CONTENTS

	Page
Abstract	i-ii
Acknowledgements	iii
Notation	iv
Introduction	v-vi
CHAPTER ONE	
Section 1(Statement of Theorem A)	1
Section 2(Some known results)	3
Section 3(Known results about linear groups)	10
Section 4(Methods from modular representation theory)	19
Section 5(Minimal polynomials of elements of prime order)	36
Section 6(Three useful lemmas)	41
CHAPTER TWO	
Section 1(Some preliminary results)	55
Section 2(On the Sylow 11-normaliser)	70
Section 3(On groups of degree 2q)	76
Section 4(C(x), for x of order 5 in N(P))	97
Section 5(Rationality implications)	104
Section 6(On the Sylow 5-subgroups)	118
Section 7(Properties of local subgroups)	133
Section 8(Relationship between 5 and 7)	138
CHAPTER THREE	
Section 1($\|S\| \neq 25$, for S a Sylow 5-subgroup)	149
Section 2($\|S\| \neq 125$)	207

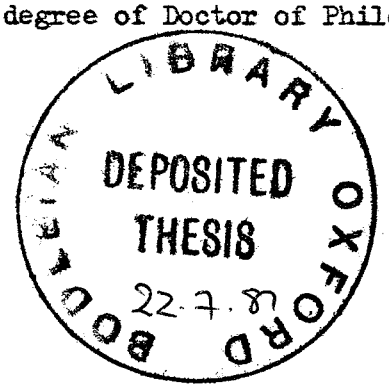
CHAPTER FOUR	Page
Section 1($[N(S):C(S)] \neq 2$)	235
Section 2($C(S) \neq S$)	259
Section 3(Either 7 divides $\|G\|$ or $\|C(S)\|$ is even)	275
Section 4(On the principal 5-block)	290
Section 5(7 divides $\|G\|$)	339
Section 6(The order of a Sylow 7-subgroup)	370
Section 7(The final contradiction)	389
REFERENCES	442-444

SOME PROBLEMS IN THE CHARACTER THEORY OF FINITE GROUPS.

Geoffrey Raymond Robinson, Worcester College.

A Thesis submitted for the degree of Doctor of Philosophy

Hilary Term, 1981.



ABSTRACT.

The main aim of this thesis is to determine the structure of the finite irreducible complex linear groups of degree 11. Some results of David Sibley allow us to concentrate our efforts on finite complex irreducible linear groups of degree 11 which have Abelian Sylow 11-subgroups.

We prove the following:-

THEOREM

Let G be a finite irreducible complex linear group of degree 11 with Abelian Sylow 11 subgroups. Then either

a) G has an Abelian normal subgroup A such that G/A is isomorphic to a transitive permutation group of degree 11,

or

b) $G' \cap Z(G) = 1$, $[G : G' \times Z(G)] \leq 2$, and G' is isomorphic to one of the following groups:

1) A_{12},

2) M_{11},

3) M_{12},

4) PSL(2,11),

5) PSL(2,23),

6) PSU(5,2).

In view of Sibley's results, and the above theorem, the structure of all finite complex irreducible linear groups of degree 11 is now known.

ACKNOWLEDGEMENTS

I am pleased to have this opportunity to thank my supervisor Michael J. Collins for his patience during the past few years, and for the encouragement and help I have received from him.

I also wish to thank Professor George Glauberman for the help and encouragement he gave me during the time he supervised me in the two-term absence of Dr. Collins, and the continued support he has given me since then.

Most of this work was completed while I was in receipt of SRC Research Studentship No: B/76/307744.

NOTATION

Our notation will largely follow that of Gorenstein's book [14], except that we occasionally will omit subscripts if it is clear which group we are working in, e.g. we might write C(s) instead of $C_G(s)$ for the "centralizer in G of s".

We will also frequently use the generalized Fitting subgroup, which does not appear in [14]. The generalized Fitting subgroup of the finite group G is denoted by F*(G) and is defined by the equation $F^*(G)=F(G)E(G)$, where F(G) is the ordinary Fitting subgroup of G, and E(G) is the central product of all quasi-simple subnormal subgroups of G.

Unless it is explicitly stated to the contrary, all groups considered in this thesis are finite. On page 15 $\pi(n)$ denotes the number of primes less than or equal to n.

INTRODUCTION

Ever since the representation theory of finite groups began, there has been some interest in determining the structure of the finite subgroups of $GL(n,\mathbb{C})$ for small values of n. C. Jordan demonstrated the existence of a function f such that for any n, each finite subgroup of $GL(n,C)$ has an Abelian normal subgroup of index at most $f(n)$. Frobenius and Blichfeldt obtained specific bounds, but there has been little improvement on the bound obtained by Blichfeldt.

The finite irreducible subgroups of $GL(n,C)$ were determined early in this century for $n \leq 4$ ($n=4$ being handled by Blichfeldt). From that time until 1965, little progress was made in this area. In 1965, R.Brauer determined the primitive irreducible subgroups of $GL(5,C)$. Brauer's theory of characters was very useful for this result.

Since that time, further progress has been made. John Lindsey determined the quasi-primitive finite irreducible subgroups of $GL(6,C)$ (a definition of quasi-primitive is given later in this thesis). Among the groups he found was a central extension of the Hall-Janko simple group of order 604 800, which had only been discovered shortly before that time.

David Wales determined the primitive irreducible subgroups of $GL(7,C)$, and Wales, W.C.Huffman and W.Feit

between them have determined the structure of the quasi-primitive irreducible subgroups of $GL(8,\mathbb{C})$ and $GL(9,\mathbb{C})$.

Feit also made some progress on the determination of the finite quasi-primitive subgroups of $GL(10,\mathbb{C})$. Using completely different methods, Feit determined the structure of the finite irreducible subgroups of $GL(11,\mathbb{Q})$.

In this thesis, we complete the determination of the structure of the finite irreducible subgroups of $GL(11,\mathbb{C})$. We also prove some results which may be of use in the study of complex linear groups in general.

The proof of our main theorem uses methods from many areas of finite group theory, and occasionally we prove results which might be of interest in a wider context.

Chapter One

Section One

First ,we state the main theorem to be proved in this thesis.

Theorem A

Let G be a finite irreducible complex linear group of degree 11 with Abelian Sylow 11-subgroups.

Then $G' \cap Z(G) = 1$, and one of the following occurs:

a) G has an Abelian normal subgroup A such that G/A is isomorphic to a transitive permutation group of degree 11.

b) $[G : G' \times Z(G)] \leq 2$, and G' is isomorphic to one of the following groups:

i) PSL(2,23) (order $2^3 .3.11.23$).

ii) PSL(2,11) (order 660).

iii) M_{11} (order 7920).

iv) M_{12} (order 95040).

v) A_{12} (order $2^9 .3^5 .5^2 .7.11$).

vi) PSU(5,2) (order $2^{10} .3^5 .5.11$).

The proof of this theorem

completes the classification of all finite irreducible complex linear groups of degree 11 , as the results of D.Sibley in [25] determine the structure of all finite irreducible complex linear groups of degree 11 which do not have Abelian Sylow 11-subgroups.

We need to make a definition before we proceed any further.

Definition

An irreducible representation R of a finite group H is primitive if R is not equivalent to any representation induced from a representation of a proper subgroup of H.

An irreducible representation R of a finite group H is quasi-primitive if for any normal subroup N of H, $R|_N$ is the sum of equivalent irreducible representations of N.

By Clifford's theorem, a primitive representation is quasi-primitive. We can, of course, speak of primitive and quasi-primitive finite linear groups in view of this definition.

We note that in a quasi-primitive linear group , every Abelian normal subgroup is contained in the centre. We also note that every irreducible representation of a quasi- simple group is quasi-primitive.

Section 2:Some Known Results

In this section,we state some known results which will frequently be required ,and may occasionally be quoted without reference.

Lemma 1.2.1 (Feit-Thompson, [12])

Let H be a finite complex linear group of degree d ; let p be a prime divisor of $|H|$.

Then if $p > 2d+1$, H has an Abelian normal Sylow p-subgroup.

Lemma 1.2.2 (Brauer, [4])

Let H be a finite complex linear group of degree $\frac{p-1}{2}$, where p is a prime divisor of $|H|$.

Then, unless $H/Z(H)$ is isomorphic to $PSL(2,p)$, H has an Abelian normal Sylow p-subgroup.

Lemma 1.2.3 (Hayden, [16])

Let H be a finite complex linear group of degree $\frac{p+1}{2}$, where p is a prime divisor of $|H|$ and $p > 7$.

Then, unless $H/Z(H)$ is isomorphic to $PSL(2,p)$, H has an Abelian normal Sylow p-subgroup.

Lemma 1.2.4 (Feit, [8])

Let H be a finite complex linear group of degree n. Let p be a prime divisor of $|H|$ with $p > n+1$, and let P be a Sylow p-subgroup of H.

Then P is Abelian and $[P:O_p(H)] \leq p$. Furthermore, there is at most one prime $q > n+1$ for which H does not possess a normal Sylow q-subgroup.

Lemma 1.2.5 (Feit)

Let H be a finite irreducible complex linear group of degree $p-2$, where p is a prime divisor of $|H|$.

Then, unless p is a Fermat prime and $H/Z(H)$ is isomorphic to $SL(2,p-1)$, H has a normal Sylow p-subgroup.

Lemma 1.2.6 (Lindsey, [20])

Let H be a quasi-primitive complex linear group of degree p-1 , where p is the largest prime divisor of H and $p \geq 7$.

Then a Sylow p-subgroup, P, of H is Abelian , and $[P:O_p(H)] \leq p$.

Lemma 1.2.7 (Sibley, [26])

Let H be a finite irreducible complex linear group of degree n and let A be an Abelian p-subgroup of H such that $C(a) = AZ(H)$ for every non-identity element of A.

