \cap H) - S$, $(\phi^G, \psi^G)_G = (\phi, \psi)_H$.

<u>Conventions</u>. By "summing over all characters of G" will be meant "summing over a full set of inequivalent irreducible complex characters of G". In Chapters 4-10, "character" will even mean an element

$\chi \in$ char (G) with $(\chi,\chi) = 1$. When exhibiting the character table of a group the entry in a given row χ_i may be $- \mathrm{tr}[M_i(g)]$, where M_i affords the proper character χ_i. As all the sums of characters in the orthogonality relations and counting formulae involve an even number of $\chi_i(g)$ in each term this will cause no error. If $\chi_i(1)$ is known it may be determined at once whether χ_i or $-\chi_i$ is the trace of an irreducible representation: for $\mathrm{tr}[M(1)]$ is the degree of representation, and so positive.

We now turn our attention to the case when K is not of characteristic zero, or more precisely when the characteristic of K divides the order of G. Take the characteristic to be p. Let $\chi_0, \chi_1, \ldots, \chi_{r-1}$ continue to denote the ordinary characters. A representation over a field of finite characteristic is called a modular representation. One useful fact about ordinary characters is that the character of an ordinary representation at once determines the equivalence classes to which its irreducible constituents belong. In order to have a similar result for modular representations we define the Brauer character of a modular representation M. If Q is the rational field, and K the modular field in which M is a representation of G, and if m is the least common multiple of the orders of elements of G whose order is prime to p, the characteristic of K, then a fixed isomorphism of the m-th roots of unity to the m-th roots of unity over K is chosen. The Brauer character of M is then a function defined on elements of G of

prime order to p as follows: suppose the eigen values of M(g) are $\delta_1, \delta_2, .. \delta_t$; then each δ_i corresponds to some root of unity ε_i over $\mathbb{Q}$: then the Brauer character of g is $\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_t$. Then we have

Proposition 2.20. Modular representations (over K) with the same Brauer character have the same composition factors.

If $g \in G$, it is always possible to write $g = xy = yx$ uniquely where x is a p-element and y is a p'-element. Call x the p-part of g. Call g p-regular if its p-part is 1. A p-regular class is one containing p-regular elements. Then

Proposition 2.21. The number of inequivalent irreducible modular representations of G is the same as the number of p-regular classes of G, if K be algebraically closed.

If $M : G \longrightarrow GL(V)$ is any ordinary representation of G, that is a representation over the complex numbers, then if p is any rational prime, M is equivalent, modulo p, to an integral representation. Reducing this representation modulo p gives a modular representation $\bar{M}$ of G over a finite field of characteristic p. This representation involves modular irreducible constituents X_i. We then define a p-block of G as follows. It is a set of ordinary irreducible representations, where X,Y are put in the same block if there is a chain

$$X = X_0, X_1, \ldots X_s = Y$$

where X_i and X_{i-1}, when reduced as above, have a modular irreducible in common. The principal p-block of G, $B_0(G)$ is that block in which the principal representation lies. Into the block B(G) is also put

the modular irreducible appearing in the ordinary irreducible in the block; and also the set

$$\{i \mid \text{the ordinary representation } M_i \text{ affording } \chi_i \text{ is in B}\}.$$

With each representation in a block is also put its character, and its Brauer character.

Proposition 2.22. (a) The intersection of the kernels of ordinary irreducible representations in $B_o(G)$ is $O_{p'}(G)$.

(b) The intersection of the kernels of modular irreducible representations in $B_o(G)$ is $O_{p'p}(G)$.

Proposition 2.23 If $\chi_i \in B_o(G)$, and χ_j is any algebraic conjugate of χ_i, then $\chi_j \in B_o(G)$.

Proposition 2.24 χ_i, χ_j are in the same block if any only if, for all k, $\left[\frac{|G|}{|C(x_k)|} \left(\frac{\chi_i(x_k)}{\chi_i(1)} - \frac{\chi_j(x_k)}{\chi_j(1)} \right) \right]^* = 0$ where

* denotes, here as always, the residue class modulo a prime divisor of p.

Proposition 2.25 Suppose p^a is the highest power of p to divide $|G|$. Then if p^a divides $\chi_j(1)$, χ_j is said to be in a block of the highest kind. Such a block contains but one ordinary irreducible, and one modular irreducible.

Now let a be a fixed element of G, of order p^s for some $s \neq o$.

Proposition 2.26 If B is a p-block of G, and $\chi_i \in B$, then

$$\chi_i(av) = \sum_j d_{ij}^a \ \phi_j^a(v) \quad \text{for all } v \in C(a),$$

and v p-regular. The ϕ_j^a are Brauer characters of modular irreducibles in certain blocks b of C(a). The d_{ij}^a are algebraic integers in the field of the p^s-th roots of unity.

Proposition 2.27 If in 2.26, $B = B_o(G)$, only the block $b = B_o(C(a))$ arises.

Propositions 2.26 and 2.27 are the content of Brauer's Second Main Theorem on Blocks. The d_{ij}^a satisfy the following properties.

Proposition 2.28 (i) If a,b are non conjugate p-elements of G then

$$\sum_{i \in B} d_{ij}^a \ \bar{d}_{ik}^b = 0$$

(ii) Otherwise,

$$\sum_{i \in B} d_{ij}^a \ \bar{d}_{ik}^a = C_{jk}^a.$$

Here C_{jk}^a is the Cartan invariant of the modular irreducibles of C(a), Ψ_j^a, Ψ_k^a with Brauer characters ϕ_j^a, ϕ_k^a.

The Cartan invariants of a group G over a field K are found as follows. The group algebra KG is written as a direct sum

$$KG = KG.\varepsilon_1 \oplus \cdots \oplus KG.\varepsilon_m$$

where the ε_i are idempotents in the centre of KG, and where further

decomposition is impossible. Then the modular irreducible modules of G over K are $F_i = \frac{KG \cdot \varepsilon_i}{(\text{rad } KG)\varepsilon_i}$. Then C_{ij} is the number of times F_j occurs as a composition factor in $KG.\varepsilon_i$.

If in a block B of C(a) a basis different from $\{\phi_j^a \mid j \in B\}$ for the space spanned by the Brauer characters in the block is chosen different d_{ij}^a will arise, but the content of propositions 2.26, 2.27, 2.28 is unaltered. (2.28(ii) now defines C_{ij}^a). We will often work with more suitable bases than the ϕ_j^a. The following propositions, which follow from the above general considerations are of use in this thesis.

Proposition 2,29 Suppose a is a p-element of G, and C(a) is nilpotent. Then

(i) For all p-regular $v \in C(a)$, $\chi_i(av) = \chi_i(a)$ for $i \in B_o(G)$

(ii) $\sum_{i \in B_o} |\chi_i(a)|^2 = |P|$ where $P \in S_p(C(a))$.

Proposition 2.30 Suppose a is a p-element of G. If, for all $v \in C(a)$, v p-regular, $\sum_{i=o}^{r-1} \chi_i(av)k_i = 0$,

then $\sum_{i \in B} k_i \chi_i(a) = 0$ where B is any p-block of G.

All these results are in (8, Chapter 12 or 1). We now turn to some definitions required later.

Definition. $\sim$ is a relation defined on the elements of G by $x \sim y$ if and only if $x = au$, $y^g = auv$ for some $g \in G$, where a is the p-part of x, y^g and where $v \in O_{p'}(C(a))$. This is at once an equivalence relation.

Definition. PBM(G), the principal block matrix of G is the matrix $[\chi_i(C_j)]$ where $\chi_i \in B_o(G)$, and C_j runs through a set of representatives of the $\sim$ classes of G which have non-trivial p-part. The entry is indeed well defined, for if $x \sim y$,

$$\chi_i(x) = \chi_i(au)$$

$$= \chi_i(auv) \quad \text{as } v \in O_{p'}(C(a)) \text{ lies in the kernel of}$$

every modular representation in $B_o(C(a))$; so that $\chi_i(au) = \chi_i(auv)$ by Brauer's Second Main Theorem.

But $\chi_i(y) = \chi_i(y^g) = \chi_i(auv)$, whence the entry does not depend on the C_j chosen as representative.

CHAPTER 3

Preliminary Lemmas

§3A The purpose of this paragraph is to investigate the structure of 2-groups normalised by D_6's, the elements of order 3 acting fixed point free.

Lemma 3.1 Let Q be a 2-group with a fixed point free automorphism θ of order 3. Then (i) cl $Q \leq 2$;

(ii) if $|Q : Q_o| = 2$ then $Q_o' = Q'$;

(iii) if $Q_o \leq Q$ and Q_o is abelian, so is $< Q_o, Q_o^\theta >$

Proof: If A_i is (an additive abelian group isomorphic to) the i-th factor of the lower central series of Q, then θ acts as an operator on A_i. Commutation in Q induces a bilinear map $A_i \times A_j \longrightarrow A_{i+j}$, and θ permutes with commutation. If Q_o is any normal subgroup of Q admitting θ, then θ is fixed point free on Q/Q_o, for each coset contains $|Q_o| = 2^a$ elements. In particular θ is fixed point free on A_i, so that $\theta^2 + \theta + 1 = 0$ on A_i.

Let $[a,b] = x$, $[a,b\theta] = y$ for $a \in A_i b \in A_j$, $x,y \in A_{i+j}$.

Then $[a,b\theta^2] = [a, -b - b\theta] = -x-y$,

and so $[a\theta,b] = [a,b\theta^2]\theta = -x\theta - y\theta$

Hence $[a\theta^2,b] = [-a-a\theta,b] = -x + x\theta + y\theta$.

But $[a\theta^2,b] = [a,b\theta]\theta^2 = y\theta^2$, so that $(x-y\theta)(1-\theta) = 0$.

As $(1-\theta)(1-\theta^2) = +3$ this implies that $x-y\theta = 0$.

That is, if $[a,b] = x$, then $[a,b\theta] = x\theta^2$, $[a\theta,b] = x\theta^2$, and $[a\theta,b\theta] = x\theta$.

Then, for $a \in A_1$, $b \in A_1$, $c \in A_1$,

$$[a\theta,b,c] = [\,[a,b]\theta^2,c] = [a,b,c]\theta \ ,$$

$$[b,c,a\theta] = [b,c,a]\theta^2 \ ,$$

$$[c,a\theta,b] = [\,[c,a]\theta^2,b] = [c,a,b]\theta.$$

But in A_3, $[a,b,c] + [b,c,a] + [c,a,b] = 0$,

so that $[a,b,c]\theta + [b,c,a]\theta + [c,a,b]\theta = 0$ . . . . . (1)

Also $[a\theta,b,c] + [b,c,a\theta] + [c,a\theta,b] = 0$,

so from the above calculation

$$[a,b,c]\theta + [b,c,a]\theta^2 + [c,a,b]\theta = 0 \quad . . . . . \quad (2)$$

Hence, from (1) and (2),

$$[b,c,a]\theta = [b,c,a]\theta^2,$$

so that $[b,c,a] = 0$, and so $A_3 = 0$, giving part (i) of the lemma.

Part (iii) also follows, as $[a,b] = 0$ implies $[a,b\theta] = [a,b]\theta^2 = 0$.

To prove part (ii) write $x = [a,b]$.

Then $x = [a,b] = [a\theta,b\theta^2] = [a\theta^2, b\theta]$.

As $|\, Q : Q_o \,| = 2$ at least one of $a, a\theta, a\theta^2$ corresponds to an element of Q_o, as θ is without non trivial fixed points on Q/Q'. The same is true of $b, b\theta, b\theta^2$. If all of $a, a\theta, a\theta^2$ lie in Q_o then choosing the relevant $b\theta^i$ gives $x = [a,b] \in Q_o'$. If only $a \in Q_o$ then $x = [a,b + \beta.a\theta]$ for any β. As $|\, Q : Q_o \,| = 2$, β can be chosen so that $b + \beta.a\theta \in Q_o$. Then $x \in Q_o'$ as required.

Lemma 3.2 Let H be a group with a normal 2-subgroup Q such that $H/Q \approx D_6$, and such that an element $t \in H$ of order 3 acts fixed point free on Q. Let $P \in S_2(H)$.

(i) If $Q_o \leqslant Q$ admits $< t >$, and $g \in P \backslash Q$, then

$$| C_{Q_o}(g) | \leqslant | Q_o |^{\frac{1}{2}}.$$

(ii) If $| Q | > 4$, then the class of Q is less than the class of any other subgroup of index 2 in P; in particular Q char P.

Proof: If $Q_1 \neq 1$ is a minimal H-invariant subgroup of Q then $| Q_1 | = 4$, and an involution inverting t cannot centralise Q_1 so that $| C_{Q_1}(g) | \leqslant 2$. The proof of part (i) is now by induction on $| Q_o |$, taking $Q_1 \leqslant Q_o$. Then $| C_{Q_o}(g) | \leqslant |C_{Q_1}(g)| \, | C_{Q_o/Q_1}(g) | \leqslant 2|Q_o/Q_1|^{\frac{1}{2}}$ by the inductive hypothesis, and as $| Q_1 | = 4$ the result follows.

From 3.1 Q is either abelian or of class 2. If Q is abelian, then an abelian subgroup R of P, not contained in Q centralises some $g \in P \backslash Q$. Then $| R |$ is at most $2| Q |^{1/2}$, so that if $| Q | > 4$, $| R | < |Q|$; that is Q is the unique abelian subgroup of P in index 2. If, on the other hand, the class of Q is 2, and R is any other subgroup of P of index 2, then by lemma 3.1, $(R \cap Q)' = Q'$. If R is of class 1 or class 2 then R must centralise R' and so $(R \cap Q)' = Q'$. But, applying part (i) to Q', it cannot be that $Q' = C_{Q'}(g)$ for $g \in P \backslash Q$. So R is of class 3 at least.

That Q is characteristic in P follows at once.

§3B The purpose of this paragraph is to investigate 2-groups normalised by $PSL(2,2^\alpha)$ in such a way that the elements of order 3 in $PSL(2,2^\alpha)$ act fixed point free. The following notation is fixed throughout this paragraph.

$H = PSL(2,2^\alpha)$, $\alpha \geq 2$.

A is a cyclic subgroup of H or order $2^\alpha-1$, $A = \langle a \rangle$.

B is a cyclic subgroup of H of order $2^\alpha+1$, $B = \langle b \rangle$.

τ is an involution in H.

ω is a primitive $(2^\alpha-1)$th root of unity.

θ is a primitive $(2^\alpha+1)$th. root of unity.

Then every element of H is conjugate to one of the following (non-conjugate) elements of H:

$1; \tau; a^j, j = 1, \ldots, 2^{\alpha-1}-1; b^k, k = 1, \ldots, 2^{\alpha-1}$.

The character table of H may be constructed by induction from N(A) and N(B), as is done in Chapter 4. It is:

	1	a^j	τ	b^k	
I	1	1	1	1	
U	2^α	1	0	-1	
C_i	$2^\alpha+1$	$\omega^{ij}+\omega^{-ij}$	1	0	$i=1,\ldots, 2^{\alpha-1}-1$.
D_i	$2^\alpha-1$	0	-1	$-(\theta^{ik}+\theta^{-ik})$	$i=1,\ldots, 2^{\alpha-1}$

Also let K be a splitting field for H of characteristic 2:

that is, if L is an algebraic extension of K, the LH irreducibles are the

KH irreducibles. From 2.21 it follows that H has as many KH irreducibles as H has 2-regular classes: that is $1 + (2^{\alpha-1} - 1) + 2^{\alpha-1}$, or 2^{α} inequivalent 2-modular irreducibles. The first task is to construct these.

Let X_o be the natural two dimensional representation of H over $GF(2^{\alpha})$: that is, if $\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in H$,

$$X_o : H \longrightarrow GL(V) \ , \ V = GF(2^{\alpha}) \oplus GF(2^{\alpha})$$

is defined by $X_o\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$.

Let X_o, X_1, ... $X_{\alpha-1}$ be those representations obtained from X_o by field automorphisms : that is

$X_j : H \longrightarrow GL(V)$ is defined by

$$X_j : \begin{bmatrix} x & y \\ z & w \end{bmatrix} \longmapsto \begin{bmatrix} x^{2^j} & y^{2^j} \\ z^{2^j} & w^{2^j} \end{bmatrix}$$

Let M_j be V regarded as KH-module in the natural way.

Lemma 3.3 A full set of 2-modular irreducibles of H is provided by the trivial representation and by the $2^{\alpha}-1$ non- empty tensor representations $M_{i_1} \otimes M_{i_2} \otimes \ldots \otimes M_{i_r}$, where $0 \leqslant i_1 < i_2 < \ldots < i_r \leqslant \alpha-1$. [The tensor product is over K].

Proof: It suffices to show that these are irreducible: for there are the right number, and they are clearly inequivalent. In fact it will even suffice to prove that

$$M = M_o \otimes M_1 \otimes \ldots \otimes M_{\alpha-1}$$

is irreducible, for then each subproduct must be irreducible. To do this consider the Brauer character of the representation on M. With a suitable choice of ω and θ it is

$$\begin{array}{ccc} 1 & a^j & b^k \\ 2^\alpha & \prod_{i=o}^{\alpha-1} (\omega^{2^i j} + \omega^{-2^i j}) & \prod_{i=o}^{\alpha-1} (\theta^{2^i k} + \theta^{-2^i k}). \end{array}$$

To evaluate these products we need the following lemma.

Lemma 3.3.1 Let ϕ be any $(2^\alpha-1)$th root of unity, ψ any $(2^\alpha+1)$th root of unity. Then

$$\prod_{i=o}^{\alpha-1} (\phi^{2^i} + \phi^{-2^i}) = 1 \quad , \qquad \prod_{i=o}^{\alpha-1} (\psi^{2^i} + \psi^{-2^i}) = -1.$$

Pf: $$\frac{X^{2^\alpha} - Y^{2^\alpha}}{X - Y} = \prod_{i=o}^{\alpha-1} (X^{2^i} + Y^{2^i}).$$

Putting $X = \phi$, $Y = \phi^{-1}$ and observing that $\phi^{2^\alpha} = \phi$, $(\phi^{-1})^{2^\alpha} = \phi^{-1}$ gives the first identity; putting $X = \psi$, $Y = \psi^{-1}$ and observing that $\psi^{2^\alpha} = \psi^{-1}$, $(\psi^{-1})^{2^\alpha} = \psi$ gives the second identity.

Returning to the proof of lemma 3.3, notice that for any j, ω^j is a $(2^\alpha-1)$th root of unity, and for any k, θ^k is a $(2^\alpha+1)$th root of unity. So the Brauer character of the representation on M is

1	a^j	b^k
2^α	1	-1

Consider now the character U of H. It is in a block of the highest kind since $U(1) = 2^{\alpha}$ is the highest power of 2 to divide $|H| = 2^{\alpha}(2^{\alpha}-1)(2^{\alpha}+1)$. Hence by 2.25 there is but one ordinary character and one modular character in this block. As the Brauer character of the representation on M is the restriction of U to 2-regular elements it follows that the representation on M is the irreducible modular irreducible in this block. This proves that M is irreducible, and lemma 3.3 is proved.

Lemma 3.4 Ext $(M_i, M_j) = 0$: that is if W is any KH-module with submodule V, $W/V \approx M_j$, $V \approx M_i$, then W has a submodule $V' \approx M_j$, with $W = V \oplus V'$ as KH-module.

Proof: Without loss take i=o. Let ζ be a primitive $(2^{\alpha}-1)$th root of unity in K. As $|A| = 2^{\alpha}-1$, $|A|$ is prime to 2, which is the characteristic of K. Hence, by Mashke's theorem (13, 16), W is completely reducible as KA-module. That is in the representation on W we may suppose that

$$\begin{bmatrix} \zeta & \cdot \\ \cdot & \zeta^{-1} \end{bmatrix} \longrightarrow \begin{bmatrix} \zeta & \cdot & \cdot & \cdot \\ \cdot & \zeta^{-1} & \cdot & \cdot \\ \cdot & \cdot & \zeta^{n} & \cdot \\ \cdot & \cdot & \cdot & \zeta^{-n} \end{bmatrix} = L(\zeta), \quad \text{where } n = 2^{j}.$$

Also

$$\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & . & a(x) & b(x) \\ x & 1 & C(x) & d(x) \\ . & . & 1 & . \\ . & . & x^n & 1 \end{bmatrix} = M(x) \ , \ x \in GF(2^{\alpha}),$$

and

$$\begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} \longrightarrow \begin{bmatrix} . & 1 & p & q \\ 1 & . & r & s \\ . & . & . & 1 \\ . & . & 1 & . \end{bmatrix} = N \ .$$

As $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix}$ and $\begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix}$ are involutions, and this is a representation

it follows that $[M(x)]^2 = I$, $N^2 = I$. That gives $p = s$ and $r = q$; and $b(x) = 0$, $xa(x) = x^n d(x)$.

Moreover $\begin{bmatrix} \xi & . \\ . & \xi^{-1} \end{bmatrix}^{-1} \begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix} \begin{bmatrix} \xi & . \\ . & \xi^{-1} \end{bmatrix} = \begin{bmatrix} 1 & . \\ x\xi^2 & 1 \end{bmatrix}$, so that

$[L(\xi)]^{-1} M(x) L(\xi) = M(x\xi^2)$. Hence $a(x\xi^2) = a(x)\xi^{n-1}$ and $C(x\xi^2) = \xi^{n+1}C(x)$.

Also $M(x) M(y) = M(x+y)$, for $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix} \begin{bmatrix} 1 & . \\ y & 1 \end{bmatrix} = \begin{bmatrix} 1 & . \\ x+y & 1 \end{bmatrix}$.

This gives $a(x) + a(y) = a(x+y)$,

$$c(x+y) = c(x) + c(y) + xa(y) + x^{1-n} y^n a(x) \ .$$

As $\begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix}$ inverts $\begin{bmatrix} \rho & . \\ . & \rho^{-1} \end{bmatrix}$ it follows that $[L(\rho)N]^2 = I$.

That is, $q(1+\rho^{1-n}) = 0$, $p(1+\rho^{1+n}) = 0$.

Now $1+\rho^{1-n} = 0$ only if $n = 2^j = 1$, as $0 \leq j \leq \alpha-1$;

and $1+\rho^{n+1} = 0$ only if $H = PSL(2,4)$, and $j = 1$, $n = 2$.

Hence there are three cases that may arise:

<u>case (i)</u>: $L(\rho) = \begin{bmatrix} \rho & . & . & . \\ . & \rho^{-1} & . & . \\ . & . & \rho & . \\ . & . & . & \rho^{-1} \end{bmatrix}$ $M(x) = \begin{bmatrix} 1 & . & . & . \\ x & 1 & 1x & . \\ . & . & 1 & . \\ . & . & x & 1 \end{bmatrix}$ $N = \begin{bmatrix} . & 1 & . & q \\ 1 & . & q & . \\ . & . & . & 1 \\ . & . & 1 & . \end{bmatrix}$

<u>case (ii)</u>: $L(\rho) = \begin{bmatrix} \rho & . & . & . \\ . & \rho^{-1} & . & . \\ . & . & \rho^{-1} & . \\ . & . & . & \rho \end{bmatrix}$ $M(x) = \begin{bmatrix} 1 & . & ax^2 & . \\ x & 1 & a & ax \\ . & . & 1 & . \\ . & . & x^{-1} & 1 \end{bmatrix}$ $N = \begin{bmatrix} . & 1 & p & . \\ 1 & . & . & p \\ . & . & . & 1 \\ . & . & 1 & . \end{bmatrix}$

and $\rho^3 = 1$, $H = PSL(2,4)$

<u>case (iii)</u>: $L(\rho) = \begin{bmatrix} \rho & . & . & . \\ . & \rho^{-1} & . & . \\ . & . & \rho^{n} & . \\ . & . & . & \rho^{-n} \end{bmatrix}$ $M(x) = \begin{bmatrix} 1 & . & a(x) & . \\ x & 1 & c(x) & d(x) \\ . & . & 1 & . \\ . & . & x^{n} & 1 \end{bmatrix}$ $N = \begin{bmatrix} . & 1 & . & . \\ 1 & . & . & . \\ . & . & . & 1 \\ . & . & 1 & . \end{bmatrix}$

and $n \neq 1$, $\rho^3 \neq 1$.

Also $\begin{bmatrix} 1 & . \\ 1 & 1 \end{bmatrix}\begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} = \begin{bmatrix} . & 1 \\ 1 & 1 \end{bmatrix}$ is of order 3, so that $[M(1).N]^3 = I$.

This gives, in case (i) $1 = q$, . in case (iii) $c(x) = 0$, Then $a(y)x^n = a(x)y^n$, so $a(x\zeta^2) = \zeta^{2n}a(x)$, and indeed $a(x) = 0$.

In case (ii) $\begin{bmatrix} 1 & . \\ \zeta & 1 \end{bmatrix}\begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix} = \begin{bmatrix} . & 1 \\ 1 & \zeta \end{bmatrix}$ is of order 5 so that

$[M(\zeta)N]^5 = I$. The matrices may then be simultaneously reduced in case (ii).

In case (i),

$$L(\zeta) = \begin{bmatrix} \zeta & . & . & . \\ . & \zeta^{-1} & . & . \\ . & . & \zeta & . \\ . & . & . & \zeta^{-1} \end{bmatrix} \quad M(x) = \begin{bmatrix} 1 & . & . & . \\ x & 1 & 1x & . \\ . & . & 1 & . \\ . & . & x & 1 \end{bmatrix} \quad N = \begin{bmatrix} . & 1 & . & 1 \\ 1 & . & 1 & . \\ . & . & . & 1 \\ . & . & 1 & . \end{bmatrix}$$

The matrix $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ reduces these simultaneously.

That is, in every case the matrices representing $\begin{bmatrix} \zeta & . \\ . & \zeta^{-1} \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ can be simultaneously put in completely reduced form.

As $\left\langle \begin{bmatrix} \zeta & \cdot \\ \cdot & \zeta^{-1} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$ is maximal in H,

being the dihedral subgroup of order $(2^{\alpha}-1)2$, it follows that the whole of H may be completely reduced. That is, Ext $(M_i, M_j) = 0$.

Lemma3.5 Hom $(M_i \otimes M_j, M_k) = 0$; that is,there are no KH-module homomorphisms $M_i \otimes M_j \longrightarrow M_k$ but the trivial one.

