AN ELEMENTARY CHARACTERIZATION OF THE SIMPLE GROUPS PSL(3,3) AND M_{11} IN TERMS OF THE CENTRALIZER OF AN INVOLUTION

BY

JOHN DOYLE, BSc. (HONS)(ADELAIDE).

A thesis submitted to the University of Adelaide in January, 1984 for the degree of Master of Science.

The research was undertaken in the Department of Pure Mathematics at the University of Adelaide.

Awarded 7-11-84.

TABLE OF CONTENTS

SUMMARY

In this thesis we investigate groups of even order containing an involution whose centralizer is isomorphic to GL(2,3). The aim of the research was to give an elementary proof (that is, without the use of character theory) that the only such groups with the additional property of having no subgroup of index 2 are the simple groups PSL(3,3) and M_{11}.

Following the introduction, chapter one consists of a few preliminary general results together with some properties of the group GL(2,3).

In chapter two we prove a few results about a group G satisfying the above two properties. In particular we show that there are four possibilities for the structure of the normalizer of a group of order 3 contained in the centralizer of an involution. Each of these cases is dealt with seperately in the ensuing chapters.

STATEMENT

This thesis contains no material which has been accepted for the award of any other degree or diploma in any University, and to the best of my knowledge and belief, contains no material previously published or written by another person, except when due reference is made in the text of this thesis.

JOHN DOYLE

Name : John Doyle Course : Master of Scie

I give consent to this copy of my thesis, when deposited in the University Library, being available for loan and photocopying.

Date : 29-1-85 Signed :

I give consent to this copy of my thesis, when deposited in the University Library, being available for loan and photocopying.

Date : 29-1-85 Signed :

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. D.L. Parrott for many simplications in the arguments I used and especially for suggesting the problem in the first place.

INTRODUCTION

If G is a group of even order, then G contains an element of order 2. Such an element is called an involution. It was Brauer who first realised the importance of involutions in finite groups of even order. During the late forties Brauer had observed that some very simple properties of involutions can be used to prove some surprisingly strong results concerning the structure of groups of even order. Using such results Fowler in his thesis ([11]) gave a characterization of the groups $SL(2,2^n)$ in terms of involutions. In these groups the centralizer of an involution is an abelian 2 - group. Fowler proved that this property actually characterizes $SL(2,2^n)$. (The centralizer of an element x in a group G is defined to be $C_G(x) = \{g \in G \mid xg = gx\}$).

The following result appeared in a paper by Brauer and Fowler in 1955 ([5]).

"If G is a group of even order g which contains m involutions and if $n=g/m$ then there exists a proper normal subgroup L of G such that G/L is isomorphic to a subgroup of the symmetric group on t letters with $t = 2$ or $t < n\frac{(n+2)}{2}$. In particular $|G:L| = 2$ or $|G:L| < [n\frac{(n+2)}{2}]!$"

If G is simple then L must be trivial and $g < [n\frac{(n+2)}{2}]!$ Let z be any involution of G. Then $|G:C_G(z)| \leq m = g/n$, hence $n \leq |C_G(z)|$ so $g \leq [|C_G\frac{(z)|(|C_G(z)| + 2)}{2}]!$

This yields the following result.

"There exists only a finite number of simple groups G which contain an involution z such that the centralizer $C_G(z)$ of z in G is isomorphic to any given group".

This result suggested to Brauer the possiblity of classifying simple groups of even order in terms of the structure of the centralizer of an involution. This proposal has come to be known as Brauer's programme. This was explicitly proposed in a talk he gave at the International Congress in Amsterdam in 1954 ([2]).

By a result of Feit and Thompson ([10]) all non-abelian simple groups have even order and hence contain involutions. This result strikingly reinforced Brauer's contention that the structure of a simple group is intimately connected with its involutions.

As an example of this programme Brauer announced the following theorem ([2]).

"Suppose G is a group of finite order which satisfies the following conditions.

(1) G contains an involution z whose centralizer $C_G(z)$ is isomorphic to $GL(2,q)$.

(2) If c is an element of the centre of $C_G(z)$, $c \neq 1$, then $C_G(c) = C_G(z)$.

(3) $G' = G$

If $q \equiv -1$ (4), $q \not\equiv 1$ (3) then G is isomorphic to $PSL(3,q)$. If $q = 3$, we have the additional case that G can be isomorphic to the simple Mathieu group of order 7920.

This was the first classification of simple groups other then $PSL(2,q)$ in terms of involutions. The proof did not appear until 1966 when Brauer proved the following more general result in [4].

"Let G be a finite group which satisfies the conditions

(1) There exists an involution z of G whose centralizer $C_G(z)$ is isomorphic with a group of the form GL(2,q)/L where L is a subgroup of the centre Z(GL(2,q)) and where $q \equiv -1$ (4)

(2) The group G does not have a normal subgroup of index 2.

We then have one of the cases.

(a) $G \cong$ PGL(3,q), PSL(3,q) or SL(3,q)

(b) G is isomorphic to a direct product of PSL(3,q) with a cyclic group of order 3, $q \equiv 1$ (3), $q \not\equiv 1$ (9)

(c) $G \cong M_{11}$ the Mathieu group of order 7920."

After elementary preliminaries the proof is divided into 2 cases according to whether $q^3 \,||\, |G|$ or not. In both cases the theory of blocks is heavily used. The first case is concluded by appealing to a previous characterisation of PSL(3,q). The second case is reduced to five numerical cases. Four of these cannot occur whereas the fifth yields M_{11}.

We note that this theorem relies heavily on the theory of characters and in fact almost all early characterizations also rely on character theory. We illustrate with a few examples.

In 1959 Suzuki generalized both Fowler's result (given above) and a result of Brauer, Suzuki and Wall ([6]). He gave a group theoretical characterization of the 1 - dimensional unimodular linear fractional group $SL(2,2^n)$. The main theorem in [17] states.

"Let G be a finite group of even order. If the centralizer of any involution in G is always abelian then we have one of the following three possibilities.

(1) Sylow 2-subgroups of G are cyclic

(2) A Sylow 2-subgroup of G is normal

(3) G is a direct product of two groups L and A where L is one of the linear groups $SL(2,2^n)$ and A is an abelian group of odd order."

The proof begins by assuming the theorem false and then studying a group G of smallest order contradiction the theorem. Some properties of G concerning Sylow 2-subgroups and centralizers are proved. Then considering a more general group satisfying weaker conditions, its structure and characters are studied and a formula for its order is derived. Applying this formula to the group G leads to a contradiction.

In a second paper on linear groups, in the same year, Suzuki gave a characterization of the 2 - dimensional linear fractional groups over a field of characteristic 2 by properties of involutions. This result is a counterpart to a similar characterization of these groups over a field of order q, $q \equiv -1$ (4) given by Brauer (as stated above). Suzuki proves the following theorem ([17]).

"Let G be a finite group of even order and z an involution of G. If the centralizer of z in G is isomorphic with the centralizer of an involution in the linear fractional group G_0 in 2 variables over a field F of q elements, q even, and if every involution of G is conjugate to z, then G is isomorphic to G_0, with one exception. The exceptional case occurs when q = 2 and in this case we have $G \cong LF(3,2)$ or $G \cong A_6$."

After an analysis of the structure of the centralizer of an involution, the case q = 2 is easily settled by making use of previous results. For the case $q > 2$ both the main theorem of the first paper on linear groups above and its order formula are used several times. Then after a complicated study of its structure and characters, G is shown to have a subgroup M of order $q^3 (q - 1)^2 (q + 1)$ and index $q^2 + q + 1$. In fact M is the normalizer of an elementary abelian group P of order q^2. G is represented as a permutation group on the set B which consists of the $q^2 + q + 1$ conjugates of P; G is doubly transitive on B. Also G is shown to contain a subgroup L of order q^2 not conjugate to P. Suzuki constructs a projective plane in which the points are elements of B and the lines are the conjugates of L. Further a point lies on a line if and only if the subgroups intersect non-trivially. This is shown to be a Desarguesian plane. This enables Suzuki to identify G with the linear fractional group and complete the proof.

Finally we mention a characterization of M_{12} given by Wong ([19]) in terms of centralizers of involutions. Specifically he proves the following theorem.

"Let $C(z_0)$ be the centralizer in M_{12} of an involution z_0 in the centre of a Sylow 2 - subgroup of M_{12}. Let G be a finite group such that

(1) G contains an involution z whose centralizer $C_G(z)$ in G is isomorphic to $C(z_0)$.

(2) G does not contain 3 mutually non-conjugate involutions.

Then either G is isomorphic with M_{12} or G has a unique nontrivial normal subgroup N. In the latter case N is elementary abelian of order 8 and G/N is isomorphic with the simple group GL(3,2) of order 168.

The theorem is proved by means of computations with characters. In particular, in one of the cases considered, G is shown to be a simple group whose order is the same as that of M_{12}. By a result of Stanton ([16]), G is isomorphic to M_{12}.

We should now like to mention something about the known finite simple groups. By early this century the families of classical simple groups over a finite field had been discovered, plus two exceptional families found by Dickson (see Dickson's book on linear groups ([9])). These together with the groups of prime order, the alternating groups and the five Mathieu groups were the only known simple groups.

Mathieu discovered his groups around 1860 in the search for highly transitive permutation groups. There are two 5-transitive groups of degrees 12 and 24 denoted by M_{12} and M_{24} respectively. The groups M_{11}, M_{22} and M_{23} are the natural one or two point stabilizers; M_{11} and M_{23} are both 4-transitive, while M_{22} is 3-transitive. They include the only known 4 and 5-transitive permutation groups apart from the symmetric and alternating groups which are trivial exceptions. The 5 groups are all simple and represent the first sporadic simple groups. Remarkably it took over a hundred years for the sixth sporadic simple group to be discovered.

In 1955 the first simple groups since Dickson's time were discovered by Chevalley. These fall into a framework which now includes all known infinite families, the alternating groups being the only exception. Steinberg and others were then able to construct the "twisted" groups as the fixed point subgroups of certain automorphisms of these groups. These groups are collectively known as the groups of Lie type.

We list the infinite families below. The groups listed may not be simple; a central subgroup needs to be factored out to obtain a simple group. The integer d denotes the order of this central subgroup.

Known Finite Simple Groups

G	d
Z_p	1
A_n, $n \geq 5$	1
$A_n(q)$	$(n + 1, q - 1)$
$B_n(q)$, $n > 1$	$(2, q - 1)$
$C_n(q)$, $n > 2$	$(2, q - 1)$
$D_n(q)$, $n > 3$	$(4, q^n - 1)$
$G_2(q)$	1
$F_4(q)$	1
$E_6(q)$	$(3, q - 1)$
$E_7(q)$	$(2, q - 1)$
$E_8(q)$	1
${}^2A_n(q)$, $n > 1$	$(n + 1, q + 1)$
${}^2B_n(q)$, $q = 2^{2m + 1}$	1
${}^2D_n(q)$, $n > 3$	$(4, q^n + 1)$
${}^3D_4(q)$	1
${}^2G_2(q)$, $q = 3^{2m + 1}$	1
${}^2F_4(q)$, $q = 2^{2m + 1}$	1
${}^2E_6(q)$	$(3, q + 1)$

NOTE: $A_n(q)$ should not be confused with the alternating groups A_n. Also $A_n(q)/Z \cong PSL(n,q)$ (where Z is the central subgroup).

We also have the 26 sporadic simple groups, so named since they do not belong to any infinte family. They are listed below. The sixth sporadic simple group J_1 was discovered by

Janko in 1966 ([14]). It was found when Janko tried to eliminate a particular possibility for the centralizer of an involution in a finite simple group. The others were discovered in the following fifteen years.

Known Finite Simple Groups

G	ORDER OF G
M_{11}	$2^4 .\ 3^2 .\ 5 .\ 11$
M_{12}	$2^6 .\ 3^3 .\ 5 .\ 11$
M_{22}	$2^7 .\ 3^2 .\ 5 .\ 7 .\ 11$
M_{23}	$2^7 .\ 3^2 .\ 5 .\ 7 .\ 11 .\ 23$
M_{24}	$2^{10} .\ 3^3 .\ 5 .\ 7 .\ 11 .\ 23$
J_1	$2^3 .\ 3 .\ 5 .\ 7 .\ 11 .\ 19$
J_2	$2^7 .\ 3^3 .\ 5^2 .\ 7$
J_3	$2^7 .\ 3^5 .\ 5 .\ 17 .\ 19$
J_4	$2^{21} .\ 3^3 .\ 5 .\ 7 .\ 11^3 .\ 23 .\ 29 .\ 31 .\ 37 .\ 43$
HS	$2^9 .\ 3^2 .\ 5^3 .\ 7 .\ 11$
Mc	$2^7 .\ 3^6 .\ 5^3 .\ 11$
Suz	$2^{13} .\ 3^7 .\ 5^2 .\ 7 .\ 11 .\ 13$
Ru	$2^{14} .\ 3^3 .\ 5^3 .\ 7 .\ 13 .\ 29$
He	$2^{10} .\ 3^3 .\ 5^2 .\ 7^3 .\ 17$
Ly	$2^8 .\ 3^7 .\ 5^6 .\ 7 .\ 11 .\ 31 .\ 37 .\ 67$
ON	$2^9 .\ 3^4 .\ 5 .\ 7^3 .\ 11 .\ 19 .\ 31$
.1	$2^{21} .\ 3^9 .\ 5^4 .\ 7^2 .\ 11 .\ 13 .\ 23$
.2	$2^{18} .\ 3^6 .\ 5^3 .\ 7 .\ 11 .\ 23$
.3	$2^{10} .\ 3^7 .\ 5^3 .\ 7 .\ 11 .\ 23$
M(22)	$2^{17} .\ 3^9 .\ 5^2 .\ 7 .\ 11 .\ 23$
M(23)	$2^{18} .\ 3^{13} .\ 5^2 .\ 7 .\ 11 .\ 13 .\ 17 .\ 23$

G	ORDER OF G
M(24)′	$2^{21}. 3^{16}. 5^{2}. 7^{3}. 11. 13. 23. 29$
F_5	$2^{15}. 3^{10}. 5^{3}. 7^{2}. 13. 19. 31$
F_3	$2^{14}. 3^{6}. 5^{6}. 7. 11. 19$
F_2	$2^{41}. 3^{13}. 5^{6}. 7^{2}. 11. 13. 17. 19. 23. 31. 47$
F_1	$2^{46}. 3^{20}. 5^{9}. 7^{6}. 11^{2}. 13^{3}. 17. 19. 23. 31. 41. 47. 59. 71$

The above list is believed to be the complete list of all finite simple groups. Although many have been characterized by centralizers of involutions relying heavily on character theory, it is of interest to see if more elementary proofs can be given. In particular, proofs without using the theory of characters.

We remark that the main application of characters is to determine the order of the group. Now if the structure of the group is not too complicated there are other ways of determining this order. If there is one class of involutions a lemma of Bender ([1]) (also see chapter 1 of this thesis) can be applied; and if there is more than one class of involutions, Thompson′s Order Formula can be used.

An example of a characterization without character theory is given by Bender. In [1] he gives a characterization of the simple groups PSL(2,7) and A_6 in terms of centralizers of involutions. In this paper he proves a lemma which he uses to determine the order of these groups. (In this case the order is enough to complete the characterization). In this same paper Bender studies Janko′s first simple group J_1 and in particular determines its order using these elementary techniques.

The purpose of this thesis is to use these ideas to give a characterization of the simple groups $PSL(3,3)$ and M_{11} in terms of centralizers of involutions. Specifically we prove the following.

THEOREM

Let G be a finite group of even order with the following properties

(a) G has no subgroup of index 2

(b) G possesses an involution z whose centralizer $C_G(z)$ in G is isomorphic to $GL(2,3)$.

Then G is isomorphic to $PSL(3,3)$ or M_{11}.

For the earlier proof of this result (due to Brauer and Wong) using character theory see [13].

The proof of this theorem uses Bender's lemma many times. We shall therefore make a few remarks concerning the lemma. To use the lemma we need to choose a suitable "large" subgroup H of the group G and count the number of involutions in each coset of H in G. From this we can determine the number of involutions in G. This fact, together with the structure of the centralizer of an involution and the fact that there is only one class of involutions in G enables us to determine the order of G.

In order to count the number of involutions in each coset we make use of the following observations.

Let u be an involution of $G-H$ and consider the coset Hu. Let $v \in Hu$ be an involution, $v = hu$ for some h in H; this implies $h = vu$.

Now

$$h^u = (vu)^u = uvuu = uv = (vu)^{-1} = h^{-1}$$

Thus u inverts h.

Conversly suppose u inverts an element h of H, $h^u = h^{-1}$ Then $v = hu$ is an involution of the coset Hu since

$$v^2 = huhu = hh^u = hh^{-1} = 1$$

Thus the number of elements in the coset Hu is equal to the number of elements of H inverted by u. All of these elements belong in the subgroup $H \cap H^u$. Thus a knowledge of $H \cap H^u$ may help to determine the number of involutions in the coset Hu.

To conclude this introduction we give a brief outline of the proof of our theorem. Suppose G is a finite group which satisfies the assumptious of the theorem. Let x be an element of order 3 in $C_G(z)$. After some initial results about G we prove that $N_G(\langle x\rangle)$ has a normal 2-complement A. There are four possibilities for the structure of A. Each of these is treated seperately in a different chapter.

In chapter 3, $A \cong Z_3$, here we prove the existence of a certain type of subgroup M. The subgroup M satisfies the conditions:

(i) $(|M|, 6) = 1$

(ii) $|N_G(M)|$ is even,

and M is chosen maximal subject to (i) and (ii). There are various possibilities for $N_G(M)$, many of which are eliminated by using Bender's lemma. We eventually obtain a possible order for G and then show that G is sharply 3-transitive in its action on the Sylow 5-subgroups. A contradiction is obtained by considering the structure of the subgroup fixing two letters.

In the other cases after proving more properties of G we choose a subgroup H, apply Bender's lemma and obtain the order of G. Once the order is obtained we proceed differently in each case. In chapter 4, $A \cong Z_3 \times Z_3 \times Z_3$, it is trivial to obtain a contradiction. The case A non-abelian of order 27 yields the group PSL(3,3) which is identified using a paper of Brauer's ([3]), this is done in chapter 5. In the final chapter $A \cong Z_3 \times Z_3$. Before identifying the group we first need to show that it has a subgroup of index 11, which is done using generators and relations. Once we have this subgroup we represent G on the cosets. This leads to an identification of G with M_{11}.

CHAPTER ONE

ASSUMED RESULTS AND PROPERTIES OF GL(2,3)

We begin with a few assumed results which will be used at various places in the proof of our theorem. The first is a simple consequence of Sylow´s theorem, it is know as the Frattini argument.

LEMMA (1.1) ([12] Theorem (1.3.7))

If $H \triangleleft G$ and P is a Sylow p - subgroup of H, then $G = N_G(P)H$.

The next two results are simple applications of the transfer homomorphism.

BURNSIDE´S TRANSFER THEOREM

If P is a Sylow p - subgroup of G and $N_G(P) = C_G(P)$ then G has a normal p - complement.

PROOF

Since $N_G(P) = C_G(P)$, $P \leq Z(N_G(P))$, the result now follows by Theorem 7.4.3 of ([12]).

THOMPSONS TRANSFER THEOREM ([13] Lemma XII. 8. 2.)

Suppose G is a group with no subgroup of index 2 and R is a subgroup such the $|G:R|$ is twice an odd number. Then any involution in G is conjugate to any involution in R.

The next two results are not readily found in the literature, we therefore include a proof.

LEMMA (1.2)

Suppose z is an involution normalizing a subgroup H of G with the property that $C_H(z) = 1$. Then z inverts H, that is

$h^z = h^{-1}$ for all $h \in H$, H is abelian and H has odd order.

PROOF

Consider the map $\theta: H \to H$ defined by $\theta: h \mapsto h^{-1}zhz$. This map is well-defined as z normalizes H so that $zhz \in H$, for all $h \in H$.