Then, unless A is normal in H,

$$n \geq \frac{|A| - 1}{2} .$$

Lemma 1.2.8 (Sibley, [25])

Suppose that H is a finite irreducible complex linear group of prime degree $p \geq 5$.

Then $[H:O_p(H)]$ is not divisible by p^2.

Lemma 1.2.9 (Rigby , [23])

Let H be a finite irreducible quasi-primitive complex linear group of degree n. Let p be a prime divisor of the order of H and Q be a normal

p-subgroup of H.

Then Q = ZE ,where Z $\leq$Z(H) and either E=1 or else E is an extra-special p-group.Furthermore , E has order p^{2k+1} where p^{k} divides n.

Lemma 1.2.10 (Shult,[24])

Let x be an automorphism of prime order q of the finite q'-group,A. . Suppose that the semi-direct product A<x> acts faithfully on some finite-dimensional complex vector space V.

Then the minimum polynomial of x on V is $X^{q}-1$ unless q is a Fermat prime , in which case the minimum polynomial is either $X^{q}-1$ or $\frac{X^{q}-1}{X-1}$.

Lemma 1.2.10 yields an easy proof of the following result.

Lemma 1.2.11 (Ito)

Let G be a finite p-soluble complex linear group of degree n for a prime p dividing the order of G.

Then if n < p and p is not a Fermat prime, a Sylow p-subgroup of G is

normal in G.

Furthermore, if $n < p-1$, and p is a Fermat prime, then G has a normal Sylow p-subgroup.

Before we state the next result, we need to define some terms.

Let G be a finite group, X be a character of G, and p be a prime divisor of $|G|$. Let β be a primitive $|G|_{p'}$-th root of unity and let $K=Q(\beta)$.

We say that X requires the p^a-th roots of unity if there is an element g of G such that $X(g)$ is not contained in $K(w)$, where w is a primitive p^{a-1}-th root of unity.

The next result is due to Blichfeldt, but for a shorter proof due to Brauer, see [7].

Lemma 1.2.12

Let G be a finite group, X be an irreducible character of G, and let $p_1, p_2, \ldots, p_n$ be the prime divisors of the order of G.

For $1 \le i \le n$, assume that X requires the $p_i^{a_i}$-th roots of unity.

Then G contains an element of order $p_1^{a_1} p_2^{a_2} \ldots\ldots p_n^{a_n}$.

Lemma 1.2.13 (Schur).

Let p be a prime ,and P be a finite p-group of order p^a , which has a faithful rational-valued character of degree n.

Then $a < \frac{np}{(p-1)^2}$.

Lemma 1.2.14 (Feit, [1])

Let H be a finite group, let p and q be distinct prime divisors of H .

Let x be a q-element of H which commutes with no p-element of H, and let P be a Sylow p-subgroup of H.

Let $B^{(p)}$ be a p-block of ordinary irreducible characters of H and let $B^{(q)}$ be any q-block of ordinary irreducible characters of H .

Then if $B^{(p)} \cap B^{(q)}$ is non-empty,

$$\sum_{X \in B^{(p)} \cap B^{(q)}} X(x)X(1) \equiv 0 \pmod{|P|}$$

In particular, there is a non-trivial irreducible character of H which lies in both the principal p-block and the principal q-block of H.

Lemma 1.2.15 (Brauer)

Let H be a finite non-Abelian simple group whose order is divisible by the prime p.

Then no non-trivial irreducible character of the principal p-block of H can have a degree which is a power of p.

Lemma 1.2.16 (J.S.Leon ,[19])

Let H be a finite simple group of order $2^a 3^b p^2$,where p is a prime Let P be a Sylow p-subgroup of H.

Then,unless P is the centralizer of each of its non-identity elements H contains a Sylow p-intersection of order p.

Lemma 1.2.17

Let G be a finite simple group whose order is of the form $2^a.3^b.5$.

Then G is isomorphic to one of the following groups:

$$A_5 , A_6 , \text{or } Sp_4(3).$$

For the sake of completeness we include the following well-known result which is due to Burnside.

Lemma 1.2.18

Let H be a finite group, X be a complex irreducible character of H and y be an element of H.

Suppose that $[H:C_H(y)]$ and $X(1)$ are relatively prime.

Then either $X(y)=0$ or $[H,y] \leq \ker X$.

Section Three

In this section, we collect some known results about complex linear groups of small degree and related topics.

We first state some known results on complex linear groups of degree eleven or less.

Lemma 1.3.1

Let H be a finite irreducible complex linear group of degree two.

Then $H/Z(H)$ is isomorphic to one of the following groups :

a) A_5 ($Z(H) \neq 1$).

b) A_4 ($Z(H) \neq 1$).

c) S_4 . ($Z(H) \neq 1$).

d) A dihedral group.

Lemma 1.3.2

Let H be a finite irreducible complex linear group of degree three which is not soluble. Then H/Z(H) is isomorphic to one of the following groups:

a) A_5.
b) A_6 (Z(H) ≠ 1 in this case).
c) PSL(2,7).

Lemma 1.3.3 (Blichfeldt,[3])

Let H be a finite irreducible quasi-simple complex linear group of degree 4 . Then H/Z(H) is isomorphic to one of the following groups:

a) A_5.
b) PSU(4,2) (Z(H) ≠ 1) .
c) A_6 (Z (H) ≠ 1) .
d) A_7 (Z(H) ≠ 1) .
e) PSL(2,7) (Z(H) ≠ 1).

Lemma 1.3.4 (Brauer, [5])

Let H be a finite irreducible primitive complex linear group of degree 5. Then H/Z(H) is isomorphic to one of the following groups:

a) A_5.

b) S_5.

c) A_6.

d) S_6.

e) PSU(4,2).

f) PSL(2,11)

g) The semi-direct product of a subgroup of GL(2,5) with $Z_5 \times Z_5$.

Lemma 1.3.5 (Lindsey, [20])

Let H be a finite irreducible quasi-primitive complex linear group of degree 6 such that 35 divides [H:Z(H)] . Then H/Z(H) is isomorphic to one of the following groups.

i) The Hall-Janko simple group of order 604,800. (Z(H) has even order in this case).

ii) PSL(3,4) (6 divides |Z(H)|).

iii) PSU(4,3) (6 divides |Z(H)|).

iv) A_7.

v) S_7.

Lemma 1.3.6 (Wales, [28])

Let H be a finite irreducible primitive complex linear group of degree 7 which has Abelian Sylow 7-subgroups.

Then H is isomorphic to one of the following groups:

a) A_8.

b) $PSL(2,13)$.

c) $Sp(6,2)$.

d) $PSL(2,7)$.

e) $SL(2,8)$.

f) $PSU(3,3)$.

Lemma 1.3.7 (Feit, [9])

Let H be a finite irreducible quasi-primitive complex linear group of degree 8.

Suppose that $|H|$ is divisible by 35 and that $Z(H)=1$.

Then $E(H)$ is isomorphic to A_9.

Lemma 1.3.8 (Feit, [9])

Let H be a finite irreducible quasi-primitive complex linear group of degree 10.

Then $[H:Z(H)]$ is divisible by no

prime apart from 2,3,5,7 or 11.

Furthermore if 7 divides [H:Z(H)] then each composition factor of H is a known simple group , whilst if 11 divides [H:Z(H)] and $O_5(H) = 1$, then every composition factor of G is a known simple group.

Lemma 1.3.9 (Feit,[10])

Let H be a finite group with a faithful,rational valued,irreducible character of degree 11.

Then H has a subgroup of index 11 or 12.

We next state some more general results about complex linear groups of arbitrary degree.

One of the first and best known results was stated by Blichfeldt for primitive linear groups , but as the proof given in [7] shows , is valid for quasi-primitive linear groups.

Lemma 1.3.10

Let H be a finite irreducible quasi-primitive complex linear group

Let x be an element of H,and

suppose that x has some eigenvalue such that all other eigenvalues of x lie within 60^{o} of it on the unit circle.

Then x belongs to the centre of H.

Lemma 1.3.10 has the following well-known consequence:

Lemma 1.3.11

Let H be a finite complex linear group of degree n.

Then H has an Abelian normal subgroup A such that :

$$[H:A] \leq n!\, 6^{(n-1)\{1+\pi(n)\}}.$$

A less well known result than Lemma 1.3.10 is sometimes useful when considering the structure of Sylow p-subgroups of complex linear groups for primes $p \leq 5$.

Lemma 1.3.12 (Brauer, [5])

Let H be a finite irreducible primitive complex linear group of degree n, let p be a prime divisor of the order of H.

Then for any Abelian p-subgroup A, of H, $[A:A \cap Z(H)] \leq p^{n-1}$.

The next few results concern the structure of complex linear groups which contain an element with a very large eigenspace.

Lemma 1.3.13 (Mitchell, [21])

Let H be a finite irreducible quasi-primitive complex linear group of degree $n \geq 8$.

Suppose that H-Z(H) contains an element x of prime order p which has an eigenspace of co-dimension 1.

Let $M = \langle x^h : h \text{ belongs to } H \rangle$. Then $M/Z(M)$ is isomorphic to S_{n+1}.

The next result is a special case of a result of Huffman and Wales, and relies ultimately on deep results of Aschbacher.

Lemma 1.3.14 (Huffman-Wales, [29])

Let H be a finite irreducible quasi-primitive complex linear group of degree $n \geq 11$ which contains an involution t with an eigenspace of co-dimension two.

Let $M = \langle t^h : h \text{ belongs to } H \rangle$. Then $M / Z(M)$ is isomorphic to A_{n+1}.