Proof: If $i \neq j$ then $M_i \otimes M_j$ has been seen in 3.3 to be irreducible, and not isomorphic to any M_k. So suppose $i = j = 0$ without any loss of generality. Finding an element in Hom $(M_o \otimes M_o, M_k)$ is the same as finding a matrix $\begin{bmatrix} p_1 & q_1 & r_1 & s_1 \\ p_2 & q_2 & r_2 & s_2 \end{bmatrix}$ such that,

for all $\begin{bmatrix} t & u \\ v & w \end{bmatrix}$ in H,

$$\begin{bmatrix} p_1 & q_1 & r_1 & s_1 \\ p_2 & q_2 & r_2 & s_2 \end{bmatrix} \begin{bmatrix} t^2 & tu & ut & u^2 \\ tv & tw & uv & uw \\ vt & vu & wt & wu \\ v^2 & vw & wv & w^{+2} \end{bmatrix} = \begin{bmatrix} t^n & u^n \\ v^n & w^n \end{bmatrix} \begin{bmatrix} p_1 & q_1 & r_1 & s_1 \\ p_2 & q_2 & r_2 & s_2 \end{bmatrix}$$

where $n = 2^k$. Taking $\begin{bmatrix} t & u \\ v & w \end{bmatrix}$ as $\begin{bmatrix} \zeta & \cdot \\ \cdot & \zeta^{-1} \end{bmatrix}$ with ζ a

$(2^{\alpha}-1)$th root of unity in $GF(2^{\alpha})$, this gives

$$p_1\zeta^2 = p_1\zeta^n,\ q_1 = q_1\zeta^n,\ r_1 = r_1\zeta^n,\ s_1\zeta^{-2} = s_1\zeta^n$$

and $p_2\zeta^2 = p_2\zeta^{-n},\ q_2 = q_2\zeta^{-n},\ r_2 = r_2\zeta^{-n},\ s_2\zeta^{-2} = s_2\zeta^{-n}$.

At once $q_1 = r_1 = q_2 = r_2 = 0$, as $n \neq 0$, $n < 2^{\alpha}$.

Taking $\begin{bmatrix} t & u \\ v & w \end{bmatrix} = \begin{bmatrix} 1 & . \\ \beta & 1 \end{bmatrix}$ gives $s_1 = s_2 = p_2 = 0$.

Taking $\begin{bmatrix} t & u \\ v & w \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ . & 1 \end{bmatrix}$ gives $p_1 = 0$

So indeed the only module homomorphism is the zero homomorphism as required.

The previous three lemmas have been proved to prepare for the proof of the following fundamental lemma.

Lemma 3.6 Let the group G have a normal subgroup Q such that G/Q $\approx$ PSL $(2,2^{\alpha})$, $\alpha \geq 2$, and suppose that an element t of G acts fixed point free on Q. Then Q is elementary abelian, and is a direct product of G-invariant subgroups of order $2^{2\alpha}$. If P is a Sylow 2-subgroup of G, and $|Q| > 2^{2\alpha}$, then Q is the only abelian subgroup of P of index 2^{α}. Moreover the class of P is two in any case.

Proof: If an element t of order 3 in PSL$(2,2^{\alpha})$ acts fixed point free in a representation of PSL$(2,2^{\alpha})$, then $-\chi(t) = \frac{1}{2}\chi(1)$, where χ is the Brauer character of this representation. For no eigenvalue of the matrix representing t can be 1; and the others must arise in pairs ω, ω^{-1} where ω is a cube root of unity, since t is conjugate to t^{-1} in PSL$(2,2^{\alpha})$. As $\omega + \omega^{-1} = -1$ this gives $-\chi(t) = \frac{1}{2}\chi(1)$. Consider now the 2-modular representations found in 3.3 for PSL $(2,2^{\alpha})$. In the representations afforded by $M_0, \ldots, M_{\alpha-1}$ t is certainly represented as fixed point free, for if χ is the Brauer character of any of these

$\chi(1) = 2$, $\chi(t) = -1$. In the higher tensor products however the degree is always greater than 2, yet the Brauer character of t is always ± 1. That is, M_o, ... $M_{\alpha-1}$ are the only irreducible K.PSL$(2,2^\alpha)$ modules on which t acts without fixed points. Moreover by lemma 3.4 any module on which t is fixed point free is completely reducible.

Hence if Q of the lemma is elementary abelian, so that it affords, under conjugation in G, a 2-modular representation of PSL$(2,2^\alpha)$ on which t acts without fixed points, then Q is a direct product of G-invariant subgroups of order $2^{2\alpha}$.

From lemma 3.5 is follows that Hom $(U \otimes V, W) = 0$ where U, V, W are any K.PSL $(2,2^\alpha)$ modules on which t acts fixed point free. Then even Hom $(Q_1 \otimes Q_2, Q_3) = 0$, where Q_1, Q_2, Q_3, are elementary abelian 2-groups on which PSL $(2,2^\alpha)$ acts with t fixed point free; the tensor product is now over the integers. Hence Q of the lemma is abelian, or there is a non-zero module homomorphism

$$(Q/\Phi(Q)) \times (Q/\Phi(Q)) \longrightarrow Q'/\Phi(Q')$$

induced by commutation.

To show that Q is elementary it is sufficient to show that, if $Q = (Z_4)^{2\alpha}$, then there is no action of PSL $(2,2^\alpha)$ on Q which induces the natural action on $Q/\Phi(Q)$. Represent automorphisms of Q by matrices whos entries are integers modulo 4, (writing Q as an additive group). Consider the matrices which represent the elements $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix}$ of PSL $(2,2^\alpha)$, as x runs through GF(2^α). Since the natural action is to be induced

on $Q/\Phi(Q) = Q/2Q$,

$$\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} I + 2A & 2B \\ X + 2C & I+2D \end{bmatrix}, \quad \text{where the}$$

X, taken modulo 2, form a matrix representation of $GF(2^\alpha)$ over $GF(2)$.

As $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix}$ is an involution it must be that

$B = 0$, $D = -I+X\ A\ X^{-1}$, mod 2. As x runs through $GF(2^\alpha)$, $A = A(x) = A(X)$.

As $\alpha \geq 2$ it is possible to choose X, Y, Z such that

$$X + Y + Z = 0 \quad , \quad X, Y, Z \text{ non zero.}$$

Then modulo 2,

$$A(x) + A(y) + A(Z) = 0$$

$$X\ A(x)\ X^{-1} + Y\ A(y)\ Y^{-1} + Z\ A(Z)Z^{-1} = I$$

But X, Y, Z, modulo 2, belong to a field, so in some extension of $GF(2)$ can be diagonalised simultaneously. Then the left hand sides of the above equations have the same elements, a contradiction. Hence Q is elementary.

It now follows that if $g \in P\backslash Q$, then $| C_Q(g) | \leq | Q |^{\frac{1}{2}}$, so that the order of an abelian subgroup of P, not contained in Q, is at most $2^\alpha | Q |^{\frac{1}{2}}$. Hence the uniqueness of Q if $| Q | > 2^{2\alpha}$.

We may choose P so that in the action induced by conjugation in P, P/Q corresponds to the matrices $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix}$ as $x \in GF(2^\alpha)$. As Q is completely reducible it suffices to prove that P is of class 2 when $| Q | = 2^{2\alpha}$.

If α is even then P is normalised by an element of order 3 in G : so the result follows in this case by 3.1 applied to P. Otherwise α is odd and in particular $\alpha \geqslant 3$. Now G contains an element $\begin{bmatrix} \theta & . \\ . & \theta^{-1} \end{bmatrix}$ modulo Q, which normalises P; θ is a primitive $(2^{\alpha}-1)$th root of unity. Let g be an element in this coset. We have that $Q = \left\{ (u,v) \mid u,v \in GF(2^{\alpha}) \right\}$ and then $Z(P) = \left\{ (u,o) \right\}$. Even $Q = Z(P) \oplus Q_1$ as $< g >$-module, $Z(P)$ and Q_1 being irreducible as $< g >$ modules. Tha action of g on $Z(P)$ is multiplication by θ, and on Q_1 multiplication by θ^{-1}. The action of g on P/Q is multiplication by θ^2, and θ^2 is an algebraic conjugate of θ but not of θ^{-1} as $2^{\alpha}-1 > 3$. If now P is not of class 2, then P', which is $< g >$ invariant lies in Q and contains $Z(P)$: hence $P' = Q$. If $\bar{P}$, $\bar{Q}$ denote $P/Z(P)$, $Q/Z(P)$, then $\bar{P}' = \bar{Q}$, $Z(\bar{P}) = \bar{Q}$, $\Phi(\bar{P}) = \bar{Q}$.

Then $\bar{P}/\bar{Q}$, $\bar{Q}$ are $GF(2^{\alpha})$-vector spaces, and commutation in $\bar{P}$ is determined exactly by the map induced on cosets modulo $\bar{Q}$, that is by $(\bar{P}/\bar{Q}) \times (\bar{P}/\bar{Q}) \longrightarrow \bar{Q}$.

Tensoring with K gives a bilinear vector space map

$$U \times U \longrightarrow V$$

where U has a basis of eigen vectors of g, U_i such that $U_i g = \theta^{2^i} U_i$, and V a basis of eigenvectors of g, v_i such that $v_i g = \theta^{-2^i} v_i$. Then it is required to find suitable images in V for U x U under the induced map. The image, $U \wedge U$ has a basis $u_i \wedge u_j$, $o \leqslant i < j \leqslant \alpha-1$ of eigen vectors of g. Thus if $u_i \wedge u_j \neq 0$, $u_i \wedge u_j = v_k$ where $2^i + 2^j + 2^k \equiv 0$ modulo $2^{\alpha}-1$. As $\alpha \geqslant 3$ this is not possible.

Thus the map

$$(\bar{P}/\bar{Q}) \times (\bar{P}/\bar{Q}) \longrightarrow \bar{Q}$$

was the zero map, a contradiction : so that indeed $P' = Z(P)$, and P is of class 2. This completes the lemma.

§3C The purpose of this paragraph is to show that PSL(2,q), with q odd and greater than 5 normalises no 2-group with the element of order 3 acting fixed point free. (The exception q = 5 is expected as PSL (2,5) $\approx$ PSL (2,4), and by §3B this does indeed normalise 2-groups with the element of order 3 acting fixed point free.)

Lemma 3.7 Let G be a group with a normal 2-subgroup T, and suppose $G/T \approx PSL(2,q)$, $q = p^n$ with p prime, $p \geqslant 5$, and $q > 5$. Suppose an element t of order 3 in PSL (2,q) acts fixed point free on T, and centralises no 2-element in G. Then T = 1.

Proof: Suppose $T \neq 1$. Then it may be assumed inductively that T is elementary abelian and has no G-invariant subgroups. Then $C_G(T) = T$; for certainly $C_G(T) \geqslant T$, and as $C_G(T) \lhd G$, and G is simple, the only other possibility is $C_G(T) = G$ which leads to an immediate contradiction.

Firstly consider the case when $q \equiv -1 \pmod 4$. Then G/T has a cyclic subgroup of odd order $\frac{1}{2}(q-1)$, and a cyclic subgroup of even order $\frac{1}{2}(q+1)$. Hence 3 divides $\frac{1}{2}(q-1)$, and so a Sylow p-subgroup of G/T is normalised by an element of order 3. Then $Q \in S_p(G)$ can be chosen such that t normalises QT. As t is fixed point free on QT, QT is

nilpotent by 2.2 Therefore $Q \lesssim C_G(T)$. This is a contradiction, so that $q \not\equiv -1 \pmod 4$.

Hence $q \equiv 1 \pmod 4$, and, as $\frac{1}{2}(q-1)$ is even, 3 must divide $\frac{1}{2}(q+1)$. It will now be sufficient to prove that PSL (2,q) has no 2-modular irreducibles on which t, an element of order 3 acts fixed point free. Recall the criterion for this: if χ is the Brauer character of the representation, t is fixed point free if and only if $\chi(t) = -\frac{1}{2}\chi(1)$. The following notation is fixed.

$H = \langle a \rangle$ is the cyclic subgroup of PSL (2,q) of order $\frac{1}{2}(q-1)=2^{\alpha}n$.

$K = \langle b \rangle$ is the cyclic subgroup of PSL (2,q) of order $\frac{1}{2}(q+1)$, which is odd.

θ is a primitive $\frac{1}{2}(q+1)$-th root of unity.

ω is a primitive $\frac{1}{2}(q-1)$-th root of unity.

q_1, q_2 denote the two classes of p-elements of PSL(2,q). Then every element is PSL (2,q) is conjugate to one of 1, q_1, q_2, a^i, b^j : and a^i is conjugate to a^{-i} only, and b^j to b^{-j} only, (of these five types.) Inducing up from N(H), N(K) gives the following character table for PSL (2,q). (cf. Note L in 3).

	1	b^j	q_1	q_2	a^k
A	1	1	1	1	1
B	$\frac{1}{2}(q+1)$	0	$\frac{1}{2}(1+\sqrt{q})$	$\frac{1}{2}(1-\sqrt{q})$	$(-1)^k$
C	$\frac{1}{2}(q+1)$	0	$\frac{1}{2}(1-\sqrt{q})$	$\frac{1}{2}(1+\sqrt{q})$	$(-1)^k$
D	q	-1	0	0	1
E_i	q-1	$-(\theta^{ij}+\theta^{-ij})$	-1	-1	0
F_i	q+1	0	1	1	$(\omega^{ik}+\bar{\omega}^{ik})$

There are $(q-1)/4$ characters E_i, and $(q-5)/4$ characters F_i. The highest power of 2 to divide the order of PSL(2,q) (which is $\frac{1}{2}q(q^2-1)$) is 2^{a+1}. But 2^{a+1} divides q-1, which is the degree of each E_i. So each E_i is in a block of the highest kind, which contains but one modular irreducible, whose Brauer character agrees with E_i on the elements of odd order. Then the Brauer character has degree q-1, and value on the 3 element $-(-1) = +1$. Hence t is fixed point free in no E_i, (modulo 2).

Now consider the partitioning of the other characters into 2-blocks. Recall that χ, ζ go in the same 2-block if

$$\left[\frac{|G|}{|C(g)|}\left(\frac{\chi(g)}{\chi(1)} - \frac{\zeta(g)}{\zeta(1)}\right)\right]^{*} = 0$$ where * denotes the residue class modulo a prime divisor of 2.

On the classes 1, b^j, q_1, q_2,

$$A + D = B + C = F_1 = \ldots = F_s, \qquad s = (q-5)/4.$$

It is therefore sufficient to consider the elements of A- $\{1\}$ when applying the above formula. For $\chi = F_i$, $\zeta = F_j$ this is

$$\left[\frac{|G|}{|C(a^k)|} \cdot \frac{1}{q+1} \left\{ \omega^{ki} + \omega^{-ki} - \omega^{kj} + \omega^{-kj} \right\} \right]^*$$

$$= \left[q(-\omega^{kj}) \ (1 - \omega^{k(i-j)}) \ (1 - \omega^{-k(i+j)}) \right]^* \text{ if } k \neq (q-1)/4$$

$$= \left[q \cdot \tfrac{1}{2} \cdot (-\omega^{kj}) \ (1-\omega^{k(i-j)}) \ (1- \omega^{-k(i+j)}) \right]^* \text{ if } k = (q-1)/4$$

But if $k = (q-1)/4$ then $\omega^k = (-1)$, so $F_i(a^k) = F_j(a^k)$ in this case, for all i,j.

We may therefore restrict our attention to the case $k \neq (q-1)/4$, or even, since q is odd and ω^{kj} is a unit to

$$\left[(1 - \omega^{k(i-j)}) \ (1- \omega^{-k(i+j)}) \right]^* = L^*$$

It will even suffice to consider only $k = 1$, for if L^* is non-zero when $k = 1$, F_i and F_j are not in the same 2-block; and if a prime divisor of 2 divides $(1- \omega^{(i-j)}) \ (1- \omega^{-(i+j)})$ then it divides $(1- \omega^{k(i-j)}) \ (1- \omega^{-k(i+j)})$. Summing up, F_i, F_j are in the same 2-block if and only if

$$\left[(1- \omega^{(i-j)}) \ (1- \omega^{-(i+j)}) \right]^* = 0.$$

If ζ is a primitive l-th root of unity, then $1-\zeta$ is a unit if l is composite, and divides p and no other rational prime if $l = p^a$.

Thus F_i, F_j are in the same 2-block if, and only if, $\omega^{(i-j)}$ or $\omega^{(i+j)}$ is a primitive 2^β-th root of unity. That is, if and only if $i \equiv \pm j \pmod n$, where $(q-1)/2 = 2^\alpha n$, n odd.

Moreover on all classes $A + D = B + C$, and A, B, C, D are in the principal block. F_i is in the principal block if and only if

$$\left[\frac{|G|}{|C(a^k)|} \cdot \left\{ 1 - \frac{(\omega^{ki} + \omega^{-ki})}{q+1} \right\} \right]^* = 0,$$

that is, if and only if $[\omega^{-ki}(1 + \omega^{2ki})]^* = 0$, or if and only if $i \equiv 0 \pmod n$.

Thus modulo a prime divisor of 2,

$$A + D = B + C = F_i \quad , \quad i \equiv 0 \pmod n ;$$

$$F_j = F_k \quad , \quad j \equiv \pm k \pmod n.$$

Consider first any non principal block B. All the characters in this block are equivalent modulo 2 : hence the Brauer character of any modular irreducible in B, which must be written as an integral combination of the ordinary characters in the block, has just the same entries as F_j. But $F_j(1) = q + 1$, and $F_j(t) = 0$ where t is a 3-element, so t is not fixed point free in these representations.

Consider now the principal 2-block, with ordinary characters A, B, C, D, F_i with $i \equiv 0 \ (n)$. B and C, and each F_i, must involve A. So modulo 2,

$$B = A + X, \quad C = A + Y, \quad D = A + X + Y, \quad F_i = 2A + X + Y.$$

X & Y are indeed irreducible: for considering how the Sylow p-normaliser is represented we have that the degree of an irreducible is at least q-1/2.

Counting 2-regular classes, and 2-modular irreducibles it follows that A,X,Y are the remaining modular irrudicibles. If $q > 5$ then t acts fixed point free in none of A,X,Y. This concludes the proof of lemma 3.7.

§3D In this paragraph are proved three results on 2-groups. They are all probably well-known.

Lemma 3.8 Let T be a 2-group containing a self centralising subgroup which is elementary of order 4. Then T is dihedral or semi dihedral.

Proof: If $|T| = 4$ the result is trivially true : for the four-group is a degenerate dihedral group. Suppose inductively that the result is true if $|T| \leqslant 2^{n+1}$. Let T now be a group of order 2^{n+2} satisfying the hypothesis of the theorem, and let V be the four-group. Then T has a (normal) subgroup of index 2 containing V, say T_o. By the inductive assumption

$$\text{either } T_o = \langle a,b \mid a^2 = b^{2^n} = 1,\ a^{-1}ba = b^{-1} \rangle \quad \ldots . \quad \text{(i)}$$

$$\text{or } T_o = \langle a,b \mid a^2 = b^{2^n} = 1,\ a^{-1}ba = b^{2^{n-1}}.b^{-1} \rangle \quad \ldots \quad \text{(ii)}$$

In case (ii), $n \geqslant 3$. In each case $Z(T) = Z(T_o) = \langle b^{2^{n-1}} \rangle$

In each case $T/C_T(T_o)$ is isomorphic to a 2-subgroup of Aut T_o; and $C_T(T_o) = Z(T) = \langle b^{2^{n-1}} \rangle$.

In case (i), $T/\langle b^{2^{n-1}} \rangle \approx \left\langle g,h \;\middle|\; \begin{matrix} g : a \to ab \\ g : b \to b \end{matrix} \quad , \quad \begin{matrix} h : a \to a \\ h : b \to b^{-1} \end{matrix} \right\rangle$

and as this group is dihedral, and as g^2 induces the inner automorphism of T_o corresponding to b it follows that there are two

possibilities for T : it is either dihedral or semidihedral of order 2^{n+2}.

If T_o is in case (ii) then $T/ < b^{2^{n-1}} >$ is isomorphic to a 2-subgroup of Aut T_o : but in this case the automorphism group is but $T_o/Z(T_o)$, so $| T : T_o | \neq 2$ as supposed.

Lemma 3.9 Let T be an elementary abelian 2-group of order 2^{α}. Let A be an abelian group of fixed point free automorphisms of T, which acts transitively on T- {1}. If $| A | = 2^{\alpha}-1$ then A is cyclic and T can be identified with the additive group of $GF(2^{\alpha})$ in such a way that A acts as field multiplication.

Proof: As A-module T is irreducible. Also $(| A |, | T |) = 1$. By Schur's Lemma (13, 16) the automorphisms commuting with A form a (finite) field. But $[A,A] = 1$, so A is a subgroup of a finite field and hence cyclic. The rest follows at once.

Lemma 3.10 Let $H \approx D_{2n}$, n odd. If H acts irreducibly and transitively on the non trivial elements of an elementary abelian 2-group T in such a way that each element of odd order acts fixed point free then n = 3.

Proof: $| H : C_H(\tau) | = | \{\tau^h \mid h \in H\} |$ by Wielandt's formula (21, Chapter 1), where τ is any element of T. Then, as H is transitive

$$| H : C_H(\tau) | = 2^{\alpha}-1$$

Hence $| C_H(\tau) | = 2$, since $C_H(\tau) = 1$ is not possible. Also $n = 2^{\alpha}-1$. Identify T with the additive group of $GF(2^{\alpha})$. Then a generator of the

cycle of order n in H acts as multiplication by θ where θ is a primitive $(2^{\alpha}-1)$th root of unity in $GF(2^{\alpha})$. If $n > 3$ then θ is not an algebraic conjugate of θ^{-1}; but, in H, g is conjugate to g^{-1}. This establishes that $n = 3$.

§3E This paragraph is devoted to the proof of a character-theoretic result of G.Higman, which is not published. (15). This result is only required in Chapter 9, where simple groups with elementary abelian Sylow 2-subgroups are being considered. The result of Walter, 2.16, would render these considerations unnecessary. As is indicated in 9.5 the assumption of Thompson's classification of minimal simple groups, 2.15, would also render this paragraph superfluous. The lemma to be proved asserts that a simple group cannot have a certain sort of Sylow 2-normaliser, and as a corollary groups with a certain sort of Sylow 2-normaliser are (2-) soluble. But firstly three preliminary lemmas.

Lemma 3.11 Let G be a p-soluble group of p-length 1. Then an ordinary irreducible character χ of G is in the principal p-block of G if (and only if) $O_{p'}(G)$ is in the kernel of a representation affording χ. (cf. 8, Chapter 12, § 88, exercise 1.)

Proof: A representation of G with $O_{p'}(G)$ in the kernel is esentially a representation of $G/O_{p'}(G)$. Factoring out $O_{p'}(G)$, it is required to prove that every character is in the principal p-block, $B_o(G)$. That is, it is required to prove that KG cannot be written as the sum of

two non trivial KG modules. Here K is the modular field. Any such direct decomposition requires $1 = e+f$ modulo rad(KG), where e and f are central idempotents of KG. In other words, if Z(KG) denote the centre of the group algebra it is required to show that

$$\frac{Z(KG)}{Z(KG) \cap \text{rad } KG} \quad \text{is one dimensional.}$$

Let $g \in O_p(G)$. Then $g - 1 \in$ rad KG, since $g \longrightarrow 1$ in any modular irreducible representation by 2.22. As a basis for Z(KG) take the class sums $[U_i] = \sum_{x \in U_i} x$. If $U_i \leqslant O_p(G)$ then

$[U_i] \equiv (\mid G \mid / \mid C(x_i) \mid) .1$ modulo rad KG.

If U_i does not lie in $O_p(G)$ no element of U_i does. Write

$[U_i] = \sum_j [U_{ij}]$ where $[U_{ij}]$ is the sum over all elements of U_i which are conjugate by elements of $O_p(G)$.

Then $[U_{ij}] \equiv \dfrac{\mid O_p(G) \mid}{\mid O_p(G) \cap C(x_{ij}) \mid} . x_{ij}$ modulo rad KG,

where x_{ij} is a representative of U_{ij}. As $O_p(G) = 1$,

$\mid O_p(G) \cap C(x_{ij}) \mid < \mid O_p(G) \mid$ by 2.12 (b). That is, each $[U_{ij}] \equiv 0$ modulo rad KG, so $[U_i] \equiv 0$ mod rad KG. Then $Z(KG)/(Z(KG) \cap \text{rad } KG)$ is indeed one-dimensional.

Lemma 3.12 Let G be a finite group, P a Sylow p-subgroup of G, and suppose P is abelian. For $x \in P$ suppose that $C_G(x)$ is p-soluble. Then

(i) $C_G(x) = (N_G(P) \cap C_G(x)).\ O_{p'}(C(x))$;

(ii) $N(P) \cap O_{p'}(C(x)) = O_{p'}(N(P) \cap C(x))$.

Proof: As all p-subgroups of G are abelian, p-solubility implies p-solubility of p-length 1 by 2.12 (a). Moreover for each $x \in P$, P is a Sylow p-subgroup of C(x). Then $O_{p'p}(C(x)) = P\, O_{p'}(C(x))$, and so P is a Sylow p-subgroup of $O_{p'p}(C(x)) \trianglelefteq C(x)$. If $g \in C(x)$ then $P^g \leq O_{p'p}(C(x))$, so $P^g = P^l$ for $l \in O_{p'}(C(x))$. Then $gl^{-1} \in N(P)$, and $gl^{-1} \in C(x)$. Hence part (i).

Now let $K = O_{p'}(N(P) \cap C(x))$. This is a p'-subgroup of N(P) and of C(x). Then it is only required to prove $K \leq O_{p'}(C(x))$.

$$\begin{aligned}[K, O_{p'p}(C(x))] &\leq [K, P.O_{p'}(C(x))] \\ &\leq [K,P].\ [K,O_{p'}(C(x))] \\ &\leq (K \cap P).\ O_{p'}(C(x)). \\ &= O_{p'}(C(x)) \qquad \text{as } K \cap P = 1\end{aligned}$$

Hence $O_{p'p}(C(x))/O_{p'}(C(x))$ is centralised by K, and so by 2.12 (b), $K \leq O_{p'p}(C(x))$. But K is a p'-group, so $K \leq O_{p'}(C(x))$.

Consider now $N(P) \cap O_{p'}(C(x))$. It is a p'-subgroup of $N(P) \cap C(x)$. Moreover

$$\begin{aligned}&[N(P) \cap O_{p'}(C(x)),\ N(P) \cap C(x)] \\ &\leq [N(P) \cap O_{p'}(C(x)),\ N(P)] \cap [N(P) \cap O_{p'}(C(x)),\ C(x)] \\ &\leq N(P) \cap O_{p'}(C(x)).\end{aligned}$$

Hence $N(P) \cap O_{p'}(C(x))$ is a normal p'-subgroup of $N(P) \cap C(x)$, and so is contained in $O_{p'}(N(P) \cap C(x))$. This completes the lemma.

The following lemma puts the results of Propositions 2.26 to 2.28 on decomposition numbers into a useful form for groups with abelian Sylow p-subgroup, and p-soluble centralisers.

Lemma 3.13 Let G be a group with abelian Sylow p-subgroup P, and suppose that for all $x \in P$, $x \neq 1$, $C_G(x)$ is p-soluble.