If $\theta(h_1) = \theta(h_2)$ for some $h_1, h_2 \in H$ then $h_1^{-1}zh_1z = h_2^{-1}zh_2z$ by definition of θ. But then $zh_1h_2^{-1} = h_1h_2^{-1}z$, that is $h_1h_2^{-1} \in C_H(z)$. And because $C_H(z) = 1$ we conclude that $h_1 = h_2$. The map is therefore $1 - 1$ and hence onto.

Let $h \in H$ then there exists $h_1 \in H$ such that $\theta(h_1) = h^{-1}$ that is $h_1^{-1}zh_1z = h^{-1}$. Taking the inverse of this expression we have $zh_1^{-1}zh_1 = h$ whence $h_1^{-1}zh_1z = zhz$. Equating gives $h^z = h^{-1}$, which is the first result.

Let $h_1, h_2 \in H$ then

$(h_1h_2)^{-1} = (h_1h_2)^z = h_1^z\ h_2^z = h_1^{-1}\ h_2^{-1}$

And as $(h_1h_2)^{-1} = h_2^{-1}\ h_1^{-1}$ we have $h_1^{-1}\ h_2^{-1} = h_2^{-1}\ h_1^{-1}$ which implies that H is abelian.

If H has even order then H contains an involution h say. But then $h^z = h^{-1} = h$, so that $h \in C_H(z)$ a contradiction. Thus H has odd order.

LEMMA (1.3)

Let M be a subgroup of odd order in G. Suppose M is inverted by an involution z and $C_G(M) = M$.

Then $N_G(M) = MC_{N_G(M)}(z)$.

PROOF

Let $n \in N_G(M)$ and $m \in M$ then $(n^{-1}zn)m(n^{-1}zn) = n^{-1}z(nmn^{-1})zn = n^{-1}(nm^{-1}n^{-1})n$ as z inverts M and $nmn^{-1} \in M$.

Thus $(n^{-1}zn)m(n^{-1}zn) = m^{-1} = zmz$ hence $(zn^{-1}zn)m(n^{-1}znz) = m$ that is $n^{-1}znz \in C_G(m)$. This is true for all $m \in M$, therefore $n^{-1}znz \in C_G(M) = M$ and so $n^{-1}zn \in Mz$, which is true for all $n \in N_G(M)$. It follows that $M\langle z\rangle$ is a normal subgroup of $N_G(M)$. As M has odd order $\langle z\rangle$ is a Sylow 2 - subgroup of $M\langle z\rangle$ so the Frattini argument yields $N_G(M) = M\langle z\rangle N_{N_G(M)}(\langle z\rangle) = MC_{N_G(M)}(z)$.

The following formula was discovered by Brauer and the result has been generalized by Wielandt in ([18]) (for which Brauer's result is a special case); it is know as the Brauer-Wielandt formula.

THE BRAUER-WIELANDT FORMULA

Let $H \leq G$, H of odd order h and suppose Aut (H) contains a 4 - group $\theta_0 = \langle\theta_1,\theta_2\rangle$ $\theta_3 = \theta_1\theta_2$. Let f_i denote the number of fixed points in H by $\theta_i, i = 0, 1, 2, 3$. Then $f_0{}^2 h = f_1 f_2 f_3$.

For our purposes we require this formula in the following form.

CORALLARY (1.4)

Let H be a subgroup of G of odd order and suppose $N_G(H)$ contains a 4 - group $V = \langle v_1,v_2\rangle, v_3 = v_1v_2$

Then:

$$|C_H(V)|^2|H| = |C_H(v_1)||C_H(v_2)||C_H(v_3)|$$

The following lemma is proved by Bender in ([1]). since it is crucial for our theorem we shall include proof.

BENDER'S LEMMA

Let G be a group with a subgroup H such that $|J| > |G:H|$ where J denotes the set of involutions in G.

Furthermore define

J_n = set of $u \in J-H$ such that $|Hu \cap J| = n$

b_n = number of cosets $Hg \neq H$ such that $|Hg \cap J| = n$

c = number of $u \in J_1$ such that $C_H(u) \neq 1$.

$$f = \frac{|J|}{|G:H|} - 1 > 0$$

Note that $|J_n| = nb_n$ Then

(1) $|J| = |J \cap H| + b_1 + 2b_2 + 3b_3 + \ldots$

(2) $b_1 = c + k|H|$ for some non-negative integer k

(3) $b_1 < f^{-1}(|J \cap H| + b_2 + 2b_3 + 3b_4 + \ldots) - 1 - b_2 - b_3 \ldots$

PROOF

Firstly (1) is obvious. For (2) note that $b_1 = c +$ the number of $u \in J_1$ such that $C_H(u) = 1$.

Let $u \in J_1$ be such that $C_H(u) = 1$

If $u^h = u^k$ for some $h,k \in H$, then $hk^{-1} \in C_H(u) = 1$, so $h = k$; also $u^h \in J_1$. Therefore u^h, for $h \in H$, are distinct involutions of J_1 such that $C_H(u^h) = 1$; (2) now follows.

To prove (3) note that

$|G:H| = 1 + b_0 + b_1 + b_2 \ldots$ hence using (1)

$|J| - |G:H| = |J \cap H| - 1 - b_0 + b_2 + 2b_3 + 3b_4 + \ldots$

Since $|J| - |G:H| = f\,|G:H|$

$\qquad = f(1 + b_0 + b_1 + b_2 + b_3 + \ldots)$

$fb_1 = |J| - |G:H| - f(1 + b_0 + b_2 + b_3 + \ldots)$

So that

$b_1 = f^{-1}(|J \cap H| - 1 - b_0 + b_2 + 2b_3 + 3b_4 + \ldots) - 1 - b_0 - b_2 - b_3 - \ldots$

and as $b_0 \geq 0$ the inequality follows.

All notation defined in this lemma will be fixed throughout this thesis. This lemma is used when the group G has one class of involutions, in this case we have the following alternate expression for f

$$f = \frac{|J|}{|G:H|} - 1 = \frac{|G:C_G(z)|}{|G:H|} - 1$$
$$= \frac{|G|/|C_G(z)|}{|G|/|H|} - 1$$
$$= \frac{|H|}{|C_G(z)|} - 1$$

So $f = \frac{|H|}{|C_G(z)|} - 1$, where z is an involution of G.

In chapter 3 we show that the group concerned is a sharply 3-transitive permutation group in which the subgroup fixing two letters is isomorphic with SL(2,3). The following lemma shows that no such group exists. This result appears in Passman's book on permutation groups ([15]). We shall include the proof since it is an interesting one.

<u>LEMMA</u> <u>(1.5)</u>

Suppose G is a sharply 3-transitive permutation group on a set Ω, suppose also that $3 \mid |G_{0*}|$ where 0,* are two points in Ω. Then G_{0*} has precisely one subgroup of order 3.

<u>PROOF</u>

Let u,v be two distinct elements of order 3 in G_{0*}. These elements fix 0 and * but no other point as G is sharply 3-transitive; therefore they have the form

$u = (0)(*)(1\ 2\ 3)\ldots$

$v = (0)(*)(1\ a\ b)\ldots$ with $a,b \neq 2,3$ respectively.

Choose $g \in G$ with $g = (1)(2\ 3)\ldots$ Then $u^g = (1\ 3\ 2)\ldots$ The element uu^g fixes the three points 1, 2 and 3 so as G is sharply 3-transitive this element is trivial, hence $u^g = u^{-1}$.

Now g must send the points fixed by u to the points fixed by u^{-1}, hence g permutes the set $\{0,*\}$. Since g already has 1 fixed point namely 1, we must have

$g = (0,*)(1)(2\ 3)\ldots$

Now choose $h \in G$ with

$h = \binom{1\ 2\ 3.\ .}{1\ a\ b\ldots}$

Then $v^{-1}u^h$ fixes the three points 1, a and b, hence $v^{-1}u^h = 1$ so that $u^h = v$. Since $u \neq v$, $h \neq 1$. Now h must send the points fixed by u to the points fixed by v and hence permutes the set $\{0,*\}$. Since h already has one fixed point, namely 1 we must have $h = (0,*)(1)\ldots$ But now g and h agree on three points and hence are equal. This yields.

$v = u^h = u^g = u^{-1}$.

Thus G_{0*} must contain precisely one subgroup of order 3.

The group PSL(3,3) occurs in chapter 5; a paper of Brauer's ([3]) is used to identify it. In this paper Brauer considers a set of postulates for a group G which permits him to define a projective plane π in terms of G. G has a natural representation by collineations of π. These postulates are the following.

(I) G contains a 4-group V, $V = \langle v,v_1\rangle$, $v_2 = vv_1$; and there exists an element of G which permutes the involutions of V.

(II) There exist subgroups M and $M^* \neq 1$ of G with the following properties

(a) M and M^* have the same order

(b) $C_G(v) \leq N_G(M)$ and $C_G(v) \leq N_G(M^*)$

(c) $M \cap M^* = M \cap C_G(v) = M^* \cap C_G(v) = 1$

(III) All involutions of $C_G(v)-\langle v\rangle$ are conjugate in $C_G(v)$.

We have the following definitions. A point p is a subset of G of the form $p = g^{-1}vMg$ with $g \in G$. A line r is a subset of G of the form $r = g^{-1}vM^*g$ with $g \in G$. The point p lies on the line r, if $p \cap r = \emptyset$ The plane Π is the set of all points and lines. For a fixed element t of G the mapping

$$r(t) : p \mapsto p^t, \; r \mapsto r^t \text{ is a collineation of } \Pi .$$

Under these assumptions it is shown that

$$M = M_1 x M_2 \text{ and } M^* = M_1^* x M_2^*$$

where $M_i = M \cap C_G(v_i)$

and $M_i^* = M^* \cap C_G(v_i) \quad i = 1,2$

and $|M_1| = |M_2| = |M_1^*| = |M_2^*| = q$

We also need the following two postulates

(IV) $|G:MC_G(v)| \leq q^2 + q + 1$

(V) Every class of $C_G(v)$ conjugate elements of M meets M_1.

Then we have the following result which is Theorem (4D) of [3].

LEMMA (1.6)

The group G has a chief series $G \geq G_0 \geq K \geq 1$ where G/G_0 is cyclic, G_0/K is isomorphic with PGL(3,q) or PSL(3,q) and K has odd order.

For $q \not\equiv 1$ (3) the groups PGL(3,q) and PSL(3,q) coincide.

In chapter 6 we have occasion to consider groups defined in terms of generators and relations. The following results will be used ([8]).

LEMMA (1.7)

Let G be a group generated by the elements R and S which satisfy the following relations

$$R^3 = S^3 = (RS)^4 = (R^{-1}S)^4 = 1$$

Then G is the simple group PSL(2,7) of order 168.

LEMMA (1.8)

Let G be a group generated by the elements R and S which satisfy one of the following relations

(i) $R^3 = S^4 = (RS)^5 = (R^{-1}S^{-1}RS)^2 = 1$ or

(ii) $R^4 = S^5 = (RS)^2 = (R^{-1}S)^5 = 1$

Then G is isomorphic to A_6.

To identify M_{11} in chapter 6 we use the following result; for the first part see [8] for the second see [7] page 151.

LEMMA (1.9)

Let G be a group satisfying either of the conditions

(i) G is generated by the elements r, m, n which satisfy the following relations

$r^{11} = m^5 = n^4 = (rn)^3 = 1$

$r^m = r^4$ and $m^n = m^2$

(ii) $G = \langle(1,2,3,4,5,6,7,8,9,10,11),(3,7,11,8)(4,10,5,6,)\rangle$

Then G is isomorphic to M_{11}.

Since the centralizer of an involution of a group in our theorem is isomorphic to GL(2,3) we shall need to know some of its properties. We state these without proof.

Let C_0 = GL(2,3), then C_0 is a group or order $48 = 2^4.3$; its centre $Z(C_0) = \langle z_0\rangle$ has order 2; C_0 contains a unique quaternion subgroup Q_0 which is therefore normal in C_0, and SL(2,3) is the unique subgroup of index 2 in C_0 and has quaternion Sylow 2-subgroup.

Let S_0 be a Sylow 2-subgroup of C_0. Then S_0 is semi-dihedral and S_0 has subgroups of index 2 which are cyclic, quaternion and dihedral of order 8; and $N_{C_0}(S_0) = S_0$. If X_0 is a Sylow 3-subgroup of C_0 then $N_{C_0}(X_0) = X_0V_0$ where V_0 is a 4 - group of C_0. Also we have $N_{C_0}(V_0)$ is dihedral or order 8.

The elements of $C_0-\langle z_0\rangle$ have orders 2,3,4,6 and 8 and their centralizers in C_0 have orders 4,6,8,6 and 8 respectively. The elements of $C_0-\langle z_0\rangle$ each form a single conjugacy class in C_0 the lengths of these classes are 12,8,6 and 8 respectively. In particular $C_0-\langle z_0\rangle$ contains 12 involutions. The elements of order 8 form two classes both containing 6 elements; and an element of order 8 is not conjugate in C_0 to its inverse.

Finally Q_0 contains all elements of order 4 in C_0, SL(2,3) also contains all elements of order 3 and C_0 is generated by its involutions.

We conclude this chapter with the following notation which is fixed thoughout this thesis.

We denote by G a group satisfying the conditions of our theorem and z is an involution of G whose centralizer in G is isomorphic to GL(2,3). Let $C = C_G(z)$, S be a Sylow 2-subgroup of C and Q the unique quaternion subgroup of C. Let t be an involution of $C-\langle z\rangle$ and denote by V the 4-group $\langle z,t\rangle$. Finally let X be a subgroup of order 3 in C inverted by t. (We note that there are two possible choices for such a subgroup X).

CHAPTER TWO

PRELIMINARY RESULTS

This chapter consists of a few basic properties of the group G. We begin with an easy lemma.

LEMMA (2.1)

$N_G(S) = S$ and so S is a Sylow 2-subgroup of G.

PROOF

As $Z(S) = \langle z\rangle$, $\langle z\rangle$ char S so $\langle z\rangle \triangleleft N_G(S)$. Therefore $N_G(S) \leq N_G(\langle z\rangle) = C$. It follows now that $N_G(S) = S$.

The next result concerns the conjugacy of involutions in G.

LEMMA (2.2)

The group G has one class of involutions.

PROOF

Firstly by assumption G has no subgroup of index 2. Secondly as S is a Sylow 2-subgroup of G, $|G:Q|$ is twice an odd number. So any involution in G is conjugate to an involution in Q by Thompsons Transfer Theorem. Since Q contains only one involution z, all involutions of G are conjugate to z, the lemma follows.

The following result deals with the conjugacy of elements of order 3 centralized by involutions.

LEMMA (2.3)

The elements of G of order 3 centralized by some involution form a single conjugacy class.

PROOF

Let b be an element of order 3 in G centralized by an involution v. By lemma (2.2) $z = v^g$ for some g in G. So as

$$b \in C_G(v), \quad b^g \in C_G(v^g) = C$$

And as the elements of order 3 in C form a single conjugacy class in C, the elements of order 3 in G centralized by some involution form a single conjugacy class in G.

We also determine the number of conjugacy classes of elements of order 4, 6 and 8 in G.

LEMMA (2.4)

The elements of order 4 and 6 in G each form a single conjugacy class. There are two classes of elements of order 8 in G.

PROOF

Let b be an element of order 4 in G. Then b^2 is an involution and so is conjugate to z by lemma (2.2). As $b \in C_G(b^2)$ some conjugate of b is contained in C. As C has one class of elements of order 4, G must have one class of elements of order 4.

The same reasoning applies if b has order 6 since b^3 is an involution and C has one class of elements of order 6.

Suppose now that b has order 8. Then some conjugate of b is contained in C. As C has two classes of elements of order 8, G has at most two classes of elements of order 8.

Consider $b \in C$, b an element of order 8. We claim b cannot be conjugate to its inverse; suppose so and let $b^g = b^{-1}$ for some g in G. Then $(b^4)^g = b^{-4}$ which is $z^g = z$; that is $g \in C$. However b is not conjugate to its inverse in C. Therefore b is not conjugate to its inverse in G. We conclude that G has two classes of elements of order 8.

The next lemma shows that there are four possible structures for the normalizer in G of a subgroup of order 3 in the centralizer of an involution. Each of these cases must be considered seperately.

LEMMA (2.5)

We have $C_G(X) = A\langle z\rangle$ and $N_G(X) = AV$ where A is either elementary abelian of order 3,9 or 27 or is non-abelian of order 27. Furthermore $A \lhd N_G(X)$.

PROOF

Let R be a Sylow 2-subgroup of $C_G(X)$ containing $\langle z\rangle$. Since $C_R(z) \leq C_{C_G(X)}(z) = C_C(X)$ is cyclic of order 6, $C_R(z) = \langle z\rangle$ and hence $R = \langle z\rangle$ (either $z \in Z(R)$ or z is centralized by an element of $Z(R)^{\#}$). As $\langle z\rangle$ is a Sylow 2-subgroup of $C_G(X)$, $C_G(X)$ has a normal 2-complement, A say, by Theorem 7.6.1 of [12]. Thus $C_G(X) = A\langle z\rangle$. Further $A \lhd N_G(X)$ and $N_G(X) = AV$.

Acting on A by the 4-group V we have, by the Brauer-Wielandt formula, that

$|A| = |C_A(z)||C_A(zt)||C_A(t)|$

(since $C_A(V) = 1$)

Now $C_A(z)$ has order 3 and $C_A(zt)$ and $C_A(t)$ have order 1 or 3 ($|A|$ being odd), so A has possible orders 3, 9 or 27. In the first two cases A is elementary abelian and in the latter case A is either elementary abelian or non-abelian of order 27.

We list the four possible cases to be considered.

Case (A) $A = Z_3$

Case (B) $A = Z_3 x Z_3 x Z_3$

Case (C) A non-abelian of order 27

Case (D) $A = Z_3 x Z_3$

We conclude with a result on a proper non-trivial normal subgroup of G, if there is one.

LEMMA (2.6)

Either G is simple or a proper non-trivial normal subgroup has order 27.

PROOF

Suppose G is not simple, let L be a proper non-trivial normal subgroup of G. If L has even order then it contains an involution and hence all involutions by lemma (2.2). As C is generated by its involutions $C \leq L$ and in particular $S \leq L$. The Frattini argument yields, since S is a Sylow 2-subgroup of L (in fact of G) by lemma (2.1) that $G = LN_G(S)$. Whence $G = L$ by the same lemma a contradiction. Hence L has odd order.

Acting on L by the 4-group V we have

$$|L| = |C_L(z)||C_L(zt)||C_L(t)| .$$

And as $z \sim zt \sim t$ in G,

$$|C_L(z)| = |C_L(zt)| = |C_L(t)| = 3,$$

and therefore $|L| = 27$.

CHAPTER THREE

CASE (A) $A \cong Z_3$

Throughout this chapter suppose that $N_G(X) = XV$.

It follows from Sylow's theorem that X is a Sylow 3-subgroup of G and hence G has one class of elements of order 3. The following lemma is easily proved.

LEMMA (3.1)

The group G is simple.

PROOF

If G contained a proper non-trivial normal subgroup L, L would have order 27 by lemma (2.6). As G does not contain a subgroup of such order G is simple.

The following lemma shows the existence of a certain type of subgroup of G. It is the normalizer of this subgroup that will be important for us in determining the order of G.

LEMMA (3.2)

There exists a subgroup M or order m such that $(m,6) = 1$ and $|N_G(M)|$ is even.

PROOF

Consider the set $\{zx\ ;\ x \in J\}$. We determine the number of involutions x for which zx has order 1, 2, 3, 4 or 6.

There is one involution for which zx has order 1 and 12 where the order is 2 (namely the involutions of $C-\langle z\rangle$).