Lemma 1.3.15 (Huffman , [17])

Let H be a finite irreducible quasi-primitive complex linear group of degree $n \geq 9$ containing an element x of order three with an eigenspace of co-dimension two . Let M be the subgroup of H which is generated by the conjugates of x.

Then $M/Z(M)$ is isomorphic to A_{n+1}.

Lemma 1.3.16 (Huffman, [17])

Let H be a finite irreducible quasi-primitive complex linear group of degree $n \geq 5$.

Then H cannot contain an element of order four with an eigenspace of co-dimension two.

Lemma 1.3.17 (Lindsey, [20])

Let H be a finite irreducible quasi-primitive complex linear group of degree $n \geq 6$.

Then H cannot contain an element of order five with an eigenspace of co-dimension two.

Lemma 1.3.18 (Huffman-Wales, [19])

Let H be a finite irreducible quasi-primitive complex linear group of degree n , let p (≥7) be a prime.

Then H cannot contain an element of order p with an eigenspace of co-dimension two.

The following result is often useful and is originally due (again) to Blichfeldt.

Lemma 1.3.19

Let H be a finite complex linear group considered as a subgroup of GL(V) for some finite-dimensional complex vector space V.

Suppose that x,y are elements of H , each having only two distinct eigenvalues on V.Let M = $\langle x, y \rangle$.

Then V may be written as a direct sum of M-invariant subspaces,each of which is one- or two-dimensional.

Section Four

In this section ,we discuss ways in which results from modular representation theory can be applied to obtain information about finite complex linear groups.

Let H be a finite irreducible complex linear group of degree n.

By a suitable choice of basis we may consider H as a subgroup of GL(n,F) , where F is an extension of finite degree of the rationals.

Let R be the ring of algebraic integers in F , p be a prime divisor of the order of H , and let $\mathfrak{p}$ be a prime ideal of R containing p.

Then F has a subring $R_{\mathfrak{p}}$,which is a principal ideal domain properly containing R , with the following property:

$R_{\mathfrak{p}}$ has a unique prime ideal,P say and $R_{\mathfrak{p}}$ / P is isomorphic to $R/\mathfrak{p}$..

We let K = $R_{\mathfrak{p}}$ / P.Of course, K is a finite field of characteristic p.

As R itself is not ,in general, a principal ideal domain , we cannot generally regard H as a subgroup of GL(n,R) .As $R_{\mathfrak{p}}$ is a principal ideal

domain whose field of fractions is F we can regard H as a subgroup of $GL(n,R_{\mathfrak{p}})$ after a suitable choice of basis . We may assume that F is a splitting field for H.

By taking residues (mod P) , we obtain a homomorphism from H into a subgroup of the finite group GL(n,K)

The kernel of this homomorphism is a p-group , a fact which we will not prove here ,as it is well-known, (although it is implicit in some of the arguments of Section Five).

We refer to the image of H under this homomorphism as a reduction of H (mod p).

There is a p-adic valuation n_P defined on F in terms of $\mathfrak{p}$ and it is sometimes necessary to work with the p-adic completion of $R_{\mathfrak{p}}$ to obtain results from modular representation theory.

Let x be a p-element of H , and let $\bar{x}$ denote the image of x under the above homomorphism . Then as K is a field of characteristic p, we certainly have: $(\bar{x} - 1)^n = 0$.

Now let k be the smallest

integer such that $p^k \geq n$.

Then $(\bar{x}^{p^k} - 1) = (\bar{x} - 1)^{p^k} = 0$ so that the order of $\bar{x}$ divides p^k. As the kernel of the above homomorphism is a p-group, $xO_p(H)$ has order at most p^k in $H/O_p(H)$.

If we could prove that the minimum polynomial of $\bar{x}$ had degree less than n, we might be able to obtain better estimates for the order of $\bar{x}$.

The next few results are concerned with methods for exploiting this simple observation.

The first two results are quoted from Feit [1].

Lemma 1.4.1

Let H be a finite irreducible complex linear group of degree n, and let p be a prime divisor of $|H|$.

Suppose that H has a cyclic Sylow p-subgroup P, and that Q is the unique subgroup of order p of P.

Then if $n \leq \frac{|P| - 1}{2}$, $N(Q)$ is also irreducible.

Lemma 1.4.2

Let H be a finite irreducible complex linear group of degree n, and let p be a prime divisor of $|H|$.

Let P be a Sylow p-subgroup of H, and let M be a proper subgroup of H which contains N(P).

Then, unless M is also irreducible there is some h in H-M such that:

$$[\, P : P \cap P^{h} \,] \leq n^{2}.$$

The next result, which utilises the methods of [11], evolved from an idea of Professor Glauberman, and my proof owes a great deal to that idea. Part of the proof is a special case of Theorem A1.6 in [22]. The proof also uses some of the central ideas in [11].

Lemma 1.4.3

Let H be a finite irreducible complex linear group of degree n.

Let p be a prime divisor of $|H|$, x be an element of order p in H, and let S be a Sylow p-subgroup of H containing x.

Let Q be the weak-closure of

x in S with respect to H , and let M be the normalizer in H of Q.

Suppose that the image of x under some reduction (mod p) acts with minimum polynomial of degree $k > 1$.

Then we have:

a) If $k \leq \frac{p-1}{2}$, M is irreducible.

b) If $k \leq \frac{p+1}{4}$ and H is quasi-primitive, then M is also quasi-primitive.
In particular , Q is extra-special and $Z(Q) \leq Z(H)$, so that $Op(H) \neq 1$.

c) If $k \leq \frac{p+5}{8}$,and H is quasi-primitive then $M = H$,so that x lies in $Op(H)$.

Proof

As in the previous discussion,we may consider H to be acting on some $R_{\mathfrak{p}}H$-module , V say , where $R_{\mathfrak{p}}$ is a principal ideal domain having only one prime ideal ,P say, and $R_{\mathfrak{p}}/P$ is a finite field of characteristic p.

In case a) , we define W to be $V \otimes V^*$,in case b) we define W to be $V \otimes V^* \otimes V \otimes V^*$, and in case c) we define W to be :

$$V \otimes V^* \otimes V \otimes V^* \otimes V \otimes V^* \otimes V \otimes V^*.$$

We first claim that in each case $C_W(H) = C_W(M)$.

Let $y_1 \ldots\ldots\ldots y_r$ be a set of representatives for the right cosets of M in H.

Then we may define a homomorphism of Rp-modules, Θ, from $C_W(M)$ to $C_W(H)$ by letting $v\Theta = vy_1 + vy_2 \ldots\ldots + vy_r$ for each v in $C_W(M)$.

It is not difficult to see that the definition of Θ does not depend on the particular choice of coset representatives.

To prove that $C_W(M) = C_W(H)$, it suffices to prove that the kernel of Θ is trivial.

Suppose then that this is not the case. Let $K = Rp/P$, and let $\overline{W}$ be the KH-module obtained from W by taking residues (mod P).

We may choose an element $w \neq O$ of $C_W(M)$ with $w\Theta = O$. In fact, w may be chosen so that $\overline{w} \neq O$, for if $w = \begin{bmatrix} w_1 \\ \cdot \\ \cdot \\ w_n \end{bmatrix}$

and i is chosen so that $n(w_i)$ is minimal, then $w_i^{-1} w$ lies in $C_W(M)$ (where w_i^{-1} is the multiplicative inverse of w_i in the complex field), and has a non-zero image (mod P).

We now derive a contradiction to the assumption that such a w exists by proving that, under the hypotheses of the Lemma, $\overline{w\emptyset} = \overline{w}$, whereas $\overline{w} \neq 0$ and $w\emptyset = 0$ by choice of w.

We first claim that $\overline{W}(x-1)^{p-1} = 0$ in each case. This follows from the hypotheses and repeated applications of the fact that if V_1, V_2 are finite dimensional vector spaces and T acts as a linear transformation of each of them, with respective minimum polynomials $(X-1)^s$ and $(X-1)^t$, then T has minimum polynomial $(X-1)^{s+t-1}$ as a linear transformation of $V_1 \otimes V_2$.

We may write $H = Mz_1Q \cup \ldots \cup Mz_jQ$ where $z_1 \ldots z_j$ are a complete set of (M,Q) double-coset representatives for H and, without loss of generality, $z_1 = 1_H$.

We note that for $i \geq 2$, $Mz_i Q \neq Mz_i$.

For if $Mz_i Q = Mz_i$, then $z_i Q z_i^{-1} \leq M$,

so for some m in M, we have :

$mz_i Q (mz_i)^{-1} \leq S$. By definition of Q,

$mz_i Q (mz_i)^{-1} = Q$, so that mz_i belongs

to $N(Q)$ $(= M)$. Thus z_i belongs to M,

and $i=1$.

We next claim that for $i \geq 2$, we may choose a conjugate x_i of x, lying in Q, such that :

$$Mz_i Q = \bigcup_{s=1}^{q_i} \bigcup_{t=0}^{p-1} M b_s x_i^t$$

We note that the double coset $Mz_i Q$ is simply the orbit containing the coset Mz_i under the action of Q by right translation on the right cosets of M in H.

By definition of Q, it is generated by conjugates of x. As Q acts transitively on $Mz_i Q$, there is a conjugate x_i of x, which fixes no right M-coset in $Mz_i Q$ (for let Q_i be a point-stabilizer, and let K be a maximal subgroup of Q containing Q_i. Then K contains all Q-conjugates of Q_i, so that no element outside K can

fix a point in this action. As K is a proper subgroup of Q, some conjugate of x, say x_i, lies outside K .).

Now we simply let q_i be the number of orbits of x_i on $Mz_i Q$, and, for $1 \le s \le q_i$, let b_{is} be a right-coset representative for one of the right cosets of M in the s-th orbit.