Then

(i) The columns of PBM(G) and PBM(N(P)) may be indexed by the same elements.

(ii) The correspondence thus established is an isometry.

(iii) Each row of PBM(G) is a linear combination, with rational integral coefficients, of the rows of PBM(N(P)).

Proof: Lemma 3.12 applies to every $x \in P$, $x \neq 1$. PBM, and $\sim$ are defined in Chapter 2, concluding definition.

(i) Every $\sim$ class of G has a representative in N(P), if its p-part is non-trivial. For let $g = au$, where a is the p-part, $a \neq 1$, and u is a p'-element in C(a). Then without loss $a \in P$. As $u \in C(a)$, then by 3.12, $u = vw$, where $v \in N(P) \cap C(a)$, and $w \in O_{p'}(C(a))$. Then $g = avw$, and $h = av$ are equivalent in G by definition. But $h = a\,v \in N(P)$ as required.

Also, if au, bv are in N(P), and $au \sim bv$ in N(P), then $au \sim bv$ in G. So it only remains to prove that if au, $bv \in N(P)$ with $au \sim bv$ in G, then $au \sim bv$ in N(P).

By assumption

$$au = au \quad , \text{ a the p-part} \; ;$$

$$(bv)^g = auw \quad , \; w \in O_{p'}(C(a)), \; u \in C(a), \quad \text{a the p-part.}$$

Raising this latter to be suitable p′-power gives that a,b are conjugate in G : as both lie in P they are conjugate in N(P), by 2.3 and the fact that P is abelian. That is, without loss suppose a = b.

Then $(av)^g$ = auw where a is the p-part, and $w \in O_{p'}(C(a))$. So g centralises a as may be seen by raising to a suitable p′-power. Hence by 3.12 $g = nk$, $n \in N(P) \cap C(a)$, $k \in O_{p'}(C(a))$. So

$$av = nkauwk^{-1}n^{-1} = nauwxn^{-1} \quad \text{where } x \in O_{p'}(C(a)), \text{ since}$$

u w ∈ (C(a). Hence $(av)^n = auw_1$, with $n \in N(P)$, $w_1 = wx \in O_{p'}(C(a))$. But $w_1 \in N(P)$ also; for $(av)^n \in N(P)$, $au \in N(P)$. So $w_1 \in O_{p'}(C(a)) \cap N(P) = O_{p'}(N(P) \cap C(a))$.

That is, au ~ av in N(P). This proves (i).

(ii) Let χ_i, i = 0, ... s denote the ordinary irreducible characters in $B_o(G)$; and ζ_i, i = 0,..t those in $B_o(N(P))$.

Then $\chi_i(au) = \sum_j d_{ij}^a \; Q_j^a(u)$ by 2.26. (as usual a is the non trivial p-part, u is in C(a)). Here the Q_j^a are in $B_o(C(a))$ by 2.27. That is, they may be regarded as Brauer characters of modular irreducibles of $C(a)/O_{p'}(C(a))$ by 2.22(a).

Also
$$C(a)/O_{p'}(C(a)) = [N(P) \cap C(a)].\, O_{p'}(C(a))/O_{p'}(C(a))$$
$$\approx (N(P) \cap C(a))/O_{p'}(N(P) \cap C(a)),$$

by 3.12 and an isomorphism theorem. So in applying 2.26 to N(P), the same Q_j^a may be chosen; that is

$$\zeta_i(au) = \overline{\sum_j D_{ij}^a \; Q_j^a}\,(u).$$

Then $$\sum_{i=o}^{s} \chi_i(au)\,\overline{\chi_i(bv)} = \sum_{j,k} Q_j^a(u) \sum_{i=o}^{s} d_{ij}^a \,\overline{d}_{ik}^{\,b}\,\overline{Q}_k^{\,b}(v).$$

If a is not conjugate to b this is 0; if a = b it gives

$$\sum_{j,k} Q_j^a(u)\, C_{ij}^a\, \overline{Q}_k^{\,a}(v);$$

where C_{ij}^a is the Cartan invariant of the irreducibles Q_i^a, and Q_j^a of the group $(N(P) \cap C(a)/O_p, (N(P) \cap C(a))$.

Similarly $$\sum_{i=o}^{t} \zeta_i(au)\,\overline{\zeta_i(bv)}$$

$$= \sum_{j,k} Q_j^a(u) \sum_{i=o}^{t} D_{ij}^a\, D_{ik}^b\, \overline{Q}_k^b(v)$$

If a is not conjugate to b this is 0 (and G-conjugation is N(P)-conjugation for $a,b \in P$); if a = b it gives

$$\sum_{j,k} Q_j^a(u)\, C_{ij}^a\, \overline{Q}_k^a(v) \quad ;$$

for by 2.28 we again get the Cartan invariant of Q_j^a and Q_k^b.

This establishes the isometry.

(iii) If $\chi_i \in B_o(G)$, then $\chi_i|_{N(P)}$ is a character of N(P), so

certainly $\chi_i(au) = \sum_j k_j \zeta_j(au)$ for rational integral coefficients k_j, and for the sum over all irreducibles of $N(P)$.

It is required to show that this holds on p-irregular elements au with $k_j = 0$ if $\zeta_j \notin B_o(N(P))$. Let M_j be a representation affording ζ_j.

Let $U = O_{p'}(N(P))$. Then $UP = C(P)$. Let $g = au$ with a the p-part.

Then $U \leqslant O_{p'}(C(a))$, so

$$U \leqslant O_{p'}(C(a)) \cap N(P) = O_{p'}(C(a) \cap N(P)).$$

Then $\chi_i(g) = \chi_i(gb)$ for any $b \in U$, and $\chi_i \in B_o(G)$.

Thus $$\chi_i(g) = \frac{1}{|U|} \sum_{b \in U} \chi_i(gb)$$

$$= \frac{1}{|U|} \sum_{b \in U} \sum_j k_j \zeta_j(gb)$$

$$= \sum_j k_j \, \mathrm{tr.}\left[M_j\left(\sum_b gb/|U|\right)\right]$$

i.e. $$\chi_i(g) = \sum_j k_j \, \mathrm{tr.}\left[M_j(g) \; M_j(\varepsilon)\right]$$

where $\varepsilon = \frac{1}{|U|} \sum_{b \in U} b$ is an idempotent in the centre of the group algebra of $N(P)$. Hence in any representation ε maps to a

scalar matrix, so $M_j(\varepsilon) = I$ or $M_j(\varepsilon) = 0$.

If $M_j(\varepsilon) = I$, then U is in the kernel of M_j, so by 3.11 M_j is in the principal block of N(P).

If $M_j(\varepsilon) = o$, then U is not in the kernel of M_j, for $\beta_j|_U$ does not contain 1_u.

So for p-irregular g,

$$\chi_i(g) = \sum_{j=o}^{t} k_j \beta_j(g) + 0$$ as required. This completes the lemma.

Now follows the main result in this paragraph. As explained at the start of the paragraph it is a criterion for non-simplicity in certain special circumstances.

Proposition 3.14 (G.Higman, lecture notes) Let G be a group with an abelian Sylow 2-subgroup P such that the following are satisfied.

(i) N(P) / C(P) is cyclic of order r.

(ii) Centralisers of involutions are (2-) soluble.

(iii) If s in the minimal length of a non trivial orbit of N(P) on P, then the number of orbits of length t, where $t > 1$, is 0, or at least $S + 2$.

(iv) P has an N(P)-invariant subgroup Q such that N(P) / C(P) acts faithfully and regularly on P/Q.

(v) $|P| > r^2$.

Then G is not simple.

Proof: The first task is to construct the characters of $B_o(N(P))$: that is of $N(P) / O_{2'}(N(P))$. Let g be an element of N(P) such that $g^r \in O_{2'}(N(P))$, and g C(P) generates N(P) / C(P). Consider the irreducible characters of P. As P is abelian these are all one-dimensional, and so form a group P^*. N(P) / C(P) permits the elements of P^*; and the action on P^* is permutation equivalent to the action on P. If $\theta \in P^*$ is in an orbit of length t then there is a character of $N(P) / O_{2'}(N(P))$ given by

$$\chi_{\theta,i}(g^j x) = \begin{cases} 0 \text{ if } t \text{ does not divide } j \\ \omega^{ij} \sum_{k=o}^{t-1} \theta(g^k \times g^{-k}) \text{ if } t \text{ divides } j. \end{cases}$$

Here ω is a fixed primitive r-th root of unity, and $x \in P$. A representation affording this character may be constructed; or note that by Brauer's characterisation of characters (8, thm. 40.1) $\chi_{\theta,i}$ is clearly a character. Then $\chi_{\theta,i}$ is irreducible, and $\chi_{\phi,j}$ is equivalent to $\chi_{\theta,i}$ if, and only if, θ and ϕ belong to the same orbit of length t, and $i \equiv j$ (modulo $\frac{r}{t}$). By calculating the sum of the squares of the degrees of the inequivalent $\chi_{\theta i}$ it is seen that the $\chi_{\theta,i}$ provide a full set of inequivalent irreducible characters of $N(P)/O_{2'}(N(P))$; that is of characters in $B_o(N(P))$.

The character $\chi_{\theta,i}$ is said to belong to the layer (t,i) of characters $B_o(N(P))$ if $\theta \in P^*$ is in an orbit of length t. Characters in the same layer represent $< g >$ in the same way; and the number of characters in the layer (t,i) is precisely the number of orbits of N(P) / C(P) on P^* (and so on P) of length t.

Henceforth assume that the proposition is false, that is that G satisfies the hypotheses, yet G is simple. Then by transfer N(P) / C(P) fixes no non trivial element of P, and so there are no non trivial orbits of length 1. Then hypothesis (iii) holds in all non trivial circumstances.

Consider now the column space of PBM (N(P)). The correspondence and isometry established in 3.13 remain valid if the bases for the column spaces of PBM(G) and PBM(N(P)) are changed in the same way. As the columns $(\chi_{\theta,i}(h))$ as h varies through the classes of $N(P) / O_{2'}(N(P))$ from the character table of $N(P) /O_{2'}(N(P))$, a basis for the column space of PBM (N(P)) is a set of column vectors $\underline{d}$ such that each $\underline{d}$ is orthogonal to every $(\chi_{\theta,i}(g^j)$, j = o, ..., r-1.

That is, for each $\underline{d}$,

$$\sum_{\theta,i} d_{\theta,i} \cdot \chi_{\theta,i}(g^j) = 0 \qquad \text{for } j = 0,\ldots,r-1$$

Now define certain columns $\underline{d}$ $(\theta, \emptyset, i)$. This column is defined if and only if $\chi_{\theta,i}$ belongs to a layer (t,i), and $\chi_{\emptyset,i}$ belongs to a layer (u,i), where t divides u.

Then $d(\theta,\emptyset,i)_{\theta,j} = 1$ if $j \equiv i$ modulo (r/u),

$d(\theta,\emptyset,i)_{\emptyset,i} = -1$

$d(\theta,\emptyset,i)_{\psi,j} = 0$ otherwise.

The first lemma shows that the $\underline{d}$ $(\theta,\emptyset,i)$ span the column space of PBM (N(P)). Bur firstly a definition. Any column of the column space

of PBM(N(P)), $\underline{d}$, such that $d_{1,j} = 0$ for all j is called <u>major</u>. A non-major column is called <u>minor</u>. Any row of PBM(N(P)) which is indexed by a $\chi_{\theta,i}$ with $\theta \neq 1$ is called <u>major</u>. A non-major row is called minor.

<u>Lemma 3.14.1</u> The columns $\underline{d}\ (\theta, \emptyset, i)$ span the column spaces of PBM(N(P)). The major $\underline{d}\ (\theta, \emptyset, i)$ span the space of the major columns of PBM(N(P)).

<u>Pf:</u> Firstly, since $1 \in P^*$ is in an orbit of length 1, and as 1 divides every t, the columns $\underline{d}\ (1,\theta,i)$ are defined. Thus any vector in the column space of PBM(N(P)) is congruent, modulo the space spanned by the $\underline{d}(\theta,\emptyset,i)$ to a vector whose only non zero coordinates are indexed by $\chi_{1,j}$. The $\underline{d}\ (\theta,\emptyset,i)$ are certainly in the column space of PBM(N(P)), so it is sufficient to prove, for the first part, that no non zero vector whose only non-zero coordinates are indexed by $\chi_{1,j}$ is orthogonal to all columns: $(\chi_{\theta,i}(g^j))$, $j = 0,\ldots r-1$. But such a non zero vector would give a non-zero linear relation between the $\chi_{1,j}$ restricted to $< g >$: and as the $\chi_{1,j}$ restricted to $< g >$ form the character table of $< g >$ this is not possible.

For the second part define $\hat{\chi}$ to be the column with 1 at χ and 0 elsewhere. If θ, $\emptyset$ have the same orbit length, then

$$\underline{d}\ (\theta, \emptyset, i) = \hat{\chi}_{\theta,i} - \hat{\chi}_{\emptyset,i}$$

Choose one θ_t for each orbit of length $t > 1$. Then the space of the major columns of PBM (N(P)) is spanned, modulo major $\underline{d}\ (\theta, \emptyset, i)$ by the $\chi_{\theta_t,i}$. If ζ_i is the character of $< g >$ given by $\zeta_i(g^j) = \omega^{ij}$, then ζ_k is a component of $\chi_{\theta_t,i}$ restricted to $< g >$ if and only if $k \equiv i$ (modulo r/t), and then just once. Let $\mu(n,j)$ be the characteristic

function on the integers of the residue class of j mod n. Then the linear relations between the $\chi_{\theta_t,i}$ restricted to $< g >$ are precisely the linear relations between the $\mu(r/t,i)$. The lemma then follows from the following description of these relations.

Lemma 3.14.2 Let K be a finite set of integers, closed under taking highest common factors. Then as a generating set for relations between the $\mu(k,i)$, $k \in K$ may be taken

$$\sum_{j \equiv i(k_1)} \mu(k_2,j) = \mu(k_1,i), \quad \text{where } k_1 \text{ divides } k_2.$$

Pf: Let k be the greatest element in K. Then $K = L \cup \{k\}$ and the hypothesis holds in L, so proceed by induction on $|K|$, the result being trivial for $|K| = 1$. By the inductive assumption it suffices to consider a relation

$$\sum_i r_i \mu(k,i) = \sum_{t,j} s_{tj} \mu(l_t,j)$$

with $l_t \in L$. Let f be the function on the integers defined by the left hand side. Then

$$f(n) = \sum_{s=1}^{p} g_s(n) \qquad \ldots\ldots\ldots \qquad (1)$$

where g_s is a function of period h_s, and the h_s may be supposed distinct. Let $m = \text{l.c.m.}\ (k,h_1,\ldots,h_p)$, and suppose $m = ku$. Then

$$f(n) = u^{-1} \sum_{i=o}^{u-1} f(n + ki), \text{ as } f \text{ is period } k.$$

Let $G_s(n) = u^{-1} \sum_{i=o}^{u-1} g_s(n + ki)$.

Then $G_s(n + k) = u^{-1} \sum_{i=o}^{u-1} g_s(n + ki) = g_s(n) + g_s(n + uk)$.

But g_s is of period h_s, and h_s divides uk, so

$$G_s(n + k) = G_s(n).$$

Also $G_s(n + h_s) = G_s(n)$.

Hence the period of G_s divides hcf (k,h_s), which is strictly less than k. But

$$f(n) = u^{-1} \sum_{i=o}^{n-1} f(n + ki) = u^{-1} \sum_{i=o}^{n-1} \sum_{s=1}^{p} g_s(n + ki)$$

i.e. $$f(n) = \sum_{s=1}^{p} G_s(n).$$

Comparing this with equation (1) gives

$$\sum_{s=1}^{p} g_s(n) = \sum_{s=1}^{p} G_s(n).$$

These functions are defined on cosets modulo elements of L, so are a

consequence of relations of the required form by the inductive hypothesis. Hence it suffices to consider

$$f(n) = \sum_{s=1}^{p} G_s(n)$$

where the period of G_s, $hcf(k,h_s)$ divides k, and is strictly less than k. But by using relations of the form $\mu(k_1,i) = \sum_{j \equiv i(k_1)} \mu(k_2,j)$, with k_1 dividing k_2, G_s may be replaced by a sum of characteristic functions $\mu(k,j)$, as $hcf(k,h_s)$ divides k. That is it suffices to consider relations of the form $\sum_i r_i \mu(k,i) = 0$; and this clearly implies that all r_i are 0, as required.

Hence lemma 3.15.1 is established. It is now possible to consider the isometry between columns in the column space of PBM(G), and columns in the column space of PBM(N(P)). Firstly, as a definition, a column of the column space of PBM(G) is called <u>major</u> (<u>minor</u>) if the corresponding column of PBM (N(P)) is <u>major</u> (<u>minor</u>). The next lemma states that the correspondence is virtually an identity on major columns.

<u>Lemma 3.14.3</u> It is possible to choose rows of PBM(G) to correspond to the rows of PBM(N(P)) in such a way that major columns of PBM (N(P)) and the corresponding major columns of PBM(G) differ only in the number

of rows in which they are all zero; and possibly in the signs of the rows.

Pf: A row of PBM(N(P)) where all major columns are zero is a minor row. So the lemma will give a definition of major and minor rows of PBM(G).

Let $\theta_1,\ldots,\theta_k$ be representatives of the orbits of length t in P^*, where $t > 1$. Then $k > s + 2 \geq 3$. Consider the columns $\underline{d}(\theta_1,\theta_j,i)$ of PBM(N(P)). These are of the form

$$\begin{array}{lccc} \chi_{\theta_1,i} & 1 & 1 & \ldots\ldots\ldots 1 \\ \chi_{\theta_2,i} & -1 & 0 & \ldots\ldots\ldots 0 \\ & \vdots & & \\ \chi_{\theta_k,i} & 0 & 0 & \qquad\qquad -1 \end{array}$$

with zeros everywhere else. Then the corresponding columns of PBM(G) are of length 2 and cross-product 1, and are columns of rational integers, each row being a rational linear combination of the rows of these $\underline{d}(\theta_1, \theta_j, i)$. Thus to within a sign in each row they are of the same form. For the reasons stated in Chapter 2, the sign in a row of a character table is negligible, so it will not be mentioned again. Thus for each layer (t,i) of rows of PBM(N(P)), $t \neq 1$, can be picked out rows of PBM(G) to correspond in a one to one fashion with the rows of PBM(N(P)). Let the row of PBM(G) corresponding to $\chi_{\theta_j,i}$ be $\chi^*_{\theta_j,i}$.

It is now necessary to show that different layers of rows of PBM(N(P)) do not become confused in PBM(G) in this correspondence. So let $\chi_{\phi_1,j}$, $\chi_{\phi_2,j}$ belong to a layer distinct from the layer of the $\chi_{\theta_s,i}$. Then $\underline{d}\ (\phi_1, \phi_2,j)$ is orthogonal to every $\underline{d}\ (\theta_1, \theta_s,i)$. Hence rows of PBM(G) corresponding to different layers are distinct.

So far, then, it is proved that if $\chi_{\theta,i}$, $\chi_{\phi,i}$ belong to the same layer, then $\underline{d}\ (\theta, \phi,i)$ is the same as the column $\underline{d}^*\ (\theta, \phi,i)$ corresponding to it in the isometry, except for the rows of PBM(G) where all major columns of PBM(G) are zero.

Let $\underline{d}\ (\theta, \phi,i)$ be any other major column of PBM(N(P)), and $\underline{d}^*(\theta, \phi,i)$ be the corresponding column of PBM(G) in the isometry. Let $\underline{d}^+\ (\theta, \phi,i)$ denote the column indexed by the rows of PBM(G), which has zeros in rows where every major column of PBM(G) has zero, and in any other row has the same entry as $\underline{d}\ (\theta, \phi,i)$ has in the corresponding row of PBM(N(P)). Call $\underline{d}^+\ (\theta, \phi,i)$ the translation of $\underline{d}\ (\theta, \phi,i)$ from N(P) to G. It is required to prove that $\underline{d}^*\ (\theta, \phi,i) = \underline{d}^+\ (\theta, \phi,i)$

$\underline{d}^+\ (\theta, \phi,i)$ has at most one non zero entry in each layer, and that is $\pm$ 1; while $d^*\ (\theta, \phi,i) - d^+\ (\theta, \phi,i)$ is constant on each major layer by orthogonality. Then

$$| d^*\ (\theta, \phi,i) | \geq | d^+\ (\theta, \phi,i) |,$$

and equality holds only if $d^*\ (\theta, \phi,i) = d^+\ (\theta, \phi,i)$.

But $| d^*\ (\theta, \phi,i) | = | d\ (\theta, \phi,i) |$ by the isometry

$= | d^+\ (\theta,\phi,i) |$ since they differ only in their number of zeros.

As the major $\underline{d}$ $(\theta,\emptyset,i)$ span PBM(N(P)) the lemma is now established. Note now that we may speak of major rows, minor rows and layers of PBM(G). A major row of PBM(G) is just one which corresponds to a major row of PBM(N(P)) in the correspondence established by the lemma. A minor row of PBM(G) is any non-major row. The next lemma states that a major part of the character table of G does not differ from that of N(P).

Lemma 3.14.4 Let $\underline{d}$ be a column of PBM(N(P)) which has the same entry in the row $\chi_{1,i}$ as in the row $\chi_{1,j}$ whenever $i \equiv j$ modulo r/s. Then the corresponding column in PBM(G) has the same entry in any major row as $\underline{d}$ does in the corresponding major row of PBM(N(P)).

Pf: If θ belongs to an orbit of length s then $\underline{d}$ is a linear combination of columns $\underline{d}$ $(1,\theta,i)$, plus a major column. Since by the previous lemma the column of PBM(G) corresponding to a major column of PBM(N(P)) is just the translation of that column to G, it suffices to prove the result for the columns $\underline{d}(1,\theta,i)$. Let $\underline{d}^*$ be the corresponding column in the isometry, $\underline{d}^+$ the translation of the major part of $\underline{d}(1,\theta,i)$. (Any column is the sum of its major part and its minor part, where the minor part vanishes on major rows, the major part on minor rows.) Then $\underline{d}^+$ has only one non zero entry, and that is $\pm$ 1; and $\underline{d}^* - \underline{d}^+$ is constant on layers. Hence if the major part of $\underline{d}^*$ differs from $\underline{d}^+$, then

$|\ d^*\ | \geq u-1$, where u is the number of characters in some

major layer. By hypothesis (iii) of proposition 3.14, this gives $|\underline{d}^*| \geq S + 1$. But $|\underline{d}| = S + 1$, and $|\underline{d}^*| = |\underline{d}|$, so the only possibility is that for some layer $|\underline{d}^*|$ vanishes outside the layer. Then there are columns

$$\begin{matrix} 1 & 1 & 1 & 0 \\ -1 & 0 & . & 1 \\ 0 & -1 & . & 1 \\ & & . & \\ 0 & 0 & -1 & 1 \end{matrix}$$, zeros

elsewhere whose sum is orthogonal to the degrees of characters of G. This is impossible, so indeed the major part of $\underline{d}^*$ is $\underline{d}^+$.

This proves the lemma.

To see the relevance of this lemma consider the column of PBM(N(P)) and the column of PBM(G) labelled by x, $x \in P$, $x \neq 1$. In PBM (N(P)) the column has the same entry in the row labelled by $\chi_{1,i}$ as $\chi_{1,j}$ whenever $i \equiv j$ modulo r/s. Hence the characters labelling major rows of PBM(G) on x are the same as the corresponding character of N(P) on x. Let $1, a_1, \ldots a_l$ be the values of the minor characters of G on x. Suppose $y \in G$, $y \neq 1$. Let b_i have the same significance for y as a_i does for x. Then

$$\sum_{i=1}^{l} (a_i - b_i)^2 = 0.$$

For in PBM(N(P)) the columns labelled by x and y differ only on major

rows, and hence, since the entries in major rows are unchanged in the isometry, the differences in minor rows cannot lead to a change of length. Then at once $a_i = b_i$ for all i : for the a_i, b_i are rational integers, being rational integral combinations of the rows of the corresponding columns of PBM(N(P), by 3.13; and these rows are rows of integers.

That is, $1, a_1, \ldots, a_l$ are independent of the choice of $x \in P$, $x \neq 1$. Let $1, x_1, \ldots, x_l$ be the degrees of the characters which form the minor rows of PBM(G). (It can be assumed that each $x_i > 0$ as the sign of the row may be altered to make this so.) The following three results are required later in the lemma.

$$x_i \equiv a_i \quad \text{modulo} \mid P \mid \qquad \ldots\ldots\ldots \qquad (1)$$

Reducing on to P gives this at once.

$$\text{If } a_i < 0 \text{ then } \mid a_i/x_i \mid \leqslant (\mid P \mid - \mid)^{-1} \qquad \ldots\ldots\ldots \qquad (2)$$

As G is simple $x_i \neq a_i$, so this is so.

$$1 + \Sigma a_i^2 = r \qquad \ldots\ldots\ldots \qquad (3)$$

Since the entries in the major rows remain unaltered this is a consequence of the isometry. The next three lemmas give a proof of

$$1 + \sum \frac{a_i^3}{x_i} = \frac{r^2}{1 + \Sigma a_i x_i} \qquad \ldots\ldots\ldots \qquad (4)$$

Lemma 3.14.5 Let θ be a character of P with Q in its kernel. (Q is defined in the hypothesis (iv) of the lemma.) If $Q \neq 1$, then

$\underline{d}$ (1,θ,0) is a linear combination of columns $\underline{\chi}(g^j y)$ of PBM(N(P)), where $\#(x^{\cdot}x^{\cdot} = g^j y) = 0$ for some involution x of Q.

Pf: By hypothesis θ belongs to an orbit of length r. ($\theta \neq 1$). Then $\underline{d}$ (1,θ,0) has entry 1 for each $\chi_{1,i}$, and an entry -1 for $\chi_{\theta,o}$. Elsewhere the entries are zero. Hence for x in Q, $[\underline{\chi}(x) - \underline{d}(1,\theta,0)]$ is major; then the column of PBM(G) corresponding to $\underline{d}(1,\theta,0)$ has entries $1,a_1,\ldots a_1$ in the minor rows, entry -1 at the row corresponding to $\chi_{\theta,0}$ and 0 elsewhere.

If $\#(x^{\cdot}x^{\cdot} = g^j y) \neq 0$, then $y \in Q$. For if $wz = g^j y$ where w,z are involutions conjugate to x, then for some conjugate w_1 of w, z_1 of z, $w_1 z_1 = y$. Each of w_1, z_1 inverts y; so as P is abelian, w_1, z_1 may be found in N(P), and so in P. Then w_1, z_1 are even N(P)-conjugates of x : so if $x \in Q$, then $w_1 \in Q$ and $z_1 \in Q$: hence $y \in Q$.