Let zx have order 3. Thus z inverts zx and every element of order 3 inverted by z is of this form. Suppose z inverts k elements of order 3. Then any involution inverts k elements of order 3 by lemma (2.2). Because there are $2^3|J| =$

$|G:C_G(zx)|$ elements of order 3 each inverted by 6 involutions and as there are $|J|$ involutions, we have $k|J| = 6.2^3\ |J|$; that is, $k = 48$. Thus z inverts 48 elements or order 3. Similarly z inverts 24 and 48 elements of order 4 and 6 respectively. Therefore the number of involutions x for which zx has order 1, 2, 3, 4 or 6 is

$$1 + 12 + 48 + 24 + 48 = 133 = 7.19.$$

For any other involution x, $|zx| = n$ with $(n,6) = 1$. So if there are no such x then $|J| = 7.19$ whence

$$|G| = 2^4.\ 3.\ 7.\ 19$$

In this case let P be a Sylow 19-subgroup of G. Then $|C_G(P)|\,|\,7.19$ and as $|Aut(P)| = 18 = 2.3^2$ and $|N_G(P)|$ is odd, $|N_G(P)|\,|\,3.7.19$. Hence $2^4\ |\ |G:N_G(P)|$ and so $|G:N_G(P)| = 2^4.x$ with x a divisor of 3.7. As $2^4 = 16 \equiv -3\ (19)$, $-3x \equiv 1\ (19)$ by Sylow's theorem. Now x = 1, 3, 7 or 21 none of which satisfy this congruence. Hence there exists an involution x for which $|xz| = n$ and $(n,6) = 1$. The subgroup $\langle zx\rangle$ satisfies the lemma.

Let M be a subgroup as in the previous lemma such that M is maximal subject to these conditions. That is, if $M \leq M_0$ with $(|M_0|,6) = 1$ and $|N_G(M_0)|$ even then $M = M_0$. We may assume $z \in N_G(M)$. We gather together a few properties of M in the next lemma.

<u>LEMMA</u> <u>(3.3)</u>

(a) z inverts M and M is abelian

(b) $C_G(M) = M$

(c) $N_G(M) = MC_{N_G(M)}(z)$

(d) $C_G(\mu) = M$ for all $\mu \in M^\#$ and hence $N_G(\langle\mu\rangle) \leq N_G(M)$

(e) If $g \in G-N_G(M)$ then $M \cap M^g = 1$

PROOF

Since $(m,6) = 1$ no element of $M^{\#}$ can centralize z. Therefore (a) follows by lemma (1.2).

Clearly z normalizes $C_G(M)$ and the order of $C_G(M)$ is prime to 6. So as $M \leq C_G(M)$, M being abelian, the maximality of M forces $C_G(M) = M$, which is (b). Now (c) follows by lemma (1.3) since z inverts M and $C_G(M) = M$.

Let $\mu \in M^{\#}$; since z inverts μ, $z \in N_G(\langle\mu\rangle)$ and as $C_G(\mu) \lhd N_G(\langle\mu\rangle)$, $z \in N_G(C_G(\mu))$. As μ cannot centralize an element of order 2 or 3 the order of $C_G(\mu)$ is prime to 6. So as $M \leq C_G(\mu)$ the maximality of M implies $C_G(\mu) = M$. Now $M \lhd N_G(\langle\mu\rangle)$ and $N_G(\langle\mu\rangle) \leq N_G(M)$, hence we have (d).

Finally, let $g \in G-N_G(M)$ and suppose $M \cap M^g \neq 1$. Let $x \in M \cap M^g$, $x \neq 1$. Then there exists $y \in M^{\#}$ such that $x = y^g$. Now $C_G(x) = C_G(y)^g$ which by (d) yields $M = M^g$; that is $g \in N_G(M)$. This is a contradiction and hence $M \cap M^g = 1$.

In the following two lemmas we determine various possibilities for the normalizer of M in G. In two of these cases a possible order for G is obtained.

LEMMA (3.4)

We have the following possibilities for the normalizer of M in G:

(a) A Sylow 2-subgroup of $N_G(M)$ is quaternion

(b) $|N_G(M)| = 2.\ 3.\ 7$

(c) $|N_G(M)| = 2.m$

(d) $|N_G(M)| = 2^2.5$

(e) $|N_G(M)| = 2^2.13$ and in this case the order of G is $2^4.3.5^2.13$

PROOF

As $N_G(M)$ cannot contain a 4-group (by theorems (6.2.2) and (5.3.16) of [12]) a Sylow 2-subgroup is either quaternion or cyclic. The former case is (a), so we may assume a Sylow 2-subgroup of $N_G(M)$ is cyclic.

Suppose firstly $3 \mid |N_G(M)|$. Then $3 \mid |C_{N_G(M)}(z)|$ since $|N_G(M)| = |M|\,|C_{N_G(M)}(z)|$ by lemma (3.3) (c), and as $C_{N_G(M)}(z) < C$, $C_{N_G(M)}(z)$ must be cyclic of order 6. Thus $|N_G(M)| = 2.3.m$.

The normalizer of a subgroup of order 3 in $N_G(M)$ is cyclic of order 6, its index in $N_G(M)$ is therefore m and Sylow's theorem yields $m \equiv 1(3)$. And as $(m,6) = 1$ either $m = 7$ which is (b) or $m \geq 13$.

In this latter case we can apply Bender's lemma to $H = N_G(M)$. We first calculate f,

$$f = \frac{|H|}{|C_G(z)|} - 1 = \frac{6m}{48} - 1 = \frac{m-8}{8}$$

Also $|J \cap H| = m$ as H contains m involutions.

Let p be a prime divisor of m and P be a Sylow p-subgroup of H. It is easily seen, by Sylow's theorem, that P is a Sylow p-subgroup of M, and hence is the only Sylow p-subgroup of H (since it is the only Sylow p-subgroup of M by lemma (3.3) (a)). Let x be an element of H of order p, so that $x \in P$ and hence $x \in M$. Thus for any prime divisor p of m, an element x of H of order p is contained in M.

Let u be an involution of G-H and consider $H \cap H^u$. Suppose a prime divisor p of m divides the order of $H \cap H^u$. Then $H \cap H^u$ contains an element, x say, of order p. Now both x and x^u are elements of order p in H and hence, by the previous paragraph are contained in M. It follows that $x \in M \cap M^u$ which contradicts lemma (3.3) (e). Thus no prime divisor of m divides $|H \cap H^u|$.

Whence $|H \cap H^u| | 6$ and $H \cap H^u$ is cyclic.

Suppose u inverts z. Either u inverts only $\langle z \rangle$, in which case $u \in J_2$ or u inverts another non-trivial element of H and in this case u inverts $H \cap H^u$ which will be cyclic of order 6 and so $u \in J_6$. As z is centralized by 12 involutions of G-H and z has m conjugates in M we have

$$|J_2| + |J_6| = 12.m = 2^2.3.m$$

Now suppose u inverts X (which we may assume belongs in H). As $N_C(X) = XV = N_G(X)$, u centralizes z in addition to inverting X, so $u \in J_6$. Since X is inverted by involutions of G-H and X has m conjugates in H we have

$$|J_6| = 6.m = 2.3.m$$

It follows that

$$|J_2| = 2.3.m;$$

thus $b_2 = 3m$ and $b_6 = m$

Now let $u \in J_1$, so that u inverts no non-trivial element of H. In particular u cannot centralize an involution of H. As an element of order 3 in H, is centralized by only one involution of G which is contained in H, we have $C_H(u) = 1$ for all $u \in J_1$. Thus $c = 0$ and $b_1 = 2.3.m.k$, k a non-negative integer.

Summarizing, we have

$$f = \frac{m-8}{8},$$

$$|J \cap H| = m,$$

$$b_2 = 3.m,\ b_6 = m,$$

$b_1 = 2.3.m.k$, k a non-negative integer and all other b_n are zero ($n \neq 0$).

By Bender's lemma we have

$$b_1 = 2.3.m.k < \frac{8}{m-8}(m + 3m + 5m) - 3m - m$$

$$= \frac{2^3.3^2.m}{m-8} - 2^2.\,m$$

therefore $3k < \dfrac{2^2 3^2}{m-8} - 2.$

As $m \geq 13$, $\dfrac{1}{m-8} \leq \dfrac{1}{5}$ so

$$3k < \frac{2^2.3^2.}{5} - 2 < 6, \text{ that is } k < 2$$

and so $k = 0$ or 1.

The number of involutions in G is

$|J| = m + 2.3.m.k + 2.3.m + 2.3.m = m(13 + 6k)$,

Whence $|G| = 2^4.3.m.(13 + 6k)$.

Suppose $k = 0$ then

$|G| = 2^4.3.13.m$

We have $0 < \dfrac{2^2.3^2.}{m-8} - 2$ which yields $m \leq 25$, so $13 \leq m \leq 25$. As $(m,6) = 1$ and $m \equiv 1$ (3) there are three possible values for m, namely 13, 19 or 25. Since $|N_G(M)| = 2.3.m$, M is a Sylow subgroup of G (in all cases). This immediately excludes $m = 13$. The index of $N_G(M)$ in G is $2^3.13$, so by Sylow's theorem $2^3.\,13 \equiv 1$ (p) where $p = 5$ or 19. However this congruence yields $103 \equiv 0$ (p) and, as 103 is prime, this is a contradiction. Thus $k = 1$ and $|G| = 2^4.3.19.m$. In this case $3 \leq \dfrac{2^2.3^2}{m-8} - 2$ which yields $m \leq 15$, therefore $13 \leq m \leq 15$. So as $(m,6) = 1$, $m = 13$. Whence $|G| = 2^4.3.13.19$.

However $N_G(M)$ has index $2^3.\,19$ which is congruent to 9 modulo 13 contradicting Sylow's theorem. We have shown that if $3 \mid |N_G(M)|$ then $m = 7$ and $|N_G(M)| = 2.3.7$.

Now assume 3 does not divide the order of $N_G(M)$. There are then three cases to consider, namely

$|N_G(M)| = 2.m$, $2^2.m$ or $2^3.m$. The first is (c).

Suppose $|N_G(M)| = 2^3.m$. As $C_{N_G(M)}(z)$ is cyclic of order 8, each involution of $N_G(M)$ centralizes only one Sylow 2-subgroup of $N_G(M)$. Thus the intersection of distinct Sylow 2-subgroups of $N_G(M)$ is trivial. It follows that $m \equiv 1$ (8). This combined with $(m,6) = 1$ implies $m \geq 17$.

Let $H = N_G(M)$. We apply Bender's lemma to H. Firstly

$$f = \frac{|H|}{|C_G(z)|} - 1 = \frac{8m}{48} - 1 = \frac{m-6}{6},$$

and $|J \cap H| = m$.

Let u be an involution of $G\text{-}H$ and consider $H \cap H^u$. By the same reasoning as above $|H \cap H^u| \mid 8$, and $H \cap H^u$ is cyclic.

No element of order 8 is inverted by an involution. So if u inverts an involution either $u \in J_2$ or J_4. Hence we have

$$|J_2| + |J_4| = 12.m = 2^2.3.m$$

If u inverts a subgroup of order 4 then $u \in J_4$. Now a subgroup of order 4 is inverted by 4 involutions of G-H and as H contains m subgroups of order 4,

$$|J_4| = 4.m = 2^2.m.$$

therefore $|J_2| = 2^3.m$ and thus

$$b_2 = 2^2.\ m \text{ and } b_4 = m$$

Applying Bender's lemma we have

$$b_1 < \frac{6}{m-6}(m + 2^2.m + 3.m) - 2^2.m - m = \frac{2^4.3m}{m-6} - 5.m$$

In particular this gives

$$0 < \frac{2^4 3.m}{m-6} - 5.m$$

which yields $m < 16$, a contradiction.

Finally consider $|N_G(M)| = 2^2.m$. As for the previous case the intersection of distinct Sylow 2-subgroups of $N_G(M)$ is trivial, so that $m \equiv 1$ (4). As $(m,6) = 1$ we have $m = 5$ or $m \geq$

13. The former case is (d) and in the latter we can use Bender's lemma applied to $H = N_G(M)$. We have

$$f = \frac{4m}{48} - 1 = \frac{m-12}{12}$$

and $|J \cap H| = m$

It is easily shown, as above, that $b_2 = 2^2.m$ and $b_4 = m$. Also we have $c = 0$ and therefore $b_1 = 2^2.m.k$, k a non-negative integer. All other b_n are zero ($n \neq 0$).

By Bender's lemma

$$b_1 = 2^2.m.k < \frac{12}{m-12}(m + 2^2.m + 3.m) - 2^2.m - m$$

$$= \frac{2^5.3.m}{m-12} - 5.m,$$

therefore $2^4.k < \frac{2^5.3}{m-12} - 5$

In particular $0 < \frac{2^5.3}{m-12} - 5$

which yields $m \leq 31$, as $m \geq 13$, so $13 \leq m \leq 31$.

As $(m,6) = 1$ and $m \equiv 1\ (4)$ there are 4 possible values for m, namely 13, 17, 25 or 29.

The number of involutions in G is

$$|J| = m + 2^2.m.k + 2^3.m + 2^2.m$$

$$= m.(13 + 4k),$$

whence $|G| = 2^4.3.m.(13 + 4k)$

Since $|N_G(M)| = 2^2.m$, M is a Sylow subgroup of G in all cases. The index of $N_G(M)$ in G is $2^2.3.(13 + 4k)$ so by Sylow's theorem $2^2.3.(13 + 4k) \equiv 1\ (m)$. (This includes the case $m = 25$ by lemma (3.3) (e)).

Firstly we assume $m \geq 17$. Then $\frac{1}{m-12} \leq \frac{1}{5}$ so that

$$2^2.k < \frac{2^5 3}{5} - 5$$

which yields $0 \leq k \leq 3$.

If $m = 17$ then $2^2.3(13 + 4k) \equiv 1$ (17) which implies $k \equiv 12$ (17), a contradiction.

If $m = 25$ then $2^2.3(13 + 4k) \equiv 1$ (25) which implies $k \equiv 15$ (25), a contradiction.

If $m = 29$ we find that $k \equiv 1$ (29) and hence $k = 1$. Thus the order of G is $2^4.3.17.29$. We can easily eliminate this case using Sylow's theorem. Let P be a Sylow 17-subgroup of G. Clearly $C_G(P) = P$. As $|Aut\ (P)| = 16$, $|N_G(P)|\,|\,2^4.17$, it follows that 3.29 divides the index of $N_G(P)$ in G. We have $|G:N_G(P)| = 3.29.x$ with x a divisor of 2^4. Since $2.29 \equiv 2$ (17), $2x \equiv 1$ (17) by Sylow's theorem. As x = 1, 2, 4, 8 or 16 and none of these satisfy the congruence, $m \neq 29$.

Finally we assume $m = 13$, and recall that $|N_G(M)| = 2^2.13$. In this case $2^2.k < 2^5.3 - 5$ and we get $0 \leq k \leq 22$. Now $2^2.3\ (13 + 4k) \equiv 1$ (13) which yields $k \equiv 3$ (13), and so $k = 3$ or 16.

The order of G is $2^4.3.13.(13 + 4k)$. The normalizer of a Sylow 3-subgroup of G has order $2^2.\ 3$ and hence index $2^2.13.(13+4k)$ which is congruent to 1 modulo 3 by Sylow's theorem. This implies $k \equiv 0$ (3) and hence $k = 3$. Whence the order of G is $2^4.3.5^2.13$, which is the final case (e), and the lemma is proved.

We observe in case (e), using Sylow's theorem, that a Sylow 5-subgroup of G is elementary abelian and its normalizer has order $2^3.3.5^2$ and hence a Sylow 2-subgroup is quaternion.

LEMMA (3.5)

If a Sylow 2-subgroup of $N_G(M)$ is quaternion then $|N_G(M)| = 2^3.3.5^2$ and $|G| = 2^4.3.5^2.13$.

PROOF

Suppose a Sylow 2-subgroup of $N_G(M)$ is quaternion. As $|N_G(M)| = |M||C_{N_G(M)}(z)|$ by lemma (3.3) (c), we have $|N_G(M)| = 2^3.e.m$ where $e = 1$ or 3 and $C_{N_G(M)}(z) \cong Q_8$ or $SL(2,3)$ respectively.

An involution centralizes only one quaternion subgroup. Therefore the intersection of distinct Sylow 2-subgroups is trivial and thus $m \equiv 1$ (8). We have $(m,6) = 1$ and therefore $m \geq 17$.

We now apply Bender's lemma to the subgroup $H = N_G(M)$. Firstly $f = \dfrac{|H|}{|C_G(z)|} - 1 = \dfrac{8.e.m}{48} - 1 = \dfrac{e.m-6}{6}$ and $|J \cap H| = m$.

Let u be an involution of G-H and consider $H \cap H^u$. As in the previous lemma no prime divisor of m divides $|H \cap H^u|$ so $|H \cap H^u| \mid 2^3.e$.

All elements of order 4 in C belong to Q and so to H. Suppose u centralizes z; then $u \in C$. In both cases $C_H(z)$ contains precisely one involution. Therefore there are 12 possibilities for u. As every involution of $C-\langle z\rangle$ inverts a subgroup of order 4 in C, u inverts a subgroup of order 4 in H.

If $e = 1$ then u can invert no other subgroup of H and thus $u \in J_4$. As H contains m involutions we have in this case that $|J_4| = 12.m = 2^2.3.m$; thus $b_4 = 3.m$.

If $e = 3$ then $C_H(z) \cong SL(2,3)$ contains all subgroups of order 3 in C. So u also inverts 2 subgroups of order 3 and 2 subgroups of order 6 in $C_H(z)$. This implies that u inverts $1 + 1 + 2 + 4 + 4 = 12$ elements of H so $u \in J_{12}$. If u inverts an element of order 3 or 4 in H it also inverts an involution of H, hence $|J_{12}| = 12.m = 2^2.3.m$; thus $b_{12} = m$.

Let $r = 1$ when $e = 1$ and $r = 0$ when $e = 3$, then

$b_4 = 3mr$ and $b_{12} = m(1 - r)$

If $u \in J_1$, u cannot invert a non-trivial element of H and it follows easily that $C_H(u) = 1$ for all $u \in J_1$. So $c = 0$ and $b_1 = 2^3.e.m.k$, k a non-negative integer.

Summarizing we have

$f = \dfrac{em-6}{6}$,

$|J \cap H| = m$,

$b_4 = 3mr$, $b_{12} = m(1 - r)$, $b_1 = 2^3.e.m.k.$, k a non-negative integer and all other b_n are zero $(n \neq 0)$; where, $e = 1$ and $r = 1$ or $e = 3$ and $r = 0$.

By Bender's lemma we have

$$b_1 < \frac{6}{em-6}(m + 3^2.m.r + 11.m\,(1 - r)) - 3.m.r - m(1 - r)$$

$$= \frac{6}{em-6}(12m - 2mr) - m - 2mr.$$

Therefore $2^3.e.k < \dfrac{6}{em-6}(12 - 2r) - 1 - 2r$.

Since $m \geq 17$, $em \geq e.17 \geq 17$ and so $\dfrac{1}{em-6} \leq \dfrac{1}{11}$ therefore

we have $2^3.k \leq 2^3.e.k \leq \dfrac{6}{11}(12 - 2r) - 1 - 2r$

$$\leq \frac{6.12}{11} - 1 < 6,$$

thus $k < \frac{6}{8} < 1$ which gives $k = 0$. Hence $b_1 = 0$.

To determine an upperbound on m we use the following inequality:

$$0 < \frac{6}{em-6}(12 - 2r) - 1 - 2r$$

which solving for m gives $m < \dfrac{78}{(1 + 2r).e}$

When $e = 1$, $r = 1$ and $(1 + 2r)e = 3$. Also $(1 + 2r)e = 3$ when $e = 3$ and $r = 0$. Hence in both cases.

$m < \frac{78}{3} = 26$, thus $m \leq 25$, and $17 \leq m \leq 25$. The condition $m \equiv 1\ (8)$ yields the two possible values for m, $m = 17$ or 25.