We recall that we have chosen an element w with $w\emptyset = 0$, $\bar{w} \neq 0$ and we wish to derive a contradiction by proving that $\overline{w\emptyset} = \bar{w}$.

Now for $2 \le i \le j$, the contribution to $\overline{w\emptyset}$ from the double coset $Mz_i Q$ is given by :

$$\sum_{s=1}^{q_i} \sum_{t=0}^{p-1} \bar{w}\, \bar{b}_{is}\, \bar{x}_i^{\,t}$$

$$= \sum_{s=1}^{q_i} \bar{w}\, \bar{b}_{is}\, (1-\bar{x}_i)^{p-1} = 0,$$ because

$\bar{w}(1-\bar{x}_i)^{p-1} = 0$, and for $1 \le i \le j$, x_i is conjugate to x in H.

Thus only the double coset $Mz_1 Q$ can make a non-zero contribution to $\overline{w\emptyset}$, and as $Mz_1 Q = M$, the contribution from $Mz_1 Q$ is just $\overline{w z_1} = \bar{w}$.

Thus $\overline{w\emptyset} = \bar{w}$, the required contradiction.

Hence $C_W(M) = C_W(H)$.

Now we may regard W as a vector space of dimension n over F, the field of fractions of Rp, and then as a complex vector space of dimension n, and we still have $C_W(M) = C_W(H)$.

Let X be the complex irreducible character of H afforded by the given representation of H.

Case i)

In this case, $\dim_{\mathbb{C}}(C_W(H)) = \|X\|$ and $\dim_{\mathbb{C}}(C_W(M)) = \|X|_M\|$, so that $1 = \|X\| = \|X|_M\|$, and $X|_M$ is irreducible, so proving i).

Case ii)

Certainly condition ii) implies condition i), so that M is irreducible

To prove that M is quasi-primitive we need to prove that whenever N is a normal subgroup of M, all irreducible constituents of $X|_N$ are equivalent.

Let N be such a subgroup. We claim that $C_{V \otimes V^*}(N)$ is H-invariant.

The condition $C_W(M) = C_W(H)$ tells us in this case that :

$$\|X\bar{X}\| = \|(X\bar{X})|_M\|,$$

which implies that every irreducible constituent of $X\bar{X}$ has an irreducible restriction to M.

Thus each irreducible constituent of $X\bar{X}|_M$ which contains N in its kernel is a restriction of an irreducible constituent of $X\bar{X}$ containing N in its kernel.

Let L be the intersection of the kernels of all irreducible constituents of $X\bar{X}$ which contain N in their kernels. Then L is a normal subgroup of H which contains N.

By definition of L, L acts trivially on $C_{V\otimes V^*}(N)$, so that, as L contains N, $C_{V\otimes V^*}(N) = C_{V\otimes V^*}(L)$.

Thus $C_{V\otimes V^*}(N)$ is certainly H-invariant. Hence, $X|_N$ has the same norm as $X|_L$.

As H is quasi-primitive, $X|_L = a\theta$ for some irreducible character θ of L and some integer a.

Thus $\|X|_N\| = \|X|_L\| = a^2$, so that $\theta|_N$ is irreducible and all

irreducible constituents of $X|_N$ are equivalent, as was required to prove that M is quasi-primitive.

We note that , as Q is a normal subgroup of M , all the irreducible constituents of $X|_Q$ are equivalent.

Now as $k > 1$, x lies outside Z(H) so that Q is non-Abelian, (for if Q is Abelian, then $Q \leq Z(H)$ as all the irreducible constituents of $X|_Q$ are equivalent. This is not the case.).

By Lemma 1.2.9 , Q is the central product of an extra-special p-group of exponent p and a cyclic p-group. As Q is generated by conjugates of x (each of which has order p) , Q has exponent p and is extra -special.

Case iii)

Certainly the condition of ii) implies the condition of ii), so that in this case, Q is extra-special of exponent p . Also, $X|_Q = a\Theta$ for some non-linear irreducible character , Θ, of Q , and some integer a.

The condition $C_W(M) = C_W(H)$

tells us in this case that $\bar{X}\bar{X}\bar{X}\bar{X}$ has

the same norm as $(X\bar{X}X\bar{X})|_M$, and an argument entirely analogous to that used in case ii), tells us that whenever N is a normal subgroup of M there is a normal subgroup, L say, of H such that $X\bar{X}|_L$ and $X\bar{X}|_N$ both have the same norm, and $L \geq N$.

Now $\theta\bar{\theta}$ is the regular character of $Q/Z(Q)$, as Q is extra-special. In particular, all of the irreducible constituents of $X\bar{X}|_Q$ are linear.

There is a normal subgroup K of H such that $X\bar{X}|_Q$ and $X\bar{X}|_K$ both have the same norm, and $K \geq Q$. Then all irreducible constituents of $X\bar{X}|_K$ are linear. Furthermore, $X|_K$ also has the same norm as $X|_Q$, so that $X|_K = a\theta^*$ where θ^* is irreducible and $\theta^*|_Q = \theta$. Let $R = \ker \theta^* \bar{\theta}^*$.

Now $R \leq Z(K)$, as θ^* is a faithful irreducible character of K. As every irreducible constituent of $\theta^* \bar{\theta}^*$ is linear, K/R is Abelian, so that K is nilpotent.

Now $Q \leq K$, so that x lies in $O_p(K)$.

Thus x belongs to Op(H),so that Q is normal in H by its definition.

The proof of Lemma 1.4.3 is now complete.

Lemma 1.4.3 has the following interesting corollary.

Corollary 1.4.4

Let H be a finite irreducible quasi-primitive complex linear group of degree n.Let p be a prime divisor of the order of H , and let x be an element of order p in H-Z(H).

Then x has at least $\frac{p+3}{4}$ distinct eigenvalues .

Let e = 1 if $p \equiv 1 \pmod 4$, let e=-1 if $p \equiv 3 \pmod 4$.Then if $n \leq \frac{p(p-e)}{4}$ and Op(H) = 1, the Sylow p-subgroups of H are elementary-Abelian.

Proof

We define Q as in Lemma 1.4.3. Suppose that x has fewer than $\frac{p+3}{4}$ distinct eigenvalues .

Then in any reduction of H (mod p) x has minimum polynomial of degree $\frac{p+1}{4}$ or less , so that we can apply Lemma 1.4.3 to deduce that Q is

extra-special and that $Z(Q) \leq Z(H)$.

Let X be the character of the given representation of H. Then Lemma 1.4.4 tells us that $X|_Q = a\theta$ for some non-linear irreducible character, θ, of Q.

Thus $\theta(x) = 0$ (as x lies outside $Z(Q)$), contradicting the fact that x has less than p distinct eigenvalues

Suppose now that $n \leq \frac{p(p-e)}{4}$, but that the Sylow p-subgroups of H are non-Abelian . Let x be an element of order p in $P' \cap Z(P)$, where P is a Sylow p-subgroup of H.

Now each linear constituent of $X|_P$ contains x in its kernel and every non-linear constituent of $X|_P$ has degree p . Thus x has at most $\frac{p+1}{4}$ distinct eigenvalues , contradicting the first part of the Lemma.

Suppose that P is not elementary Abelian , and let y be an element of order p^2 in P. Let $\bar{y}$ be the image of y in some reduction (mod p) of H.

Then $(\bar{y} - 1)^{\frac{p(p-e)}{4}} = 0$, so that $(\bar{y}^p - 1)^{\frac{p-e}{4}} = 0$. As $O_p(H) = 1$, this contradicts part b) of Lemma 1.4.3 ,

(since y^p satisfies all hypotheses required by part b)).

There is one more result which will often be useful to us, though it is of a slightly different nature from the other results of this section.

Lemma 1.4.5

Let H be a finite irreducible quasi-primitive complex linear group of degree n. Let p be a prime divisor of the order of H , and let x be an element of order p in H-Op(H).

Suppose that $n \geq 8$, and that x acts as a transvection in some reduction of H (mod p).

Then $p = 2$, and H has a normal subgroup N such that $N/Z(N) \cong A_{n+1}$.

Proof

As x lies outside Op(H), there is a conjugate x^h of x such that $\langle x, x^h \rangle$ is not a p-group. Let $K = \langle x, x^h \rangle$. Now x has quadratic minimum polynomial in some reduction (mod p) of H. Then if p is odd, the argument in Lemma 3.8.3 of [14] shows that K involves SL(2,p)

Suppose first that $p > 3$.

Then K' contains an element of order 6, say z. Then in the reduction (mod p) in which x has a fixed-point subspace of codimension one, $\langle x, x^h \rangle$, so in particular z, has a fixed-point subspace of codimension at most two.

As z is a p'-element, z has a fixed-point subspace of codimension at most two in the complex vector space on which H acts. As z has order six and z lies in H', the eigenvalues of z are 1 (with multiplicity $n-2$) $w, \bar{w}$ (with multiplicity 1 each), where w is a primitive 6th-root of unity. This contradicts Lemma 1.3.10.

If $p=3$, an argument similar to the above shows that K' contains an element z of order four such that z has the eigenvalues i and $-i$ (with multiplicity one each) and has the eigenvalue 1 with multiplicity $n-2$, contradicting Lemma 1.3.16. Thus $p=2$.

Now K' contains a non-identity element, z say, of odd order, such that z has a fixed-point subspace of co-dimension two . We claim that z has

order three.

If z has order greater than three then some power of z contradicts one of Lemma 1.3.10 or Lemma 1.3.17.

Thus z has order three and the final part of the conclusion of this lemma follows from Lemma 1.3.15

Section Five

We have seen that, given a finite irreducible quasi-primitive complex linear group ,H, and a prime p which divides the order of H , any element of order p in H acting with minimum polynomial of small enough degree in some reduction (mod p) of H , lies in Op(H).