$\underline{d}$ (1,θ,0) is a sum of columns $\underline{\chi}(g^j y)$, so let the coefficient of $\underline{\chi}(g^j y)$ in this expansion be $a(g^j y)$. Then from the orthogonality

$$a(g^j y) = \frac{1}{|\, C(g^j y)\,|} \sum_{\chi} \chi(g^j y)\ d(1,\theta,0)_{\chi}\ , \quad \text{that is}$$

$$a(g^j y) = \frac{1}{|\, C(g^j y)\,|} \left\{ \sum_{i=o}^{r-1} \omega^{ij} - \delta_{oj} \sum_{i=o}^{r-1} \theta(g^{-i} y g^i) \right\}$$

If $j \neq 0$, then $a(g^j y) = 0$; if $j = 0$ then $\sum_{i=o}^{r-1} \theta\,(g^{-1} y g^i) = 1$

whenever $\#(x^{\cdot}x^{\cdot} = y) \neq 0$; that is $a(g^j y) = 0$ unless $\#(x^{\cdot}x^{\cdot}=g^j y) = 0$.

Lemma 3.14.6 If $Q \neq 1$, formula (4) holds.

Pf: In the proof of 3.14.5 we have remarked on the form of $\underline{d}^*(1,\theta,0)$. For all $\underline{\chi}(g^j y)$ which enter into $\underline{d}(1,\theta,0)$, $\#(x^{\cdot}x^{\cdot} = g^j y) = 0$: so

$$\sum_{\chi} \frac{\chi(x)^2}{\chi(1)} \overline{\chi(g^j y)} = 0$$ the sum being over all

irreducible characters of G. But in the proof of 3.14.5 it was seen that for any v of odd order in C(y),

$$\#(x^{\cdot}x^{\cdot} = vy) = 0 \quad \text{if and only if} \quad \#(x^{\cdot}x^{\cdot} = y) = 0.$$

Hence the sum may be restricted (by 2.30) to those χ which lie in $B_o(G)$. Adding for the various $\underline{\chi}(g^j y)$ in $\underline{d}^*(1,\theta,0)$ gives

$$\sum_{\chi \in B_o(G)} \frac{\chi(x)^2}{\chi(1)} \overline{d^*(1,\theta,0)_\chi} = 0.$$

But in view of the remarks in 3.14.5 on the values of $\underline{d}^*(1,\theta,0)$ this gives

$$1 + \sum \frac{a_i 3}{x_i} = \frac{\zeta(x)^2}{\zeta(1)}$$

where ζ is the (major) character of $B_o(G)$ corresponding to $\chi_{\theta,0}$. As $x \in Q$, $\chi_{\theta,0}(x) = r$; and so, since ζ is a major row, $\zeta(x) = r$. The column $\underline{d}^*(1, \theta,0)$ is orthogonal to the column of degrees of G, so

$\zeta(1) = 1 + \sum a_i x_i$. These values give the required formula (4).

Lemma 3.14.7 If Q = 1 formula (4) holds.

Pf: Let $x^2 = 1$, $x \neq 1$, $x \in P$. There are but $\frac{1}{2}(r^2-r)$ products $x^{\cdot}x^{\cdot}$ in P distinct from one another and from 1. So for some y in P, $\#(x^{\cdot}x^{\cdot} = y) = 0$. Then for all v of odd order in C(y), $\#(x^{\cdot}x^{\cdot}=vy) = 0$. Then the character counting formula may be used in $B_o(G)$ to give

$$\sum_{\chi \in B_o} \frac{\chi(x)^2}{\chi(1)} \chi(y) = 0.$$

As Q = 1 all major rows correspond to characters of G of degree

$1 + \Sigma a_i x_i$. (There is but one layer) Then we have

$$1 + \Sigma \frac{a_i^3}{x_i} = \frac{K}{1 + \Sigma a_i x_i},$$ where K depends only on major rows, and so has some value in G as the corresponding K in N(P). That is, $K = -r^2$.

Conclusion of proof of 3.14 Equations (1) - (4) are shown to be inconsistent with the assumption $|P| > r^2$, thus proving that the assumption that G is simple is false.

Formula (4) yields

$$1 + \left(\sum a_i^2\right).\min\left(\frac{a_i}{x_i}\right) \leq \frac{r^2}{1 + \Sigma a_i x_i} \leq 1 + \left(\sum a_i^2\right).\max\left(\frac{a_i}{x_i}\right)$$

If $x_i > 0$, $a_i < 0$, then the number of times the trivial character of P appears in the restriction of the i-th minor character of G to P

is non-negative: that is

$$\frac{1}{|P|}\left\{x_i + (|P|-1)\,a_i\right\} \geqslant 0.$$

That is, $x_i \geqslant -(|P|-1)a_i$, or $\min\left(\frac{a_i}{x_i}\right) \geqslant -\frac{1}{|P|-1}$

From formula (3), $a_i \leqslant \sqrt{r}$; and $x_i \neq a_i$, so $x_i \geqslant |P| + 1$

Hence $\max\left(\frac{a_i}{x_i}\right) \leqslant \frac{\sqrt{r}}{|P|+1}$. Then using the above adaptation of (4),

$$|-\frac{r-1}{|P|-1} \leqslant \frac{r^2}{|+\Sigma a_i x_i} \leqslant |+\frac{(r-1)\sqrt{r}}{|P|+1}$$

Here we have used the value of Σa_i^2, and the estimates for $\min\left(\frac{a_i}{x_i}\right)$ and $\max\left(\frac{a_i}{x_i}\right)$.

As $\frac{r-1}{|P|-1} < 1$, since $|P| > r^2$, the first inequality gives

that $1 + \Sigma a_i x_i \geqslant 0$. From the second inequality it cannot be that $1 + \Sigma a_i x_i = r$, so by the congruence relations $1 + \Sigma a_i x_i \geqslant |P| + r$.

The first inequality then gives $1 - \frac{r-1}{|P|-1} \leqslant \frac{r^2}{|P|+r}$;

that is $|P| \leqslant r^2$, a manifest contradiction, establishing the non-simplicity of G.

The following corollary is the form in which the result is required in Chapter 10.

Corollary 3.15 Let G be a group with elementary abelian Sylow 2-subgroup P, and $N(P) / C(P)$ be cyclic of order r, where r is prime to 30. Let g generate $\frac{N(P)}{C(P)}$ over $O_{2'}(N(P))$, and suppose the minimal equation of g on P is either $x^r - 1 = 0$ or $(x^r-1) / (x-1) = 0$. Then G is (2-) soluble.

Proof: It will be shown that a minimal counter example to the corollary is a counter example to proposition 3.14. Let G be a minimal counter example to corollary 3.15. Then by minimality G has no subgroup of index 2, and in particular g has no fixed point on P, or by transfer G would have such a subgroup of index 2. Then the minimal equation of g on P is $(x^r-1) / (x-1) = 1$. As centralisers of involutions are proper subgroups of G they are 2-soluble.

Moreover G is simple. For suppose $N \triangleleft G$. If N is of odd order then G / N satisfies the hypothesis, and so $N = 1$ by the minimality of G. If $|N|$ is even suppose $Q \in S_2(N)$. Then $G = N.N_G(Q)$ by a Sylow argument, and so PN is 2-soluble, where $P \in S_2(G)$ containing Q : for $PN < G$, as G has no normal sobgroup of index 2. As PN is 2-soluble so is N. If G is not 2-soluble, then N(Q) is not 2-soluble. So by minimality $N(Q) = G$. $N(Q) / C(Q)$ is of odd order since $C(Q) \geq P$, so even C(Q) is not 2-soluble, and $G = C(Q)$. Then if $Q \neq 1$, G has a normal subgroup of index 2, for g has fixed points in P, viz Q. So in fact G is simple.

Moreover G satisfies the hypothesis of proposition 3.14. Certainly (i) and (ii) hold. In (iii) take for s the smallest prime dividing r. Then if t divides r, and $t \neq 1$, the part of P on which g acts as though of order t is at least of dimension $\varphi(t)$; φ being Euler's φ-function. Then the number of orbits of length t is as least $(2^{\varphi(t_o)} - 1) / t_o$ for any prime t_o dividing it. But for prime t_o, $(2^{\varphi(t_o)} - 1) / t_o \geqslant t_o + 2$ if $t_o \geqslant 7$. As $(r,30) = 1$, hypothesis (iii) is indeed satisfied. For hypothesis (iv) note that $| P | \geqslant 2^{r-1}$, and that, for $r \geqslant 7$, $2^{r-1} > r^2$. Hence G is a counter example to proposition 3.14, and this cannot be so. The corollary is thus established.

CHAPTER 4

Dihedral Normalisers

This chapter is devoted to the construction of the character table (or part of the character table) of a group G which satisfies the following conditions.

D(A)
- (i) $1 < A < G$.
- (ii) If $a \in A$, $a \neq 1$, then $C_G(a) = A$.
- (iii) $| N_G(A) / A | = 2$.

In the latter part of the chapter theorem I of the introduction is proved.

§4A Firstly is proved a lemma about the Sylow structure of a group G satisfying D(A).

Lemma 4.1 Let G satisfy D(A). Then A is an abelian Hall Subgroup; that is $| A |$ and $| G : A |$ are coprime and A is abelian. $| A |$ is odd. Elements of A are conjugate in G if and only if they are conjugate in N(A).

Proof: N(A) induces a fixed point free automorphism of order 2 on A : hence by 2.1 A is abelian of odd order. Let $P \in S_p(A)$, $P \leq P_1 \in S_p(G)$. Then $Z(P_1) \leq C(P) = A$. Let $g \in Z(P_1)$, $g \neq 1$. Then $g \in A$. So $P_1 \leq C(g) = A$. Hence $P_1 = P$, and A is a Hall subgroup. Also $N(A) \leq N(P)$ as P char A. But $A \leq C(P)$, even $A = C(P)$. So $N(P) \leq N(A)$. That is, $N(P) = N(A)$. As A is abelian it is only required to prove the

last remark for p-elements. It is an immediate consequence of Burnside's result on normal complexes, 2-3, in that case. This proves the lemma.

For the rest of §4A the following notation is fixed.

G is a finite simple group satisfying D(A).

τ is a fixed involution in N(A).

a,b are general non conjugate elements of A - {1}. (If $|A| = 3$ this is impossible, but in that case b is not required.)

g,h are general elements of G, not conjugate to any element of A - {1}. Possibly g = h.

Then the character table of N(A) may be constructed. There are two one dimensional representations with A in their kernel. Their characters are 1 and α. There are also $\frac{1}{2}(|A|-1)$ two dimensional representations of N(A), got from the $|A| - |$ non trivial representations of A. Their characters are denoted by α_i.

Lemma 4.2 The following is a fragment of the character table of G. Any other character of G vanishes on the elements of A - {1}. (The entries in each row are determined to within a $\pm$ in accord with our convention.)

	1	a	τ	g	h
1	1	1	1	1	1
χ	χ	1	u	v	w
χ_i	χ+1	α_i(a)	u+1	v+1	w+1

Proof: For any $k \in G$, $A \cap A^k = 1$ or A. For if $a \in A \cap A^k$, $a \neq 1$, then $A, A^k \leq C(a) = A$. So A is a trivial intersection set in G. The characters $\phi_i - \phi - 1$ form a Z-basis for the difference characters of $N(A)$ which vanish outside $A - \{1\}$. Induction to G for these characters is an isometry by 2.19. So for each i, $(\phi_i - \phi - 1)^G = \chi_i - \psi_i - \theta_i$ where each χ_i, each ψ_i, each θ_i is an irreducible character of G, to within a $\pm$. By Frobenius reciprocity each $(\phi_i - \phi - 1)^G$ contains the principal character of G. So let each $\theta_i = 1$ without loss. As all cross products are 2, each pair $(\phi_i - \phi - 1)^G$, and $(\phi_j - \phi - 1)^G$ contain one more common constituent. So in fact $\psi_i = \chi$ for each i. (If $|A| = 3$ the choice of notation gives $\psi_1 = \chi$). If $a \in A$, $a \neq 1$, then the values of $\chi(a)$, $\chi_i(a)$ can be calculated. For

$$(\phi_i - \phi - 1)^G(a) = (\phi_i - \phi - 1)(a).$$

So suppose $\chi(a) = k+1$ Then $\chi_i(a) = \phi_i(a) + k$.

Then $$1 + |\chi(a)|^2 + \sum_i |\chi_i(a)|^2 \leq |C(a)| = |A|.$$

k may be supposed real as each element of A is conjugate to its inverse, even in $N(A)$. Then we have, from above,

$$(|A| + 1)\, k^2 \leq 0,$$

and so $k = 0$, as required by the lemma. But then in fact precise equality holds, so that every other irreducible character of G vanishes on $A - \{1\}$. The other columns follow from orthogonality, and choice of notation.

Lemma 4.3 $$\#(g^{\cdot}h^{\cdot} = a) = \frac{|G|}{|C(g)|\,|C(h)|}\,\frac{(x-v)(x-w)}{x(x+1)} \neq 0$$

$$\#(g^{\cdot}b^{\cdot} = a) = \frac{|G|}{|C(g)|\,|A|}\,\frac{(x-v)(x-1)}{x(x+1)} \neq 0.$$

Proof: The formula of 2.17 is used to evaluate each left hand side, the known values of $\sum_i \phi_i(a)$, $\sum \phi_i(a)\phi_i(b)$ being used.

That neither expression is zero follows from the assumption that G is simple: $x=v$ or $x=w$ implies that g or h is in the kernel of a non trivial representation: $x = 1$ implies that G has a proper derived group and so is not simple.

Lemma 4.4 All involutions in G are conjugate to τ.

Proof: Let g be some other involution of G, not conjugate to τ. Then by 4.3, $\#(g^{\cdot}\tau^{\cdot} = a) \neq 0$: that is, for some g_1, τ_1, conjugates of g, τ respectively, $g_1\tau_1 = a$. But then $< g_1, \tau_1 >$ is a dihedral group of twice odd order, so that g_1, τ_1 are conjugate in $< g_1, \tau_1 >$. This contradicts the assumption that g is not conjugate to τ, and so the lemma follows.

Lemma 4.5 For some integer R, $|G| = |A|\,x(x+1)\,R^2$, and $|C(\tau)| = (x-u)R$.

Proof: By 4.3, $\#(\tau^{\cdot}\tau^{\cdot} = a) = \frac{|G|}{|C(\tau)|^2}\,\frac{(x-u)^2}{x(x+1)}$. But

if $\rho\sigma$ = a with ρ,σ involutions, then ρ,σ invert a, and so, as C(a) = A, are in N(A). The number of such pairs of involutions in N(A) is $|A|$. Hence

$$\frac{|G|}{|A|\,x(x+1)} = \frac{|C(\tau)|^2}{(x-u)^2} = R^2 \quad \text{say.}$$

By Lagrange's theorem $|A|$ divides $|G|$; and x, x+1 divide $|G|$, being the degrees, or minus the degrees, of irreducible characters. But x, x+1 are coprime, so x(x+1) divides $|G|$. Also each of x, x+1 is coprime to $|A|$: for reduce χ and χ_1 on to A. Hence $|A|\,x(x+1)$ divides $|G|$, so the left hand side of the above identity is an integer, and so R is an integer as required. (Note that R may be negative.)

Remark. If R could be seen to be ± 1, or just odd, much of the later work would be simplified.

Lemma 4.6 If 3 divides $|A|$ then elements of order 4 in G are conjugate to their inverses inside S_4's.

Proof: Suppose $h^2 = \tau$ without loss. Let t be an element of order 3 in A. Then $(\tau^{\cdot}h^{\cdot} = t) \neq 0$. But if some solution is $\sigma f = t$, then

$$\langle \sigma, f \rangle = \langle \sigma, f \mid \sigma^2 = f^4 = (\sigma f)^3 = 1 \rangle \approx S_4$$

; as f is conjugate to f^{-1} in this S_4, h is conjugate to h^{-1} in some conjugate of it.

Lemma 4.7 If 3 divides $|A|$, then all elements of order 3 in G are conjugate, and the Sylow 3-subgroup of G is cyclic.

Proof: As A is a Hall subgroup conjugacy classes of 3-elements have

representatives in A. Let $s,t \in A$, $s^3 = t^3 = 1$, and suppose s,t are non conjugate in G. Then by 4.3, $(\tau^\circ s^\circ = t) \neq 0$, hence, for some σ, r, $\sigma r = t$,

$$< \sigma, r > = < \sigma, r \mid \sigma^2 = r^3 = (\sigma r)^3 = 1 > \approx A_4.$$

If r, $t = \sigma r$ are not conjugate in G, then r is conjugate to t^{-1} in A_4. But t is conjugate to t^{-1} in G. This proves the first part. A Sylow 3-subgroup of G, which, without loss, lies in A is now cyclic. For if not A has a subgroup elementary abelian of order 9. As elements of A which are G-conjugate are N(A) - conjugate this would imply that G has at least four classes of elements of order three contrary to the first part of the lemma. Hence the Sylow 3-subgroup is cyclic.

Lemma 4.8 If 3 divides $|A|$ and 5 divides $|G|$ then G contains A_5's.

Proof: Let t be of order 3 in A. Let f be an element of order 5 in G. Whether f has a conjugate in A or not, 4.3 gives that $(\tau^\circ f^\circ = t) \neq 0$. If σ is a conjugate of τ, h a conjugate of f with $\sigma h = t$, then

$$< \sigma, h > = < \sigma, h \mid \sigma^2 = h^5 = (\sigma h)^3 = 1 > \approx A_5.$$

This proves the lemma.

§4B This paragraph contains a proof of theorem I of Chapter 1. It relies essentially upon piecing together two fragments of the character table of G, and applying lemma 4.5 to the two different subgroups which enter the hypothesis. For convenience the theorem is restated here.

Theorem I. Let G be a finite simple group with two non-conjugate subgroups

A,B, such that G satisfies D(A) and D(B). Then G is isomorphic to some PSL $(2,2^{\alpha})$, $\alpha \geq 2$.

The proof is by a series of lemmas

Lemma 4.9 A and B are abelian Hall subgroups of odd coprime orders.

Proof: That they are abelian Hall subgroups of odd order follows from lemma 4.1. If their orders are not coprime then after suitable conjugation $1 \neq a \in A \cap B$ for some p-element a. Then $A = C_G(a) = B$, which is not so. Hence the lemma is established.

Now fix the following notation for § 4B. a is a general element of $A - \{1\}$. b is a general element of $B - \{1\}$. τ is a representative involution in G, (there is just one class of involutions by lemma 4.4). g is a representative of a conjugacy class of G not meeting N(A) or N(B). Without loss $|A| > |B|$. Then the following lemma describes the character table of G.

Lemma 4.10 The following is a fragment of the character table of G. Any other irreducible character vanishes on $A - \{1\}$ and on $B - \{1\}$, and has degree divisible by $|A| . |B|$.

	1	a	τ	b	g
1	1	1	1	1	1
χ	x	-1	u	1	v
χ_i	x-1	$-\phi_i(a)$	u-1	0	v-1
ξ_j	x+1	0	u+1	$\psi_j(b)$	v+1

Here $i = 1,\ldots \frac{1}{2}(|A| - 1)$ and the φ_i are the 2-dimensional irreducibles of N(A); and $j = 1,\ldots \frac{1}{2}(|B| - 1)$ and the ψ_j are the 2-dimensional irreducibles of N(B). Also u,v are rational.

Proof: $1, \chi, \chi_i$ are provided, at least on the classes 1, a, τ, g by lemma 4.2 (but the signs in the rows of χ, χ_i have been changed and -x substituted for x etc.). Similarly, $1, \zeta, \zeta_j$ are provided by 4.2; with the required values on the classes 1, b, τ, g, if $\zeta = -\chi$; so the first part will follow if it is established that $\zeta = -\chi$, and that the χ_j and ζ_j are distinct. If some $\chi_i = \pm\zeta, \pm\zeta_j$ then, as $|A| > |B| \geq 3$ an automorphism of the $|A|$ $|B|$-th roots of unity which fixes the $|B|$-th roots of unity would give either two characters $\zeta, \zeta' \neq 1$ which do not vanish on $A - \{1\}$ yet which take the value 1 on B : which is impossible, as no $\psi_j(b) = 1$; or would give two distinct characters ζ_j, ζ_j' of G taking the same non-zero values on $B - \{1\}$ which again is not so. By a similar argument $\chi \neq \zeta_j$ for any j. However if $1, \zeta, \chi, \zeta_j, \chi_i$ are all distinct then, by the orthogonality of the columns, $\sum_{\xi} \xi(a)\ \overline{\xi(b)} = 0$ for $a \in A - \{1\}$, $b \in B - \{1\}$, the sum being over all characters of G. This gives $1 = 0$. Hence $\chi = \pm\zeta$, and again by orthogonality $\chi = -\zeta$. That is, the fragment of the character table is as stated. The fact that any other irreducible has degree divisible by $|A|$ $|B|$ is a consequence of 4.2. If χ were not rational then there would be am algebraically

conjugate character χ' with value - 1 on a and + 1 on b. This cannot be so. Hence u,v are rational, in fact χ is a rational character. The lemma is now completely proved.

Lemma 4.11 $x = |A| - 1 = |B| + 1$, and $|G| = |A|(|A|-1).(|A|-2)R^2$.

Proof: By 4.5, for some integers R,S,

$$|G| = |A| x(x-1)R^2 = |B| x(x+1)S^2,$$

and $$|G(\tau)| = -(x-u)R = (x-u)S.$$

Hence $R = -S$ and so $|A|(x-1) = |B|(x+1)$. Now $|A|$, $|B|$ are odd coprime integers, and so the highest common factor of x-1, x+1 is at most 2. Hence either $|A| = x+1$, $|B| = x-1$ which give the lemma, or $|A| = -x-1$, $|B| = -x+1$. But in the latter case $|B| - 2 = |A|$, and, as $|A| > |B|$ this is not so. In particular the lemma states that $x > 0$; that is $1, \chi, \chi_i, \xi_j$ are proper characters of G.

Lemma 4.12 Every irreducible character of G is equivalent to one of $1, \chi, \chi_i, \xi_j$; every class of G meets N(A) or N(B). Also $u = 0$, $R^2 = 1$.

Proof: Consider $\chi\chi_1$. It is a proper character, so is expressible, with positive integral coefficients as a sum of irreducible characters of G. $(\chi\chi_1)$ has degree only $(|A|-1)(|A|-2)$ which is less than $|A||B|$, so that $(\chi\chi_1)$ can involve only $1, \chi, \chi_i, \xi_j$. On the class of g this yields an equation for v : an equation of the form

$$v(v-1) = Lv + M.$$

where L, M do not depend on g. But the roots of this equation are known. Taking g = 1 yields v = x. By Burnside's result (5), for some g, v = 0. As G is simple only the class 1 can give the root v = x, so for all others (except classes meeting A or B), v = 0. In particular u = 0.

Also $0 = (\chi, 1)_G = \sum_{h \in G} \overline{\chi}(h)$. That is,

$$|G| = |A|(|A|-1)(|A|-2), \quad \text{so } R^2 = 1.$$

Evaluating $\sum_{\xi} \overline{\xi}(1)^2$ over all irreducibles of G gives

$$|A|(|A|-1)(|A|-2) + \sum{}' \overline{\xi}(1)^2 = |A|(|A|-1)(|A|-2),$$

where Σ' is over the irreducibles other than $1, \chi, \chi_i, \xi_j$,

That is, there are no others. But the number of classes is equal to the number of inequivalent irreducibles, so that every class in fact meets N(A) or N(B).

Lemma 4.13 For some α, $x = 2^{\alpha}$, $|C(\tau)| = 2^{\alpha}$.

Proof: By 4.12, $|C(\tau)| = \pm x$. As $x > 0$, $|C(\tau)| = x$. If some element of order p, $p \neq 2$, centralises τ, then, since p is prime to $|A|$, and to $|B|$, there would be an extra class. This is not so. Hence no odd p divides $|C(\tau)|$, as required.

Lemma 4.14 The Sylow 2-subgroup of G, T, is elementary abelian.

Proof: G has no elements of order 4.

Lemma 4.15 $| G : N(T) | = 2^{\alpha} + 1$

Proof: For any $\tau \in T$, $| C(\tau) | = 2^{\alpha}$, so $C(\tau) = T$. As T is abelian conjugacy of elements of T takes place in N(T). Then, as all involutions are conjugate, and as $(2^{\alpha}-1, 2^{\alpha}+1) = 1$, it follows that $| N(T) / C(T) | = 2^{\alpha}-1$, as required.

To complete the proof of Theorem I it is now possible to exhibit G as PSL $(2,2^{\alpha})$ in its doubly transitive permutation representation on the cosets of N(T). However, in view of 4.13, Suzuki's characterisation of CIT groups may be used; the result follows as a result of the remark after 2.14, and the fact that for odd q, $q > 5$, PSL(2,q) does not satisfy the hypotheses of Theorem I. It can also be seen that any PSL $(2,2^{\alpha})$, $\alpha \geqslant 2$ has subgroups A,B which satisfy the hypotheses of the theorem.

CHAPTER 5

The Main Theorem

In this chapter a (seemingly) more general theorem than theorem II of Chapter 1 is stated. In view of the preliminary lemmas however a minimal counter example to one is a minimal counter example to the other. The restatement in fact makes the inductive assumptions rather easier to handle. The theorem is:

Theorem III Let G be a finite group, and A a subgroup of G such that the following hold.

(i) If $a \in A$, $a \neq 1$, then $C_G(a) = A$.

(ii) $| N_G(A) / A | \leq 2$.

(iii) 3 divides A.

Then G has a nilpotent normal subgroup N such that G/N is isomorphic to A, N(A) or to some PSL (2,q).

Corollary. Theorem II of Chapter 1 follows from this theorem.

Proof of corollary If G is simple, then in hypothesis (ii) it is not possible that $| N_G(A) / A | = 1$, or Burnside's transfer theorem gives a normal subgroup of prime power index. If G is simple the only possible conclusion is $G \approx PSL(2,q)$. Hence Theorem II follows.

The remaining chapters of the thesis are concerned with the proof of Theorem III, and in this chapter various facts about a minimal counter example are proved. Henceforth let G be a minimal counter example to Theorem III.

Lemma 5.1 $| N_G(A) / A | = 2$.

Proof: If not $N_G(A) = A$. By the hypothesis (1) it follows that A is abelian, and even that A is a Hall subgroup. By repeated use of Burnside's transfer theorem, 2.5, G has a normal complement N for A. Then as 3 divides A, G induces a fixed point free automorphism of order 3 on N. Hence by 2.2 N is nilpotent. This contradicts the choice of G, so that $| N_G(A) / A | = 2$ as required.

The next lemma justifies the claim about minimal counter examples to theorems II and III.

Lemma 5.2 G is simple.

Proof: If not, G has a minimal normal subgroup H.