The number of involutions in G is

$|J| = m + 12.m.r + 12.m\ (1 - r) = 13.m.$

Whence $|G| = 2^4.3.13.m.$

The index of the normalizer of a Sylow 3-subgroup of G is $2^2.13.m$, which is congruent to 1 modulo 3 by Sylow's theorem. This gives $m \equiv 1\ (3)$ and as $17 \equiv 2\ (3)$, m must be 25. Hence the order of G is $2^4.3.5^2.13$.

Finally the index of $N_G(M)$ in G is $\frac{2^4.3.5^2 13}{2^3.\ e.\ 5^2} = \frac{2.3.13}{e}$ and as M is a Sylow 5-subgroup of G, Sylow's theorem yields $\frac{2.3.13}{e} \equiv 1\ (5)$ which implies $e \equiv 3\ (5)$. Hence $e = 3$ and $|N_G(M)| = 2^3.3.5^2$, completing the proof of the lemma.

We make the following observations for M in the previous lemma. If M is cyclic of order 5^2 then $|Aut\ (M)| = 2^2.5$ (lemma (5.4.1) of [12]), and as $C_G(M) = M$ by lemma (3.3) (b), $|N_G(M)|\,|\,2^2.5^2$ which is not the case. Thus M is elementary abelian of order 5^2. Also, using Sylow's theorem, it is easily shown that the normalizer of a Sylow 13-subgroup of G has order $2^2.13$ which is precisely case (e) of lemma (3.4).

We shall now determine the number of involutions in G in terms of some parameters. This expression will be useful in a later lemma.

If $x \in J$ and $zx \in M^g$ for some g in G, then as z and x both invert zx lemma (3.3) (d) shows that $z, x \in N_G(M^g)$ (since M^g has the same properties as M). By lemma (3.3) (c), $N_G(M^g) = M^g C_{N_G(M^g)}(z)$ which therefore contains m involutions. Thus the number of involutions x in J for which $zx \in (M^g)^{\#}$ is $m - 1$.

If $z \in N_G(M^g)$ then $z^{g^{-1}} \in N_G(M)$ so that $z^{g^{-1}} = z^{\mu}$ for some $\mu \in M$. Then $z = z^{\mu g}$ so that $\mu g = c \in C$. Now $M^{\mu g} = M^c$ implies $M^g = M^c$. So z inverts only conjugates of M of the form M^c for some $c \in C$. Since C acts by conjugation on the conjugates of M in G and the stabilizer of M is $C_M = C_{N_G(M)}(z)$, the number of conjugates of M under this action is $|C : C_{N_G(M)}(z)|$. So if $|C_{N_G(M)}(z)| = r$ then z inverts $\frac{2^4.3}{r}$ conjugates of M.

Thus there exists $(m - 1)\frac{2^4.3}{r}$ involutions x such that zx belongs in a conjugate of $M^{\#}$. This is true for any $x \in J$ such that $|zx| = n$ with $(n, 6) = 1$. So as there are 133 involutions x for which zx has order 1, 2, 3, 4 or 6 we have the following lemma.

<u>LEMMA</u> <u>(3.6)</u>

$$|J| = 133 + \sum_i (m_i - 1)\frac{2^4.3}{r_i}$$

where $|M_i| = m_i$, $|C_{N_G(M_i)}(z)| = r_i$, the M_i satisfy the same properties as M (and hence satisfy lemmas (3.3), (3.4) and (3.5)) and the summation is over the distinct conjugate classes of subgroups with the same properties as M.

We shall use this lemma to eliminate cases (b) (c) and (d) of lemma (3.4) where M is chosen to have maximal order. The remaining cases give us the order of G.

<u>LEMMA</u> <u>(3.7)</u>

The order of G is $2^4.3.5^2.13$. Furthermore the normalizers of the Sylow 5 and 13-subgroups have orders $2^3.3.5^2$ and $2^2.13$ respectively.

PROOF

If the lemma is false then there exists a subgroup M of G such that

(i) $(|M|,6) = 1$

(ii) $|N_G(M)|$ is even

(iii) M has maximal order subject to (i) and (ii) and

(iv) M satisfies case (b), (c) or (d) of lemma (3.4)

By lemma (3.6) we have

$$|J| = 133 + \sum_i (m_i - 1)\frac{2^4.3}{r_i} = 133 + 48r, \quad \text{where}$$

$$r = \sum_i \frac{(m_i - 1)}{r_i}$$

We note that $r > 0$.

It is easily seen using lemma (3.4) that r is an integer. Also $r_i \geq 2$ for all i, therefore

$$r \leq \sum_i \frac{(m_i - 1)}{2}$$

By the maximality of m, $m_i \leq m$ for all i.

We first show $m \geq 25$, so that it will be possible to apply Bender's lemma. To do this we need to eliminate the cases $m = 5, 7, 11, 13, 17, 19$ or 23. (These are also the possible values for each m_i). We will use the fact that $133 + 48r \equiv 0 \ (m)$ (that is $m \mid |J|$) to determine r.

Suppose firstly $m = 5$. Then

$$r \leq \sum_i \frac{(m_i - 1)}{2} = \frac{5-1}{2} = 2,$$

and $133 + 48r \equiv 0 \ (5)$ implies $r \equiv 4 \ (5)$, a contradiction.

If $m = 7$ then $r \leq 2 + \frac{(7-1)}{2} = 5$, and $133 + 48r \equiv 0 \ (7)$

implies $r \equiv 0$ (7), a contradiction (as $r > 0$).

We have shown $m \geq 11$, and therefore $|N_G(M)| = 2.m$ by lemma (3.4). In all cases M is a Sylow subgroup of G. Therefore

$$|G:N_G(M)| = \frac{2^3.3.|J|}{m} \equiv 1 \ (m).$$

We use this fact to eliminate the remaining cases.

If $m = 11$ then $r \leq 5 + \frac{(11-1)}{2} = 10$ and $133 + 48r \equiv 0$ (11) implies $r \equiv 8$ (11) so $r = 8$. This yields $|J| = 517 = 11.47$ and $|G:N_G(M)| = 2^3.3.47$ which is congruent to 6 modulo 11. Thus $m \neq 11$.

If $m = 13$ then $r \leq 10 + \frac{(13-1)}{2} = 16$ and $133 + 48r \equiv 0$ (13) implies $r \equiv 4$ (13) so $r = 4$. Now $|J| = 5^2 13$ and $|G:N_G(M)| = 2^3.3.5^2 \equiv 2$ (13), so $m \neq 13$.

When $m = 17$, $r \leq 16 + \frac{(17-1)}{2} = 24$ and $r \equiv 16$ (17) so that $r = 16$. Then $|J| = 17.53$ and $|G:N_G(M)| = 2^3.3.53 \equiv 14$ (17), a contradiction.

If $m = 19$, then $r \leq 24 + \frac{(19-1)}{2} = 33$, and $133 + 48r \equiv 0$ (19) implies $r \equiv 0$ (19) so that $r = 19$. Then $|J| = 5.11.19$ and $|G:N_G(M)| = 2^3.3.5.11 \equiv 9$ (19), so $m \neq 19$.

Finally if $m = 23$, $r \leq 33 + \frac{(23-1)}{2} = 44$ and $133 + 48r \equiv 0$ (23) implies $r \equiv 14$ (23), so $r = 14$ or 37. In the first case $|J| = 5.7.23$, $|G:N_G(M)| = 2^3.3.5.7 \equiv 12$ (23). And in the second $|J| = 23.83$, $|G:N_G(M)| = 2^3.3.83 \equiv 14$ (23) so $m \neq 23$.

We shall also eliminate the case $m = 25$ in the same way. We have $r \leq 44 + \frac{(25-1)}{2} = 56$ and $133 + 48r \equiv 0$ (25) implies $r \equiv 4$ (25) so $r = 4$, 29 or 54. The first case gives $|J| = 5^2.13$ and

$|G:N_G(M)| = 2^3.3.13 \equiv 12\ (25)$. In the second $|J| = 5^2.61$ and $|G:N_G(M)| = 2^3.3.61 \equiv 14\ (25)$. Finally $r = 54$ implies $|J| = 5^2.109$ and $|G:N_G(M)| = 2^3.3.109$ is congruent to 16 modulo 25.

This all shows that $m \geq 29$. We now apply Bender's lemma to the subgroup $H = N_G(M)$. Firstly

$$f = \frac{|H|}{|C_G(z)|} - 1 = \frac{2.m}{48} - 1 = \frac{m-24}{24} \text{ and } |J \cap H| = m.$$

Let u be an involution of $G-H$ and consider $H \cap H^u$. By previous reasoning $|H \cap H^u| \mid 2$, so if u inverts a non-trivial element of H then $u \in J_2$. It follows that $|J_2| = 12.m = 2^2.3.m$ and so $b_2 = 2.3.m$.

It is easily seen that $c = 0$, so therefore $b_1 = 2.m.k$, k a non-negative integer. By Bender's lemma.

$$b_1 = 2.m.k < \frac{24}{m-24}(m + 2.3.m) - 2.3.m$$

$$= \frac{2^3.3.7m}{m-24} - 2.3.m$$

therefore $k < \frac{2^2.3.7}{m-24} - 3$

As $m \geq 29$, $\frac{1}{m-24} \leq \frac{1}{5}$, thus

$$k < \frac{2^2.3.7}{5} - 3 = \frac{69}{5} < \frac{70}{5} = 14$$

Hence $0 \leq k \leq 13$.

We can also use this inequality to determine an upperbound for m. In particular it gives

$$0 < \frac{2^2.3.7}{m-24} - 3,$$

which yields $m < 52$ so $29 \leq m \leq 51$. And m being prime to 6 implies the following eight possibilities for m: 29, 31, 35, 37, 43, 47 or 49.

The number of involutions in G is

$|J| = m + 2.m.k + 2^2.3.m = m\ (13 + 2k)$.

Hence $|G| = 2^4.3.m.\ (13. + 2k)$.

If m is a prime power then M is a Sylow subgroup of G so as $N_G(M)$ has index $2^3.3\ (13 + 2k)$, Sylow's theorem yields

$2^3.3(13 + 2k) \equiv 1\ (m)$ thus $48k \equiv -\ 311\ (m)$.

We use this congruence to eliminate most of the above cases.

If $m = 29$ then $48k \equiv -311\ (29)$ which implies $k \equiv 5\ (29)$ and hence $k = 5$ as $0 \leq k \leq 13$ Thus $|G| = 2^4.3.23.29$

Let P be a Sylow 23-subgroup of G ; then $C_G(P) = P$ and $|Aut\ (P)| = 22 = 2.11$ so $|N_G(P)|\,|2.23$. We must have $|N_G(P)| = 2.23$ else $N_G(P) = C_G(P)$ and G has a normal 23-complement by Burnsides Transfer Theorem, contradicting lemma (3.1). Then $|G:N_G(P)| = 2^3.3.29$ is congruent to 6 modulo 23. Thus $m \neq 29$.

If $m = 31$ then $48k \equiv -\ 311\ (31)$ which implies $k \equiv 20\ (31)$, a contradiction.

If $m = 37$ then $48k \equiv -\ 311\ (37)$ implies $k \equiv 2\ (37)$ so that $k = 2$ and $|G| = 2^4.3.17.37$.

However in this case the index of $N_G(X)$ is $2^2.17.37$ which is congruent to 2 modulo 3 contradicting Sylow's theorem.

In the last four cases, as $0 \leq k \leq 13$, k cannot satisfy the required congruence. For when $m = 41, 43, 47$ or 49 k is congruent to 20, 41, 18 or 17 respectively modulo m (The last congruence applies because of lemma (3.3) (e)).

We are thus left with the case $m = 35$. To eliminate this value of m, we use the fact that $|J| = 133 + 48r$ so that $|J| \equiv -11\ (48)$. And as $|J| = 5.7.(13 + 2k)$ we have $5.7(13 + 2k) \equiv -11\ (48)$ which implies $k \equiv 5\ (12)$. However the above inequality for k with $m = 35$ gives

$0 \le k < \dfrac{2^2.3.7}{35-24} - 3 < 5$, a contradiction.

This has all shown that cases (b) (c) and (d) of lemma (3.4) does not apply for $N_G(M)$ when M is chosen to have maximal order. So case (a) or (e) applies (in fact case (a) must apply) and in both cases the conclusion of the lemma holds.

Before obtaining the final contradiction we should like to remark that it is not possible to eliminate G by counting the number of elements in the conjugacy classes of G.

By lemmas (2.2), (2.3) and (2.4) there is one class each of elements of order 2, 3, 4 and 6 and two classes of elements of order 8. It is easy to show that there is one class of elements of order 5, and the elements of order 13 form three classes. Let x_i denote a representative from each conjugacy class of G, i = 1, 2, ..., 11. In the table we list the orders of the centralizer in G of each respresentative and the order of its conjugacy class.

$\lvert x_i\rvert$	$\lvert C_G(x_i)\rvert$	$\lvert G:C_G(x_i)\rvert$
1	$2^4.3.5^2.13$	1
2	$2^4.3$	$5^2.13$
3	2.3	$2^3.5^2.13$
4	2^3	$2.3.5^2.13$
5	5^2	$2^4.3.13$
6	2.3	$2^3.5^2.13$
8	2^3	$2.3.5^2.13$
8	2^3	$2.3.5^2.13$
13	13	$2^4.3.5^2$
13	13	$2^4.3.5^2$
13	13	$2^4.3.5^2$

Summing the number of elements in the conjugacy classes of G we find the total to be $2^4.3.5^2.13$, which is precisely the order of G.

A contradiction will be obtained once we have the following lemma.

LEMMA (3.8)

The group G is a sharply 3-transitive permutation group of degree 26 and the subgroup fixing two letters is isomorphic to SL(2,3).

PROOF

We will consider G as a permutation group in its action (by conjugation) on the Sylow 5-subgroups of G. But before doing this we need to make a few observations.

Let M be a Sylow 5-subgroup of G inverted by z. By lemma (3.3) (c), $N_G(M) = MC_{N_G(M)}(z)$ and $C_{N_G(M)}(z)$ has index 2 in C (because of lemma (3.7)) so $C_{N_G(M)}(z) \cong SL(2,3)$.

Let $u \in C - C_{N_G(M)}(z)$. Then z inverts the Sylow 5-subgroup M^u and $M^u \neq M$. Thus each involution inverts at least two Sylow 5-subgroups of G. We show in fact that each involution inverts exactly two Sylow 5-subgroups of G.

Since $N_G(M)$ contains 5^2 involutions and as there are 2.13 Sylow 5-subgroups, the set of involutions contained in the normalizers of the Sylow 5-subgroups (counting repetitions) has order $2.5^2.13$. As this is twice the number of involutions, each involution inverts precisely two Sylow 5-subgroups of G.

As above, z inverts both M and M^u, so that:

$$N_G(M) = MC_{N_G(M)}(z)$$

and $\quad N_G(M^u) = M^u C_{N_G(M^u)}(z)$

As $C_{N_G(M)}(z)$ and $C_{N_G(M^u)}(z)$ are both subgroups of index 2 in C they are equal. Therefore $N_G(M) \cap N_G(M^u) = C_{N_G(M)}(z)$.

Let w be an involution inverting M, $w \neq z$. Then w cannot invert M^u else $w \in N_G(M) \cap N_G(M^u) = C_{N_G(M)}(z)$. And so $N_G(M)$ contains a 4-group $\langle z,w \rangle$. Thus no two involutions of $N_G(M)$ invert the same Sylow 5-subgroup besides M. As there are 5^2 Sylow 5-subgroups besides M, and $N_G(M)$ contains 5^2 involutions, any two Sylow 5-subgroups are inverted by a unique involution.

Let T be the set of Sylow 5-subgroups of G, so T has order 26. The group G acts by conjugation on T and under this action G is transitive by Sylow's theorem.

For $M \in T$, $G_M = N_G(M)$ is the stabilizer of the point M. Now $N_G(M)$ acts by conjugation on $T-\{M\}$. If $M_1 \in T-\{M\}$, the stabilizer of M_1 under this action is

$N_G(M)_{M_1} = N_G(M) \cap N_G(M_1) = C_{N_G(M)}(v)$ where v is the unique involution inverting both M and M_1. As $C_{N_G(M)}(v)$ has index 5^2 in $N_G(M)$, M_1 has 5^2 conjugates in $T-\{M\}$. And as $T-\{M\}$ contains precisely 5^2 elements, $N_G(M)$ is transitive on $T-\{M\}$.

Now $N_G(M)_{M_1} = C_{N_G(M)}(v)$ acts by conjugation on $T-\{M,M_1\}$. For $M_2 \in T-\{M,M_1\}$ the stabilizer of M_2 under this action is $C_{N_G(M)}(v)_{M_2} = C_{N_G(M)}(v) \cap N_G(M_2) = 1$, (as an involution inverts exactly two Sylow 5-subgroups). Since $|C_{N_G(M)}(v)| = 24$, M_2 has 24 conjugates in $T-\{M,M_1\}$. And as $T-\{M,M_1\}$ contains 24 elements, $C_{N_G(M)}(v)$ is transitive on $T-\{M,M_1\}$.

It follows that G is 3-transitive on T and as the stabilizer of 3 points is trivial, G is in fact sharply 3-transitive.

The stabilizer of the two points M and M_1 is $C_{N_G(M)}(v)$ which is isomorphic to $SL(2,3)$ and we have the result.

Now G satisfies the hypotheses of lemma (1.5), therefore by its conclusion the subgroup fixing two letters contains exactly one subgroup of order 3. However $SL(2,3)$ contains four subgroups of order 3, we conclude that there does not exist a group G satisfying the assumption that $N_G(X) = XV$.

CHAPTER FOUR

CASE (B) $A \cong Z_3 \times Z_3 \times Z_3$

Throughout this chapter suppose that $N_G(X) = AV$ where $A \cong Z_3 \times Z_3 \times Z_3$ and $A \triangleleft N_G(X)$.

Let $A_1 = C_A(z)$ $(=X)$, $A_2 = C_A(zt)$ and $A_3 = C_A(t)$, then $A = A_1 A_2 A_3 = A_1 \times A_2 \times A_3$. Let $A_i = \langle a_i \rangle$, $i = 1, 2, 3$; $a_1 \sim a_2 \sim a_3$ in G by lemma (2.3). Also put $N = N_G(A)$. The first three lemmas concern the structure of N.

LEMMA (4.1)

$z \sim t \sim zt$ in N

PROOF

By lemma (2.2) $z = t^g$ for some g in G. As $A_3 \leq C_G(t)$, $A_3{}^g \leq C_G(t^g) = C$. So A_1 and A_3 are Sylow 3-subgroups of C and hence conjugate in C. So for some $c \in C$, $A_1 = A_3{}^{gc}$, and $t^{gc} = z^c = z$. Replacing gc by g we have, for some $g \in G$, $z = t^g$ and $A_1 = A_3{}^g$.

Now $A \leq C_G(A_3)$ (A being an abelian group containing A_3) implies $A^g \leq C_G(A_3{}^g) = C_G(A_1)$. Thus A and A^g are Sylow 3-subgroups of $C_G(A_1)$ and because $C_G(A_1)$ has a normal Sylow 3-subgroup (lemma (2.5)), $A = A^g$; that is $g \in N$. As $z = t^g$, $z \sim t$ in N. Similarly $z \sim zt$ in N.

LEMMA (4.2)

V is a Sylow 2-subgroup of N.

PROOF

We first make the following observation: as $C \cap N$ normalizes $C_A(z) = X$ and $N_C(X) = XV$, $C \cap N = XV$.

Let R be a Sylow 2-subgroup of N containing V. If $R > V$, $N_R(V) > V$ and as all involutions in V are conjugate in N we may suppose $z \in Z(N_R(V))$. However now $N_R(V) \leq C \cap N = XV$ a contradiction, and we conclude that $R = V$.