We now examine ways in which we can deduce that a p-element of H has a minimum polynomial of low degree in any reduction (mod p) of H (for in general the minimum polynomial of a p-element in a reduction (mod p) of a complex linear group need not be invariant under choice of basis).

Let R be the ring of algebraic integers in some splitting field, K, for H (where [K:Q] is finite), and

let $R_{\mathfrak{p}}$ denote the localisation of R at the prime ideal $\mathfrak{p}$ containing the rational prime p.

Let V be an $R_{\mathfrak{p}}H$-module obtained from the given representation of H by a suitable choice of basis (after restriction of scalars).

Let M be any subgroup of H, and let $B_1, B_2, \ldots\ldots, B_n$ be the p-blocks of ordinary irreducible characters of H.

Now for $1 \leq i \leq n$, there is an element e_i in the centre of $R_{\mathfrak{p}}M$, given by:

$$e_i = \frac{1}{|M|} \sum_{X \in B_i} X(1) \sum_{h \in M} X(h^{-1})\, h$$

Furthermore, for $1 \leq i \leq n$, we have:

$$e_i e_j = \begin{cases} e_i & \text{if } i=j \\ 0 & \text{otherwise.} \end{cases}$$

Thus we may write V as a direct sum of $R_{\mathfrak{p}}M$-modules, i.e.:

$$V = Ve_1 \oplus Ve_2 \oplus \ldots \oplus Ve_n .$$

In particular, if M is a p'-group then each p-block of M contains only one irreducible character of M Thus for each i, Ve_i is homogeneous as a $\mathbb{C}M$-module.

Thus V may be written as a direct

sum of $R_{\mathfrak{p}}M$-modules which are in fact homogeneous when considered as CM-modules.

Suppose that M is not a p'-group and that x is a p-element of M. Let P be the unique prime ideal of Rp, and let bars denote images (mod P).

Then $\bar{V} = \bar{Ve}_1 \oplus \bar{Ve}_2 \oplus \ldots \bar{Ve}_n$. Let x act with minimum polynomial of degree k on $\bar{V}$. Then for some $i \leq n$, we know that $\bar{Ve}_i(1-x)^{k-1} \neq 0$. Let $W = Ve_i$.

Now let T be a p'-subgroup of $C_M(x)$. Then $W = Wf_1 \oplus Wf_2 \oplus \ldots Wf_m$ as a sum of $R_{\mathfrak{p}}T$-modules, where each f_j is a primitive central idempotent of $R_{\mathfrak{p}}T$. As x centralizes T, $xf_j = f_j x$ for each j, so that x acts on each Wf_j.

Now we may choose a j such that $\bar{Wf}_j(1-x)^{k-1} \neq 0$, as $\bar{W}(1-x)^{k-1} \neq 0$. Let $N = Wf_j$. We now consider N as a $\mathbb{C}T\langle x\rangle$-module. We claim first that x has at least k distinct eigenvalues on N.

If this were not the case, then x would have minimum polynomial of degree at most k-1 on N (regarded as

a $\mathbb{C}\langle x\rangle$-module) ,and this would still be the case if N were regarded as an $R_{\underline{p}}\langle x\rangle$-module.As x is a p-element,the same would be true of $\bar{N}$,contrary to the choice of N.

We know that N is a direct sum of isomorphic irreducible $\mathbb{C}T$-modules as T is a p'-group . We claim that N is the direct sum of at least k such modules.Let $t = \dim_{\mathbb{C}}(N)$, and let N_o be an irreducible $\mathbb{C}T$-submodule of N of dimension s.

Still regarding N as a $\mathbb{C}T\langle x\rangle$-module we note that T acts on each distinct eigenspace of x.

Let V_o be one such eigenspace. Then V_o is a direct sum of isomorphic copies of N_o , so $\dim_{\mathbb{C}}(V_o) = bs$ for some integer b.

As x has at least k distinct eigenvalues on N, $t \geq ks$,so that N is the direct sum of at least k copies of N_o ,as required.

In particular,we may apply the above arguments when x is some p -element of H and $M = C(x)$. This yields the following result.

Lemma 1.5.1

Let H be a finite irreducible quasi-primitive complex linear group of degree n.Let p be a prime divisor of the order of H , and let x be a p-element of H . Let X(h) = trace(h) for each h in H.

Suppose that the image of x in some reduction (mod p) of H acts with minimum polynomial of degree k .

Then for any p'-subgroup T of C(x) there is some p-block,B, of ordinary irreducible characters of C(x) and some irreducible character, θ , of T such that :

$$\sum_{\mu \in B} (X|_C, \mu)_C (\mu|_T, \theta)_T \geq k.$$

It is perhaps worth pointing out one other consequence of the above arguments which we shall frequently use.

Lemma 1.5.2

Let H be a finite irreducible quasi-primitive complex linear group of degree n.Let p be a prime divisor of the order of H , and let x be a

p-element of H .

Suppose that the image of x in some reduction (mod p) of H acts with minimum polynomial of degree k . Let y be any p'-element of C(x).

Then y has at least one eigenvalue such that x has k or more distinct eigenvalues in its action on the associated eigenspace of y.

This concludes our summary of some ideas from modular representation theory which we will frequently use.

Of course, we will also make use of the Brauer main theorems and the character theory of finite groups whose order is divisible by a prime to the first power only.

These results are all well known, so we do not include them here but we quote them frequently without reference.

Section Six

In this section we prove two results which will be useful to us later and may be of some independent interest . We also prove an easy

character theoretic result which may be well-known.

First, we prove the character-theoretic result:

Lemma 1.6.1

Let H be a finite group, and suppose that for some prime divisor p of |H|

i) $O_{p'}(H)$ has odd order

ii) H has a cyclic Sylow p-subgroup P of order p with [N(P):C(P)] = 3.

Then unless H has odd order, all of the non-exceptional characters in the principal p-block are rational-valued.

Proof

There are three non-exceptional characters in the principal p-block of H. Also, the principal p-block of H is invariant under all algebraic conjugation. Suppose then that H has even order but some non-exceptional character in the principal p-block is not rational-valued.

Then the non-exceptional characters in the principal p-block comprise the principal character and two more characters which must be algebraic

conjugates, say θ_1 and θ_2.

As H has even order, there is an involution t in H. Let x be a generator of P. As $[N(P):C(P)] = 3$, t inverts no conjugate of x.

Let $\{\mu^{(i)}\}$ be the exceptional characters in the principal p-block of H. These characters all agree (and assume rational values) on p-regular elements of H. Also, there is a sign e such that:

$$\sum_i \mu^{(i)}(x) = e$$

Let $a = \theta_1(1)$, $b = \theta_1(t)$ let $d = \theta_1(x)$ and let $c = \mu^{(i)}(1)$. Then we have:

i) $1 + 2ad + ec = 0$.

ii) $1 + 2bd + e\mu^{(i)}(t) = 0$.

Hence $e = -d$, $c = 2a+d$ and $\mu^{(i)}(t) = 2b + d$. Thus, as t inverts no p-singular element, we have:

$$1 + \frac{2b^2 d}{a} - \frac{d(2b+d)^2}{(2a+d)} = 0$$

Consequently, $a = b$, and t is in the kernel of each irreducible character in the principal p-block of H. Thus t lies in $O_{p'}(H)$ which contradicts the fact that $O_{p'}(H)$ has odd order.

This contradiction completes the proof of Lemma 1.6.1.

The next result is motivated by a situation that frequently occurs in signalizer functor analysis and will allow us to avoid quoting [ ]

Lemma 1.6.2

Suppose that H is a finite group and that P is a Sylow p-subgroup of H for some prime p.

Suppose that some Abelian normal subgroup of P is not cyclic and that H possesses a subgroup M such that whenever D is a subgroup of P which contains an Abelian subgroup of type (p,p) , M contains $N(D)$.

Then $P \cap H' = P \cap M'$.

Proof

Let F denote the set of subgroups of P such that for any D in F and for $N = N(D)$:

i) $N_P(D)$ is a Sylow p-subgroup of N.

ii) N is p-constrained.

iii) D is a Sylow p-subgroup of $O_{p',p}(N)$

Then by Theorem 4.9 of [30], we know that $P \cap H' = \langle P \cap N(D)' : D \in F \rangle$ Hence we only need to prove that M contains N(D) for any D in F.

Suppose that there is some D in F such that $N(D) \not\leq M$. Then D contains no Abelian subgroup of type (p,p), so D is either cyclic or generalized quaternion. Let $N = N(D)$ and let $\bar{N}$ denote $N/Op'(N)$.

Now certainly $D \neq P$, so that $N_P(D)$ is strictly greater than D. We first prove that $p = 2$ and D is quaternion of order 8.

As D is a Sylow p-subgroup of $Op'p(N)$, $\bar{N}/Z(\bar{D})$ acts faithfully as group of automorphisms of $\bar{D}$. If D is cyclic, then $\bar{N}/\bar{D}$ is Abelian, so has order prime to p , contradicting the fact that $N_P(D) > D$. If $p = 2$, and D is quaternion of order greater than 8, then $Aut(\bar{D})$ is a 2-group, so that $\bar{N}/Z(\bar{D})$ is a 2-group , whereas D is a Sylow 2-subgroup of $Op'p(N)$ and D is strictly contained in $N_P(D)$. This contradiction proves our assertion that D is quaternion of order 8.

Now $\bar{N}/\bar{D}$ acts faithfully as a

group of automorphisms of $\bar{D}/\Phi(\bar{D})$, so is isomorphic to a subgroup of GL(2,2). Since $\bar{N}/\bar{D}$ is not a 2-group, $\bar{N}/\bar{D}$ is isomorphic to GL(2,2). In particular $N_P(D)$ has order 16, and for any a in $N_P(D) - D$, $[D,a] \not\leq Z(D)$.