(a) Suppose $A_o = A \cap H \neq 1$. For any $h \in G$, $A_o^h \leq H$. But as A_o is the centraliser of each of its elements in H, A_o is an abelian Hall subgroup of H, and so $A_o^h = A_o^n$ for some $n \in H$ (It is only necessary to choose n such that $P_o^h = P_o^n$ for $P_o \in S_p(A_o)$). That is,

$$G = H.N_G(A_o) = H.N_G(A).$$

Then $(G/H) \approx (H.N(A)/H) \approx N(A) / H \cap N(A)$.

But N(A) has no normal subgroup containing an involution except N(A), so that A_o is self normalising in H : for $(G/H) \neq 1$. Hence H has a normal complement for A_o by repeated use of Burnside's transfer theorem, 2.5. By minimality of H this normal complement is trivial, for it is characteristic in H, being a Hall subgroup. That is, $H = A_o$. Then $G = N(A_o) = N(A)$, and G is no counter example.

(b) Suppose $A \cap H = 1$. Then (G/H) satisfies the hypotheses of the theorem in respect of the subgroup (AH/H). For suppose $Hn \in N_{G/H}(AH/H)$. Then $n^{-1}An \leqslant AH$, and as A is an abelian Hall subgroup of AH (by 4.1) it follows that $n^{-1}An = (ah)^{-1}A\,(ah)$ for $a \in A$, $h \in H$, by 2.9. Then $n \in N(A).H$, and so $N_{G/H}(AH/H) = N_G(A)H/H$, showing that hypothesis (ii) is satisfied.

If $g \in G$ centralises $aH \in AH/H$ then $g^{-1}ag = ah$ for some $h \in H$. But $ah = a^k$ for $k \in H$. Hence $g \in N(A)H$. Hence gH is of order dividing $2 \mid A \mid$. If its order does not divide $\mid A \mid$ then G/H has elements of order 2p for p dividing $\mid A \mid$. So even G has such elements, contrary to hypothesis. So (i) is established for G/H. Hypothesis (iii) follows at once : for $\mid AH/H \mid = \mid A \mid$ as $\mid A \cap H \mid = 1$.

Then by the inductive hypothesis G/H has a normal subgroup N/H such that $(G/N) \approx (G/H) / (N/H)$ is isomorphic to N(A)H/H or to some PSL (2,q); that is G has a normal subgroup N such that G/N is isomorphic to N(A) or to some PSL (2,q). But in each case N has a fixed point free automorphism of order 3, and so is nilpotent by 2.2. Then G is no counter example to the theorem, so that G has no normal subgroup. Hence G is simple, and the lemma proved.

The following notation is fixed for the rest of this thesis. G is a minimal counter example to theorem III. The results of lemmas 4.1 to 4.8 are at once applicable to G as a result of lemmas 5.1 and 5.2.

t is a fixed element or order 3 in A; and all elements of G of order 3 are conjugate to t by 4.7.

τ is a fixed involution inverting it; all involutions of G are conjugate to τ by 4.4.

The following is a fragment of the character table of G. Every other irreducible character vanishes on A - $\{1\}$.

	1	a $\in$ A - $\{1\}$	τ	
1	1	1	1	
χ	x	1	u	
χ_i	x+1	$\phi_i(a)$	u+1	$i=1,\ldots,\frac{1}{2}(\|A\|-1)$.

Here the ϕ_i are the two-dimensional irreducibles of N(A).

L denotes the number of conjugacy classes of A_4's in G, with any class of A_4's which do not lie in S_4's counted twice; i.e.

L = #(Conjugacy classes of S_4's in G) + 2 #(conjugacy classes of A_4's in G which do not lie in S_4's)

The following formulas hold.

$$|G| = |A| x(x+1)R^2 \quad \ldots\ldots \quad (a)$$

$$|C(\tau)| = (x-u)R \quad \ldots\ldots \quad (b)$$

$$|A| x(x+1)R = (x-u)\left\{|A|L + [(|A|-1)x+1]R\right\} \quad \ldots\ldots \quad (c)$$

Here R is an integer, and of these only (c) has not been proved in Chapter 4.

Lemma 5.3 Formula (c) holds.

Proof: Using the character table of G, and the counting formula 2.17,

$$\#(t^{\cdot}\tau^{\cdot} = t) = \frac{Rx(x+1)}{(x-u)} \cdot \frac{|A|x(x+1) - (x-u)[(|A|-1)x+1]}{x(x+1)}$$

Here $|G|$, $|C(\tau)|$ have been replaced by the values given in (a), (b). If $s\sigma = t$ is any solution of $t^{\cdot}\tau^{\cdot} = t$, then $\langle s,\sigma \rangle \approx A_4$; and as all elements of order 3, and all involutions of G are conjugate, any class of A_4's gives a solution: for every A_4 contains a conjugate of t.

If $\langle s,\sigma \rangle$ does not lie in an S_4 then $|N(A)|$ members of the conjugacy class of $\langle s,\sigma \rangle$ contain t. If $\langle s,\sigma \rangle$ lies in an S_4 then only $|A|$ members of the class of this A_4 contain t. That is $\#(t^{\cdot}\tau^{\cdot} = t) = |A|.L$. For there are 3 solutions in any A_4, and only the elements of order 3 in A fix $\langle s,\sigma \rangle$. As the Sylow 3-subgroup is cyclic that gives 3. $\frac{|A|}{3}$ solutions. Simplifying the expression for $\#(t^{\cdot}\tau^{\cdot} = t)$

after substituting $\#(t^{\cdot}\tau^{\cdot} = t) = |A|.L$ gives the formula (C).

Now consider any proper subgroup H of G whose order is divisible by 3. Then the hypotheses of the theorem apply to H, so that, if $A_o = A \cap H$, H has a nilpotent normal subgroup N such that

$(H/N) \approx A_o$, or $\langle A_o, \tau \rangle$, or some PSL (2,q).

where τ inverts A_o. (Without loss $t \in H$). There is one further point to notice: if $N \neq 1$ then $N = F(H)$, for A_o acts without fixed points on N. In particular this will always happen if $Q \neq 1$, $Q < G$, Q is a 2-group and Q is normalised by t. Taking $H = N(Q)$ we will always write

"$N(Q) / F(N(Q)) \approx A_o$ or $< A_o, \tau >$ or some PSL (2,q), for some $A_o \leq A$, by the inductive hypothesis."

CHAPTER 6

Structure of the Sylow 2-subgroup of G

§6A The purpose of this chapter is to prove that the Sylow 2-subgroup of G is either dihedral or elementary abelian. To this end maximal elements of $\mathcal{M}_G(D;2)$ are studied. Here $D \approx D_6$, and as all D_6's in G are conjugate we will usually write $\mathcal{M}(D_6;2)$. If Q is such a maximal element, then by the inductive hypothesis the following cases may occur (a priori).

1. $Q = 1$
2. $|Q| = 4$, $N(Q) / F(N(Q)) \approx D_6$
3. $|Q| > 4$, $N(Q) / F(N(Q)) \approx \langle A_0, \tau \rangle$ for $A_0 \leq A$.
4. $|Q| > 4$, $N(Q) / F(N(Q)) \approx PSL(2,2^\alpha)$, and even $|Q| > 2^{2\alpha}$
5. $|Q| > 4$, $N(Q) / F(N(Q)) \approx PSL(2,2^\alpha)$, and $|Q| = 2^{2\alpha}$, with $\alpha \geq 3$.
6. $|Q| = 16$, $N(Q) / F(N(Q)) \approx PSL(2,4)$.

To see this note that if $Q \neq 1$, then $N(Q)$ is a proper subgroup of G of order divisible by 3. Hence $N(Q)$ has a normal nilpotent subgroup N such that $N(Q) / N \approx A_0$, $\langle A_0, \tau \rangle$ or some $PSL(2,q)$. As $Q \leq N$, $N \neq 1$, so that in fact $N = F(N(Q))$. Moreover Q is normalised in an involution inverting t, an element of order 3 in A. Hence $N(Q) / F(N(Q)) \approx A_0$ is impossible. Cases 2 and 3 cover the possibilities for $N(Q) / F(N(Q)) \approx \langle A_0, \tau \rangle$. By lemma 3.7 a $PSL(2,q)$ with q odd

cannot act on a 2-group with an element of order 3 fixed point free unless $q = 3^n$ or $q = 5$. As the Sylow 3-subgroup of PSL $(2,3^n)$ is not cyclic this case does not arise. Also PSL $(2,5)$ = PSL $(2,4)$ so this case is covered by the cases PSL $(2,2^\alpha)$. That $|Q| > 4$ in each case when a PSL $(2,2^\alpha)$ acts follows since by lemma 3.6, Q, on which the PSL $(2,2^\alpha)$ acts is a product of PSL $(2,2^\alpha)$ invariant subgroups of order 2^α. Cases 4,5,6 then partition the cases when PSL $(2,2^\alpha)$ acts in a convenient way. It is also worth noting that $Q \in S_2(F(N(Q)))$: this by maximality of Q in $\mathcal{N}(D_6; 2)$.

Paragraph 6B will deal with cases 1 and 2. Successive paragraphs will then show that each of the cases 3,4,5,6 does not arise. After each case is dealt with it may be assumed that any maximal element of $\mathcal{N}(D_6; 2)$ is in one of the later cases, since the purpose of this chapter is to prove:

Proposition $P \in S_2(G)$ is dihedral or elementary abelian.

§ 6B

Lemma 6.1 If G has no non-trivial 2-subgroup normalised by a D_6 then G has elementary abelian Sylow 2-subgroups.

Proof: Any element f of order four is conjugate to its inverse in an S_4 by lemma 4.6. As D_6 normalises no 2-group there are no S_4's : hence every 2-element of G is an involution, and any Sylow 2-subgroup is elementary abelian.

Lemma 6.2 If Q is any maximal element of $\mathcal{M}(D_6; 2)$, and $|Q| = 4$, then the Sylow 2-subgroup is dihedral, and L = 2.

Proof: Certainly Q is not cyclic as then its unique involution would centralise an element of order 3 which is not so. Then Q is elementary of order 4, and N(Q) satisfies the inductive hypothesis, so $N(Q) / F(N(Q)) \approx \langle A_o, \tau \rangle$ or some PSL(2,q). As $|Q| = 4$, and A_o, or a cyclic subgroup of PSL (2,q) acts fixed point free, $|A_o| = 3$, and no PSL (2,q) can occur. So $N(Q) / F(N(Q)) \approx D_6$. Moreover $Q \in S_2$ (F (N(Q))), and C(Q) = F(N(Q)), as no element of D_6 centralises Q. That is, if $Q \leq P \in S_2(G)$, Q is a self centralising four-group in P. Then by lemma 3.8, P is either dihedral or semi-dihedral.

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

Then P has two non conjugate, non cyclic subgroups of order 4, namely $\langle a, b^{2^{n-1}} \rangle$ and $\langle ab, b^{2^{n-1}} \rangle$. By transfer each is normal in an S_4 in any simple group having P as its Sylow 2-subgroup. If they are not conjugate in G then L = 2, and the lemma is proved.

Any non cyclic subgroup X of P is $X = \langle b^{2^k}, ab^{\alpha} \rangle$ for some k,α. If $X < P$ then $k \neq 0$, and $N_p(X) = \langle b^{2^{k-1}}, ab^{\alpha} \rangle$, so that $|N_p(X) : X| = 2$. As this is true for any non cyclic subgroup of P it follows that $N_p(X)$ is a Sylow 2-subgroup of $N_G(X)$. Then if X,Y are non cyclic subgroups of P, conjugate in G, then $N_G(X)$ and $N_G(Y)$ are conjugate in G, so $N_p(X)$, $N_p(Y)$ are conjugate in G. Taking $\langle b^{2^{n-1}}, a \rangle = X$, $\langle b^{2^{n-1}}, ab \rangle = Y$ and applying this argument (n-2) times, it follows

that X,Y are conjugate in G only if $< b^2, a >$ and $< b^2, ab >$ are. But each of these is of index 2 in P, and so normal : hence by 2.3 they are conjugate in G only if they are conjugate in N(P). But such a conjugation requires an automorphism of P of even order, which is impossible.

Case (ii) In this case $P = < a,b \mid a^2 = b^{2^n} = 1, \quad a^{-1}ba = b^{2^{n-1}}.b^{-1} >$. Then P has but one class of non cyclic subgroups of order 4, $< a, b^{2^{n-1}} >$. By transfer each is contained in an S_4, so that L = 1. This is proved to be impossible.

ab, and $b^{2^{n-2}}$ are elements of order 4 : they are therefore conjugate in G, for each lies in an S_4, and there is but one class of S_4's in G. Now $b^{2^{n-2}}$ and ab are conjugate in $N(< b^{2^{n-2}}, ab >)$. For suppose $X = N_p (< b^{2^{n-2}}, ab >) = < b^{2^{n-3}}, ab >$. Then the intersection of P with the (unique) cyclic subgroup of order 8 in X is $< b^{2^{n-3}} >$.

As ab, $b^{2^{n-2}}$ are conjugate it follows that P_1, a Sylow 2-subgroup of $N(< ab >)$ is isomorphic to a Sylow 2-subgroup of $N(< b^{2^{n-2}} >)$, that is to P. As $b^{2^{n-2}}$ normalises ab, P_1 may be chosen to contain $< b^{2^{n-2}}, ab >$. Then $X = N_p (< b^{2^{n-2}}, ab >)$ and $X_1 = N_{p_1} (< b^{2^{n-2}}, ab >)$ are Sylow 2-subgroups of $N_G (< b^{2^{n-2}}, ab >)$, and so conjugate in this normaliser, such a conjugation carrying $b^{2^{n-2}}$ to ab.

But this is impossible. For $b^{2^{n-2}}$, ab, $b^{2^{n-1}}$ ba are permuted

transitively by $N(< b^{2^{n-2}}, ab >)$ which therefore contains an element of order 3. As $< b^{2^{n-2}}, ab >$ is quaternion this means that G contains an element of order 6, which is not so. This contradiction establishes lemma 6.2.

§6C It may now be assumed that if Q is any maximal element of $\mathcal{M}(D_6;2)$, then $| Q | > 4$. In this paragraph is proved, by a series of lemmas, the following.

Lemma 6.3 There is no maximal element of $\mathcal{M}(D_6;2)$, say Q, such that $N(Q) / F(N(Q)) \approx < A_0, \tau >$.

In the following lemmas, 6.4 to 6.13, it is assumed that Q is one such, and that $H = N_G(Q)$.

Lemma 6.4 If $Q \lneq P \in S_2(G)$, then $| P:Q | = 2$, and Q is weakly closed in P.

Proof: Let $P_o \in S_2(H)$; then H has a subgroup H_o of odd index such that $(H_o / O_{2'}(F(H))) / (F(H) / O_{2'}(F(H))) \approx D_6$; and $F(H) / O_{2'}(F(H)) \approx Q$. Then by lemma 3.2 it follows that $F(H) / O_{2'}(F(H))$ char $P_o O_{2'}(F(H)) / O_{2'}(F(H))$, and hence Q char P_o. Then $N(P_o) \leq N(Q) = H$, so in fact $P_o \in S_2(G)$. Hence $| P:Q | = 2$. If $Q^g \leq P$, then Q^g is of index 2 in P, and so $Q^g \lhd P$. Then Q, Q^g are conjugate normal complexes of $P \in S_2(G)$, so by 2.3 they are conjugate in $N(P) \leq N(Q)$. That is, $Q^g = Q$, and so Q is weakly closed in P.

Lemma 65 $Z(Q) = Q' = \Phi(Q)$ is elementary abelian of order 4.

Proof: As Q is weakly closed in a Sylow 2-subgroup of G, and as all involutions in G are conjugate, it follows from 2.4 that all central involutions of Q are conjugate in N(Q). That is N(Q) acts transitively on $\Omega Z(Q) - \{1\}$. By 3.9 and 3.10, $N(Q) / F(N(Q)) \approx D_6$ and $|\Omega Z(Q)| = 4$. Suppose $Z(Q) = Z_{2^n} \times Z_{2^n}$, with $n > 1$. Then elements of order 4 are conjugate to their inverses, and so by the weak closure of Q, D_6 must invert each element of order 4 in $Z(Q)$. There is no action of D_6 permuting the involutions which does this, so $|Z(Q)| = 4$. Now Q has a fixed point free automorphism of order 3 induced by the action of N(Q), so by 3.1 Q is abelian or of class 2. As $|Q| > 4$, $|Z(Q)| = 4$, Q is of class 2. Then $1 < Q' \leq Z(Q)$, and as Q' admits a fixed point free automorphism of order 3, $Q' = Z(Q)$. Moreover for any $g,h \in Q$, $[g^2,h] = [g,h]^2 = 1$ as Q is of class 2, and Q' of exponent 2. Then squares in Q are central, so $\Phi(Q) = Z(Q) = Q'$ is elementary abelian of order 4.

Lemma 6.6 If D is any maximal abelian subgroup of Q, then D is $< t >$ invariant, where t is an element of order 3 in N(Q). Also $|D| = 4^{k+1}$, $|Q| = 4^{2k+1}$, and $|P| = 4^{2k+1}$. 2.

Proof: Let θ be the automorphism induced on Q/Q' and on Q' by t. Then $\theta^2 + \theta + 1 = 0$, so Q/Q', which is a $GF(2) - < \theta >$ module is a GF(4) vector space. Then commutation in Q induces, and is completely determined by a map $(Q/Q') \times (Q/Q') \longrightarrow Z(Q)$. Moreover $[g,h\theta] = [g,h]\theta^2$,

so identify $Z(Q)$ with $GF(4)$ in such a way that the action of t on Q/Q' and on $Z(Q)$ correspond. Then commutation is a bilinear, skew-symmetric, non singular inner product on Q/Q'. So Q/Q' has order 4^{2k} for some $k > 0$. Any maximal abelian subgroup D is $< t >$ invariant by lemma 3.1. It contains $Z(Q) = Q'$, so corresponds to a subspace of Q/Q'. Then as D is maximal abelian the order of D/Q' is 4^k. As $| Q' | = 4$ and as $| P | = 2 | Q |$ the lemma now follows.

Lemma 6.7 If D is any maximal abelian subgroup of Q, and if $D^g \leqslant P$ for some $g \in G$, then $D^g \leqslant Q$.

Proof: $| P:Q | = 2$, so if $D_o = D^g \cap Q$ then $| D^g:D_o | \leqslant 2$.
Let $C = < D_o, D_o^{\theta} >$. By lemma 3.1 C is abelian. Hence by 6.6, $| C | \leqslant 4^{k+1}$. If $| D^g:D_o | = 2$ then there is an element h in D^g but not in D_o; and such an element is not in Q. As D^g is abelian, $D_o \leqslant C_C(h)$; then by lemma 3.2, C admitting θ, $| C_C(h) | \leqslant | C |^{\frac{1}{2}} \leqslant 2^{k+1}$. That is, $| D^g | = 2 | D_o | \leqslant 2^{k+2}$. But $| D^g | = | D | = 4^{k+1}$ by 6.6, so that $4^{k+1} \leqslant 2^{k+2}$. This is not so as $k > 0$. So $| D^g:D_o | = 1$, and $D^g \leqslant Q$.

Lemma 6.8 Any maximal abelian subgroup of Q which is normal in P is weakly closed in P. Moreover there is at least one such, B say.

Proof: The number of maximal subgroups of Q is odd, so one at least is normal in P. Suppose $D \lhd P$, and D is maximal abelian in Q. Suppose $D^g \leqslant P$. Then by 6.7 we have $D^g \leqslant Q$. As D^g is also maximal abelian $D^g \geqslant Z(Q) = Q'$. So D, D^g are normal complexes of Q, conjugate in G.

As Q is weakly closed in P, so $D^g = D^n$ for $n \in N(Q)$. But $D \lhd P$, and D admits t being maximal abelian, and $N(Q) / C(Q) \approx D_6$ so that $D \lhd N(Q)$. That is, $D^n = D$, or $D^g = D$. Hence D is weakly closed in P as required.

Lemma 6.9 Either $B = Z_4 \times Z_4$ or B is elementary abelian. (B is chosen in 6.8.)

Proof: As B is weakly closed in $P \in S_2(G)$, its involutions are conjugate in N(B), so are certainly equivalent under Aut B. That is, B is homocyclic. As the exponent of Q is 4, either $B = (Z_2)^r$ or $B = (Z_4)^r$. In the latter case $1 < \Phi(B) \leq \Phi(Q)$. As $\Phi(B)$ admits a fixed point free automorphism of order 3, $\Phi(B) = \Phi(Q)$. Hence, by 6.5, $B = Z_4 \times Z_4$.

Lemma 6.10 If D is any maximal abelian subgroup of Q then N(D) acts transitively on the involutions of D.

Proof: If $D \lhd P$ this is so by 6.8. Otherwise suppose that $D = D_1$ and D_2 are a pair of P-conjugates. Let d be an involution in D_1. As $D_1 \cap D_2 \geq Z(Q)$ there is some involution $y \in Z(P) \cap D_1 \cap D_2$. For some $g \in G$, $y = d^g$. Then $D_1 \leq C(d)$, $D_1{}^g \leq C(d^g) = C(y)$. Hence for some h in C(y), $D_1{}^{gh} \leq P \in S_2(C(y))$. Then by 6.7, $D_1{}^{gh} \leq Q$. So $D_1, D_1{}^{gh}$ are normal complexes of Q, and are conjugate. As Q is weakly closed in P, D_1, $D_1{}^{gh}$ are conjugate in N(Q); and so under the action of $N(Q) / F(N(Q)) \approx \langle t, \tau \rangle$. But D_1 admits t, so $D_1{}^{gh} = D_1$ or $D_1{}^{\tau} = D_2$. So for some $k \in P$, $D_1{}^{ghk} = D_1$. That is $ghk = n \in N(D_1)$.

As $h \in C(y)$, $k \in P$, and $y \in Z(P)$,

$$y = y^{hk} = d^{ghk} = d^{h} \quad : \text{ so } y,d \text{ are conjugate in } N(D)$$

which gives the lemma.

Lemma 6.11 $|Q| = 64$, $|P| = 128$.

Proof: If $B = Z_4 \times Z_4$, then $|B| = 4^{1+1}$, and the lemma follows from 6.6. Otherwise B is elementary, and Q contains an element of order 4, x, not in B. Then by 3.1, $\langle x,x^t \rangle$ is abelian, so is isomorphic to $Z_4 \times Z_4$. Let D be any maximal abelian subgroup of Q containing $\langle x,x^t \rangle$. Then $1 < \Phi(D) \leq \Phi(Q)$, so, as D admits t, $\Phi(D) = \Phi(Q) = Z_2 \times Z_2$. This gives $D = Z_4 \times Z_4 \times Z_2 \times \ldots \times Z_2$. But by 6.10 N(D) acts transitively on the involutions of D. So in fact $D = Z_4 \times Z_4$ is of order 4^{1+1}, so $|Q| = 64$ by 6.6.

Lemma 6.12 Q has no elementary abelian subgroups of order 16.

Proof: Suppose D is one such. By 6.11 and 6.6 D is maximal abelian, and so admits t. That is, $t \in N(D) < G$, so the inductive hypothesis holds for N(D). So, as $D \lhd N(D)$, $N(D) / F(N(D)) \approx A_o, \langle A_o, \tau \rangle$, or some PSL (2,q). We prove that only $N(D) / F(N(D)) \approx$ PSL (2,4) can occur.

As Q is not elementary it contains a $Z_4 \times Z_4$: say $\langle a,b \rangle = \langle a,a^t \rangle$. Then $Q = \langle a,b,x,y \rangle$, and $Z(Q) = \langle a^2,b^2 \rangle$, and $D = \langle a^2,b^2,x,y \rangle$. The involution τ in N(Q), which inverts t, fixes $\langle a^2,b^2 \rangle$. Moreover it fixes $\langle \bar{a},\bar{b} \rangle$ and $\langle \bar{x},\bar{y} \rangle$ in $\bar{Q} = Q/Q'$. Hence τ fixes D, and

$N(D) / F(N(D))$ is not isomorphic to any $A_o \leq A$.

The second possibility, $N(D) / F(N(D)) \approx < A_o, \tau >$, cannot occur. For by 6.10 all involutions in D are conjugate in N(D). As A_o is fixed point free on D, and $| D | = 16$, $A_o \approx Z_{15}$. Then by 3.10 this is impossible, only a D_6, and not a D_{30} acting in this way.

So indeed $N(D) / F(N(D)) \approx PSL(2,q)$. As D is a 2-group and as an element of order 3 in PSL (2,q) acts fixed point free on D, of order 16, lemmas 3.6 and 3.7 give $q = 4$. By 3.6 D may be identified with vectors (u,v) with $u,v \in GF(4)$, and the action of $N(D) / F(N(D))$ on D is given by

$(u,v) \longrightarrow (au + cv, bu + dv)$ where a,b,c,d are in GF(4), $ad + bc = 1$. But $D \lhd < t > Q$, and the factor is isomorphic to A_4. The A_4 (a subgroup of PSL (2,4)) acts as $(u,v) \longrightarrow (au + bv, a^{-1}v)$, $a,b \in GF(4)$. So Z(Q) (which lies in D) corresponds to the vectors (u,o). t acts on D like $(u,v) \longrightarrow (u\omega , v\omega^2)$ where ω is a cube root of unity in GF(4). τ, which inverts t, acts like $(u,v) \longrightarrow (v,u)$. So $[Z(Q)]^{\tau}$ corresponds to the vectors (o,v). That is D, any maximal abelian subgroup of Q which is elementary, is unique, being $< Z(Q), Z(Q)^{\tau} >$. If Q contains any (non central) involution x not in D this will give a contradiction : for $< Z(Q), x, x^t >$ will be a distinct maximal abelian subgroup of order 16. However Q is a Sylow 2-subgroup of N(D). For by 3.6 the Sylow 2-subgroup of F(N(D)) is of order 4^s, so if Q is not a Sylow 2-subgroup of N(D), N(D) has a Sylow 2-subgroup

of order 4^4. But by 6.11 the Sylow 2-subgroup of G is only of order 2.4^3. Hence $Q \in S_2(N(D))$. So it suffices to find involutions in N(D) which do not lie in D to provide a contradiction. Such involutions certainly exist, e.g. τ, the involution inverting t. This contradiction establishes the lemma : all maximal abelian subgroups of Q are of type (4,4).

Lemma 6.13 An involution normalising Q centralises Z(Q).

Proof: Q is of order 64, normalised by a D_6 it does not intersect. $Q' = Z(Q) = \Phi(Q)$ is elementary of order 4. All involutions of Q are central by lemma 6.12. Commutation in Q is GF(4)-bilinear, skew symmetric, and non singular, so that Q has the following structure:

$Q = \langle a,b,c,d \mid a^2 = c^2 = x \; ; \; b^2 = d^2 = y \; ;$

$[a,b] = [c,d] = 1 \; ; \; [a,c] = y \; ; \; [b,d] = xy \; ;$

$[a,d] = [b,c] = x \; ;$ x and y are central involutions of Q. $\rangle$

Also $Z(Q) = \langle x,y \rangle$. We have chosen $x \in C(\tau)$.