As V is a Sylow 2-subgroup of N and $\langle z\rangle$, $\langle t\rangle \triangleleft V$, $z \sim t$ in $N_N(V)$ by [12] theorem (7.1.1) since they are conjugate in N. It follows from $C_N(V) = V$ and Aut $(V) \cong S_3$ that $N_N(V)/V \cong Z_3$. Let M be a subgroup of order 3 in $N_N(V)$ so that $N_N(V) = MV$. If $M = \langle m\rangle$ then m permutes the involutions of V and $MV \cong A_4$. As $MV \leq N$, $AMV \leq N$. We can in fact say more than this.

LEMMA (4.3)

$N = AMV$.

PROOF

Clearly m permutes the elements a_1, a_2 and a_3 as it permutes the involutions z, zt and t.

Let $L = AMV$. It is easy to determine the conjugacy classes of $A^{\#}$ in L; namely $A^{\#}$ has four classes of lengths 4, 4, 6 and 12 with representatives $a_1a_2a_3$, $(a_1a_2a_3)^{-1}$, a_1 and a_1a_2 respectively.

Suppose by way of contradiction that $L < N$. Then $|N| = 2^2 . 3^4 . r$ with $r > 1$. As $|N:C_N(a_1)| = |N:A\langle z\rangle| = 6r$, a_1 has more than 6 conjugates in N. We cannot have a_1 conjugate to $a_1a_2a_3$ or $(a_1a_2a_3)^{-1}$ since $\langle a_1a_2a_3\rangle = Z(AM)$ and so centralizes AM a group of order 3^4. Therefore a_1 is conjugate to a_1a_2 in N and has 18 conjugates. If follows that $|N| = 2^2.3^5$.

Let $K = N/A$. Then K is a group of order 36 which contains a subgroup H of order 12 isomorphic to MV. Representing K on the cosets of H we have, as $|K:H| = 3$, K/I isomorphic to a subgroup of S_3 where I is the intersection of the conjugates of H in K. Because $|K/I| \mid 6$ and K has order 36, $6 \mid |I|$. Also $|I| \mid 12$ (I being a subgroup of H), therefore $|I| = 6$ or 12. Now $H \cong A_4$ does not contain a normal subgroup of order 6, so I has order 12 and I = H. Hence $H \triangleleft K$. As H contains a normal Sylow 2-subgroup V, $V \triangleleft K$ and K/V has order 9. However $C_K(V) = V$ and $|Aut(V)| = 6$ so $|K/V|$ divides 6, a contradiction. This completes the proof of the lemma.

We can now determine the order of a Sylow 3-subgroup of G.

<u>LEMMA</u> <u>(4.4)</u>

$N_G(AM) = AM$ and so AM is a Sylow 3-subgroup of G. Also a Sylow 3-subgroup of G contains a unique abelian subgroup of order 27.

<u>PROOF</u>

Since $C_A(M)$ has order 3, A is the only abelian subgroup of order 27 in AM. It is therefore characteristic in AM and hence normal in $N_G(AM)$, thus $N_G(AM) \leq N$. As $N/A \cong A_4$, $N_G(AM) \cap N = AM$. It follows that $N_G(AM) = AM$ and the remaining parts of the lemma follow easily.

The following lemma is easily proved.

<u>LEMMA</u> <u>(4.5)</u>

The subgroup $\langle a_1 a_2 a_3 \rangle$ is not inverted by an involution.

<u>PROOF</u>

As $\langle a_1 a_2 a_3 \rangle = Z(AM)$, $AM \leq C_G(a_1 a_2 a_3)$ and is in fact a Sylow 3-subgroup of $C_G(a_1 a_2 a_3)$ by lemma (4.4). The Frattini argument yields that $N_G(\langle a_1 a_2 a_3 \rangle) = C_G(a_1 a_2 a_3) N_{N_G(\langle a_1 a_2 a_3 \rangle)}(AM)$.

Which because of lemma (4.4), implies $N_G(\langle a_1a_2a_3\rangle) = C_G(a_1a_2a_3)$. Thus $a_1a_2a_3$ is not conjugate to its inverse.

Let $Y = C_A(M)M = \langle a_1a_2a_3\rangle \times M$ and let $Z = N_N(Y)$. Then $Z = \langle m, a_1a_2a_3, a_1a_2^{-1}\rangle$ is non-abelian of order 27. (This is verified by a simple computation using the fact that no involution normalizes $\langle a_1a_2a_3\rangle$). With the help of the normalizer $N_G(Z)$ we shall determine the conjugacy classes of elements of order 3 in G. But first a lemma concerning the order of $N_G(Z)$.

<u>LEMMA</u> <u>(4.6)</u>

$N_G(Z)$ has odd order.

<u>PROOF</u>

As $\langle a_1a_2a_3\rangle = Z(Z)$, $\langle a_1a_2a_3\rangle \triangleleft N_G(Z)$ so $N_G(Z) \leq C_G(a_1a_2a_3)$ by lemma (4.5). Thus $|N_G(Z)|$ is odd as $|C_G(a_1a_2a_3)|$ is odd.

<u>LEMMA</u> <u>(4.7)</u>

m is inverted by an involution but $m \not\sim_G a_1$.

<u>PROOF</u>

Suppose m is conjugate to a_1 in G, so that $m = a_1^g$ for some g in G. Then $C_G(m) = B\langle v\rangle$ where $B = A^g$ and $\langle v\rangle = \langle z\rangle^g$. As $Y \leq C_G(m)$, clearly $Y \leq B$ and $B \leq C_G(Y)$ B being abelian. Also $C_G(Y) \leq C_G(m) = B\langle v\rangle$ and as Y is not centralized by an involution, we have $C_G(Y) = B$. Thus $B \triangleleft N_G(Y)$ so $N_G(Y) \leq N_G(B)$, and as $Z \leq N_G(Y)$, $Z \leq N_G(B)$. Then ZB is a 3-group of $N_G(B)$ which properly contains Z. It must therefore be a Sylow 3-subgroup of G. Now Z has index 3 in ZB and so is normal in ZB, which implies that $ZB \leq N_G(Z)$. Also $AM \leq N_G(Z)$ as well, since $Z \leq AM$.

Now $C_G(Z) \leq C_G(Y) = B$ as $Y \leq Z$; therefore $C_G(Z) =$

$\langle a_1a_2a_3\rangle = Z(Z)$. As Z is non-abelian of order 27, $Aut(Z)$ is a $\{2,3\}$-group. (For if r is an automorphism of Z then it is an automorphism of $Z(Z)$ and $Z/Z(Z)$, both of whose automorphism groups are $\{2,3\}$ - groups). Thus $N_G(Z)$ is a 3-group by lemma (4.6). However this gives $N_G(Z) = AM = BZ$, so that AM contains two abelian subgroups of order 27, namely A and B, contradicting lemma (4.4). Thus $m \not\sim_G a_1$.

We know V is normalized by a dihedral group and also by M. As $C_G(V) = V$ and $Aut(V) \cong S_3$ we get $N_G(V)/V \cong S_3$. Thus $N_{N_G(M)}(M) \cong S_3$ and hence m is inverted by an involution.

LEMMA (4.8)

We have $m \sim_G a_1a_2$.

PROOF

Let P be a Sylow 3-subgroup of $C_G(m)$ containing Y and suppose $P = Y$. By the Frattini argument $N_G(\langle m\rangle) = C_G(m)N_{N_G(\langle m\rangle)}(P)$, so P is normalized by an involution of $N_G(\langle m\rangle)$, v say. If $C_P(v) = 1$ then v inverts P (lemma (1.2)) and in particular inverts $a_1a_2a_3$ contrary to lemma (4.5). So v centralizes some subgroup of order 3 in P. Now P has four subgroups of order 3, namely $\langle m\rangle$, $\langle a_1a_2a_3\rangle$, $\langle a_1a_2a_3m\rangle$ and $\langle(a_1a_2a_3)^{-1}m\rangle$. And as $m^{a_1^{-1}a_3} = a_1a_2a_3m$ and $m^{a_1^{-1}a_2} = (a_1a_2a_3)^{-1}m$ no subgroup of order 3 in P is centralized by an involution. Thus $Y < P$.

If P has order 3^4 then $\langle m\rangle$ is its centre and so will be conjugate to $\langle a_1a_2a_3\rangle$ by Sylow's theorem and lemma (4.4). However $\langle m\rangle$ is inverted by an involution while $\langle a_1a_2a_3\rangle$ is not. Thus P has order 3^3.

As $\langle a_1a_2a_3\rangle$ is not conjugate to the other subgroups in

Y, $\langle a_1a_2a_3\rangle \triangleleft P$, it follows that $[P,\langle a_1a_2a_3\rangle] = 1$. Thus $\langle m,a_1a_2a_3\rangle \leq Z(P)$ and P must be abelian of order 3^3, and hence elementary abelian by lemma (4.4). By Sylow's theorem $P^g \leq AM$ for some g in G, hence $P^g = A$ and therefore $m^g \in A$. We have seen in the proof of lemma (4.3) that $A^\#$ has four conjugacy classes in N with representatives $a_1a_2a_3$, $(a_1a_2a_3)^{-1}$, a_1 and a_1a_2. So as m is not conjugate to the first three elements by lemmas (4.5) and (4.7) it is conjugate to the last, that is $m \sim_G a_1a_2$.

To calculate the order of G we shall need to know the normalizer of $\langle a_1a_2\rangle$ and of a non-abelian subgroup of order 27. We determine these normalizers in the next two lemmas.

LEMMA (4.9)

We have $N_G(\langle a_1a_2\rangle) = A\langle t\rangle$.

PROOF

By lemmas (4.7) and (4.8) $C_G(a_1a_2)$ has odd order. Since A is a Sylow 3-subgroup of $C_G(a_1a_2)$ and $N_{C_G(a_1a_2)}(A) = C_{N_G(a_1a_2)}(A) = A$, $C_G(a_1a_2)$ has a normal 3-complement L say, by Burnside's Transfer Theorem. Therefore $C_G(a_1a_2) = AL$ and $N_G(\langle a_1a_2\rangle) = AL\langle t\rangle$.

Assume by way of contradiction that $L \neq 1$. No involution can centralize any element of $L^\#$, therefore $C_L(t) = 1$. Also t inverts $\langle a_1\rangle$, hence $C_{\langle a_1\rangle L}(t) = 1$. As t normalizes $\langle a_1\rangle L$ it follows that t inverts it and in particular that $\langle a_1\rangle L$ is abelian. However $C_L(a_1) = 1$ which is a contradiction, and the lemma follows.

LEMMA (4.10)

The normalizer of a non-abelian group of order 27 is a Sylow 3-subgroup of G.

PROOF

It is enough to consider the normalizer of a non-abelian group L of order 27 in AM because of lemma (4.4). If $L \cap \langle a_1 a_2 a_3 \rangle = 1$ then $AM = L\langle a_1 a_2 a_3 \rangle$, but then $Z(L)\langle a_1 a_2 a_3 \rangle$ is a subgroup of order 9 in $Z(AM)$. Thus $\langle a_1 a_2 a_3 \rangle \leq L$ and hence $\langle a_1 a_2 a_3 \rangle \triangleleft L$. It follows that $N_G(L) \leq N_G(\langle a_1 a_2 a_3 \rangle)$. As Aut (L) is a $\{2,3\}$ - group so is $N_G(L)$. If $N_G(L)$ contains an involution then $N_G(\langle a_1 a_2 a_3 \rangle)$ does also, contradicting lemma (4.5). Therefore $N_G(L)$ is a 3-group and hence is a Sylow 3-subgroup of G.

The simplicity of G is now trivially proved.

LEMMA (4.11)

The group G is simple.

PROOF

By lemma (2.6) a proper non-trivial subgroup L of G, if one exists, has order 27. By lemmas (4.3) and (4.10) a subgroup of order 27 is not normal in G. Thus G must be simple.

We have now enough information to be able to determine the order of G, which we now do.

LEMMA (4.12)

The order of G is $2^4.3^4.7$.

PROOF

Choose H = AM as the subgroup for application of

Bender's lemma firstly

$$f = \frac{|H|}{|C_G(z)|} - 1 = \frac{81}{48} - 1 = \frac{11}{16}$$

Also H has odd order and therefore contains no involutions; that is $|J \cap H| = 0$.

Let u be an involution of G and consider $H \cap H^u$. Since u is an involution it normalizes $H \cap H^u$. Therefore because $N_G(H) = H$ (lemma (4.4)), $H \cap H^u < H$, so $|H \cap H^u| \mid 27$. If $H \cap H^u$ is non-abelian of order 27, by lemma (4.10), its normalizer is a Sylow 3-subgroup of G which therefore cannot contain u. Thus $H \cap H^u$ is an abelian group.

Suppose u inverts a_1. Then $u \in N_G(\langle a_1\rangle) = AV$ and so u normalizes A as $A \triangleleft AV$; thus $H \cap H^u = A$. In this case u inverts a subgroup of order 9 in H and so $u \in J_9$. The same applies to all conjugates of a_1 in A. If u inverts a_1a_2 then $u \in N_G(\langle a_1a_2\rangle) = A\langle t\rangle$ (lemma (4.9)). Again u normalizes A and $u \in J_9$. The same applies to all conjugates of a_1a_2 in A. We have that if u inverts an element of $A^{\#}$ then u normalizes A and $u \in J_9$.

Now consider the elements of H-A. In H-A there are three conjugate classes of subgroups with respresentatives $\langle m\rangle$, $\langle a_1m\rangle$ and $\langle a_1^{-1}m\rangle$; the orders of these subgroups are 3, 9 and 9 respectively. Since $(a_1m)^3 = a_1a_2a_3$ and $(a_1^{-1}m)^3 = (a_1a_2a_3)^{-1}$, no element of order 9 is inverted by an involution because of lemma (4.5). Thus if an element $b \in H-A$ is inverted by u then b is conjugate to m. As $C_H(b) = \langle a_1a_2a_3, b\rangle$ and $H \cap H^u$ is abelian, in this case, $H \cap H^u$ has order 3 or 9. If u inverts a subgroup of $H-\langle b\rangle$ then u inverts a subgroup of order 9 in $H \cap H^u$ which will be $\langle a_1a_2a_3, b\rangle$. In particular u inverts $a_1a_2a_3$ a contradiction. Thus $u \in J_3$.

Since m is inverted by 9 involutions by lemmas (4.8) and (4.9) and has 9 conjugates in H-A, $|J_3| = 9.9 = 3^4$, thus $b_3 = 3^3$.

Also as N contains 27 involutions $|J_9| = 27$ and so $b_9 = 3$.

If $u \in J_1$ then u inverts no non-trivial element of H. If u centralizes an element of $A^{\#}$, then u normalizes A and so inverts a subgroup of order 9 in A, so therefore $C_A(u) = 1$. Also no element of H - A is centralized by an involution so $C_H(u) = 1$ for all $u \in J_1$. Thus $c = 0$ and $b_1 = 3^4.k$, k a non-negative integer.

We summarize what we have so far:

$$f = \frac{11}{16}$$

$$|J \cap H| = 0$$

$$b_3 = 3^3, \quad b_9 = 3$$

$b_1 = 3^4.k$, k a non-negative integer and all other b_n are zero ($n \neq 0$).

To get information on k we apply Bender's lemma.

$$b_1 = 3^4.k < \frac{16}{11}.(2.3^3 + 2^3.3) - 3^3 - 3$$

$$= \frac{918}{11}$$

Therefore $k < \frac{918}{891} < 2$,

hence, $k = 0$ or 1.

The number of involutions in G is

$$|J| = 3^4.k + 3^4 + 3^3$$

$$= 3^3 (4 + 3k).$$

We now see that k must be 1 else $|J|$ is even. Thus $|J| = 3^3.7$, whence the order of G is $2^4.3^4.7$ and the lemma is proved.

Now that we have this order it is easy to obtain a contradiction using Sylow's theorem. Let P be a Sylow 7-subgroup of G. Then as $|C_G(P)|$ is odd and $\mathrm{Aut}(P) \cong Z_6$, $|N_G(P)| \mid 2.3^4.7$. Therefore $2^3 \mid |G : N_G(P)|$ and $|G : N_G(P)| = 2^3.x$ with x a divisor of 2.3^4. As $2^3 = 8 \equiv 1$ (7), we have by Sylow's theorem $x \equiv 1$ (7). It follows that $x = 1$ or 2.3^4 and therefore $|N_G(P)| = 2.3^4.7$ or 7

In the first case as G is simple and $|G:N_G(P)| = 8$, G is isomorphic to a subgroup of A_8. However $3^4 \nmid |A_8|$, so this case cannot occur. In the second case $N_G(P) = C_G(P)$, which implies by Burnside's Transfer Theorem that G has a normal 7-complement, contradicting the simplicity of G. Thus there does not exist a group G satisfying the assumptions of this chapter.

CHAPTER FIVE

CASE (C) A NON-ABELIAN OF ORDER 27

Throughout this chapter suppose that $N_G(X) = AV$ where A is non-abelian of order 27 and $A \lhd N_G(X)$.

Let $A_1 = C_A(z)$ $(=X)$, $A_2 = C_A(zt)$ and $A_3 = C_A(t)$ then $A = A_1 A_2 A_3$. Also let $A_i = \langle a_i \rangle$, $i = 1, 2, 3$,; $a_1 \sim a_2 \sim a_3$ in G by lemma (2.3). The first lemma is easily proved.

LEMMA (5.1)

$A_1 = Z(A)$ and $N_G(A) = AV$; it follows that A is a Sylow 3-subgroup of G.

PROOF

Since A_1 is a normal subgroup of order 3 in A and A is non-abelian of order 27, $A_1 = Z(A)$. As $Z(A)$ char $A \lhd N_G(A)$, $Z(A) \lhd N_G(A)$ and $N_G(A) \leq N_G(Z(A)) = AV$. Also as $A \lhd AV$, $AV \leq N_G(A)$ thus $N_G(A) = AV$.

For later calculations we determine a relationship between a_1, a_2 and a_3. Since $A/Z(A)$ has order 9 it is abelian and therefore $A' = Z(A) = A_1$. So as a_2 and a_3 do not commute $[a_2,a_3] \in A_1^{\#}$ and we may assume

$[a_2,a_3] = a_1 \ldots .(*)$.

It is easily verified that $A^{\#}$ has four conjugacy classes in $N_G(A)$ with representatives a_1, a_2,a_3 and $a_1a_2a_3$; the lengths of the classes are 2, 6, 6 and 12 respectively. Together with the next lemma this shows that G has two classes of elements of order 3 with representatives a_1 and $a_1a_2a_3$.

LEMMA (5.2)

$a = a_1a_2a_3$ is inverted but not centralized by an involution.

PROOF

Using the relation (*) we easily check that z inverts a. Suppose a is centralized by an involution, v say, then a is conjugate to a_1 by lemma (2.3). So $N_G(\langle a\rangle) = \bar{A}\langle z,v\rangle$ where $\langle z,v\rangle$ is a 4-group (we may choose v to centralize z), and $\bar{A}$ is a normal subgroup of order 3^3. As $a_1 \in N_G(\langle a\rangle)$, $a_1 \in \bar{A}$ so that $C_{\bar{A}}(z) = \langle a_1\rangle$. But then v must invert a_1 and so $v \in N_G(\langle a_1\rangle)$. However $N_G(\langle a_1\rangle) = AV$ does not contain an involution centralizing a. This contradiction shows that a is not centralized by an involution.

The next four lemmas concern the normalizers in G of various subgroups of A.

LEMMA (5.3)

We have $N_G(\langle a_1,a\rangle) = A\langle z\rangle$.