Now let A be an elementary Abelian normal subgroup of P which is not cyclic. Then $N_{AD}(D) > D$, as $D \neq DA$. Hence there is an element a in $N_A(D) - D$. Consequently, however, $[D,a] \leq A \cap D \leq Z(D)$, a contradiction.

Thus M contains N(D) for any D in F, as required.

Before we prove the third main result of this section, we need to quote a result which appears early in [2], and does not require the main result of that paper.

Lemma 1.6.3 (Aschbacher-Hall)

Let H be a finite group, and let D be a conjugacy class of subgroups of order 3 of H such that any two subgroups in D either commute or generate a subgroup of H which is isomorphic to SL(2,3).

Then $\langle D \rangle$ is either soluble or is isomorphic to PSU(3,3).

Lemma 1.6.4 (Thompson)

Let A be a p'-group of automorphisms of the p-group B, where p is prime.

Suppose that $B = [B,A]$, and that A centralizes every characteristic Abelian subgroup of B. Then B is a non-Abelian special p-group.

The third result may be regarded as a special case of an analogue of Glauberman's Z^*- theorem for the prime 3.

Lemma 1.6.5

Let H be a finite group which acts faithfully on some FH-module V, where F is a field of characteristic 3.

Let T be a Sylow 3-subgroup of H. Suppose that T contains an element x of order 3 such that :

i) $V(1-x)^2 = 0$.

ii) Whenever x^g lies in T, $x^g = x$.

iii) x lies outside Z(H).

Then [H,x] is a non-Abelian special 2-group.

Proof

Suppose that the Lemma is false . Then we may choose a pair (H,V) to violate the Lemma with |H| minimal and dim (V) minimal subject to this.
F

We may suppose that F is algebraically closed . We next claim that V is irreducible . We note that x lies outside $O_3(H)$, for otherwise every conjugate of x lies in T , and x lies in Z(H) by ii) , so iii) is violated.

Suppose that V is reducible.Then as x lies outside $O_3(H)$, there is an FH-composition factor of V,say W, on which x acts non-trivially . By the minimality of the pair (H,V), H does not act faithfully on W.Let K be the kernel of the action of H on W.

Certainly, $H \neq K\langle x \rangle$,as H acts irreducibly on W . By the minimality of the pair (H,V), either [K,x] = 1, or [K,x] is a non-Abelian special 2-group.

Let $\bar{H} = H/K$.By the minimality of the pair $(\bar{H},V)$,either $[\bar{H},x] = 1$ or else $[\bar{H},x]$ is a non-Abelian special 2-group.Let $\bar{M}$ be the inverse image in H of $[\bar{H},x]$.

Suppose that $H \neq M\langle x\rangle$. Then by the minimality of the pair (H,V) , either $[M,x] = 1$ or $[M,x]$ is a non-Abelian special 2-group . Now by the definition of M , $[H,x] \leq M$.

We prove that $[H,x,x] = [H,x]$, so that $[H,x] = [M,x]$ contrary to the fact that $[H,x]$ is not a non-Abelian special 2-group. Let $B = [H,x]\langle x\rangle$. Then B contains all the conjugates of x in H. Also, if x^h lies in B, then for some b in B, there is a Sylow 3-subgroup of B which contains both x and x^{hb} .

By ii) , $x = x^{hb}$, so that $[x,h] = [x, b^{-1}]$ and $[x,h]$ lies in $[B,x]$. Thus $[H,x] \leq [B,x] = [H,x,x]$ and $[H,x,x] = [H,x]$, the required contradiction.

Thus $H = M\langle x\rangle$. We next prove that H is 3-soluble. As M/K is a 2-group, it is sufficient to prove that K is 3-soluble.

Let $Q = K \cap T$. Then Q is a Sylow 3-subgroup of K . Suppose that K is not 3-soluble. Then Q is certainly not normal in K. Now $H = K\,N(Q)$ and $N(Q) < H$, so that by the minimality of the pair (H,V), either $[N(Q),x] = 1$

or else $[N(Q),x]$ is a non-Abelian special 2-group.

Now for any k in K and any h in $N(Q)$, $[kh,x] = [k,x]^h [h,x]$. Now $[K,x]$ is contained in $O_2(K)$, so that $[kh,x]$ is contained in the 2-group:

$$O_2(K)[N(Q),x].$$

As $H = K\,N(Q)$, $[H,x]$ is a 2-group. By the Hall-Higman theorem and condition i), x centralizes every characteristic Abelian subgroup of $[H,x]$. By Lemma 1.6.4, $[H,x]$ is a non-Abelian special 2-group, since we know that $[H,x,x] = [H,x]$. However this contradicts our assumption that (H,V) violates the Lemma.

Thus H is 3-soluble. We next prove that $H = O_{3'}(H)\,C(x)$. We use an argument which is probably well-known, and appears in [6]. Let $\bar{T}$ be the image of T in $H/O_{3'}(H)$. Then $\bar{x}$ is not conjugate in $\bar{H}$ to any other element of $\bar{T}$. Thus $\bar{x}$ lies in $Z(\bar{T})$, so centralizes $O_3(\bar{H})$. Now $\bar{x}$ must lie in $O_3(\bar{H})$, so that every conjugate of $\bar{x}$ lies in $\bar{T}$. Thus $\bar{x}$ must lie in $Z(\bar{H})$. Now by a Frattini argument,

$$H = O_{3'}(H)\,N(\langle x\rangle).$$

As x is not conjugate to its inverse

in H (by i)) , $H = O_{3'}(H)\, C(x)$.

Now $[H,x] = [O_{3'}(H), x]$. By i) and the Hall-Higman theorem , x centralizes every subgroup of odd order of [H,x] which it normalizes , and also every Abelian 2-subgroup of [H,x] which it normalizes. By Lemma 1.6.4 , [H,x] is a non-Abelian special 2-group ,which contradicts the fact that (H,V) does not satisfy the conclusion of the Lemma.

This contradiction establishes that H acts irreducibly on V.We next show that $\dim_F(V) \neq 2$.

Suppose that $\dim_F(V) = 2$. Then every 3-regular element of C(x) acts as a scalar on V.Hence C(x) has a normal 3-complement . As x lies in Z(T), and $\langle x \rangle$ is weakly closed in T with respect to H ,two elements of T which are conjugate in T are already conjugate in $N(\langle x \rangle) = C(x)$. As C(x) has a normal 3-complement,so has H . Thus H is 3-soluble, a contradiction as above.

We next prove that two distinct conjugates of x generate a proper subgroup of H. As F is algebraically closed there is an element v of V and an f in F such that $v(x-y) = fv$.

Let $W = \langle v, vx \rangle$. Then we see easily that $W = \langle v, vy \rangle$. We claim that W is $\langle x, y \rangle$ invariant. Now vx is in W and $(vx)x = vx^2 = v(2x-1)$ (since $V(1-x)^2 = 0$.).

Hence $(vx)x = 2vx - v$, so that $(vx)x$ lies in W and W is x-invariant. Also $V(1-y)^2 = 0$, as y is conjugate to x, so that, as $W = \langle v, vy \rangle$, a similar argument shows that W is y-invariant

Thus W is $\langle x, y \rangle$-invariant, as claimed. As $\dim_F(W) \leq 2$ and H acts irreducibly on V, $\langle x, y \rangle$ is a proper subgroup of H (for we have proved already that $\dim_F(V) \neq 2$).

Now we prove that for any distinct conjugate, z say, of x, $\langle x, z \rangle$ is isomorphic to $SL(2,3)$. Let z be such a conjugate of x and $M = \langle z, x \rangle$.

By the minimality of the pair (H,V), $[M,x]$ is a non-Abelian special 2-group or else $[M,x] = 1$. As $[M,x]\langle x \rangle$ is normal in M and x is not conjugate to its inverse in H, $M = [M,x]C_M(x)$ by a Frattini argument Also, z is already conjugate to x in M.

As $M = [M,x]\ C_M(x)$, $z = x^u$ for some u in $[M,x]$. Thus we see that: $z = x(x^{-1})^u$, so that z lies in $[M,x]\langle x\rangle$. Hence $M = \langle x,z\rangle \leq [M,x]\langle x\rangle$ so that $M = [M,x]\langle x\rangle$.

By ii), x does not commute with z so that $[M,x] \neq 1$, and $[M,x]$ is a non Abelian special 2-group. As $x^{-1}z$ lies in $[M,x]$, it has order 2 or 4.

In fact, $x^{-1}z$ cannot have order 2, for if it did, then $\langle x,z\rangle$ would be isomorphic to A_4, whereas $\langle x,z\rangle$ has a non-Abelian Sylow 2-subgroup. Let $u = x^{-1}z$, and let $t = u^2$.

Now t lies in $Z([M,x])$ and is centralized by both x and z (for x acts trivially on $Z([M,x])$). Thus t lies in $Z(M)$. Let $\bar{M} = M/\langle t\rangle$.

$\bar{M} = \langle \bar{x}, \bar{z} : \bar{x}^3 = \bar{z}^3 = (\bar{x}^{-1}\bar{z})^2 = 1\rangle$ so that $\bar{M}$ is isomorphic to A_4.

As M has non-Abelian Sylow 2-subgroups, M is isomorphic to $SL(2,3)$.

As any two distinct conjugates of x generate a group isomorphic to $SL(2,3)$, Lemma 1.6.3 allows us to deduce that the subgroup of H which is generated by the conjugates of x in H is either soluble, or else is

isomorphic to PSU(3,3).