There are five cosets of Z(Q) in Q whose elements have square x; viz. a, c, abc, acd, abcd. (Z(Q)).

Also $[a,c] = [a,abc] = y \; ; \; [a,acd] = [a,abcd] = yx$.

As GF(4) module $Q/Q' = U \oplus W$ where U has a basis u_1, u_2 of eigen vectors of t, and W a basis w_1, w_2 of eigen vectors of t. That is $u_i t = u_i \theta^i$, $w_i t = w_i \theta^i$, where θ is a cube root of unity in GF(4). Then, under the action of τ the eigen vector basis elements are interchanged in pairs,

so that the dimension of the fixed space of τ is 2. So, in group theoretic language, τ has two fixed points on Q/Q'. With no loss $\bar{a}$ is one of these. If the second $\bar{s}$, is any one of $\bar{c}$, $\overline{abcd}$, $\overline{abc}$, $\overline{acd}$, then τ fixes $[a,s] \neq x$, and so τ centralises $Z(Q)$. If s is not one of these then τ fixes $s^2 \neq x$, so again τ centralises $Z(Q)$. This proves the lemma.

Proof of lemma 6.3 It is only necessary to deduce a contradiction from 6.4 - 6.13 : then the assumed existence of Q is contradicted. As G contains elements of order 4 it contains S_4's. As all involutions of Q are central, $N(Z(Q))$ contains S_3's. But the involution in such an S_3 does not centralise $Z(Q)$: and the involution can even be chosen to normalise Q, a maximal element of $\mathcal{N}(D_6;2)$. This contradicts 6.13 as required.

§6D It may now be assumed that if Q is any maximal element of $\mathcal{N}(D_6; 2)$ then $N(Q) / F(N(Q)) \approx PSL(2,2^\alpha)$. By maximality $Q \in S_2(F(N(Q)))$; and by 3.6, $|Q| = (2^{2\alpha})^k$, and Q is elementary abelian. In this paragraph it is shown that $k = 1$; and the structure of $P \in S_2(N(Q))$ is studied. Paragraphs 6E and 6F will continue this study in the distinct cases $\alpha \geq 3$ and $\alpha = 2$. So let Q be a maximal element of $\mathcal{N}(D_6; 2)$, and suppose $N(Q) / F(N(Q)) \approx PSL(2,2^\alpha)$, and $|Q| = (2^{2\alpha})^k$, and $P \in S_2(N(Q))$.

Lemma 6.14 If $k > 1$ then $P \in S_2(G)$ and Q is weakly closed in P.

Proof: In this case 3.6 gives that Q is the unique subgroup of

P which is abelian of index 2^{α}. So Q char P, and $N(P) \leq N(Q)$, so $P \in S_2(N(P))$, and then $P \in S_2(G)$. The uniqueness of Q gives weak closure at once.

Lemma 6.15 $k > 1$ is impossible.

Proof: If $k > 1$, then Q is weakly closed in a Sylow 2-subgroup of G. Hence all involutions of Q are conjugate in N(Q). If $k > 1$ this is not so in view of the action of PSL $(2,2^{\alpha})$ on Q described in 3.6. Now let $Q = Q_o \oplus Q_1$ where $|Q_o| = 2^{\alpha}$; and identify Q_o, Q_1 with the additive group of $GF(2^{\alpha})$ in such a way that PSL $(2,2^{\alpha})$ acts naturally on Q i.e. conjugation by $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in PSL $(2,2^{\alpha})$ gives

$(u,v) \longrightarrow (au + cv, bu + dv)$; in particular let the cosets of P/Q correspond to the matrices $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix}$ in PSL $(2,2^{\alpha})$.

Lemma 6.16 $P' = Z(P) = Q_o$

Proof: With the above identification let $(u,v) \in Q$. Then $(u,v)\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix}$ $= (u + vx, v)$ so that Z(P), which is contained in Q, is even $\{(u,0)\}$. In the action of N(Q) on Q some element g acts like $\begin{bmatrix} \theta & . \\ . & \theta^{-1} \end{bmatrix}$ with θ a primitive $(2^{\alpha}-1)$th. root of unity in $GF(2^{\alpha})$. This element normalises P, Q_o, Q_1 : in fact Q_o, Q_1, P/Q are irreducible as $< g >$ modules. But $P' \leq Q$ is fixed by $< g >$; and by 3.6 P is of class 2, so $P' \leq Z(P) = Q_o$.

Then $P' = Q_o$.

Lemma 6.17 $P' = Z(P) = \Phi(P)$ is elementary of order 2^{α}.

Proof: It only remains to show that squares are central: and if $x,y \in P$, $[y,x^2] = [y,x]^2$ $[y,x,x^{-1}] = 1$ as P is of class 2, and Q of exponent 2.

In view of 6.17 commutation in P not only induces a map $(P/\Phi(P)) \times (P/\Phi(P)) \longrightarrow Z(P)$ on the cosets of $\Phi(P)$, but is completely determined by such a map.

§6E The purpose of this paragraph is to prove the following lemma :

Lemma 6.18 There is no Q maximal in $\mathcal{N}(D_6; 2)$ such that $N(Q) / F(N(Q)) \approx PSL(2,2^{\alpha})$, where $\alpha \geqslant 3$.

Suppose Q is one such. Then by § 6D, $|Q| = 2^{2\alpha}$, and if $P \in S_2(N(Q))$, $P' = Z(P) = \Phi(P)$. By §6B, §6C it may be assumed that any maximal element Q^* of $\mathcal{N}(D_6;2)$ is such that $N(Q^*) / F(N(Q^*) \approx PSL(2,2^{\beta})$ for some β ; and that $|Q^*| = 2^{2\beta}$ by 6.15. The first task is to determine the structure of $P \in S_2(N(Q))$. To do this it is necessary to know the map $(P/P') \times (P/P') \longrightarrow Z(P)$ induced by commutation in P; and the map $P/Z(P) \longrightarrow Q$ induced by squaring in P. To fix notation let P be chosen in N(Q) so that P/Q corresponds to the matrices $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix}$. Let g be an element of N(Q) which acts on Q as $\begin{bmatrix} \theta & . \\ . & \theta^{-1} \end{bmatrix}$ where θ is a primitive $(2^{\alpha}-1)$-th root of unity in $GF(2^{\alpha})$.

Then g normalises P, Q, Q_o. In fact $P/\Phi(P) = P/Q_o$ can be identified with a $GF(2^\alpha) = GF(2)\ (\theta)$ vector space of dimension 2; that is with the set of vectors (u,v), u,v in $GF(2^\alpha)$. Here (u,o) correspond to elements of P/Q, (o,v) to elements of $Q/\Phi(P)$. $Q_o = Z(P)$ can be identified with the additive group of $GF(2^\alpha) = GF(2)\ (\theta)$. Then g acts on $Q_o = Z(P)$ as multiplication by θ, on Q/Z(P) as multiplication by θ^{-1}, and on P/Q as $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & . \\ x\theta^2 & 1 \end{bmatrix}$ i.e. as multiplication by θ^2.

As $\alpha \geqslant 3$ θ and θ^2 are algebraic conjugates, and θ, θ^{-1} are not; so the action on P/Q, Z(P) is essentially the same, and the action on Q/Z(P) different.

<u>Lemma 6.19</u> $P/\Phi(P)$ can be identified with $GF(2^\alpha)$ vectors (u,v) and Z(P) with $GF(2^\alpha)$ in such a way that commutation in P is determined by

$$[\ (u_1,v_1),\ (u_2,v_2)\ ] = u_1^{\,2}\, v_2 + u_2^{\,2}\, v_1.$$

<u>Proof</u>: $P / \Phi(P)$ is certainly able to be identified with $U \oplus V$ as $GF(2) - \langle g \rangle$ module, where U,V are α-dimensional vector spaces corresponding to P/Q, $Q/\Phi(P)$ respectively. Z(P) is able to be identified with W, an α-dimensional GF(2) vector space. Form $X = U \otimes GF(2^\alpha)$, $Y = V \otimes GF(2^\alpha)$, $Z = W \otimes GF(2^\alpha)$, the tensor products being over GF(2). Then commutation in P induces a skew-symmetric bilinear map

$$(X \oplus Y) \times (X \oplus Y) \longrightarrow Z.$$

In view of the action of g on P/Q, $Q/\Phi(P)$, Z(P) it is possible to

pick bases of X, Y, Z which are eigenvectors of g; that is

$x_1, \ldots x_\alpha$ such that $x_i g = x_i \theta^{2^i}$, $i = 0, \ldots \alpha-1$;

$y_1, \ldots y_\alpha$ such that $y_i g = y_i \theta^{-2^i}$, $i = 0, \ldots \alpha-1$;

$z_1, \ldots z_\alpha$ such that $z_i g = z_i \theta^{2^i}$, $i = 0 \ldots \alpha-1$.

Let the image of a subspace K of $X \oplus Y$ in the commutation map be denoted by $K \wedge K$. Then the image of $X \oplus Y$ is completely determined by $X \wedge X$, $Y \wedge Y$ and the symmetric space $X \otimes Y$. As Y corresponds to the abelian subgroup Q, $Y \wedge Y = 0$.

$X \wedge X$ has a basis of eigen vectors $x_i \wedge x_j$ of g : but the eigen values are $\theta^{2^i + 2^j}$, whereas the eigen values of g in Z are θ^{2^k} . As $\alpha \geqslant 3$ it is not possible that $2^i + 2^j \equiv 2^k$ modulo $2^\alpha - 1$: so every $x_i \wedge x_j = 0$.

$X \otimes Y$ has a basis of eigenvectors $x_i \otimes y_j$ of g, whose eigen values are $\theta^{2^i - 2^j}$. The image of $X \oplus Y$ in Z is a $< g >$ sub-module of Z, so is either Z or 0, as Z is irreducible quâ g-module. As P is not abelian $X \otimes Y = Z$, and $x_i \otimes y_j$ is the eigen vector of g in Z with eigen value $\theta^{2^i - 2^j}$. Now $\theta^{2^i - 2^j} = \theta^{2^k}$ if, and only if, $2^i - 2^j = 2^k$ if $i \geqslant j$ or $2^i - 2^j = 2^k - 2^\alpha + 1$ if $i < j$. That is $i = j + 1$, $k = j$ if $j = 0, \ldots, \alpha-1$, taking $x_\alpha = x_0$. Hence the commutation map is uniquely defined.

Now write $P/\Phi(P)$ as $GF(2^\alpha)$, vectors (u,v), and identify $\Phi(P) = Z(P)$ with the additive group of $GF(2^\alpha)$. Then $[(u_1,v_1), (u_2,v_2)] = u_1^2 v_2 + u_2^2 v_1$ is a bilinear skew-symmetric form

on which g acts like θ : it vanishes for $u_1 = u_2 = 0$ and for $v_1 = v_2 = 0$. Hence it gives the (uniquely determined) commutation in P, as required by the lemma.

The next lemma determines squaring in P. Continue the identification $P/\Phi(P) = \{(u,v) \mid u,v \in GF(2^\alpha)\}$. Then as $P' = \Phi(P) = Z(P)$ squaring induces, and is completely determined by a map $P/\Phi(P) \longrightarrow Z(P)$. As commutation is already determined, and as Q is elementary it suffices to know the images of (u,o) as $u \in GF(2^\alpha)$: denote the image of (u,v) by $(u,v)^{(2)}$.

Lemma 6.20 Either (I) $(u,o)^{(2)} = 0$

or (II) $(u,o)^{(2)} = ku$ for some fixed $k \in GF(2^\alpha)$, $k \neq 0$.

Proof: The image $U^{(2)}$ of U in the square map is $< g >$-invariant, and is even a $< g >$ submodule. Hence $U^{(2)}$ is trivial or all of $\Phi(P)$. Identifying $\Phi(P)$ with $GF(2^\alpha)$ as before, the lemma follows : in the latter case $(1,0)^{(2)} = k$.

These two cases will be referred to throughout this paragraph, §6E, as I and II.

Lemma 6.21 Case I does not occur.

Proof: Let $P = < x_1, \ldots x_\alpha; \ y_1, \ldots y_\alpha >$, $Z(P) = < z_1, \ldots z_\alpha >$, $Q = < z_1, \ldots z_\alpha \ ; \ y_1, \ldots y_\alpha >$, $T = < x_1, \ldots x_\alpha \ ; \ z_1, \ldots z_\alpha >$.

Firstly Q and T are the unique maximal abelian subgroups of P which are elementary. For they are elementary. Also any maximal abelian subgroup of P contains $Z(P) = \Phi(P)$. Moreover if $x \in < x_1, \ldots x_\alpha >$,

$y \in \langle y_1, \ldots y_\alpha \rangle$ then

$$(xy)^2 = x^2y^2\,[x,y] = [x,y].$$

From 6.19 it is clear that $[x,y] \neq 1$ unless $x = 1$ or $y = 1$. So Q and T are the only maximal subgroups of P which are elementary.

Secondly Q is weakly closed in P. For suppose $Q^h \leq P$ for $h \in G$. If $Q^h \neq Q$ then $Q^h = T$. Then $N(T) = [N(Q)]^h$. That is, N(T) has a normal elementary abelian subgroup of order $2^{2\alpha}$ on which N(T) acts like PSL $(2,2^\alpha)$. Then T may be decomposed $T = T_o \oplus T_1$ where an element of order $2^\alpha - 1$ in N(T) acts on T_o like multiplication by θ, on T_1 like multiplication by θ^{-1}. But if $g \in N(P)$ corresponds to a matrix $\begin{bmatrix} \theta & . \\ . & \theta^{-1} \end{bmatrix}$ in PSL $(2,2^\alpha)$ as before, g^h normalises T, and acts like multiplication by θ on each factor. (For T_o, T_1 correspond to Z(P), P/Q). As $\alpha \geq 3$ θ is not an algebraic conjugate of θ^{-1} so this is impossible. That is $Q^h \neq T$, and $Q^h = Q$. It also follows that T is weakly closed in P.

Thirdly $P \in S_2(G)$. For if $h \in N(P)$ then $Q^h \leq P$, so $Q^h = Q$. That is $N(P) \leq N(Q)$, and $P \in S_2(N(P))$: and so $P \in S_2(G)$. So T, Q are weakly closed in a Sylow 2-subgroup of G.

Fourthly $N(T) / F(N(T)) \approx A_o \leq A$. For T is weakly closed in $P \in S_2(G)$, so in particular all its involutions are conjugate in N(T), by 2.4. T has $2^{2\alpha}-1$ involutions, so if $a \in T$, $2^{2\alpha}-1 = |\, N(T) : N(T) \cap C(a) \,|$. Hence 3 divides $|\, N(T) \,|$. So the inductive hypothesis applies to N(T). If $N(T) / F(N(T)) \approx$ PSL $(2,2^\beta)$ then $\beta = \alpha$, for T is certainly acted

regularly on by an element of order $2^{\alpha}-1$ in P. But then, by the same argument as used previously, an element of PSL $(2,2^{\alpha})$ must act on $T = T_o \oplus T_1$ as θ on T_o, θ^{-1} on T_1, whereas g (in N(P)) acts on T as θ on each factor. If $N(T) / F(N(T)) \approx < A_o, \tau >$, then either T is maximal in $\mathcal{N}(D_6; 2)$ or it is not. With such a normaliser it cannot be maximal in $\mathcal{N}(D_6;2)$ by 6.3, since $| T | = 2^{2\alpha} > 4$. But if it is not, then $T < Q^*$ where Q^* is maximal with respect to being normalised by a D_6. But then by 6.3 it may be assumed $N(Q^*) / F(N(Q^*)) \approx$ PSL $(2,2^{\beta})$, and, as $| Q^* | > | T | = 2^{2\alpha}$, $\beta > \alpha$, by 3.6, so that a Sylow 2-subgroup of G is of order greater than $2^{3\alpha}$. As P is a Sylow 2-subgroup of G this is not so.

Hence $N(T) / F(N(T)) \approx A_o \lesssim A$ as asserted. By lemmas 3.9, 3.10 A_o is cyclic of order $2^{2\alpha}-1$. Let P_1 be a Sylow 2-subgroup of N(T). Then T, being weakly closed in P is weakly closed in P_1. So if $h \in N(P_1)$, $T^h \lesssim P_1$ and so $T^h = T$. Then $h \in N(T)$, and so $N(P_1) \lesssim N(T)$, and P_1 is a Sylow subgroup of $N(P_1)$. So without loss $P = P_1$. Moreover P is then a Sylow 2-subgroup of F(N(T)), and is normalised by a fixed point free cycle of order $2^{2\alpha}-1$. But $N(P) \lesssim N(Q)$, and there is no such cycle in N(Q). This is a contradiction, so case I does not arise, and the lemma is proved.

<u>Lemma 6.22</u> If case II occurs, and α is odd, then the following are the maximal abelian subgroups of P. $Q \approx (Z_2)^{2\alpha}$, $T = (Z_4)^{\alpha}$, $S_i = (Z_2)^2 (Z_4)^{\alpha-1}$, $i = 1,\ldots, 2^{\alpha}-1$. All the S_i are conjugate in N(P).

Moreover Q and T are weakly closed in P, and $P \in S_2(G)$.

Proof: From 6.19 and 6.20, if $P / \Phi(P)$ is identified with $GF(2^\alpha)$ vectors, and $\Phi(P)$ with $GF(2^\alpha)$, commutation and squaring are given by

$[(u_1,v_1), (u_2,v_2)] = u_1^2 v_2 + u_2^2 v_1$

$(u,0)^{(2)} = ku$, $k \neq 0$, $(o,v)^{(2)} = 0$.

Any maximal abelian subgroup of P contains $Z(P) = \Phi(P)$, so corresponds to a subgroup of $P/\Phi(P)$. Then at once P has the maximal abelian subgroups Q, T as stated. Otherwise, if $v_1 \neq 0$, $[(u_1,v_1), (u_2,v_2)] = 0$ if and only if $u_1^2/v_1 = u_2^2/v_2$. That is $\{(u,v) \mid u^2 = iv,$ $i \in GF(2^\alpha), i \neq 0\}$ corresponds to a maximal abelian subgroup of P. As θ^i, $i = 1,\ldots 2^\alpha-1$ runs through the non zero elements of $GF(2^\alpha)$, where θ is a primitive $(2^\alpha-1)$-th root of unity in $GF(2^\alpha)$ set S_i to be the maximal abelian subgroup of P corresponding to the subspace $\{(u,v) \mid u^2 = \theta^i v\}$ of $P/\Phi(P)$. Let g be the element of N(Q) which normalises P and corresponds to the matrix $\begin{bmatrix} \theta & . \\ . & \theta^{-1} \end{bmatrix}$ in PSL $(2,2^\alpha)$. Then g acts like multiplication by θ on P/Q, by θ^{-1} on $Q/\Phi(P)$, and like multiplication by θ on $\Phi(P)$. So

$$S_i^g = \{(u,v) \mid u^2 = \theta^i\theta^3 v\} \quad \text{modulo} \quad \Phi(P),$$

or, since g fixes $\Phi(P)$, $S_i^g = S_{i+3}$, suffices being reckoned modulo $2^\alpha-1$. As α is odd $2^\alpha-1 \not\equiv 0 \bmod 3$, so that under the action of g all S_i are conjugate. In particular consider S, the S_i corresponding to $\{(u,v) \mid u^2 = k^{-1}v\}$.

Let (u,v) be a coset of $\Phi(P)$ in S. Then

$$(u,v)^{(2)} = (u,o)^{(2)} + (o,v)^{(2)} + [(u,o), (o,v)]$$
$$= ku + u^2v$$
$$= ku + ku^4$$

So (u,v) is a coset of involutions if and only if $k(u + u^4) = 0$, that is, if and only if $u + u^4 = 0$. The map $u \longrightarrow u + u^4$ is an additive homomorphism of $GF(2^\alpha)$ to $GF(2^\alpha)$. Since α is odd, so that $GF(2^\alpha)$ has no cube roots of unity but 1, the kernel of this map is of order 2. So there are $2^{\alpha-1}$ squares in S. As S has order 2^α over $\Phi(P)$, and $\Phi(P)$ has order 2^α, it follows that $S \approx (Z_2)^2 . (Z_4)^{\alpha-1}$. The S_i are all conjugates of S, so are isomorphic to S.

It now is easy to see that Q and T are weakly closed in P; for they are each unique of their type in P. So also $N(P) \leq N(Q)$, so that $P \in S_2(N(P))$, and even $P \in S_2(G)$.

Lemma 6.23 If case II holds then α is even.

Proof: Suppose on the contrary α is odd. Then the result of lemma 6.22 holds. Let $a \in S \cap Z(P)$, $a^2 = 1$, $a \neq 1$, and let $b \in S - Z(P)$, $b^2 = 1$, $b \neq 1$. (S is the S_i chosen in 6.22). As all involutions in G are conjugate there is some $h \in G$ such that $a^h = b$. Then $S \leq C(a)$, $S^{h^{-1}} \leq C(a)$. As $P \in S_2(C(a))$, $S^{h^{-1}} \leq P^c$ for $c \in C(a)$. Then $S^{h^{-1}c^{-1}} \leq P$. So $S^{h^{-1}c^{-1}} = S^{g^i}$ for some i. That is, $h^{-1}c^{-1}g^{-i} = n$, with $n \in N(S)$, and $b = a^h = a^{c^{-1}g^{-i}n^{-1}} = a^{g^{-i}n^{-1}}$, or $b^n = a^{g^{-1}}$. Hence $b^n = a_1$ where a_1 is another central involution of P. Consider N(S) /C(S). It

acts on the factor $S/(Z_4)^{\alpha-1}$ so that either $N(S) = C(S)$ or $|N(S) / C(S)| = 3$. If $N(S) = C(S)$ there is an immediate contradiction: for $b \notin Z(P)$, but $a_1 \in Z(P)$, and $b^n = b$ as $b \in S$. So in fact for some element s of order 3, $b^s = a_1$. Let $S \leq Q^*$ where Q^* is maximal with respect to being a 2-group normalised by a 3-element. Then

$$N(Q^*) / F(N(Q^*)) \approx A_o \text{ or } < A_o, \tau > \text{ or } PSL(2,2^\beta).$$

If the first case were to occur then a Sylow 2-subgroup of $F(N(Q^*))$, which is Q^*, would be a Sylow 2-subgroup of its normaliser. So without loss $Q^* = P$. But as α is odd, and as $N(P) \leq N(Q)$, P is normalised by no element of order 3. So in fact Q^* is normalised by a D_6, and is even a maximal element of $\mathcal{N}(D_6;2)$. As a result of 6.3 $N(Q^*) / F(N(Q^*))$ is not isomorphic to $< A_o, \tau >$. If the last case, $N(Q^*) / F(N(Q^*))$ were to occur, then by 3.6, Q^* is elementary. But $Q^* \geq S$ so this too is a contradiction. That is, if α is not even, case II leads to a contradiction.

Lemma 6.24 If case II occurs, then Q is the unique elementary abelian subgroup of P of order $2^{2\alpha}$. P has maximal abelian subgroups of type $(Z_2)^4 (Z_4)^{\alpha-2}$, and of type $(Z_4)^\alpha$. Also $P \in S_2(G)$.

Proof: By 6.23 α is even, so 3 divides $2^\alpha - 1$. As before, with $P/\Phi(P)$ identified with $GF(2^\alpha)$ vectors (u,v), and $\Phi(P)$ with $GF(2^\alpha)$, commutation and squaring are given by

$$[(u_1,v_1), (u_2,v_2)] = u_1^2 v_2 + u_2^2 v_1$$

$$(u,o)^{(2)} = ku \quad , \quad (o,v)^{(2)} = 0.$$

At once P has maximal abelian subgroups Q, corresponding to vectors $\{(o,v)\}$, of type $(Z_2)^{2\alpha}$; and R, corresponding to vectors $\{(u,o)\}$, of type $(Z_4)^{\alpha}$. Otherwise if $v \neq 0$, $[(u_1,v_1), (u_2,v_2)] = 0$ if and only if $u_1^2/v_1 = u_2^2/v_2 = i$ say; hence $\{(u,v) \mid u^2 = iv,$ $i \in GF(2^{\alpha}), i \neq 0\}$ corresponds to a maximal abelian subgroup of P, say S_i. The coset of $\Phi(P)$ in S_i corresponding to (u,v) consists of involutions if and only if $(u,v)^{(2)} = 0$, that is, if and only if $(u,o)^{(2)} + (o,v)^{(2)} + [(u,o), (o,v)] = 0$. That is, (u,v) consists of involutions if and only if $u(ik + u^3) = 0$. The map $u \longrightarrow iku + u^4$ is a homomorphism of the additive structure of $GF(2^{\alpha})$, and u is in the kernel if and only if $u(ik + u^3) = 0$. If ik is a cube this map has kernel of order 4; if ik is not a cube the kernel is u = 0. Hence S_i is of type $(Z_4)^{\alpha}$ if ik is not a cube, and of type $(Z_2)^4 (Z_4)^{\alpha-2}$ if ik is a cube. As $1 = k^{-1}k$ is a cube, since 3 divides $2^{\alpha-1}$, there is always $S_{k^{-1}}$ of type $(Z_2)^4 (Z_4)^{\alpha-2}$.

At any rate Q is unique in P, so Q char P, and $N(P) \leq N(Q)$. So $P \in S_2(N(P))$ and even $P \in S_2(G)$.

Lemma 6.25 Case II does not occur.

Proof: Suppose it does. Then α is even, and 6.24 holds. Let $S = S_{k^{-1}}$ be the maximal abelian subgroup corresponding to $\{(u,v) \mid u^2 = k^{-1}v\}$. Then S is of type $(Z_2)^4 (Z_4)^{\alpha-2}$. Let g be an element of order $2^{\alpha}-1$ in N(Q) corresponding to $\begin{bmatrix} \theta & . \\ . & \theta^{-1} \end{bmatrix}$ in

PSL $(2,2^{\alpha})$, where θ is a primitive $(2^{\alpha}-1)$-th root of unity. Then g normalises P.

Firstly $(N(P) \cap N(S) / (C(P) \cap C(S))$ is of order 3. For $N(P) / C(P)$ corresponds to matrices $\begin{bmatrix} \theta^{i} & . \\ . & \theta^{-i} \end{bmatrix}$ in PSL $(2,2^{\alpha})$. This fixes the subspace corresponding to S if and only if $(u_1\theta^{i}, ku_1^{2}\theta^{-i}) = (u_2, ku_2^{2})$ for every u_1, and some $u_2 = u_2(u_1)$. That is, if and only if $ku_1^{2}\theta^{-i} = k(u_1\theta^{i})^{2}$. That is, if and only if $\theta^{3i} = 1$. So the only elements g^{i} in N(P) to fix S correspond to $\begin{bmatrix} \omega & . \\ . & \omega^{-1} \end{bmatrix}$ where ω is a cube root of unity in $GF(2^{\alpha})$.