PROOF

The subgroup $\langle a_1,a\rangle$ contains four subgroups of order 3 namely $\langle a_1\rangle$, $\langle a\rangle$, $\langle a_1a\rangle$ and $\langle a_1^{-1}a\rangle$ the last 3 being conjugate in A. so $\langle a_1\rangle$ is the only subgroup of order 3 in $\langle a_1,a\rangle$ centralized by an involution (lemma (5.2)). Therefore $N_G(\langle a_1,a\rangle) \leq N_G(\langle a_1\rangle) = AV$. Now A and z normalize $\langle a_1,a\rangle$ but as $a^t = (a_1a_2a_3)^t = a_1{}^t a_2{}^t a_3{}^t = a_1{}^{-1}a_2{}^{-1}a_3 \notin \langle a_1,a\rangle$, $t \notin N_G(\langle a_1,a\rangle)$. Therefore $N_G(\langle a_1,a\rangle) = A\langle z\rangle$.

LEMMA (5.4)

We have $N_G(\langle a_2\rangle) \leq N_G(\langle a_1,a_2\rangle)$.

PROOF

The 4-group V normalizes $\langle a_2\rangle$ and as a_2 is conjugate to

a_1, $N_G(\langle a_2\rangle) = \bar{A}V$ where $\bar{A}$ is a normal Sylow 3-subgroup of $N_G(\langle a_2\rangle)$ of order 27. As a_1 centralizes a_2, $\langle a_1,a_2\rangle \leq N_G(\langle a_2\rangle)$, so $\langle a_1,a_2\rangle \leq \bar{A}$ As $\langle a_1,a_2\rangle$ has index 3 in $\bar{A}$, $\langle a_1,a_2\rangle$ is normal in $\bar{A}$ thus $\bar{A} \leq N_G(\langle a_1,a_2\rangle)$. As V also normalizes $\langle a_1,a_2\rangle$, $N_G(\langle a_2\rangle) \leq N_G(\langle a_1,a_2\rangle)$.

Let $b \in A$, $b = a_2{}^n$ for $n \in N_G(\langle a_1\rangle)$. Then

$$\begin{aligned} N_G(\langle b\rangle) = N_G(\langle a_2\rangle)^n &\leq N_G(\langle a_1,a_2\rangle)^n \\ &= N_G(\langle a_1{}^n,a_2{}^n\rangle) \\ &= N_G(\langle a_1,b\rangle). \end{aligned}$$

As the conjugates of a_2 in $N_G(\langle a_1\rangle)$ are a_2, $a_2{}^{-1}$, a_1a_2, $a_1a_2{}^{-1}$, $a_1{}^{-1}a_2$ and $a_1{}^{-1}a_2{}^{-1}$, we have $N_G(\langle b\rangle) \leq N_G(\langle a_1,a_2\rangle)$. The same reasoning applies if we replace a_2 by a_3.

LEMMA (5.5)

$N_G(\langle a_1,a_2\rangle) = \langle a_1,a_2\rangle.C_G(t)$, also t is fixed-point-free on $\langle a_1,a_2\rangle$.

PROOF

Clearly t inverts $\langle a_1,a_2\rangle$. As $C_G(\langle a_1,a_2\rangle) \leq C_G(a_1)\cap C_G(a_2) = \langle a_1, a_2\rangle$, $C_G(\langle a_1,a_2\rangle) = \langle a_1, a_2\rangle$. Therefore by lemma (1.3) $N_G(\langle a_1,a_2\rangle) = \langle a_1, a_2\rangle\, C_{N_G(\langle a_1,a_2\rangle)}(t)$.

Put $N = N_G(\langle a_1,a_2\rangle)$; we have $AV \leq N$ and a_2 has 6 conjugates in AV. All conjugates of a_2 in N are contained in $\langle a_1,a_2\rangle^\#$ which has order 8. So since

$|N| = |N:C_N(a_2)||C_N(a_2)| = 2.3^3.|N:C_G(a_2)|$ (as $C_G(a_2) \leq N$ by lemma (5.4)), a_2 cannot have 6 conjugates in N (because of lemma (5.1)) so it must have 8. Thus $|N| = 2^4.3^3$. Now as $|N| = |\langle a_1,a_2\rangle C_N(t)| = |\langle a_1,a_2\rangle||C_N(t)| = 3^2|C_N(t)|$, $|C_N(t)| = 2^4.3 = |C_G(t)|$, and therefore $C_N(t) = C_G(t)$. Hence $N = \langle a_1,a_2\rangle C_G(t)$.

LEMMA (5.6)

$N_G(\langle a\rangle) = \langle a_1, a, z\rangle$.

PROOF

As a_1 centralizes a, $P = \langle a_1, a\rangle \leq C_G(a)$. If P is not a Sylow 3-subgroup of $C_G(a)$ then a is contained in the centre of a Sylow 3-subgroup of G and so will be conjugate to a_1 contrary to lemma (5.2). Therefore P is a Sylow 3-subgroup of $C_G(a)$. Assume by way of contradiction that $P < C_G(a)$.

Using lemma (5.3) $N_{C_G(a)}(P) = C_{C_G(a)}(P) = P$, so by Burnside's Transfer Theorem $C_G(a)$ has a normal 3-complement, M say, $M \neq 1$.

Since z inverts a, $N_G(\langle a\rangle) = C_G(\langle a\rangle)\langle z\rangle$ which therefore has order $2.3^2.m$ ($|M| = m$); let $H = N_G(\langle a\rangle)$. By lemma (5.3) $N_H(\langle a_1, a\rangle) = \langle a_1, a, z\rangle$ which has index m in H, therefore by Sylow's theorem $m \equiv 1$ (3).

By the proof of lemma (5.3) $\langle a_1\rangle$ is the only subgroup of $\langle a_1, a\rangle$ centralized by an involution. So each Sylow 3-subgroup of H contains exactly one subgroup of order 3 centralized by an involution; they must all be conjugate to $\langle a_1\rangle$ in H and there are m of them. It is easily seen that $N_H(\langle a_1\rangle) = C_H(\langle a_1\rangle) = \langle a_1, a, z\rangle$ so no involution of H inverts a_1.

Also no involution of H inverts $a_1^{-1}a = a_2a_3$ for suppose so and let $(a_2a_3)^v = a_3^{-1}a_2^{-1}$ for some involution v of H.
Then

$$\begin{aligned} a_3^{-1}a_2^{-1} &= (a_2a_3)^v = (a_1^{-1}a)^v = (a_1^{-1})^v a^v \\ &= (a_1^{-1})^v a^{-1} = (a_1^{-1})^v a_3^{-1}a_2^{-1}a_1^{-1}, \end{aligned}$$

which implies that $a_1^v = a_1^{-1}$, contradicting the previous paragraph. Similarly $a_1a = a_1^{-1}a_2a_3$ is not inverted by an involution of H. Thus no element b of $H-\langle a\rangle$ of order 3 is inverted by an involution of H.

As M char $C_G(a) \triangleleft H$, $M \triangleleft H$. Therefore z normalizes M and as $C_M(z) = 1$, z inverts M and M is abelian by lemma (1.2). Hence also $L = M\langle a\rangle$ is abelian, and $L \triangleleft H$ as both M and $\langle a\rangle$ are normal in H.

Because L is abelian $L \leq C_G(L)$. If $b \in C_G(L)$ then b centralizes a and M, so

$$\begin{aligned} b &\in C_G(a) \cap C_G(M) \\ &= \langle a_1, a\rangle M \cap C_G(M) \\ &= M\langle a\rangle = L, \end{aligned}$$

thus $C_G(L) \leq L$ and hence $C_G(L) = L$.

If $x \in M^{\#}$, as z inverts x, $z \in N_G(\langle x\rangle)$. Since $C_G(x) \triangleleft N_G(\langle x\rangle)$, z normalizes $C_G(x)$. No element of $C_G(x)^{\#}$ centralizes z, therefore $C_G(x)$ is abelian (lemma (1.2)). Since L is abelian and $x \in L$, $L \leq C_G(x)$. Now as $C_G(x)$ is abelian also, $C_G(x) \leq C_G(L) = L$. Thus $C_G(x) = L$ for all $x \in M^{\#}$.

For $u \in G-H$ we claim $M \cap M^u = 1$. Suppose not and let $x \in M \cap M^u$, $x \neq 1$. Then $x = y^u$ for some $y \in M^{\#}$, and so $C_G(x) = C_G(y)^u$ which implies by the previous paragraph, $L = L^u$, that is $u \in N_G(L)$. However as $\langle a\rangle$ char L, being a normal Sylow 3-subgroup, $\langle a\rangle \triangleleft N_G(L)$. So $N_G(L) \leq H$. Thus $u \in H$ a contradiction.

We shall apply Bender's lemma to H; note that $H = L\langle a_1, z\rangle = L\, C_H(z)$. Firstly.

$$f = \frac{|H|}{|C_G(z)|} - 1 = \frac{18m}{48} - 1 = \frac{3m-8}{8},$$

and $|J \cap H| = 3m$.

Let u be an involution of G-H and consider $H \cap H^u$. We can apply the reasoning in lemma (3.4) to show that if $p \mid |H \cap H^u|$, where p is a prime divisor of m, then $M \cap M^u \neq 1$.

It follows that $p \nmid |H \cap H^u|$ and so $|H \cap H^u| \mid 2.3^2$.

Suppose in fact $|H \cap H^u| = 2.3^2$. Then u centralizes some involution v in $H \cap H^u$ as there are an odd number of involutions in $H \cap H^u$. Let Q be the Sylow 3-subgroup of $H \cap H^u$, then u normalizes Q (since u normalizes $H \cap H^u$ and $Q \triangleleft H \cap H^u$); also v normalizes Q. Therefore $N_G(Q)$ contains the 4-group $\langle u,v \rangle$. However Q is conjugate to $\langle a_1,a \rangle$, this contradicts lemma (5.3) so $|H \cap H^u| \neq 2.3^2$.

Suppose u inverts a subgroup of order 3 in H. If u inverts another subgroup of H of order 3 then u will invert a subgroup of order 9 in H. This subgroup contains a and so u in particular inverts a, a contradiction. Therefore u can only invert one subgroup of order 3.

Suppose u inverts $\langle a_1{}^{-1}a \rangle$ (or $\langle a_1 a \rangle$). If u also inverts an involution then $H \cap H^u$ has order 6. But then $\langle a_1{}^{-1}a \rangle$ (or $\langle a_1 a \rangle$) is either centralized or inverted by an involution of H neither of which is correct; thus $u \in J_3$ in this case.

If u inverts $\langle a_1 \rangle$ then $H \cap H^u$ cannot contain a subgroup of order 9 else u normalizes it and will in fact invert it (lemma (1.2)), so $|H \cap H^u| \mid 2.3$. The centralizer $C_H(a_1) = \langle a_1,a,z \rangle$ contains three involutions z_i say $i = 1, 2, 3$. the elements $a_1 z_i$ $i = 1,2,3$ have order 6 and are each inverted by 6 involutions of $G-H$. Therefore a_1 is inverted by 18 involutions which also centralize an involution of H. As a_1 is inverted by 18 involutions, any involution inverting a_1 in fact inverts a subgroup of order 6 in M; thus $u \in J_6$ in this case.

Suppose now that u inverts an involution v of H, either u inverts only $\langle v \rangle$ in which case $u \in J_2$ or u inverts another element of $H - \langle v \rangle$ and then u inverts a subgroup of order 6 and u

$\in J_6$. In this latter case u inverts a subgroup of order 3. Therefore the involutions of J_6 are all the involutions inverting a subgroup of order 3 which is conjugate to $\langle a_1 \rangle$ in H. As $\langle a_1 \rangle$ has m conjugates in H and is inverted by 18 involutions of G-H.

$$|J_6| = 18.m = 2.3^2.m$$

and $$b_6 = 3.m$$

An involution of H is inverted by 12 involutions of G-H and has 3m conjugates, therefore

$$|J_2| + |J_6| = 12.3.m = 2^2.3^2.m,$$

thus $$|J_2| = 2.3^2.m \text{ and } b_2 = 3^2.m.$$

The subgroups $\langle a_1 a \rangle$ and $\langle a_1^{-1} a \rangle$ being conjugate to $\langle a \rangle$ in G are inverted by 3m involutions none of which belong in H, and as there are m conjugates of each in H,

$$|J_3| = 2.3.m.m = 2.3.m^2$$

so $$b_3 = 2.m^2,$$

Now let $u \in J_1$ so that u inverts no non-trivial element of H and consider $C_H(u)$. This will have order 3 if it is not trivial. Suppose u centralizes $\langle a_1 \rangle$ so that $u \in C_G(a_1) = A\langle z \rangle$. Now the three subgroups in $\langle a_1, a \rangle$ of order 3 other than $\langle a_1 \rangle$ are conjugate in $A\langle z \rangle$. So as $\langle a \rangle$ is inverted by three involutions of $A\langle z \rangle$, the subgroups $\langle a_1 a \rangle$ and $\langle a_1^{-1} a \rangle$ are each inverted by three involutions of $A\langle z \rangle$, these involutions are all distinct. Since $A\langle z \rangle$ contains 9 involutions each one inverts some subgroup of order 3 in H. Thus $C_H(u) = 1$ for all $u \in J_1$ and so $c = 0$. Hence $b_1 = 2.3^2.m.k$, k a non-negative integer.

We summarize what we have so far:

$$f = \frac{3m-8}{8},$$

$$|J \cap H| = 3m,$$

$$b_2 = 3^2.m, \quad b_3 = 2.m^2, \quad b_6 = 3.m$$

$b_1 = 2.3^2.m.k$, k a non-negative integer and all other b_n are zero ($n \neq 0$).

To determine b_1 we use Bender's lemma.

$$b_1 = 2.3^2.m.k < \frac{8}{3m-8}(3m + 3^2.m + 2^2m^2 + 3.5m) - 3^2.m - 2m^2 - 3m$$

hence,
$$3k < \frac{-m^2 + 2m + 52}{3m-8}$$
$$= \frac{-m^2}{3m-8} + \frac{2}{3} + \frac{57\frac{1}{3}}{3m-8}$$
$$< \frac{-m^2}{3m-8} + 1 + \frac{58}{3m-8}$$

Clearly $(m,6) = 1$ and as $m \equiv 1$ (3) also, $m \geq 7$.

Therefore $\frac{1}{3m-8} \leq \frac{1}{13}$ and $-m^2 \leq 49$,

hence $3k < \frac{-49}{13} + 1 + \frac{58}{13}$

yielding $k < \frac{2}{3}$ thus $k = 0$ and $b_1 = 0$.

The number of involutions in G is

$$|J| = 3.m + 2.3^2.m + 2.3.m^2 + 2.3^2.m$$
$$= 3.m.(13 + 2m)$$

whence $|G| = 2^4.3^3.m.(13 + 2m)$.

By lemma (5.1) the normalizer of a Sylow 3-subgroup has order $2^2.3^3$, so the index is $2^2.m.(13 + 2m)$. Sylow's theorem gives then $2^2.m.(13 + 2m) \equiv 1$ (3). However as $m \equiv 1$ (3) $2^2.m.(13 + 2m) \equiv 0$ (3), this contradiction completes the proof of the lemma.

We now have enough information to be able to determine the order of G, this is done in the next lemma.

<u>LEMMA</u> <u>(5.7)</u>

The order of G is $2^4.3^3.13$.

PROOF

We use Bender's lemma with $H = N_G(A) = N_G(\langle a_1\rangle)$ to determine $|G|$. Firstly

$$f = \frac{|H|}{|C_G(z)|} - 1 = \frac{2^2.3^3}{48} - 1 = \frac{9}{4} - 1 = \frac{5}{4}$$

Also as H contains 27 involutions, $|J \cap H| = 27$.

Let u be an involution of G-H. Recall that $A^{\#}$ has four conjugacy classes in H with representatives a_1, a_2, a_3 and a. Clearly u cannot invert any element of the first class.

As $N_G(\langle a\rangle) = \langle a_1, a, z\rangle$ (lemma (5.6)) which is contained in H, the normalizers of all conjugates of $\langle a\rangle$ in H are contained in H. Thus u cannot invert a conjugate of a in H; and so conjugates of a_2 and a_3 in H are the only elements of $A^{\#}$ which can be inverted by u.

The conjugates of a_2 in H are a_2, a_2^{-1}, a_1a_2, $a_1^{-1}a_2$, $a_1a_2^{-1}$, and $a_1^{-1}a_2^{-1}$. Suppose u inverts $\langle a_2\rangle$; then u cannot invert a conjugate of a_2 besides a_2 and a_2^{-1}, else u inverts $\langle a_1, a_2\rangle$ and in particular inverts a_1. As u inverts $\langle a_2\rangle$ it normalizes $\langle a_1, a_2\rangle$ by lemma (5.4), If u inverts a conjugate of a_3 then u also normalizes $\langle a_1, a_3\rangle$ by the remarks following lemma (5.4). But then u normalizes A which is not true. Thus u cannot invert another subgroup of order 3. For the same reason if u inverts $\langle a_3\rangle$ then u cannot invert another subgroup of order 3 in H.

We have $C_H(a_2) = \langle a_1, a_2, zt\rangle$ which contains 3 involutions and $N_H(\langle a_2\rangle) = \langle a_1, a_2\rangle V$ which contains 15. So $\langle a_2\rangle$ is inverted by 12 involutions of H. As $\langle a_2\rangle$ is inverted by 18 involutions it is inverted by 6 involutions of G-H.

Now $N_G(\langle a_2\rangle) = \bar{A}V = \langle a_1, a_2, m\rangle V$ where $\langle m\rangle = C_{\bar{A}}(t)$. The involutions mz, $m^{-1}z$, a_2mz, $a_2^{-1}mz$, $a_2m^{-1}z$ and $a_2^{-1}m^{-1}z$ invert

$\langle a_2\rangle$ and belong to G-H. These are therefore all the involutions of G-H inverting $\langle a_2\rangle$. Since mz centralizes t, it also centralizes a subgroup of order 3 in $\langle a_1,a_2\rangle$, $\langle r\rangle$ say (since the 4-group $\langle t, mz\rangle$ acts on $\bar{A}$). Thus mz centralizes the involutions t, rt and $r^{-1}t$ of H. We have $\langle a_1,a_2,t\rangle \leq H \cap H^{mz}$ and in fact $\langle a_1,a_2,t\rangle = H \cap H^{mz}$, it follows that $mz \in J_6$. It is easily checked that mz is conjugate to all involutions of G-H inverting a_2 by an element of H. So if mz centralizes the involution v say of H, then $(mz)^h$ centralizes the involution v^h of H. Thus all involutions of G-H inverting $\langle a_2\rangle$ invert a further 3 involutions of H and therefore belong in J_6. We note that these involutions of H are conjugate in H to t as $rt = t^r$ and $r^{-1}t = t^{r^{-1}}$.

The same argument applies if u inverts $\langle a_3\rangle$, so we have again that $u \in J_6$. In this case however the involutions of H centralizing u are conjugate to zt in H. We have that if u inverts a subgroup of order 3 in H then $u \in J_6$.

Now suppose u inverts $\langle t\rangle$. Either u only inverts $\langle t\rangle$, in which case $u \in J_2$, or u inverts some other subgroup of H. If u inverts an element of order 3 then $u \in J_6$. If it inverts an involution v say, then vt must have order 3 or 6 and is centralized by u. Suppose the order is 3; then $\langle vt\rangle$ is conjugate to $\langle a_2\rangle$ or $\langle a_3\rangle$ in H. Therefore $N_G(\langle vt\rangle) \leq N_G(\langle a_1,vt\rangle)$ and so $N_G(\langle a_1,vt\rangle)$ contains the 4-group $\langle t,u\rangle$. Thus u inverts some subgroup of order 3 in $\langle a_1,vt\rangle$ and again $u \in J_6$. If vt has order 6 the previous argument applied to $(vt)^2$ shows that u inverts a subgroup of order 3 and so $u \in J_6$.

Thus if u inverts a conjugate of t in H either $u \in J_2$ or u inverts a subgroup of order 3 in H and $u \in J_6$. The same reasoning applies to zt.