Let K be the subgroup of H which is generated by the conjugates of x. Then $K \geq [H,x]\langle x \rangle$, so that $[H,x,x]$ is contained in $[K,x]$. We have seen that $[H,x,x] = [H,x]$, so $[K,x] = [H,x]$ Thus $[K,x]$ is not a non-Abelian special 2-group, so that $H = K$ by the minimality of the pair (H,V).

The argument used earlier to show that H could not be 3-soluble allows us to conclude that H is isomorphic to PSU(3,3). Thus $|H| = 6048$ and T, the Sylow 3-subgroup of H which contains x, is extra-special of order 27 . Also $\langle x \rangle = Z(T)$ by ii) .

However, any element which is in the centre of a Sylow 3-subgroup of PSU(3,3) is conjugate to its inverse a contradiction to our hypotheses. The proof of Lemma 1.6.5 is complete.

Chapter Two

In this chapter, we state and prove some further properties of finite irreducible complex linear groups of prime degree.

We assume from now on that G is a finite irreducible complex linear group of degree eleven which does not satisfy the conclusion of our main theorem.

We state some properties of G most of which are easy consequences of the results of Chapter One.

From now on, X will denote the complex ireducible character of G with $X(g)=\text{trace}(g)$ for all g in G.

Section One

Some Preliminary Results

The following result is well-known, but we include a proof for the sake of completeness.

Lemma 2.1.1

Let H be a finite primitive complex irreducible linear group of prime

degree $p > 2$ with $Z(H)=1$.

Then H has a cyclic Sylow p-subgroup of order p which contains its own centralizer.

Proof

Let P be a Sylow p-subgroup of H and let $C = C(P)$.

Suppose that P is non-Abelian. Then $1 \neq Z(P) \leq Z(H)$, contrary to the hypotheses. Thus P is Abelian and it only remains to prove that C has order p.

Let y be a non-identity element of C, X be the character of the given p-dimensional representation of H.

Then $([H:C(y)], X(1))=1$, so that $X(y)=0$ as H has trivial centre.

Thus $|C|\,(X|_C, 1_C) = p$, and $|C|$ divides p. As $P \leq C$, $|C| = p$, as required.

The following result is due to Brauer, though we present a different proof.

Lemma 2.1.2

Let H be a finite primitive complex irreducible linear group of prime degree $p > 2$ with Abelian Sylow p-

subgroups . Then H' is a non-Abelian simple group.

Proof

Let P be a Sylow p-subgroup of H. By elementary transfer, $P \cap H' \cap Z(H) = 1$. As in Lemma 2.1.1, $X(h) = 0$ for each h in $P - Z(H)$.

Now $|P|(X|_P, X|_P)_P = p^2 |P \cap Z(H)|$

as X vanishes identically on $P - Z(H)$. However, $(X|_P, X|_P)_P \geq p$ as $X(1) = p$ and P is Abelian. Thus $[P : P \cap Z(H)] \leq p$.

In fact, $[P : P \cap Z(H)] = p$, as the degree of every irreducible character of H divides $[H : Z(H)]$.

As H has no normal p-complement and P is Abelian, the order of H' is divisible by p. Thus $P = (P \cap H') \times (P \cap Z(H))$. Let $R = P \cap H'$.

Let Q be a q-subgroup of C(R) for some prime $q \neq p$. Now $C(R) = C(P)$, so that $X(y) = 0$ for each y in $Q - Z(H)$. Thus we see that $|Q|(X|_Q, X|_Q) = p^2 |Q \cap Z(H)|$. As $q \neq p$, we see that $Q \leq Z(H)$.

Thus $C(R) = R \times Z(H)$. Now $Z(H) \cap H'$ is a p'-group, so that $Z(H) \cap H' = 1$, since $X(1) = p$, and each element of H' is

certainly unimodular, while any scalar unimodular matrix has order 1 or p.

As $O_{p'}(H) \leq Z(H)$ by the primitivity of H, $O_{p'}(H') = 1$. As P is not a normal subgroup of H, $O_p(H') = 1$. Thus $F(H') = 1$ so that $E(H') \neq 1$. Let $E = E(H')$. Then $R \leq E$.

We claim that $E = H'$, and that E is simple. We see that E is simple, as E is not divisible by p^2 and $O_{p'}(H) = 1$. By a Frattini argument, $H = EN(R)$. Now H/E is isomorphic to $N_H(R)/N_E(R)$. As $C(R) = R \times Z(H)$ and $N(R)/C(R)$ is cyclic, $N(R)$ is soluble. Thus $N(R)$ has a Hall p'-subgroup, A. Now $A \cap C(R) \leq Z(H)$, and $A / A \cap C(R)$ is cyclic, so that A is Abelian. Thus $(P \cap Z(H)) \times A$ is an Abelian complement to R in $N(R)$.

Thus $N_H(R)/N_E(R)$ is Abelian and H/E is Abelian. Hence we have:

$$H' \leq E = E' \leq H',$$

so that $E = H'$, as required

Remark

We note that G is primitive, for otherwise, G has a subgroup of index 11 and with respect to some suitable basis, G is a monomial group and so satisfies part a) of Theorem A.

In view of Lemma 2.1.2, we make the following additional hypothesis:

Hypothesis

G is a non-Abelian simple group.

From now on, P will denote a fixed Sylow 11-subgroup of G.

The following result enables us to restrict the structure of proper subgroups of G which contain P. This will eventually allow us to show that any subgroup of G which contains P and has order divisible by 25 is itself irreducible. This in turn will allow us to obtain a good bound on the power of 5 dividing the order of G.

Lemma 2.1.3

Let H be a finite simple complex irreducible primitive linear group of degree p, where p is an odd prime.

Let Q be a Sylow p-subgroup of H and let M be a proper subgroup of H which contains Q.

Then one of the following occurs:

i) M itself is irreducible.

ii) E(M) is isomorphic to a primitive irreducible complex linear group of degree p-1 .

iii) M has a normal subgroup N such that [M:N] ≤ 2 and N is isomorphic to PSL(2,p).

iv) M ≤ N(Q).

Furthermore , Q has a fixed-point subspace of dimension one which is M-invariant in all cases except i).

Proof

Let V be the p-dimensional complex vector space on which H acts. Let Ø be the irreducible character of H defined by Ø(h) = trace(h) for each h in H . Let y be a generator of Q.

By Lemma 2.1.1 , C(Q) = Q and Ø(y) = 0.Also , Q has order p.Since Ø(y) = 0 and Ø(1) = p , y has the eigenvalue 1 with multiplicity one, so that Q has a one-dimensional fixed-point subspace, V_0 say.

Suppose that neither case i) nor case iv) occurs . We may write:

$V = W_1 \oplus \ldots\ldots \oplus W_k$, where $k>1$, and each W_i is an irreducible $\mathbb{C}M$-module . We

may also suppose that $V \leq W_1$.

We first prove that for $j>1$, M acts faithfully on W_j. For let K_j be the kernel of the action of M on W_j. Then K_j is a p'-group, as $V \leq W_1$. If $K_j \neq 1$, then QK_j must act irreducibly on V, contradicting the assumption that M does not act irreducibly on V. Thus $K_j = 1$.

As Q is not normal in M (by hypothesis), $\dim_{\mathbb{C}}(W_j) \geq \frac{p-1}{2}$ for $j \geq 2$, by Lemma 1.2.1. Thus $k \leq 3$.

If $k=3$, then M is isomorphic to $PSL(2,p)$ by Lemma 1.2.2, (for $Z(M) = 1$, as $C(Q) = Q$), so iii) holds. Furthermore, $\dim_{\mathbb{C}}(W_1) = 1$, so that $W_1 = V_o$.

Suppose that $k=2$, but that $\dim_{\mathbb{C}}(W_2) < p-1$.

Then Q acts non-trivially on W_1, so that M acts faithfully on W_1. By Lemmas 1.4.1 and 1.2.2, $\dim_{\mathbb{C}}(W_1) \geq \frac{p+1}{2}$ (as $V_o \leq W_1$).

Thus $\dim_{\mathbb{C}}(W_2) = \frac{p-1}{2}$ and $\dim_{\mathbb{C}}(W_1) = \frac{p+1}{2}$. Furthermore, M is

isomorphic to PSL(2 , p) , which contradicts the fact that PSL(2,p) cannot have a complex irreducible character of degree $\frac{p+1}{2}$ and a complex irreducible character of degree $\frac{p-1}{2}$.

Thus when k=2, $\dim_{\mathbb{C}}(W_2) = p-1$, and $W_1 = V_o$.

Suppose that W_2 is an imprimitive $\mathbb{C}M$-module .Then we may write: $W_2 = W_o^M$, where, for some proper subgroup N of M , W_o is an irreducible $\mathbb{C}N$-module.

Now $\dim_{\mathbb{C}}(W_2) = [M:N] \dim_{\mathbb{C}}(W_o)$ so that [M:N]=t,where t divides p-1. Thus M has a normal subgroup ,K say such that $K \leq N$ and M/K acts as a transitive permutation group on the right cosets of N in M.

As $t < p$, $Q \leq K$.Also,as Q is not normal in M, Q is not normal in K . Now W_2 is not irreducible as a $\mathbb{C}N$-module, as $W_2 = W_o^M$. Thus W_2 is not an irreducible $\mathbb{C}K$-module.

By Clifford's theorem,we may write : $W_2 = W_{21} \oplus \ldots\ldots W_{2m}$,where

the W_{2i} are irreducible CK-modules and each W_{2i} has the same dimension (as a complex vector space). Also, m is greater than 1.

By an argument earlier in the Lemma, K acts faithfully on W_{2i} for each i. Thus $\dim_{\mathbb{C}}(W_{2i}) \geq \frac{p-1}{2}$ for each i, by Lemma 1.2.1.