Hence the inductive hypothesis holds for N(S),as 3 divides the order of N(S). So $N(S) / F(N(S))$ is isomorphic to A_o, or $< A_o, \tau >$ or to PSL $(2,2^{\beta})$. The third case cannot occur, for by 3.6 the Sylow 2-subgroup of F(N(S)) must be elementary, and S is not, (as $\alpha \geqslant 3$.) If $N(S) / F(N(S)) \approx < A_o, \tau >$ then S is normalised by a D_6, so is contained in Q^{*} a maximal element of $\mathcal{M}(D_6; \mathfrak{2})$. But we have that for every maximal element Q^{*} of $\mathcal{M}(D_6; \mathfrak{2})$, $N(Q^{*}) / F(N(Q^{*})) \approx$ PSL $(2,2^{\beta})$ and again $Q^{*} \geqslant S$ would be elementary by 3.6.

So indeed $N(S) / F(N(S)) \approx A_o$. Then, as $S \trianglelefteq P$, $P \leqslant F(N(S))$; and even P char $F(N(S))$, and P char N(S). Thus $N(S) \leqslant N(P)$, so that $N(S) / C(S)$ is cyclic of order 3.

Let $a \in S \cap Z(P)$, $b \in S - Z(P)$, where a,b are involutions. For

some $h \in G$, $a^h = b$. Then $S \leqslant C(a)$, and $S^{h^{-1}} \leqslant C(a)$. As $P \in S_2(C(a))$, $S^{h^{-1}c^{-1}} \leqslant P$ for some $c \in C(a)$. So $S^{h^{-1}c^{-1}}$, S are conjugate normal complexes of $P \in S_2(G)$. Then by 2.3 they are conjugate in N(P). As $N(P) \leqslant N(Q)$, that is $S^{h^{-1}c^{-1}} = S^{g^i}$. Then $h^{-1}c^{-1}g^{-i} = n^{-1} \in N(S)$. So $b = a^h = a^{ch} = a^{g^{-i}n}$. Take $d = a^{g^{-i}}$, another central involution of P ; then $b = d^n$ with $n \in N(S)$. That is, some element of N(S) has moved a central involution of P out of the centre. But $N(S) \leqslant N(P)$, from above, so this is not possible. The contradiction establishes the result.

Proof of 6.18 If Q is maximal in $\mathcal{M}(D_6; 2)$, and $N(Q)/F(N(Q))$ is isomorphic to PSL $(2,2^\alpha)$ for $\alpha \geqslant 3$, then by 6.15, $|Q| = 2^{2\alpha}$. The structure of $P \in S_2(N(Q))$ is given by 6.19 and 6.20. Each of the two cases of 6.20 has been shown not to occur. So 6.18 is proved.

§6F There is but one case left to examine, the case where Q is maximal in $\mathcal{M}(D_6; 2)$, and $N(Q) / F(N(Q)) \approx$ PSL (2,4). The methods of the previous paragraph do not apply because in GF(4), θ is an algebraic conjugate of θ^{-1}. However, in this case, by 6.15, $|Q| = 16$, so small and manageable. This paragraph proves the following lemma.

Lemma 6.26 There is no maximal element Q of $\mathcal{M}(D_6; 2)$ with $N(Q) / F(N(Q)) \approx$ PSL (2,4).

Let $P \in S_2(N(Q))$. Then by 6.17, $P' = Z(P) = \Phi(P)$ is elementary of order 4. As remarked above $|Q| = 16$, and so $|P| = 64$. The first

few lemmas show that $P \in S_2(G)$: but for the present let $P_1 \in S_2(N(P))$.

Lemma 6.27 $N(P)$ has a normal nilpotent subgroup M with $N(P)/M \approx Z_3$. Moreover $Z(P_1) = P_1' = \Phi(P_1) = Z(P)$.

Proof: In $N(Q)$, P is normalised by an element t of order 3. Hence $N(P)$ has a normal nilpotent subgroup M (by the inductive hypothesis) with $N(P)/M \approx A_0$, $\langle A_0 \tau \rangle$ or $PSL(2,2^\beta)$. Now $P \leq M$, as $P \lhd N(P)$, and P is nilpotent. So neither of the last two cases arise, as $Q < P$, and Q is maximal in $M(D_6; 2)$. So $N(P)/M \approx A_0$. Now $Z(P)$ char $P \lhd N(P)$, so $Z(P)$ admits A_0. As $|Z(P)| = 4$, $|A_0| = 3$. Also $P_1 \in S_2(M)$. Now $Z(P_1) \cap Z(P) \neq 1$, and admits A_0 : so $Z(P_1) \geq Z(P)$. Hence $Z(P) = Z(P_1)$, since trivially $Z(P_1) \leq Z(P)$. Now P_1 is of class 2 by 3.1, so $1 < P_1' \leq Z(P_1)$. As P_1' admits A_0, $P_1' = Z(P_1)$. As P_1 is of class 2, and P_1' of exponent 2, squares are central, and $\Phi(P_1) = P_1' = Z(P_1) = Z(P)$.

Lemma 6.28 $P \in S_2(G)$.

Proof: $Q \geq Z(P) = P_1'$, so $Q \lhd P_1$. Hence $P_1 \leq N(Q)$, so $P_1 = P$, as $P \in S_2(N(Q))$. That is $P \in S_2(N(P))$, and so $P \in S_2(G)$.

Lemma 6.29 Any maximal abelian subgroup of P admits $N(P)$, and is weakly closed in P.

Proof: Let $t \in N(P)$ be an element of order 3 such that $N(P) = \langle t, F(N(P)) \rangle$. If B is a maximal abelian subgroup of P then B contains $Z(P) = P'$, so is normal in P. Also, by 3.1, $\langle B, B^t \rangle$ is

abelian, so $B = B^t$, and B admits N(P). If $B^g \leq P$ for $g \in G$, then $B, B^g \geq Z(P) = P'$, so are conjugate normal complexes of P. So by 2.3, $B^g = B^{t^i c}$, where $c \in F(N(P)) \leq N(B)$. Hence $B^g = B$, and B is weakly closed in P.

Lemma 6.30 Q is the unique elementary abelian subgroup of P of order 16.

Proof: Let B be any abelian subgroup of P which is elementary of order 16. As $|P| = 64$ and is of class 2, B is maximal abelian in P. Then N(B) satisfies the inductive hypothesis, as it admits N(P). So $N(B) / F(N(B)) \approx A_1$, $< A_1, \tau >$, or $PSL(2, 2^\beta)$. If the first case holds then $P \leq F(N(B))$, and even $P \lhd N(B)$. So $N(B) \leq N(P)$, and $N(B) = N(P)$ as B admits N(P). But then all involutions of B are not conjugate in N(B), as they must be since B is weakly closed in P : for no element of N(P) moves a central involution of P from the centre. If the second alternative holds then, as $P \leq N(B)$, D_6 normalises a subgroup of P of index 2. This possibility cannot arise by 6.3. So $N(B) / F(N(B)) \approx PSL(2,2^\beta)$, and of necessity $\beta = 2$. Then B can be identified with GF(4) vectors (u,v), where the action of PSL(2,4) is given in the natural way. Let t be the element of order 3 in N(B) which normalises P. Choosing P/B to correspond to matrices $\begin{bmatrix} 1 & . \\ x & 1 \end{bmatrix}$, $x \in GF(4)$, it is clear that $Z(P) = \{(u,o)\}$. Then if τ is an involution inverting t, τ corresponds to $\begin{bmatrix} o & 1 \\ 1 & o \end{bmatrix}$, and

$[Z(P)]^\tau = \{(o,v)\}$. Thus $B = \langle Z(P), [Z(P)]^\tau \rangle$. As $Z(P)$ is fixed by t any involution inverting t will give the same result. That is, if τ is any involution inverting t, a fixed element of order 3 in $N(P)$, then $B = \langle Z(P), Z(P)^\tau \rangle$. Hence Q is unique.

Lemma 6.31 Every involution of P lies in Q.

Proof: Suppose a is an involution in $P - Z(P)$. Then $a \notin Z(P)$, and by 3.1, $\langle Z(P), a, a^t \rangle$ is abelian of order 16. So $a \in Q$.

Lemma 6.32 P contains involutions not in Q.

Proof: As $P \in S_2(N(Q))$ it suffices to find such involutions in $N(Q)$. An involution τ inverting t, an element of order 3 is such.

Proof of lemma 6.26 Assuming that Q is maximal in $\mathcal{M}(D_6; 2)$ with $N(Q) / F(N(Q)) \approx PSL(2,4)$, lemmas 6.31 and 6.32 have been proved : but they are in conflict, so no such Q exists.

§6G The results of this chapter are summarised in the following proposition.

Proposition 6.33 Let G be a minimal counter example to Theorem III: then either the Sylow 2-subgroup of G is dihedral and $L = 2$, or the Sylow 2-subgroup of G is elementary abelian.

The proof has run as follows: the various cases into which $N(Q)$ may fall when Q is maximal in $\mathcal{M}(D_6; 2)$ are listed in §6A. If either of cases 1 or 2 arise for any Q, then lemmas 6.1 and 6.2 give the result. Lemma 6.3 states that case 3 does not arise. So assuming that every

Q is in cases 4, 5 or 6, lemmas 6.15, 6.18, and 6.26 show that there are no such Q, establishing the proposition. In later chapters it is only the result 6.33 that is required. If Walter's result, 2.16, on finite simple groups with abelian Sylow 2-subgroups is assumed, then this, with the Gorenstein and Walter result, 2.13, on groups with dihedral Sylow 2-subgroups would finish the proof of Theorem III.

Chapter 7

The Value of L, and the Character Table of G.

In this chapter the structure of the Sylow 2-subgroup is used to evaluate certain of the constants introduced in Chapter 5, formulas (a), (b) and (c). To fix notation let $T \in S_2(G)$, where G is still a minimal counter example to Theorem III.

Lemma 7.1 $L = 0$ or 2; and if T is abelian and $L = 2$ then $N(T)/C(T)$ is cyclic of order $2^{\alpha}-1$, α is even, and 3 divides $2^{\alpha}-1$.

Proof: If T is dihedral (even a four group), $L = 2$ by 6.33. So suppose T is abelian. If t, an element of order 3 normalises no 2-group, then there are no S_4's, and no A_4's in G, so $L = 0$. Otherwise, since T is elementary there are no elements of order 4, and so by 4.6 there are no S_4's, but t normalises some four group $V = \langle a,b \rangle$. Then N(V) satisfies the inductive hypothesis, and as $\mathcal{N}(D_6; 2)$ is empty, there being no S_4's, $N(V) / F(N(V)) \approx A_o \lesssim A$. As T is abelian, and $V \lesssim T$ without loss, $T \lesssim F(N(V))$, and $T \lhd N(V)$. So $t \in N(T)$, and the inductive hypothesis applies to N(T), giving $N(T) / F(N(T)) \approx A_1 \lesssim A$. But A_1 acts fixed point free on T, and all involutions in T are conjugate by 4.4, and so conjugate by N(T). F(N(T)) being nilpotent, $F(N(T)) = C(T)$. By 3.9, A_1 is cyclic of order $2^{\alpha}-1$; and 3 divides $2^{\alpha}-1$. So α is even. Suppose now that H, K are two A_4's in G. Then if V_1, V_2 are their normal four groups, V_1, $V_2 \lesssim T$ without loss, as a

conjugate of each certainly does. If t_i is an element of order 3 normalising V_i then $t_i \in N(T)$ as above, so, A_1 being cyclic, V_1 and V_2 are normalised by the same element of order 3, say t. Let $V_1 = \langle a_1, b_1 \rangle$, $V_2 = \langle a_2, b_2 \rangle$. If $V_1 \neq V_2$ then $V_1 \cap V_2 = 1$. For some $h \in N(T)$, $a_2 = a_1^h$, as conjugation takes place in N(T) by 2.3. Then $b_2 = a_2^t = a_1^{ht} = a_1^{th}$ as A_1 is cyclic, and $a_1^{th} = b_1^h$. So V_1, V_2 are conjugate. So there is but one class of A_4's in G, and as there are no S_4's, L = 2 as required.

Recall now formulas (a), (b), (c) of Chapter 5.

$$| G | = | A | x(x+1)R^2 \quad \ldots . \quad (a)$$

$$| C(\tau) | = (x-u)R \quad \ldots . \quad (b)$$

$$| A | x(x+1)R = (x-u) \left\{ | A | L + [(| A | -1) x+1]R \right\} \ldots \quad (c)$$

Lemma 7.2 R is odd.

Proof: As all involutions are conjugate, $| G:C(\tau) |$ is odd. But from (a), (b), (c) this number is $| A | L + [(| A | -1) x+1]R$. By 7.1 L is even; and as $| A |$ is odd, $(| A | -1)xR$ is even, so that R is indeed odd.

Lemma 7.3 Let 2^α be the highest power of 2 to divide $| G |$: then 2^α divides x or x+1.

Proof: In (a), $| A | R^2$ is odd, so the result follows, since x and x+1 are coprime.

Lemma 7.4 2^{α} divides (x-u).

Proof: As all involutions are conjugate 2^{α} divides $|C(\tau)|$: so as R is odd the result follows from (b).

Now let B_o denote the principal 2-block of G, and recall the characters χ, χ_i defined in Chapter 5.

Lemma 7.5 Either 2^{α} divides x, χ is not in B_o, all χ_i are in B_o, and u = 0 ;

or 2^{α} divides x+1, χ is in B_o, no χ_i is in B_o, and u =-1.

Proof: Consider $\left[\frac{|G|}{|C(a)|} \cdot \frac{\zeta(a)}{\zeta(1)} \right]^* = k^*$ where * denotes the residue class modulo a prime divisor of 2, $a \in A - \{1\}$, and ζ is an irreducible character of G.

When $\zeta = 1$, $k^* = 0$

When $\zeta = \chi$, $k^* = 1$ if $x \equiv 0 \ (2^{\alpha})$

or $k^* = 0$ if $x+1 \equiv 0 \ (2^{\alpha})$.

When $\zeta = \chi_i$ $k^* = 0$ if $x \equiv 0 \ (2^{\alpha})$

or $k^* = 1$ if $x+1 \equiv 0 \ (2^{\alpha})$.

Then certainly if 2^{α} divides x, χ is not in B_o, and if 2^{α} divides x+1 no χ_i is in B_o. But every irreducible character of G but 1, χ, χ_i is zero on $A - \{1\}$ by 4.2, so by orthogonality some of χ, χ_i are in B_o. The χ_i being constant outside $A - \{1\}$ either all lie in B_o

or no one of χ_i does. This gives the lemma, except for the value of $u = \chi(\tau)$. This comes at once from evaluating $\Sigma\ \zeta(a)\ \zeta(\tau) = 0$ for $a \in A - \{1\}$, and summing over B_o.

Lemma 7.6 The following are the only possible solutions for (a), (b), and (c).

Case	L	u	R	x
I	0	0	?	$1 - \lvert A \rvert$
II	2	0	1	$\lvert A \rvert + 1$
III	2	0	-1	$1 - 3\lvert A \rvert$
IV	2	-1	1	$1 + 2\lvert A \rvert$
V	2	-1	-1	$1 - 2\lvert A \rvert$

Proof: For $L = 0$, (c) gives no information about R. Putting $u = 0$ gives case I. Putting $u = -1$, (c) gives $x = 1$. This contradicts the assumed simplicity of G.

For $L = 2$, and $u = 0$, (c) gives

$$R\ \{\lvert A \rvert - 1 + x\} = 2\lvert A \rvert.$$

But R is odd, and since A is a Hall subgroup of G, $(\ \lvert G \rvert, \lvert G{:}A \rvert\ ) = 1$. So $(R, 2\lvert A \rvert\ ) = 1$. and $R = \pm 1$. This gives cases II and III.

For $L = 2$, and $u = -1$, (c) gives

$$R\ \{x - 1\} = 2\lvert A \rvert.$$

Again $(R, 2|A|) = 1$, so $R = \pm 1$. This gives cases IV and V. There being no other cases lemma 7.6 is complete.

For convenience the fragment of the character table of G is now given for each case. Characters not written down vanish on $A - \{1\}$, and have degrees divisible by $|A|$. Examination of the entry in the column of degrees will determine whether the entries in the row are the values of an irreducible character proper, or their negatives. Throughout the rest of the thesis the cases will be referred to simply by number.

<u>Case I</u> $L = 0$, $u = 0$, $x = 1 - |A|$, R is odd, 2^{α} divides x.

	1	$a \in A - \{1\}$	τ	
1	1	1	1	
χ	$1 - \|A\|$	1	0	
χ_i	$2 - \|A\|$	$\phi_i(a)$	1	$i = 1, \ldots, \frac{1}{2}(\|A\|-1)$

$$|G| = |A| \ (|A|-1) \ (|A|-2)R^2$$

$$|C(\tau)| = (1 - |A|)R.$$

In this case, $T \in S_2(G)$ is elementary abelian by 6.33.

Case II $L = 2$, $u = 0$, $x = |A| + 1$, $R = 1$, 2^{α} divides x.

	1	$a \in A - \{1\}$	τ
1	1	1	1
χ	$\lvert A \rvert + 1$	1	0
χ_i	$\lvert A \rvert + 2$	$\phi_i(a)$	1

$i = 1, \ldots, \frac{1}{2}(|A| - 1)$

$$|G| = |A| \, (|A| + 1) \, (|A| + 2)$$

$$|C(\tau)| = |A| + 1$$

Case III $L = 2$, $u = 0$, $x = 1 - 3|A|$, $R = -1$, 2^{α} divides x.

	1	$a \in A - \{1\}$	τ
1	1	1	1
χ	$1 - 3\lvert A \rvert$	1	0
χ_i	$2 - 3\lvert A \rvert$	$\phi_i(a)$	1

$i = 1, \ldots, \frac{1}{2}(|A| - 1)$

$$|G| = |A| \, (1 - 3|A|) \, (2 - 3|A|)$$

$$|C(\tau)| = 3|A| - 1.$$

(Note: this is a pathological case, and only arises for $|A| = 3$, giving PSL (2,7).

Case IV $L = 2$, $u = -1$, $x = 2|A| + 1$, $R = 1$, 2^{α} divides $x + 1$.

	1	$a \in A - \{1\}$	τ
1	1	1	1
χ	$2\|A\| + 1$	1	-1
χ_i	$2(\|A\| + 1)$	$\phi_i(a)$	0

$i = 1, \ldots, \frac{1}{2}(|A| - 1)$.

$$|G| = |A| (2|A| + 1) (2|A| + 2).$$

$$|C(\tau)| = 2(|A| + 1).$$

Case V $L = 2$, $u = -1$, $x = 1 - 2|A|$, $R = -1$, 2^{α} divides $x + 1$.

	1	$a \in A - \{1\}$	τ
1	1	1	1
χ	$1 - 2\|A\|$	1	-1
χ_i	$2(1 - \|A\|)$	$\phi_i(a)$	0

$i = 1, \ldots, \frac{1}{2}(|A| - 1)$.

$$|G| = |A| (2|A| - 1) (2|A| - 2).$$

$$|C(\tau)| = 2(|A| - 1).$$

Chapter 8

The Case L = 2

By Chapter 7, one of the cases II-V holds. This chapter proves that each of these leads to $G \approx PSL(2,q)$ for some q, and contradicts the assumption that G is a counter example to Theorem III. The cases when T, a Sylow 2-subgroup of G is dihedral, and elementary abelian are dealt with separately.

§ 8A Suppose that $T \in S_2(G)$ is dihedral. The four group $V = \langle x,y \mid x^2 = y^2 = (xy)^2 = 1 \rangle$ is counted as dihedral.

Lemma 8.1 If $T \in S_2(G)$ is dihedral then G is no counter example to Theorem II.

Proof: This is an immediate consequence of the Theorem of Gorenstein and Walter, and the succeeding remark, 2.13.

Remark: In fact the full result of Gorenstein and Walter is not necessary. It can be proved that $C(\tau)$ is 2-nilpotent, and then, using the fragment of the character table of G, a calculation almost identical with that in (12) would lead to the same result.

§ 8B Let $T \in S_2(G)$ be elementary abelian, and suppose L = 2. Then one of cases II-V holds, and by 7.1, $N(T) / C(T)$ is cyclic of order $2^\alpha - 1$, where α is even, so that 3 divides $2^\alpha - 1$. It may be assumed, by § 8A, that T is not a four-group, that is, that $\alpha \geq 4$.

Lemma 8.2 $C(\tau)$ has a normal 2-complement, and $C(T)$ is nilpotent.

Proof: As 3 divides $2^{\alpha}-1 = |\ N(T)\ /\ C(T)\ |$, $N(T)$ satisfies the inductive hypothesis. Then as in 7.1, $N(T)\ /\ C(T) \approx A_o \leq A$, $|\ A_o\ |$ is $2^{\alpha}-1$. and $C(T) = F(N(T))$. Then $N(T) \cap C(\tau) \leq C(T)$, A_o being fixed point free on T, so by Burnside's transfer theorem, 2.5, $C(\tau)$ has a normal 2-complement, since $T \in S_2\ (C(\tau))$.

Let $C(T) = T \times P_1 \times \ldots \times P_s$, where $P_i \in S_{p_i}\ (C(T))$.

Lemma 8.3 If $1 \neq Q_i$ char P_i then $N(Q_i) = N(T)$. In particular $N(P_i) = N(T)$, and $P_i \in S_{p_i}(G)$, if $P_i \neq 1$.

Proof: First observe that as $N(T)\ /\ C(T)$ is fixed point free on $C(T)$, $|\ C(T)\ |$ and $|\ N(T)\ /\ C(T)\ |$ are coprime. Let Q_i char P_i. Then $N(T) \leq N(Q_i)$, so $N(Q_i)$ satisfies the inductive hypothesis. That is, for some normal nilpotent subgroup H, $N(Q_i)\ /\ H$ is isomorphic to A_1, $< A_1, \tau >$ or some PSL (2,q). As a whole Sylow 2-subgroup of G, viz. T, centralises Q_i, $N(Q_i)\ /\ H \approx A_1$. But then $T \leq H$, so $T \lhd N(Q_i)$, so $N(Q_i) \leq N(T)$. Taken with the remark $N(T) \leq N(Q_i)$ this gives $N(Q_i) = N(T)$. Taking $P_i = Q_i$ gives, as $C(T)$ is a Hall subgroup of $N(T)$, $P_i \in S_{p_i}(N(P_i))$, so that $P_i \in S_{p_i}(G)$.

Lemma 8.4 $C(\tau) = U.C(T)$, with $U \lhd C(\tau)$, $U \cap C(T) = 1$.

Proof: By 8.2, $C(\tau)$ has a normal complement V for T. It is only necessary to show that V has a complement for $P_1 x \ldots x P_s$. For any Q_i char P_i, $C(\tau) \cap N(Q_i) = C(\tau) \cap N(T)$ contains no p_i' element which does

not centralise Q_i, so by repeated use of Thompson's transfer theorem, 2.6, $C(\tau)$ has a normal complement U for C(T).

Lemma 8.5 $C(\tau) = C(T)$.

Proof: T has a subgroup $< x_1,y_1,x_2,y_2 >$ where $x_i^t = y_i$, $y_i^t = x_iy_i$ where $t^3 = 1$, $t \in N(T)$. This is a result of 7.1, and the assumption $\alpha \geqslant 4$.

The inductive hypothesis applies to $N(< x_1,y_1>)$, and as a whole Sylow 2-subgroup of G centralises $< x_1,y_1>$ it can only be that $N(< x_1,y_1>) / L \approx A_1 \leq A$ where L is a normal nilpotent subgroup of $N (< x_1,y_1 >)$ containing C(T). But $C(< x_1,y_1>) = L$, the factor $N(< x_1,y_1>) / L$ being fixed point free of order 3. So $C(T) = C (< x_1,y_1>)$. Let U be the normal complement for C(T) in $C(x_1)$ given by 8.4. Then y_1 must invert every element of U, or $U \cap C(< x_1,y_1>) \neq 1$, that is $U \cap C(T) \neq 1$. So U is abelian by 2.1, and admits T.

Let $V = C_U(x_2)$. By the same argument as above $C(T) = C (< x_2,y_2>)$, so that y_2 must invert every element of V. But now y_1y_2 centralises V, and x_1x_2 centralises V. But as above $C(T) = C (< x_1x_2,y_1y_2>)$, so this is a contradiction unless $V = 1$. So x_2 centralises no element of U, and hence, by 2.1, x_2 inverts every element of U. The same must be true of y_2. But then x_2y_2 centralises U, and taking $V = C_U (x_2y_2)$ (=U) leads to the same contradiction, unless $U = 1$. This is precisely what is required by the lemma.

Lemma 8.6 Only case II can hold.

Proof: $N(T) / C(T)$ is cyclic of order $2^{\alpha}-1$ (by 7.1) and acts fixed point free on $C(T)$ by the inductive hypothesis.

Then $| C(\tau) | = | C(T) |$ by 8.5

$= 1 + k| A_o|$, where $2^{\alpha}-1 = | A_o|$ divides $| A |$

In case III this gives $3| A | -1 = 1 + k| A_o|$, so $2 \equiv 0 \bmod 3$, as 3 divides $| A_o |$ and $| A |$, a manifest contradiction.

In case IV, this gives $2| A | + 2 = 1 + k| A_o |$, so $1 \equiv 0 \bmod 3$, a contradiction.

In case V this gives $2| A |-2 = 1 + k| A_o |$, so $3 \equiv 0$ modulo $| A_o |$, and hence $| A_o | = 3$. Then $| T | = 4$, a case which is dealt with by 8.1.

So indeed only case II can hold.

Lemma 8.7 $T = C(\tau)$.

Proof: $| T | = 2^{\alpha}$, $| N(T) / C(T) | = 2^{\alpha}-1$, and $2^{\alpha}-1$ divides $| A |$ as 3 divides $2^{\alpha}-1$. So $| A | = k(2^{\alpha}-1)$ for some k. That is, $2^{\alpha} = (| A | / k) + 1$. As $C(\tau)$ is 2-nilpotent by 8.2, $| T | = \Sigma | \zeta(\tau) |^2$, where the sum is over all ζ in the principal 2-block of G, by 2.29. Then since $\zeta(\tau)$ is rational, being written in the field of the square roots of unity,

$1 + \frac{1}{2}(| A | -1) \leq | T |$, using the character table of case II.

That is, $1 + \frac{1}{2}(| A | -1) \leq 2^{\alpha}$, and $2^{\alpha} = (| A | /k) + 1$.