Suppose finally that u inverts a conjugate of z in H. Then u cannot invert an element of order 3 for we have seen in this case that u inverts only conjugates of t or zt in H. Nor can it centralize another involution for this would imply, as above that u inverts a subgroup of order 3. Thus $u \in J_2$.

We can now determine the order of J_2 and J_6.

All involutions of G-H inverting a subgroup of order 3 in H belong to J_6 and these yield all the involutions of J_6. The only subgroups of order 3 in H inverted by involutions of G-H are conjugates of $\langle a_2 \rangle$ and $\langle a_3 \rangle$ in H. There are 6 such subgroups each inverted by 6 involutions of G-H. Therefore $|J_6| = 6.6 = 2^2.3^2$ and so $b_6 = 2.3$.

An involution of G-H centralizing a conjugate of t is either contained in J_2 or J_6. Suppose k_1 of these are contained in J_6. As t is centralized by 6 involutions of G-H, $0 \leq k_1 \leq 6$. Also suppose k_2 involutions of G-H centralizing zt are contained in J_6; $0 \leq k_2 \leq 6$. Then as t and zt each have 9 conjugates in H and since each involution of J_6 centralizes 3 involutions of H we have

$$|J_6| = \frac{k_1.9 + k_2.9}{3} = 3(k_1 + k_2)$$

But we know that $|J_6| = 2^2.3^2$, this implies that $k_1 + k_2 = 12$ and hence $k_1 = k_2 = 6$. Thus every involution of G-H centralizing a conjugate of t or zt in H is contained in J_6. Hence an involution of J_2 centralizes a conjugate of z in H.

As z is centralized by 6 involutions of G-H and has 9 conjugates in H

$|J_2| = 6.\ 9 = 2.3^3$ and thus $b_2 = 3^3$.

If $u \in J_1$ then u cannot centralize an involution of H, nor can it centralize an element of order 3 in H. For suppose u centralizes $b \in H$, b of order 3, then $u \in N_G(\langle a_1, b\rangle)$ by the remarks following lemma (5.4) and u must invert some subgroup of order 3 in $\langle a_1, b\rangle$. Thus $C_H(u) = 1$ for all $u \in J_1$, so $c = 0$ and therefore $b_1 = 2^2.3^3.k$, k a non-negative integer.

Summarizing we have:

$$f = \frac{5}{4},$$

$$|J \cap H| = 27$$

$b_2 = 3^3$, $b_6 = 2.3$, $b_1 = 2^2.3^3.k$, k a non-negative integer and all other b_n are zero $(n \neq 0)$.

By Bender's lemma

$$b_1 = 2^2.3^3.k < \frac{4}{5}\ (3^3 + 3^3 + 2.3.5) - 3^3 - 2.3$$

which implies $k < \frac{57}{180} < 1$, so $k = 0$ and $b_1 = 0$.

The number of involutions in G is

$$|J| = 3^3 + 2.3^3 + 2^2.3^2$$
$$= 3^2.13$$

whence the order of G is $2^4.3^3.13$

We easily prove the following lemma.

<u>LEMMA</u> <u>(5.8)</u>

The group G is simple.

<u>PROOF</u>

If G is not simple then by lemma (2.6) a proper non-trivial normal subgroup has order 27. However a subgroup of this order is not normal in G by lemma (5.1). We conclude that G is simple.

It is now possible to identify G.

THEOREM

If G is a group satisfying the assumptions of this chapter then G is isomorphic to $PSL(3,3)$.

PROOF

We show that G satisfies the postulates made in [3], which are listed preceeding lemma (1.6).

Firstly G contains the 4-group V. Next, as V is abelian $V \leq C$ and $V \leq C_G(t)$, so V is contained in a dihedral group D_1 of C and also one of $C_G(t)$, D_2 say. Now $D_1 \neq D_2$ as $Z(D_1) = \langle z\rangle$ and $Z(D_2) = \langle t\rangle$. Therefore as $\langle D_1, D_2\rangle \leq N_G(V)$ ($|D_i : V| = 2$ $i = 1,2$), we must have $N_G(V)/V \cong S_3$. So there is an element which permutes the involutions of V. Thus postulate (I) is satisfied.

Let $M = \langle a_1, a_2\rangle$; M is inverted by t so $M \cap C_G(t) = 1$ and by lemma (5.5) $C_G(t) \leq N_G(M)$.

In C there is a subgroup, $\langle b\rangle$ say, of order 3 inverted by t and $\langle b\rangle \neq \langle a_1\rangle$. Now $N_G(\langle b\rangle) = BV$ with B a non-abelian Sylow 3-subgroup of order 3 normalized by V. Also $B = \langle b_1, b_2, b_3\rangle$ where $\langle b_1\rangle = C_B(z) = \langle b\rangle$, $\langle b_2\rangle = C_B(zt)$ and $\langle b_3\rangle = C_B(t)$.

Put $M^* = \langle b_1, b_2\rangle$; M^* has the same order as M and clearly $M^* \cap C_G(t) = 1$ and $C_G(t) \leq N_G(M^*)$.

Consider $M \cap M^*$, as $M \neq M^*$ if $M \cap M^* \neq 1$ then $M \cap M^* = \langle y\rangle$ has order 3. But then $\langle y\rangle$ is normalized by V, so as $M \cap C = \langle a_1\rangle \neq M^* \cap C = \langle b_1\rangle$ and t is fixed-point-free on M and M^*, $M \cap M^* \leq C_G(zt)$ by [12] theorem 5.3.16. So $\langle y\rangle = \langle a_2\rangle = \langle b_2\rangle$.

Now

$M^* \leq N_G(\langle b_2\rangle) = N_G(\langle a_2\rangle) = \bar{A}V$, so $M^* \leq \bar{A}$, in particular $\langle b_1\rangle \leq \bar{A}$. But then $\langle b_1\rangle = C_{\bar{A}}(z) = \langle a_1\rangle$, that is $\langle b_1\rangle = \langle a_1\rangle$, a contradiction, and hence postulate (II) is satisfied.

Postulate (III) we already have.

Postulate (IV) is trivial as $|G:MC_G(t)| = |G:N_G(M)| = 13$ and $q^2 + q + 1 = 3^2 + 3 + 1 = 13$.

Finally we consider postulate (V). As a_1 has 8 conjugates in $N_G(M) = MC_G(t)$ all of which lie in $M^{\#}$, we see that $C_G(t)$ is transitive on $M^{\#}$ which is a stronger statement then (V).

Thus by lemma (1.6) the group G has a chief series $G \geq G_0 \geq K \geq 1$ where G/G_0 is cyclic, $G_0/K \cong PSL(3,3)$ and K is a normal subgroup of odd order. As $|G| = |PSL(3,3)|$ we must have $G_0 = G$, $K = 1$ and $G \cong PSL(3,3)$.

CHAPTER SIX

CASE (D) $A \cong Z_3 X Z_3$

Throughout this chapter suppose that $N_G(X) = AV$ where $A \cong Z_3 x Z_3$ and $A \triangleleft N_G(X)$.

Let $C_A(z) = \langle a_1 \rangle$ and $C_A(zt) = \langle a_2 \rangle$ (which we may suppose to be non-trivial) so that $C_A(t) = 1$ and therefore t inverts A by lemma (1.2) ; $A = \langle a_1, a_2 \rangle$. Note that $a_1 \sim_G a_2$ by lemma (2.3). The structure of $N = N_G(A)$ is determined in the first lemma.

LEMMA (6.1)

$N = AC_N(t)$ has order $2^4.3^2$ and so A is a Sylow 3-subgroup of G.

PROOF

Since $C_G(A) \leq C_G(a_1) \cap C_G(a_2)$, $C_G(A) = A$, and as t inverts A, $N = AC_N(t)$ by lemma (1.3).

We show that V is not a Sylow 2-subgroup of N. By the proof of lemma (4.1) z and zt are conjugate in N. So if V is a Sylow 2-subgroup of N, by [12] theorem (7.7.1), N has one class of involutions. But then z and t would be conjugate in N contrary to the fact that $C_A(z)$ has order 3 while $C_A(t)$ is trivial. Thus a Sylow 2-subgroup of N has order 8 or 16 ; if the order is 8 a Sylow 2-subgroup is dihedral since it contains a 4-group.

Now as $N = AC_N(t)$ there are four possible orders for N namely $2^3.3^2, 2^3.3^3, 2^4.3^2$, or $2^4.3^3$.

All conjugates of a_1 in N lie in $A^{\#}$, therefore as $|A^{\#}|=8$, a_1 has at most 8 conjugates in N, thus $|N:C_N(a_1)| \leq 8$. As $C_G(a_1) = A\langle z \rangle \leq N$, $C_N(a_1) = C_G(a_1)$ which has order 2.3^2. It follows that $|N| \leq 2^4.3^2$. This condition eliminates the possibilities $2^3.3^3$ and $2^4.3^3$.

We prove now that the elements of order 3 in G form a single conjugacy class.

The subgroup $R = C_N(t)$ is a Sylow 2-subgroup of order 8 or 16 (which contains V); in either case $Z(R) = \langle t\rangle$ and $z \sim_R zt$. As $N_R(V) \cong D_8$ there is an involution $v \in R$ with $z^v = zt$.

As $C_A(z) = \langle a_1\rangle$, $C_A(zt) = \langle a_2\rangle$ and $z^v = zt$, $\langle a_1\rangle^v = \langle a_2\rangle$, without loss we may assume $a_1{}^v = a_2$. Then $a_1{}^{v^2} = a_1 = a_2{}^v$, so $(a_1a_2)^v = a_1{}^va_2{}^v = a_2a_1 = a_1a_2$, that is $a_1a_2 \in C_G(v)$. By lemma (2.3) $a_1a_2 \sim a_1$ in G and as $(a_1a_2)^z = a_1a_2{}^{-1}$ also $a_1a_2{}^{-1} \sim a_1$ in G. Since $\langle a_1\rangle$, $\langle a_2\rangle$, $\langle a_1a_2\rangle$ and $\langle a_1a_2{}^{-1}\rangle$ are the only subgroups of order 3 in A and A is a Sylow 3-subgroup of G (since it is a Sylow 3-subgroup of N) the assertion follows.

Now let $a \in A^{\#}$, then $A \leq C_G(a)$. By the previous paragraph $a_1 = a^g$ for some $g \in G$. Then

$$A^g \leq C_G(a)^g = C_G(a^g) = C_G(a_1) = A\langle z\rangle.$$

Thus $A^g = A$ that is $g \in N$. Therefore a_1 is conjugate in N to all elements of $A^{\#}$ and so has 8 conjugates in N. Thus $|N| = |N:C_N(a_1)||C_N(a_1)| = 8.2.3^2. = 2^4.3^2$ and the lemma is proved.

We note that by the proof of this lemma the elements of order 3 in G form a single conjugacy class.

LEMMA (6.2)

The order of G is $2^4.3^2.5.11$.

PROOF

Bender's lemma is used to determine $|G|$ with $H = N$.

Firstly

$$f = \frac{|H|}{|C_G(z)|} - 1 = \frac{2^4.3^2}{2^4.3} - 1 = 2$$

We have $H = AC_H(t)$ and $C_H(t)$ is a Sylow 2-subgroup of H of order 16 by lemma (6.1) ; $C_H(t)$ has 2 classes of involutions with representatives t and z. As t and z are not conjugate in H, H has 2 classes of involutions with representatives t and z. Since t has 9 conjugates and z has 12, H contains 21 involutions, therefore $|J \cap H| = 21$.

By the proof of lemma (6.1) the subgroups of order 3 in H are conjugate in H. As $N_G(\langle a_1 \rangle) = AV \leq H$, the normalizer in G of every subgroup of order 3 in H is contained in H.

Let u be an involutions of G-H and consider $H \cap H^u$. Since u does not normalize A, $A \cap A^u < A$, and if $A \cap A^u$ is not trivial it has order 3. As $A \cap A^u$ is normalized by u, $A \cap A^u = 1$ by the previous paragraph. Thus $A \cap (H \cap H^u) = 1$ (as $A \cap H^u \leq A \cap A^u = 1$) which shows that $H \cap H^u$ is a 2-group.

Suppose u centralizes 2 involutions, v_1 and v_2 say, of H, then u centralizes $\langle v_1 v_2 \rangle$ which contains a unique involution v say. But now u centralizes the 4-group $\langle v_1, v \rangle$ of H. Thus u centralizes at most one involution of H. Since every involution of $C_G(t) - \langle t \rangle$ inverts exactly one subgroup of order 4, u inverts at most one subgroup of order 4 in H. It follows that the elements of H inverted by u form cyclic subgroups of order 1, 2 or 4.

If u inverts z, then u cannot invert an element of H of order 4 else $C_H(z) = A_1 V$ contains an element of order 4, so $u \in J_2$.

An element of order 4 is inverted by 4 involutions, these involutions belong in the same Sylow 2-subgroup of G. Now $C_H(t) = R$ has 3 cyclic subgroups of order 4, one of these is inverted by 4 involutions of H, the other two are each inverted by 4 involutions of G-H. As t is centralized by 8 involutions of G-H, if u inverts t, it also inverts a subgroup of H of order 4 and $u \in J_4$.

As t has 9 conjugates in H,

$|J_4| = 8.9 = 2^3.3^2$;

thus $b_4 = 2.3^2$.

As z is centralized by 6 involutions of G-H and has 12 conjugates in H,

$|J_2| = 6.12 = 2^3.3^2$

and so $b_2 = 2^2.3^2$.

By Bender's lemma we have

$$b_1 < \frac{1}{2}(21 + b_2 + 3b_4) - 1 - b_2 - b_4$$

$$= \frac{1}{2}(19 - b_2 + b_4)$$

$$= \frac{1}{2}(19 - 36 + 18) = \frac{1}{2}$$

and hence $b_1 = 0$.

Thus $|J| = 3.7 + 2^3.3^2 + 2^3.3^2 = 3.5.11$ and the order of G is $2^4.3^2.5.11$.

The proof of the following lemma is the same as that of lemma (3.1).

LEMMA (6.3)

The group G is simple.

Using Sylow's theorem we easily determine the structure of the normalizer of the Sylow 5 and Sylow 11-subgroups of G; these normalizers are Frobenius groups of order 20 and 55 respectively. We can also determine the conjugacy classes of $G^{\#}$, there are 9 in all. There is one class each of elements of order 2, 3, 4, 5 and 6; the elements of order 8 and 11 each form two classes.

We shall need the following result.

LEMMA (6.4)

The intersection of two distinct Sylow 3-subgroups of G is trivial.

PROOF

Let A and B be two Sylow 3-subgroups of G and suppose $a \in A \cap B$, $a \neq 1$. Then $C_G(a) = A\langle v \rangle = B\langle v \rangle$ where v is an involution centralizing a. Now $B \leq A\langle v \rangle$ and as A is a normal Sylow 3-subgroup of $A\langle v \rangle$ and B has order 9, A = B. So if $A \neq B$ then $A \cap B = 1$.

To identify G we use the permutation respresentation on the cosets of a subgroup of index 11. We show that such a subgroup exists in the following two lemmas.

LEMMA (6.5)

The group G contains a subgroup of index 22 isomorphic to A_6.

PROOF

We have the following: A is a Sylow 3-subgroup of G inverted by the involution t, $N = AC_N(t)$ and $C_N(t)$ is a Sylow 2-subgroup of G. Recall that if $\langle r \rangle$ is a subgroup of A of order 3 then $N_G(\langle r \rangle) \leq N$ (see the proof of lemma (6.2)).

Now all Sylow 2-subgroups of $C_G(t)$ contain the unique quaternion group, say $Q_0 \lhd C_G(t)$. Let R be a Sylow 2-subgroup of $C_G(t)$, $R \neq C_N(t)$, so that $R \cap C_N(t) = Q_0$. Let D be dihedral of order 8 in R; then $Q_0 \cap D$ is cyclic of order 4. Put $Q_0 \cap D = \langle x \rangle$, then $x^2 = t$, x normalizes A but D does not.

Let $D = \langle a,b \rangle$ a,b involutions of D with $ab = x$; $a,b \notin N$ else $D \leq N$. Also $a^x = a^{ab} = a^b = bab = a.abab = at$, and $b^x = bt$.

Let $A = \langle r \rangle \times \langle s \rangle$. As x normalizes A we may suppose $r^x = s$. Now $r^{x^2} = s^x$ and $r^{x^2} = r^t = r^{-1}$, therefore $s^x = r^{-1}$.

We have the following relations

$a^2 = b^2 = t^2 = r^3 = s^3 = x^4 = 1$,

$ab = x$, $x^2 = t$, $a^x = at$, $b^x = bt$,

$[a,t] = [b,t] = [r,s] = 1$,

$r^t = s^{-1}$, $s^t = r^{-1}$,

$r^x = s$ and $s^x = r^{-1}$

Consider the elements ar and as. Since

$(ar)^{r^{-1}t} = r^{-1}tar.\, r^{-1}t = r^{-1}tat = r^{-1}a = (ar)^{-1}$,

ar is inverted by the involution $r^{-1}t$. As the only elements of $G^\#$ inverted by an involution have orders 2, 3, 4, 5 or 6, these are the only possible orders of ar. Similarly as has possible orders 2, 3, 4, 5 or 6.

If $(ar)^2 = 1$ then $r^a = r^{-1}$ so $a \in N_G(\langle r \rangle) \leq N$ a contradiction. Therefore $(ar)^2 \neq 1$ and for the same reason $(as)^2 \neq 1$.

If $(ar)^3 = 1$ then

$$
\begin{aligned}
1 &= (ararar)^x \\
&= a^x r^x a^x r^x a^x r^x \\
&= atsatsats \\
&= atsas^{-1}at^2s \\
&= atsas^{-1}as
\end{aligned}
$$

Therefore $at = s^{-1}asas^{-1} = s^{-1}(asas)s$.

So as $(at)^2 = 1$, $(as)^4 = 1$.

Thus if $(ar)^3 = 1$ then $(as)^4 = 1$.

Similarly $(as)^3 = 1$ implies $(ar)^4 = 1$.

Assume now that $(ar)^4 = 1$, then

$$\begin{aligned} 1 &= (arararar)^x \\ &= a^x r^x a^x r^x a^x r^x a^x r^x \\ &= atsatsatsats \\ &= as^{-1}asas^{-1}as \\ &= as^{-1}(asas)sas \end{aligned}$$

Therefore $s^{-1} = as^{-1}(asas)sa$

So $as(s^{-1})^3 = 1$, $(as)^6 = 1$

We also have from these steps

$$1 = a(s^{-1}as)a(s^{-1}as),$$

So that $s^{-1}as \in C_G(a)$. Also $t \in C_G(a)$, so $(s^{-1}as)^t = sas^{-1} \in C_G(a)$ and $sas^{-1}.s^{-1}as = sasas \in C_G(a)$ as well.

Now $(as)^6 = 1$ yields

$$1 = a(sasas)a(sasas) = (sasas)^2.$$

If $sasas = 1$ then $(s^{-1}a)s(as) = s$, that is $as \in C_G(s)$. Therefore $a \in C_G(s)$ and as $C_G(s) \leq N$, $a \in N$ a contradiction. Thus sasas has order 2.

Now

$$\begin{aligned} (ts^{-1}as)^2 &= ts^{-1}asts^{-1}as \\ &= sas^{-1}s^{-1}as \\ &= sasas \end{aligned}$$

So as sasas has order 2, $ts^{-1}as$ has order 4 and since $ts^{-1}as$ is also an element of $C_G(a)$ its square is equal to a. That is $sasas = a$ which implies $(as)^3 = 1$.

Thus if $(ar)^4 = 1$ then $(as)^3 = 1$.

Similarly $(as)^4 = 1$ implies $(ar)^3 = 1$.

Now assume $(ar)^5 = 1$. The preceeding arguments show that $(as)^3 \neq 1$ and $(as)^4 \neq 1$.

Suppose $(as)^6 = 1$. We have

$$1 = (ararararar)^x$$

$$= a^x r^x a^x r^x a^x r^x a^x r^x a^x r^x$$

$$= atsatsatsatsats$$

$$= atsas^{-1}asas^{-1}as$$

$$= tasas^{-1}asas^{-1}as$$

Therefore $t = asas^{-1}asas^{-1}as$, the element $asas^{-1}asas^{-1}as$ inverts s (that is t inverts s).

Also as $(as)^6 = 1$ equating with the above yields

$$atsas^{-1}asas^{-1}as = asasasasasas,$$

which on cancellation and solving for t yields

$$t = sasasasas^{-1}as^{-1}asas^{-1}.$$

So as $t^2 = 1$ we have

$$1 = sasasasas^{-1}as^{-1}asas^{-1}sasasasas^{-1}as^{-1}asas^{-1},$$

and after simplification yields

$$s = (asasas^{-1}as^{-1}a)s^{-1}(asasas^{-1}as^{-1}a).$$

Thus $asasas^{-1}as^{-1}a$ is also an element inverting s. Multiplying by the previous element inverting s gives

$$asasas^{-1}as^{-1}a.asas^{-1}asas^{-1}as$$

$$= asasasasas^{-1}as$$

$$= (as)^6 s^{-1}as^{-1}a.as^{-1}as$$

$$= s^{-1}asas,$$

which must be an element centralizing s, thus $s^{-1}asas \in C_G(s)$ which implies $s^a \in C_G(s)$.

Now A is a normal Sylow 3-subgroup of $C_G(s)$; therefore as s^a has order 3, $s^a \in A$ and then $s \in A^a$. Thus $s \in A \cap A^a$ which implies by lemma (6.4) that $A = A^a$ and so $a \in N$, a contradiction.

We conclude that if $(ar)^5 = 1$ then $(as)^5 = 1$.

Also $(as)^5 = 1$ implies $(ar)^5 = 1$.

Finally suppose $(ar)^6 = 1$; all cases have been eliminated except $(as)^6 = 1$.

Now

$$1 = (ararararararar)^x$$
$$= a^x r^x a^x r^x a^x r^x a^x r^x a^x r^x a^x r^x$$
$$= atsatsatsatsatsats$$
$$= as^{-1}asas^{-1}asas^{-1}as$$

Therefore $a = (s^{-1}asas^{-1})a(sas^{-1}as)$, and so $s^{-1}asas^{-1} \in C_G(a)$.

It is easily shown, using $(as)^6 = 1$, that $s^{-1}asas^{-1}$ has order 3.

Also $(sa)^2 = sasa$ has order 3 since $(sa)^6 = 1$. Since

$$(s^{-1}asas^{-1})^{sasa} = as^{-1}as^{-1}.s^{-1}asas^{-1}.sasa$$
$$= a(s^{-1}asas^{-1})a$$
$$= s^{-1}asas^{-1},$$

$s^{-1}asas^{-1}$ and $sasa$ commute. If $sasa \in \langle s^{-1}asas^{-1}\rangle$ then $sasa \in C_G(a)$ so that

$$s.s^a = sasa = a(sasa).a = asas = s^a.s, \text{ thus } s^a \in C_G(s).$$

We have seen however that this implies $a \in N$. Thus $sasa \notin \langle s^{-1}asas^{-1}\rangle$ and it follows that $B = \langle sasa, s^{-1}asas^{-1}\rangle$ is a Sylow 3-subgroup of G.

Since a centralizes $s^{-1}asas^{-1}$, a normalizes B. Now

$$s^{-1}asas^{-1}.sasa = s^{-1}as^{-1}a \in B \text{ and so } asas \in B.$$

Therefore since

$$(sasa)^s = s^{-1}(sasa)s = asas \in B$$

and $(s^{-1}asas^{-1})^s = s^{-1}(s^{-1}asas^{-1})s = sasa \in B$, $s \in N_G(B)$.

This implies, because s has order 3 and B is a normal Sylow 3-subgroup of $N_G(B)$, that $s \in B$. Thus $s \in A \cap B$ and by lemma (6.4) $A = B$. However a normalizes B, that is a normalizes A, a contradiction. Therefore ar cannot have order 6 and hence neither can as.

Thus we have the following possibilities

(i) $(ar)^3 = (as)^4 = 1$

(ii) $(ar)^4 = (as)^3 = 1$ and

(iii) $(ar)^5 = (as)^5 = 1$

The same reasoning applies to the elements br and bs. So by interchanging r and s and also a and b if necessary, there are four cases to consider, namely:

(I) $(ar)^3 = (as)^4 = (br)^3 = (bs)^4 = 1$

(II) $(ar)^3 = (as)^4 = (br)^4 = (bs)^3 = 1$

(III) $(ar)^3 = (as)^4 = (br)^5 = (bs)^5 = 1$ and

(IV) $(ar)^5 = (as)^5 = (br)^5 = (bs)^5 = 1$

<u>CASE (I)</u> $(ar)^3 = (as)^4 = (br)^3 = (bs)^4 = 1$

Let $R = ar$ and $S = br$; then

$R^3 = S^3 = 1$

and $R^{-1}S = r^{-1}abr = x^r$ therefore

$(R^{-1}S)^4 = 1$

Since $ararar = brbrbr$

$$\begin{aligned} rbr &= ba(rar)ab \\ &= (rar)^x \\ &= r^x a^x r^x \\ &= sats. \end{aligned}$$

Therefore $RS = arbr = asats$ and

$$\begin{aligned} (RS)^2 &= asatsasats \\ &= asas^{-1}as^{-1}as \\ &= as(as^{-1})^4 sasa.as \\ &= as^{-1}as^{-1}, \end{aligned}$$

which has order 2, thus

$(RS)^4 = 1.$

But now by lemma (1.7) the subgroup G generated by R and S has order 168, a contradiction as $7 \nmid |G|$.

<u>CASE</u> <u>(II)</u> $(ar)^3 = (as)^4 = (br)^4 = (bs)^3 = 1$

Let $R_0 = br$ and $S_0 = ar$; then

$R_0{}^4 = S_0{}^3 = 1$

and $R_0{}^{-1}S_0 = r^{-1}bar = (x^{-1})^r$ so

$(R_0{}^{-1}S_0)^4 = 1$

Since $ararar = brbrbrbr$,

$$\begin{aligned} rar &= ab(rbrbr)ba \\ &= (rbrbr)^{x^{-1}} \\ &= r^{x^{-1}}b^{x^{-1}}r^{x^{-1}}b^{x^{-1}}r^{x^{-1}} \\ &= s^{-1}bts^{-1}bts^{-1} \\ &= s^{-1}bsbs^{-1} \end{aligned}$$

Therefore

$$\begin{aligned} R_0S_0 &= brar \\ &= bs^{-1}bsbs^{-1} \\ &= bs^{-1}bs(bs^{-1})^3sbsb \\ &= bs^{-1}bs^{-1}bsb \\ &= (bs^{-1})^3sb.bsb \\ &= s^{-1}b \end{aligned}$$

which has order 3, so $(R_0S_0)^3 = 1$

Now let $R = R_0{}^{-1}S_0{}^{-1}$ and $S = S_0{}^{-1}$. Then R has the same order as R_0S_0. Therefore $R^3 = 1$ also $S^3 = 1$.

Now $RS = R_0{}^{-1}S_0{}^{-1}S_0{}^{-1} = R_0{}^{-1}S_0$, therefore

$(RS)^4 = 1$.

And $R^{-1}S = S_0R_0S_0{}^{-1} = r_0{}^{S_0^{-1}}$, so

$(R^{-1}S)^4 = 1$

So again the subgroup of G generated by R and S has order 168, a contradiction.

CASE (III) $(ar)^3 = (as)^4 = (br)^5 = (bs)^5 = 1$

Let $R = ar$ and $S = ba$; then

$R^3 = S^4 = 1$

and $RS = arba = (rb)^a$ therefore $(RS)^5 = 1$

also $R^{-1}S^{-1}RS = r^{-1}aabarba$

$= r^{-1}barba$

$= r^{-1}x^{-1}rx^{-1}$

$= r^{-1}sx^{-1}x^{-1}$

$= r^{-1}st,$

which has order 2, therefore $(R^{-1}S^{-1}RS)^2 = 1$

So by lemma (1.8) (i) the subgroup of G generated by R and S is isomorphic with A_6.

CASE (IV) $(ar)^5 = (as)^5 = (br)^5 = (bs)^5 = 1$

We have

$A = \langle r\rangle x\langle s\rangle = \langle rs\rangle x\langle r^{-1}s\rangle = \langle u\rangle x\langle v\rangle$

where $u = rs$ and $v = r^{-1}s$; then

$u^3 = v^3 = [u,v] = 1,$

$u^x = (rs)^x = r^x\, s^x = sr^{-1} = r^{-1}s = v$

and $v^x = (r^{-1}s)^x = (r^{-1})^x\, s^x = s^{-1}r^{-1} = (rs)^{-1} = u^{-1}$

Also u and v are inverted by the involution t. These are precisely the relations satisfied by r and s so all the above reasoning applies with u, v replacing r and s. Thus if

$(au)^3 = (av)^4 = 1$ then $(bu)^5 = (bv)^5 = 1$

and $\langle au,ba\rangle \cong A_6$. Suppose then that

$(au)^5 = (av)^5 = (bu)^5 = (bv)^5 = 1.$

Let $R_0 = x^{-1}r$ and $S_0 = b$ then

${S_0}^2 = 1$

and $R_0{}^2 = x^{-1}rx^{-1}r = sx^{-1}x^{-1}r = str = sr^{-1}t$, which has order 2, therefore

$$R_0{}^4 = 1.$$

Also $R_0S_0 = x^{-1}rb = barb = (ar)^b$, so

$$(R_0S_0)^5 = 1.$$

And
$$\begin{aligned} R_0{}^2S_0 &= x^{-1}r\, x^{-1}rb \\ &= sx^{-1}x^{-1}rb \\ &= strb \\ &= sr^{-1}bt, \end{aligned}$$

therefore
$$\begin{aligned} (R_0{}^2S_0)^x &= s^x(r^{-1})^x b^x t^x \\ &= r^{-1}s^{-1}bt.t \\ &= (rs)^{-1}b \\ &= u^{-1}b \\ &= (bu)^{-1}, \end{aligned}$$

which has order 5, therefore $(R_0{}^2S_0)^5 = 1$.

Now let $R = R_0{}^{-1}$ and $S = R_0S_0$; then

$$R^4 = S^5 = 1,$$

$RS = R_0{}^{-1}R_0S_0 = S_0$, so

$$(RS)^2 = 1$$

And $R^{-1}S = R_0R_0S_0 = R_0{}^2S_0$, therefore

$$(R^{-1}S)^5 = 1.$$

So by lemma (1.8) (ii) the subgroup of G generated by R and S is isomorphic to A_6.

As all cases have been considered we conclude that G has a subgroup isomorphic to A_6 which has index 22 in G.

LEMMA (6.6)

The group G possesses a subgroup of index 11.

PROOF

By lemma (6.5) G has a subgroup, H say, isomorphic to A_6. Let D be a dihedral group of H with Z(D) = <t> and let A be a Sylow 3-subgroup of H inverted by t. Then H = <D,A>. If Q_0 is the unique quaternion subgroup of $C_G(t)$ then Q normalizes D and also Q normalizes A (lemma (6.1)). Therefore $Q \leq N_G(H)$ and as G is simple we must have $N_G(H) = HQ$ which has index 11.

Finally we can identify G.

THEOREM

If G is a group satisfying the assumptions of this chapter then G is isomorphic to M_{11}.

PROOF

By the previous lemma G has a subgroup of index 11. Representing G on the cosets of this subgroup then, as G is simple, G is isomorphic to a subgroup of A_{11}.

By the structure of the normalizers of a Sylow 5 and Sylow 11-subgroup of G, we see that G possesses elements r, m and n of orders 11, 5 and 4 respectively satisfying the relations

$$r^m = r^4 \text{ and } m^n = m^2.$$

We may suppose

$$r = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11)\ ;$$

then $r^4 = (1\ 5\ 9\ 2\ 6\ 10\ 3\ 7\ 11\ 4\ 8)$

and we may assume

$$m = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 5 & 9 & 2 & 6 & 10 & 3 & 7 & 11 & 4 & 8 \end{pmatrix}$$

$$= (2\ 5\ 6\ 10\ 4)(3\ 9\ 11\ 8\ 7)$$

since then $r^m = r^4$ as required.

Let $n = \begin{pmatrix} 2 & 5 & 6 & 10 & 4 & 3 & 9 & 11 & 8 & 7 \\ a_1 & a_2 & a_3 & a_4 & a_5 & b_1 & b_2 & b_3 & b_4 & b_5 \end{pmatrix}$

then $m^n = (a_1\ a_2\ a_3\ a_4\ a_5)(b_1\ b_2\ b_3\ b_4\ b_5)$,
which then equals $m^2 = (2\ 6\ 4\ 5\ 10)(3\ 11\ 7\ 9\ 8)$.

Therefore $(a_1\ a_2\ a_3\ a_4\ a_5) = (2\ 6\ 4\ 5\ 10)$ or $(3\ 11\ 7\ 9\ 8)$

and $(b_1\ b_2\ b_3\ b_4\ b_5) = (3\ 11\ 7\ 9\ 8)$ or $(2\ 6\ 4\ 5\ 10)$

(Note that if $(a_1\ a_2\ a_3\ a_4\ a_5) = (2\ 6\ 4\ 5\ 10)$ then $(a_1\ a_2\ a_3\ a_4\ a_5) = (6\ 4\ 5\ 10\ 2)$ or any other cycle of these five numbers).

If $(a_1\ a_2\ a_3\ a_4\ a_5) = (3\ 11\ 7\ 9\ 8)$

and $(b_1\ b_2\ b_3\ b_4\ b_5) = (2\ 6\ 4\ 5\ 10)$; then considered as ordered 5-tuples there are 5 choices for $(a_1\ a_2\ a_3\ a_4\ a_5)$ and 5 for $(b_1\ b_2\ b_3\ b_4\ b_5)$ which implies 25 possibilities for n. However in all these cases n is an odd permutation. Thus

$(a_1\ a_2\ a_3\ a_4\ a_5) = (2\ 6\ 4\ 5\ 10)$

and $(b_1\ b_2\ b_3\ b_4\ b_5) = (3\ 11\ 7\ 9\ 8)$

(considered as permutations).

There are 25 choices for n. However for a fixed n, conjugating by powers of m yields all the elements of order 4 in $N_G(\langle m\rangle)$ taking m to m^2, so in fact there are only 5 cases to consider.

Fix $b_1 = 3$ then the ordered 5-tuple $(b_1\ b_2\ b_3\ b_4\ b_5)$ is determined. Successively take $a_1 = 2, 6, 4, 5$ and 10 so$(a_1\ a_2\ a_3\ a_4\ a_5)$ is determined; this yields all 5 cases, which we list:

(a) $n = (4\ 10\ 5\ 6)(7\ 8\ 9\ 11)$

(b) $n = (2\ 6\ 5\ 4)(7\ 8\ 9\ 11)$

(c) $n = (2\ 4\ 6\ 10)(7\ 8\ 9\ 11)$

(d) $n = (2\ 5\ 10\ 6)(7\ 8\ 9\ 11)$

(e) $n = (2\ 10\ 4\ 5)(7\ 8\ 9\ 11)$

CASE (a)

Let $n_1 = n^{m^2} = (2\ 10\ 4\ 5)(3\ 8\ 7\ 9)$, then $rn_1 = (1\ 10\ 11)(2\ 8\ 3\ 5\ 6\ 9\ 4)(7)$, which has order 21. However G does not contain an element of order 21 thus $n \neq (4\ 10\ 5\ 6)(7\ 8\ 9\ 11)$.

CASE (b)

Let $n_1 = n^{m^2} = (3\ 8\ 7\ 9)(4\ 10\ 5\ 6)$, then $rn_1 = (1\ 2\ 8\ 3\ 10\ 11)(4\ 6\ 9\ 5)(7)$ which has order 12 and as G does not contain an element of this order $n \neq (2\ 6\ 5\ 4)(7\ 8\ 9\ 11)$.

CASE (c)

Let $n_1 = n^{m^2} = (2\ 6\ 5\ 4)(3\ 8\ 7\ 9)$ then $rn_1 = (1\ 6\ 9\ 10\ 11)(2\ 8\ 3)(4)(5)(7)$ which has order 15 so $n \neq (2\ 4\ 6\ 10)(7\ 8\ 9\ 11)$.

CASE (d)

Let $n_1 = n^m = (3\ 7\ 11\ 8)(4\ 10\ 5\ 6)$. By lemma (1.9)(ii) the subgroup of G generated by r and n_1 is isomorphic to M_{11} and as $|G| = |M_{11}|$, $G \cong M_{11}$.

CASE (e)

Let $n_1 = n^m = (2\ 6\ 5\ 4)(3\ 7\ 11\ 8)$, then $rn_1 = (1\ 6\ 11)(2\ 7\ 3)(4)(5)(8\ 9\ 10)$ which has order 3. Thus the following relations hold between r, m and n_1.

$$r^{11} = m^5 = {n_1}^4 = (rn_1)^3 = 1,$$

$$r^m = r^4 \text{ and } m^{n_1} = m^2.$$

Therefore by lemma (1.9)(i) the subgroup of G generated by r, m and n_1 is isomorphic to M_{11} and hence G is isomorphic to M_{11}. This completes the proof of the theorem.

BIBLIOGRAPHY

[1] Bender, H. : Finite groups with large subgroups. Ill. Jour. Math., 18 (1974) 223 - 228.

[2] Brauer, R. : On the structure of groups of finite order., Proc. Internat. Congr. Math. Amsterdam 1954, I. 209 - 217 (Noordhoff/N. Holland, 1957).

[3] Brauer, R. : On finite Desarguesian planes, I. Math. Zeit., 90 (1965) 117 - 123.

[4] Brauer, R. : On finite Desarguesian planes, II. Math. Zeit., 91 (1966) 124 - 151.

[5] Brauer, R., and Fowler, K.A. : On groups of even order. Ann. Math., 62 (1955) 565 - 583.

[6] Brauer, R., Suzuki, M., and Wall, G.E. : A characterization of the one-dimensional unimodular groups over finite fields. Ill. Jour. Math., 2 (1958), 718 - 745.

[7] Carmichael, R.D. : Groups of finite order. Dover publications Inc. (1956).

[8] Coxeter, H.S.M., and Moser, W.O.J. : Generators and relations for discrete groups. Springer - Verlag (Berlin, Heidelberg, New York 1980).

[9] Dickson, L.E. : Linear groups with an exposition of the Galois field theory, 1901, Dover (New York, 1958).

[10] Feit, W., and Thompson, J.G. : Solvability of groups of odd order. Pac. Jour. Math., 13 (1963), 775 - 1029.

[11] Fowler, K.A. : Thesis, University of Michigan (1951).

[12] Gorenstein, D. : Finite groups. Chelsea publishing company (New York, 1980).

[13] Huppert, B., and Blackburn, N. : Finite groups III Springer - Verlag (Berlin, Heidelberg, New York, 1982).

[14] Janko, Z. : A new finite simple group with abelian Sylow 2-subgroups and its characterization. Jour. Alg. 3 (1966) 147 - 186.

[15] Passman, D.S. : Permutation groups. W.A. Benjamin, Inc. (New York, Amsterdam, 1968).

[16] Stanton, R. : The Mathieu groups Can. Jour. Math 3 (1951) 164 - 174.

[17] Suzuki, M. : On characterizations of linear groups I, II. Trans. Amer. Math. Soc. 92 (1959) 191 - 219.

[18] Wielandt, H. : Beziehungen zwischen den Fixpunktzahlen von Automorphismengruppen einer endlichen Gruppe, Math. Zeit., 73 (1960), 146 - 158.

[19] Wong, W.J. : A characterization of the Mathieu group M_{12}. Math. Zeit., 84 (1964) 378 - 388.