If $k - 2 > 0$ this gives $| A | < 1 + 2 (k - 2)^{-1}$, so that $| A | = 3$ or 2. The latter case is impossible. If $| A | = 3$ then it can only be that

$k = 3$ and $2^{\alpha}-1 = 1$, and $|T| = 2$ which is not possible. Otherwise $k = 1$ or $k = 2$. If $k = 2$ then $|A|$ is even which is certainly not so. Therefore $k = 1$, and $|N(T) / C(T)| = |A|$, so that $|A| + 1 = 2^{\alpha}$. But $|C(\tau)| = |A| + 1$, so indeed $C(\tau) = T$.

Lemma 8.8 If $L = 2$ and $T \in S_2(G)$ is elementary abelian then G is no counter example to Theorem III.

Proof: By lemma 8.7 G is now a CIT group. So by Suzuki's characterisation of such groups, 2.14, and the remark following 2.14, G is isomorphic to PSL $(2,2^{\alpha})$. Then G is no counter example to Theorem III.

Chapter 9

The Case L = 0

As L = 0, case I holds. Let $T \in S_2(G)$, and $|T| = 2^{\alpha}$. As all involutions in G are conjugate, the involutions of T are permuted transitively by N(T) / C(T). The purpose of this chapter is to show that G is a CIT group, and to do this the structure of N(T) and of $C(\tau)$ is first investigated. Then the character theory of Chapter 3, § E is used, which after some arithmetic gives the required result. It may be assumed for the present that $\alpha \geq 3$, for $|T| = 4$ is dealt with by 8.1 : after the next lemma it is clear that if L = 0, then α is odd.

Lemma 9.1 $|N(T) / C(T)| = (2^{\alpha}-1)r$. T may be identified with the additive group of $GF(2^{\alpha})$ in such a way that the automorphisms induced by N(T) / C(T) are given by $x \longrightarrow ax^{\sigma}$, where $a \in GF(2^{\alpha})$, and σ is a field automorphism of $GF(2^{\alpha})$.

Proof: Let A(T) = N(T) / C(T). Then A(T) is a group of automorphisms of T. For any $\tau \in T - \{1\}$, by (22, Chapter 1)

$|A(T) : C_{A(T)}(\tau)| = 2^{\alpha}-1$, as A(T) must act transitively on $T - \{1\}$. This gives the first part.

Consider now the (abstract) group T.A(T), with $T \lhd T.A(T)$ and the action of A(T) on T given in the obvious way. Then T.A(T) acts on T as a doubly transitive permutation group by

$$\tau \longrightarrow \tau^{a}\sigma \quad \text{under } \sigma a, \quad \sigma \in T, \ a \in A(T).$$

This group is certainly soluble (by 10), so by a result of Huppert, (16), T may be identified with $GF(2^\alpha)$, and T A(T) with a group of semilinear transformations of $GF(2^\alpha)$,

$$x \longrightarrow ax^\sigma + b \quad , \quad a,b \in GF(2^\alpha), \quad \sigma \text{ a field automorphism.}$$

T corresponds to the subgroup $x \longrightarrow x + b$, so the required action of A(T) follows.

Lemma 9.2

$$X = C_{A(T)}(\tau) \text{ is a cyclic group of order } r.$$

Moreover r divides α.

Proof: All involutions of T being equivalent under A(T), take τ to correspond to 1 in $GF(2^\alpha)$, in the identification of 9.1.

Then $X = C_{A(T)}(\tau) = \{ x \longrightarrow x^\sigma \mid \sigma \text{ is a field automorphism} \}$ so X is cyclic, being a subgroup of the automorphism group of a finite field.

As we are trying to show that G is a CIT group, our interest turns to $C(\tau)$. $C(\tau)$ has elementary abelian Sylow 2-subgroup T, and $N(T) / C(T)$ (in $C(\tau)$) is cyclic of order r. Choose g such that $\langle g, C(T) \rangle = N(T)$ and such that $g^r \in O_{2'}(N(T))$. This notation is fixed until after 9.12, where it is proved that $r = 1$.

Lemma 9.3 If $h \in X$ is of order s, then $| C_{TX}(h) | = r.2^{\alpha/s}$.

Proof. The fixed field of $GF(2^\alpha)$ under h is $GF(2^{\alpha/s})$ which gives the result, as X is cyclic of order r.

Lemma 9.4 r is prime to 30.

Proof: As T is a Sylow 2-subgroup of G at once r is odd. As no element of order 3 centralises any involution it is clear that r is prime to 3. If 5 even divides $|G|$ then by 4.8 G contains A_5's and so A_4's. So, if L = 0, 5 does not divide $|G|$. Hence r is prime to 30.

Lemma 9.5 $C_G(\tau)$ is 2-soluble.

Proof: From the earlier remarks on the structure of $C(\tau)$ and by 9.4, the result will follow from Corollary 3.15 if the minimal equation of g on T is $x^r-1 = 0$ or $(x^r-1)/(x-1) = 0$. But $X = \langle g \rangle$ is a cyclic group of field automorphisms, so by the Normal Basis Theorem for fields the minimal equation of g is of the former form. This proves the lemma.

Remark: A different proof of 9.5, not depending on the results of Chapter 3, §E may be given. It depends, however, on the deep result of Thompson, as given in 2.15. For 3 does not divide $|C_G(\tau)|$. So if $C_G(\tau)$ involves a simple group it involves a Sz(q). But whereas Sz(q) does not have elementary abelian Sylow 2-subgroup, $C(\tau)$ does. Hence $C_G(\tau)$ is soluble.

The next lemmas use lemma 3.13. The purpose is to provide a bound for the number of distinct irreducibles in the principal 2-block of G, and hence prove $|A| = 2^{\alpha} + 1$, r = 1, and that G is a CIT group.

Lemma 9.6 PBM (N(T)) has columns labelled by τg^s, s = 1,...,r and rows labelled by ζ_i where ζ_i are the irreducible characters of N(T) in the principal block of N(T). The entries are $\zeta_i(\tau g^s) = \sum_j d_{ij} \omega^{js}$ where ω is a primitive r-th root of unity.

Proof: The first results are definition. The entries are $\zeta_i(\tau g^s)$, and $\zeta_i(\tau g^s) = \sum_j d_{ij} \phi_j(g^s)$, where ϕ_j are Brauer characters of modular irreducibles of $C(\tau) \cap N(T)$ in the principal block, and so effectively (by 3.11) of the modular irreducibles of $C(\tau) \cap N(T) / O_{2'}(C(\tau) \cap N(T))$. i.e. of TX. As $C(\tau)$ is 2-soluble (of 2-length 1 as T is abelian), each of these irreducibles has T in the kernel, as $T\, O_{2'}(C(\tau) \cap N(T)) = O_{2'2}(C(\tau) \cap N(T))$. So the ϕ_j are given by $\phi_j(g^s) = \omega^{js}$ as asserted.

Lemma 9.7 PBM(G) has columns labelled by τg^s, s = 1,...r, and rows labelled by ξ_i where ξ_i are the irreducible characters of G in the principal 2-block of G. The entries are $\xi_i(\tau g^s) = \sum_j D_{ij} \omega^{js}$, where ω is the same primitive r-th root of unity as in 9.6.

Proof: The first remarks are definitional as a result of 3.13 (i). The entries are $\xi_i(\tau g^s) = \sum_j D_{ij} \psi_j(g^s)$, where ψ_j are Brauer characters of modular irreducibles of $C(\tau) \cap G$. But as $C(\tau)$ is 2-soluble of 2-length 1, $C(\tau) / O_{2'}(C(\tau)) \approx TX$ by 3.12 and an isomorphism theorem. Then the result follows as in 9.6.

Lemma 9.8 $\sum_i \xi_i(\tau g^s)\ \overline{\xi_i(\tau g^u)} = 0$ if $s \neq u$

$= r.2^{a/n}$ if $s = u$ and

g is of order n. The sum is over the principal 2-block of G.

Proof: By the isometry established in 3.13,

$$\sum_i \xi_i(\tau g^s)\ \overline{\xi_i(\tau g^u)} = \sum_i \beta_i(\tau g^s)\ \overline{\beta_i(\tau g^u)}.$$

where the latter sum is over the principal block of N(T) i.e. over all characters of T.A(T). As $C_{TA(T)}(\tau g^s) = C_{TX}(\tau g^s)$, the result follows from orthogonality and 9.3.

Lemma 9.9 $D_{ij} = (1/r) \sum_{s=0}^{r-1} \xi_i(\tau g^s)\ \omega^{-js}$

Proof: From 9.7, $\xi_i(\tau g^s)\ \omega^{-js} = \sum_k D_{ik} \omega^{ks}\ \omega^{-js}$.

So summing over s, $\sum_s \xi_i(\tau g^s)\ \omega^{-js} = \sum_k D_{ik} \sum_s \omega^{s(k-j)}$.

If $k \neq j$, then $\omega^{(k-j)}$ is an r-th root of unity, not 1, and so $\sum_s \omega^{s(k-j)} = 0$. When $k = j$ the sum is r, which gives the lemma.

Lemma 9.10 There are at most 2^{a+1} inequivalent irreducibles in the principal block of G.

Proof: If for any ξ_i in the principal block all $D_{ij} = 0$, then $\xi_i(\tau) = 0$. Then counting the multiplicity of the principal character of T in $\xi_i \big|_T$ gives 2^α divides $\xi_i(1)$. Then by 2.25 ξ_i is in a block of the highest kind, so not in the principal block as supposed. So for each i some $D_{ij} \neq 0$. Hence in the principal block there are at most $\sum_i \sum_j | D_{ij} |^2$ distinct characters. The D_{ij} are integers in the field of the square roots of unity, so are rational integers.

Now $\sum_i D_{ij} \bar{D}_{ij} = \frac{1}{r^2} \sum_{s,u} \omega^{-js} \omega^{ju} \overline{\sum_i \xi_i(\tau g^s)} \overline{\xi_i(\tau g^u)}$

by 9.9, So by 9.8,

$$\sum_i D_{ij} \bar{D}_{ij} = (1/r^2) \sum_s r.2^{\alpha/n} \quad \text{where } g^s \text{ is of order n.}$$

$$= (1/r) \sum_{n/r} \phi(n)\, 2^{\alpha/n} \quad \text{where } \phi \text{ is Euler's}$$

ϕ-function, and the sum is over all divisors of r.

Then $\sum_{i,j} | D_{ij} |^2 = r. \ (1/r). \ \sum_{n/r} \phi(n) \ 2^{\alpha/n}$

If $r = 1$ this gives 2^α. Otherwise, it must be that $\alpha \geq 7$, as r divides α and is prime to 30. Then

$$\sum_{i,j} | D_{ij} |^2 = \sum_{n/r} \phi(n) \ 2^{\alpha/n} \leq 2^\alpha + (r-1)2^{\alpha/2} \leq 2^{\alpha+1}.$$

By the opening remarks in the proof this is sufficient to establish the lemma.

Lemma 9.11 $|A| = 2^{a} + 1$.

Proof: In case I, 1 and all the χ_i lie in the principal 2-block of G. That is, at least $\frac{1}{2}(|A| - 1) + 1$ characters lie in the principal 2-block. So by 9.10, $\frac{1}{2}(|A| + 1) \leq 2^{a+1}$, or $|A| + 1 \leq 2^{a+2}$. So $|A| - 1 \leq 2^{a+2}$. But in case I, 2^{a} divides $|A| - 1$, which is the degree of χ. So $|A| - 1 = 2^{a}$, or 2.2^{a}, or 3.2^{a}. But 3 divides $|A|$, so is prime to $|A| - 1$. Also if 2^{a+1} divides $|A| - 1$ it divides $|C(\tau)|$ and so $|G|$, which by definition it does not. So $|A| - 1 = 2^{a}$ as required.

Lemma 9.12 $r = 1$; that is $|N(T) / C(T)| = 2^{a}-1$.

Proof: This is done by providing a better bound for the number of irreducible characters in the principal 2-block than the rather crude estimate got in 9.10. First observe that for no ξ_i in the principal 2-block can $D_{io} = 0$ and all $D_{ij} - D_{io} = 0$. Then, the D_{ij} being rational integers, the total number of characters is bounded by

$$\sum_{i} D_{io}^{2} + \sum_{i,j} (D_{ij} - D_{io})^{2}.$$

Suppose now $r \neq 1$. As r is prime to 30, any divisor of r but 1 is not less than 7.

By 9.9 and 9.8 $\sum_{i} D_{io}^2 = (1/r) \sum_{n|r} \phi(n) \; 2^{a/n}$

$$\leq (1/r) \left\{ 2^a + (r-1) \; 2^{a/7} \right\} .$$

By 9.9 and 9.8,

(*).... $\sum_{i} (D_{io} - D_{ij})^2 = (1/r) \sum_{n=o}^{r-1} 2^{a/n} \; (2 - \omega^{js} - \omega^{-js})$ where g^s

is of order n (over $O_{2'}(N(T))$.)

So $\sum_{i,j} (D_{io} - D_{ij})^2 = \sum_{j=1}^{r-1} (1/r) \sum_{n=1}^{r-1} 2^{a/n} \; (2 - \omega^{js} - \omega^{-js})$,

as only g^r is of order 0.

Then $\sum_{i,j} (D_{io} - D_{ij})^2 \leq (r-1). \; (1/r). \; 2^{a/7}. \; (r-1).4$

$$\leq \frac{4(r-1)^2 \; 2^{a/7}}{r}$$

Hence the total number of characters is at most

$$N = \frac{4(r-1)^2 \; 2^{a/7}}{r} + \frac{2^a + (r-1) \; 2^{a/7}}{r}$$

$$= (2^a/r) + \frac{(r-1) \; (4r-3)}{r} . \; 2^{a/7}$$

But certainly, as 1 and all χ_i are in the principal block, and as

$| A | = 2^a + 1, \quad N \geq 2^{a-1}$.

That is, $2^{a-1} \leq (2^a/r) + \frac{(r-1) \; (4r-3)}{r} \; 2^{a/7}$

But if $r \neq 1$, $r \geqslant 7$, so

$$2^{\alpha-1} \leqslant (2^{\alpha} / 7) + \frac{r-1}{r} \cdot 4.4^{\alpha/2}.2^{\alpha/7}$$

$$\leqslant (2^{\alpha} / 7) + 2^{9\alpha/14}.4.$$

Thus $\alpha \leqslant 11$.

As r divides α the only cases left to consider are $r = \alpha = 7$, and $r = \alpha = 11$. In these cases the expression (*) is evaluated precisely, as each g^s is of order α.

$$\sum_{i} (D_{ij} - D_{io})^2 = (1 / \alpha) \sum_{n=o}^{\alpha-1} 2^{\alpha/n} (2 - \omega^{js} - \omega^{-js})$$

$$= 4(\alpha-1) / \alpha$$

So the total number of characters in the principal 2-block is at most $N = (2^{\alpha} / \alpha) + 4(\alpha-1)^2 / \alpha$, and N exceeds $(\mid A \mid + 1) / 2 = 2^{\alpha-1} + 1$; if $\alpha = 7$ or 11 this is certainly not so. This contradiction establishes that $r = 1$; lemma 9.1 gives the last part.

Lemma 9.13 $C(\tau)$ has a normal 2-complement.

Proof: Consider $N(T) \cap C(\tau)$. Since $N(T) / C(T)$ is of order $2^{\alpha}-1$ by 9.12, and since the action on T is fixed point free by 9.2, it follows that $C(T) \geqslant N(T) \cap C(\tau)$. So, T being a Sylow 2-subgroup of $C(\tau)$, $C(\tau)$ has a normal 2-complement by Burnside's transfer theorem, 2.5.

Lemma 9.14 $C(T) = T$.

Proof: Case I holds. Let X be a matrix representation affording χ.

Let $a \in C(T)$, and suppose $a^p = 1$ where p is an odd prime. Now any algebraic conjugate of χ takes the value (-1) on $A - \{1\}$, and no character but 1, χ or χ_i could do this : in fact only χ does, so χ is rational. For $h \in G$, $\chi(h) = v$ say. Then $\chi_i(h) = v+1$, if h is conjugate to no element of $A - \{1\}$. In particular, for $h = a^i\tau$, $\tau \in T$, $\tau \neq 1$, $\chi(a^i\tau) = \chi_j(a^i\tau) - 1$. As the χ_j are in the principal 2-block, and as $C(\tau)$ is 2-nilpotent by the previous lemma 2.29 gives $\chi(a^i\tau) = \chi_j(a^i\tau) - 1 = \chi_j(\tau) - 1 = \chi(\tau)$. This is true for each $i = 0, \ldots, p - 1$. Now let ξ be any irreducible character of T. Then ξ has degree 1, and $\langle \chi|_T, \xi \rangle = 1$. That is $\chi|_T = \Sigma\, \xi(1).\xi$, or in X, T is represented in its (left) regular representation. By a theorem of Schur, 2.10, the matrices commuting with each $X(\tau)$ as $\tau \in T$ are spanned by the (right) regular representation of T. As T is abelian left and right regular representations coincide, so

$$X(a) = \sum_j m_j\, X(\tau_j) + m\, I$$

where τ_j runs through $T - \{1\}$, and I is the identity matrix.

So $X(a\tau_i) = \sum_j m_j\, X(\tau_j\tau_i) + m\, X(\tau_i)$ for any i.

Taking traces, $\chi(a\tau_i) = m_i.2^a$, since in the regular representation only $1 = \tau_i^{-1}.\tau_i$ has non zero trace. But by the earlier part $\chi(a\tau_i) = \chi(a\tau_i) = \chi(\tau) = 0$. So each $m_i = 0$. Then $X(a) = m\, I$. As $\chi(a)$ is rational, m is rational. But $[X(a)]^p = I$, so $m = 1$. Then if $a \neq 1$, there is a non-trivial element in the kernel of a non trivial representation, and G is not simple; so $a = 1$, and $C(T) = T$.

The next three lemmas show that even $C(\tau) = T$.

Lemma 9.15 For any $h \in G$, h not conjugate to an element of A, $| C(h) |$ divides $R(2^{\alpha} + \chi(h))$.

Proof: $\#(\tau \cdot h \cdot = a) \neq 0$, and is an integer, for any $a \in A - \{1\}$.

That is, $$\frac{| G |}{| C(\tau) | \; | C(h) |} \cdot \left\{ 1 - \frac{\chi(h) + 1}{2 - | A |} \right\}$$ is an integer

Substituting for $| C(\tau) |$, $| G |$, $| A |$ gives

$$(2^{\alpha} + 1)R \quad (\chi(h) + 2^{\alpha}) / | C(h) | \text{ is an integer.}$$

As $| A | = 2^{\alpha} + 1$ is prime to $| C(h) |$ the lemma follows.

Lemma 9.16 There is no $h \in O_2 / (C(\tau))$, $h \neq 1$, with $2^{\alpha-1}$ dividing $| C(h) |$.

Proof: Suppose there were. Then by 9.15, $2^{\alpha-1}$ divides $R(\chi(h) + 2^{\alpha})$. As R is odd this means $2^{\alpha-1}$ divides $\chi(h)$. As χ is rational, $\chi(h)$ is an integer. So $\chi(h) = \pm 2^{\alpha}$ or $\pm 2^{\alpha-1}$, since $|\chi(h) | \leq | \chi(1) | = 2^{\alpha}$. As G is simple $|\chi(h) | < | \chi(1) |$ or G is represented as having a centre, which it does not. If $\chi(h) = 2^{\alpha-1}$, then in the representation X affording χ, if $X(h)$ is diagonalised, there are $2^{\alpha-1}$ 1's and k sets $(1 \; \omega \ldots \; \omega^{p-1})$, where ω is a p-th root of unity : for it may be supposed that h is of prime order p. Then p divides $2^{\alpha-1}$, which is not so for an odd prime. If $\chi(h) = -2^{\alpha-1}$, then diagonalising $X(h)$, there are $2^{\alpha-1}$ sets of eigen values $(\omega \ldots \; \omega^{p-1})$ and k sets $(1 \; \omega \ldots \; \omega^{p-1})$. That is, as $\chi(1) = 2^{\alpha}$, $2^{\alpha} = 2^{\alpha-1}(p-1) + k\,p$.

That is, $2^{\alpha-1}$ divides k p, and so divides k. But then $2^{\alpha} = 2^{\alpha-1}(p-1) + 2^{\alpha-1} k_1 p$, which is not so as $p \geqslant 3$ being odd. So there is no such h of prime order, so a fortiori no such h.

Lemma 9.17 $C(\tau) = T$.

Proof: If not, then $O_{2'}(C(\tau)) \neq 1$, and so an $h \in O_{2'}(C(\tau))$ with 2 dividing $| C(h) |$. We prove by induction that there is an h in $O_{2'}(C\tau))$ with $2^{\alpha-1}$ dividing $| C(h) |$, even, by induction, that for each s, $s = 1, \ldots, \alpha-1$ there is an $h \in O_{2'}(C(\tau))$ with 2^s dividing $| C(h) |$, $h \neq 1$.

Suppose that there is no element $h \in O_{2'}(C(\tau))$ with 2^{s+1} dividing $| C(h) |$, yet 2^s divides $| C(h) |$, where $1 \leqslant s < \alpha-1$. Let $U = O_2(C(\tau))$. Let $V = C_U(T_o) \neq 1$, where T_o is some subgroup of order 2^s. As $T_o \lhd T$, V admits T. As α is odd, $\alpha \geqslant 3$, so unless the lemma is true there are certainly involutions σ_1, σ_2, $\sigma_1\sigma_2$ not in T_o, but in T. Then σ_i does not centralise any non-trivial emenent v of V, or for that v, 2^{s+1} divides $| C(v) |$. So σ_i inverts V by 2.1, and so $\sigma_1\sigma_2$ centralises V. Hence for $v \in V$, $< T_o, \sigma_1\sigma_2 > \leqslant C(v)$, so 2^{s+1} divides $| C(v) |$. As there is an h with 2 dividing $| C(h) |$, by induction there is an $h \in O_{2'}(C(\tau))$ with $2^{\alpha-1}$ dividing $| C(h) |$. But this contradicts 9.16 ; hence the hypothesis $C(\tau) \neq T$ is untenable, and the lemma established.

Lemma 9.18 If L = 0 then G is no counter example to Theorem III.

Proof: By 9.17 G is a CIT group. By Suzuki's characterisation of such groups, 2.14, and the succeeding remark, $G \approx PSL(2,2^{\alpha})$. Hence G is no counter example to Theorem III.

Chapter 10

Conclusion.

Firstly, Theorems II and III are now proved. For it was seen in Chapter 5 that Theorem II is a corollary of Theorem III, and even that a minimal counter example to Theorem III is a counter example to Theorem II. Theorem III is proved : for in Chapter 6 it was seen that the Sylow 2-subgroup of a counter example was dihedral or elementary abelian, and in Chapter 7 that L = 0 or 2. In Chapter 9 it was seen that the dihedral case is no counter example by the result of Gorenstein and Walter, and the elementary abelian case with L = 2 no counter example by the results of Suzuki. In Chapter 10, the remaining possibility, that L = 0 and a Sylow 2-subgroup is elementary abelian, was also seen to lead to a CIT group, so again was no counter example.

Secondly it might be asked what happens if the hypothesis " (111) 3 divides | A |" is dropped. If "(111)′ 3 divides | G |" is substituted, the same result might be hoped for, except for a few cases for each A. The fragment of the character table could be constructed, but A_4's and S_4's could not be counted using it; and A_5's only if 5 divides | A |. Moreover the central part of the proof of Theorem II is Chapter 6, and without 3 dividing | A | this would not get off the ground; less seriously the arithmetical calculation in Chapter 9, and the proof that involution-centralisers are soluble would not go through unaltered. If hypothesis (111) is ommitted altogether, then it might be hoped that the conclusion "$G \approx PSL(n,q)$ or $Sz(q)$" could

be substituted. This, however, seems much more difficult. Even a theorem analogous to Theorem I, which would characterise $Sz(q)$ as a simple group with non conjugate subgroups A,B,C, each the centraliser of each of its non trivial elements, and with $| N(A) / A | = 2$, $| N(B) / B | = | N(C) / C | = 4$ seems more difficult.

BIBLIOGRAPHY

1. R.Brauer: Some Applications of the Theory of Blocks of Characters of Finite Groups. J.Alg., 1, (1964) 152-167, 307-334, 3, (1966) 225-255.

2. R.Brauer, M.Suzuki and G.E.Wall: A characterisation of the one dimensional unimodular projective linear groups. Illinois J.Maths., 2, (1958) 718-745.

3. W.Burnside: The Theory of Groups of Finite Order. C.U.P., 2nd. edition, 1911.

4. W.Burnside: On Groups in which every two conjugate operations are permutable. Proc. L.M.S., 35, (1902) 28-37.

5. W.Burnside: On an Arithmetical theorem connected with the roots of unity, and its application to group characteristics. Proc. L.M.S.,(2) 1, (1904) 112-116.

6. R.W.Carter: Simple groups and Simple Lie Algebras. Journal L.M.S., 40, (1965) 193-240.

7. H.S.M.Coxeter and W.O.J.Moser: Generators and Relations for Finite Groups. Springer-Verlag, 2nd. edition, 1965.

8. C.W.Curtis and I.Reiner: Representation Theory of Finite Groups and Associative Algebras. Interscience, 1962.

9. W.Feit and J.G.Thompson: Finite Groups which contain a self-centralising element of order 3. Nagoya Math.J., 21, (1962) 185-197.

10. W.Feit and J.G.Thompson: Solvability of Groups of Odd Order. Pacific J.Math., 13, (1963) 771-1029.

11. D.Gorenstein and J.H.Walker: The Characterisation of Finite groups with Dihedral Sylow 2-subgroups. I,II,III. J.Alg., 2, (1965) 85-151, 218-270, 354-393.

12. D.Gorenstein and J.H.Walker: On Finite Groups with Dihedral Sylow 2-subgroups.
Illinois J.Math., 6, (1962) 553-593.

13. M.Hall, jr.: The Theory of Groups.
MacMillan, 1959.

14. P.Hall and G.Higman: The p-length of a p-soluble group and reduction theorems for Burnside's Problem.
Proc. L.M.S.,(3) 6, (1956) 1-42.

15. G.Higman: Lecture notes. (unpublished).

16. B.Huppert: Zweifach transitive, auflösbare permutationsgruppen.
Math. Zeitschr., 68, (1957) 126-150.

17. M.Suzuki: On a New Type of simple groups of finite order.
Proc.Nat.Acad.Sci., 46, (1960) 868-870.

18. M.Suzuki: Finite Groups with nilpotent centralizers.
Trans.Amer.Math.Soc., 99, (1961) 425-470.

19. M.Suzuki: On a class of doubly transitive groups.
Ann.Math., 75, (1962) 105-114.

20. J.G.Thompson: Normal p-complements for finite groups.
J.Alg., 1, (1964) 43-46.

21. J.G.Thompson: Non Solvable groups all of whose local subgroups are solvable.
Typescript, University of Chicago.

22. H.Wielandt: Finite Permutation Groups.
Academic Press, 1964.

23. H.Wielandt: Zum Satz von Sylow.
Math.Zeitschr., 60, (1954) 407-408.