Hence $m=2$ and $\dim_{\mathbb{C}}(W_{21}) = \frac{p-1}{2}$ so that K is isomorphic to $PSL(2,p)$ by Lemma 1.2.2. Furthermore, as K is normal in M, $M = KN_M(Q)$, so that $[M:K] \leq 2$, as $|N_K(Q)| = \frac{p-1}{2}$, and Q is self-centralizing.

Thus if W_2 is an imprimitive CM-module, then case iii) occurs. Suppose then that W_2 is primitive. Let $E = E(M)$. As $F(M) = 1$, $Q \leq E$. Suppose that W_2 is not irreducible as a CE-module.

Then, as W_2 is a primitive CM-module, W_2 is a direct sum of isomorphic CE-modules, each of which is faithful, as Q has no non-trivial fixed-points on W_2 and $O_{p'}(E) = 1$. As Q is not normal in M, E can have

no faithful complex representation of degree less than $\frac{p-1}{2}$, and can only have one of degree $\frac{p-1}{2}$ if E is isomorphic to PSL(2,p).

If E is isomorphic to PSL(2,p) we again see that $[M:E] \leq 2$, so that case ii) occurs. Thus we may assume that E acts irreducibly on W_2. If W_2 is imprimitive as a CE-module then an earlier argument may be used to show that E possesses a subgroup K which is isomorphic to PSL(2,p) and such that $[E:K] \leq 2$.

As E is simple, E = K, and as M = E N(Q), we see that $[M:E] \leq 2$, so that case iii) occurs. Hence we may assume that W_2 is primitive as a CE-module, so that case ii) occurs.

The proof of Lemma 2.1.3 is now complete.

Lemma 2.1.4

No prime larger than 11 divides the order of G.

Proof

Suppose that the Lemma is false.

Let q be a prime divisor of the order of G which is greater than 11. By Lemmas 1.2.2 and 1.2.4 , q is either 17 or 19.

Let Q be a Sylow q-subgroup of G. Then $|Q| = q$ and $C(Q) = Q$.

As q does not divide X(1),X lies in the principal q-block of G. Then for some e dividing q-1 we see that q divides 11-e or 11+e,which is a contradiction , so completing the proof of the Lemma.

Lemma 2.1.4

G has elementary Abelian Sylow 7-subgroups of order at most 7^9.

Proof

As G is simple ,and $11 < \frac{7(7+1)}{4}$, we see from Lemma 1.4.3 that G has elementary Abelian Sylow 7-subgroups which clearly have order at most 7^{10} as $Z(G)=1$.

Let T be a Sylow 7-subgroup of G and suppose that $|T| = 7^{10}$. As every element of T is unimodular ,there is an element ,y, of T which is similar

to $diag(w,w,w,w,w,w,w,w,w,w,w^4)$, for a primitive 7-th root of unity, w.

Then y acts with a quadratic minimum polynomial in any reduction (mod 7) of G, which contradicts Lemma 1.4.3, as $2 = \frac{7+1}{4}$.

Corollary 2.1.5

i) Let Q be a 7-subgroup of G. Then N(Q) is not irreducible.

ii) No element of order 7 can act with minimum polynomial of degree smaller than four in any reduction (mod 7) of G.

iii) Let u be an element of order 7 in G. Then each 7-regular element of C(u) has some eigenvalue of multiplicity greater than three.

iv) Let T be a Sylow 7-subgroup of G. For some g in G-N(T), $[T:T \cap T^g] \leq 49$.

Proof

i) Suppose that N(Q) is irreducible. Then 11 divides $|N(Q)|$, and we may suppose that $P \leq N(Q)$. As $|Q| < 7^{10}$ and $C(P)=P$, this is a contradiction

ii) This follows from Lemma 1.4.3,

as $3 = \frac{7-1}{2}$ and no 7-local subgroup of G is irreducible.

iii) Follows from Lemma 1.5.2 and ii)

iv) Follows from Lemma 1.4.2 and i)

Lemma 2.1.6

No non-identity element of G has an eigenspace of codimension 2 or 1.

Proof

Suppose that G contains some non-identity element with an eigenspace of codimension 2 or 1.

As G is a finite simple irreducible primitive complex linear group of degree 11, Lemmas 1.3.13 to 1.3.18 force us to conclude that G is isomorphic to A_{12}, contradicting our assumption that G does not satisfy the conclusion of Theorem A.

Lemma 2.1.7

Let p be a prime divisor of the order of G, and let y be an element of order p in G.

Then y does not act as a transvection in any reduction (mod p) of G.

Proof

This is an immediate consequence of Lemma 1.4.5 and the assumption that G does not satisfy the conclusion of Theorem A.

Lemma 2.1.8

i) 2^{18} does not divide the order of G.

ii) 3^{14} does not divide the order of G.

Proof

i) Let R be a Sylow 2-subgroup of G, and let A be an Abelian subgroup of R. Then $|A| \leq 2^{10}$ by Lemma 1.3.12 .

Now as R is a 2-group, we may write $X|_R = \theta + \theta_1$ for some character θ (not necessarily irreducible) of R of degree 8 and some character θ_1 of R. We claim that θ is faithful.

If this is not the case, then ker θ contains an involution t. As G=G', t has the eigenvalue -1 with even multiplicity. As $\theta(1) = 8$ and t lies in ker θ, t has the eigenvalue 1 with multiplicity 9, contradicting Lemma 2.1.5 .

Now, R has an Abelian

subgroup, D, of index at most 2^7. Thus $|R| \leq 2^{17}$, as $|D| \leq 2^{10}$.

ii) Let T be a Sylow 3-subgroup of G. Then $X|_T$ can contain no irreducible constituent of degree 9, for if it does, every non-identity element of Z(T) has an eigenspace of dimension 9 or more, contradicting Lemma 2.1.6.

We may suppose that T consists of monomial matrices. Let D be the diagonal subgroup of T. Then as $X|_T$ contains no irreducible constituent of degree nine, and at most three irreducible constituents of degree 3 T/D is elementary Abelian of rank at most three. Thus $[T:D] \leq 27$.

By Lemma 1.3.12, $|D| \leq 3^{10}$, so that $|T| \leq 3^{13}$, as required.

Lemma 2.1.9

i) The Sylow 5-subgroups of G have exponent dividing 25.

ii) The Sylow 3-subgroups of G have exponent dividing 27.

iii) The Sylow 2-subgroups of G have exponent dividing 16.

Proof

As G is simple, all parts of the Lemma follow from the remarks which precede Lemma 1.4.1.

Section Two

In this section, we take the first step towards determining the 5-local structure of G . We prove that N(P) contains an element of order five. We will see later that the centralizer of such an element has a restricted structure , and this in turn places stong restrictions on the size of a Sylow 5-subgroup of G.

The main result of this section has an important bearing on our later work, but the ideas of the proof are rather different from any to be found elsewhere in this thesis

Lemma 2.2.1

[N(P):C(P)] ≠ 2, so that N(P) contains an element of order five.

Proof

Suppose that the Lemma is false, so that [N(P):P] = 2 . Then by Lemma 2.1.3, we know that the order of G is not divisible by any prime greater than 11.

Now $(X\bar{X},1)=1$ as X is irreducible, so that, as $X\bar{X}(1)=121$, $X\bar{X}$ contains an irreducible constituent, say θ, of degree prime to 11. In fact, for a generator, x, of P, we have: $X\bar{X}(x)=0$. Thus we may suppose that either θ is a non-exceptional character in the principal 11-block of G with $\theta(x)=-1$ or θ is an exceptional character in the principal 11-block such that $\theta(1)\equiv 2 \pmod{11}$. In the latter case, all of the exceptional characters in the principal 11-block occur with equal multiplicity in $X\bar{X}$, as they all agree on 11-regular elements and $X\bar{X}$ vanishes on 11-singular elements. In particular, $50(1)\leq 120$, so $\theta(1)\leq 24$.

If 11 divides $\theta(1)-2$, then as $\theta(1)<121$ and $(\theta(1)-1)$ also divides $|G|$ (for $\theta(1)-1$ is the degree of a non-exceptional character in the principal 11-block of G), we have a contradiction, as $2<\theta(1)\leq 24$, and neither 13 nor 23 divides $|G|$.

If 11 divides $\theta(1)+1$, then $\theta(1)-1$ is again a character degree, so again $\theta(1)<121$ and $\theta(1)-1$ also divides $|G|$. Thus $\theta(1)=10$ or 21.

If $\theta(1)=10$, then the exceptional characters of the principal 11-block each have degree 9, which contradicts Lemma 1.2.5, as G is simple.

We prove that if $\theta(1)=21$, then $|G| = 3.4.5.7.11$, and then we quickly derive a contradiction.

Let t be any involution of G, x be a non-identity element of P. Then we have:

$$(*) \qquad \#(t\dot{t}=x) = \frac{|G|}{|C(t)|}^2 \quad \frac{(21-\theta(t))^2}{21.20} \neq 0.$$

as θ is faithful.

Thus t is conjugate to an involution of N(P) and , as C(P)=P, exactly 11 conjugates of t invert x

As $(\det\theta)(t)=1$, $\theta(1)\equiv\theta(t) \pmod 4$.

Also $22\,(\theta|_{N(P)}, 1)_{N(P)} = 11+11\,\theta(t)$

so that $\theta(t)\geq -1$. Similarly, $\theta(t)\leq 1$, so that in fact $\theta(t)=1$.

Substituting in (*) yields:

$$11 = 20\,\frac{|G|}{21\,|C(t)|}^2 \qquad (**)$$

Then $231|C(t)| = 20[G:C(t)]$. As G has one conjugacy class of involutions, $[G:C(t)]$ is odd, so that 8 does not divide $|C(t)|$, and 8 does not divide the order of G.

Let R be a Sylow 7-subgroup of G, u a non-identity element of Z(R).

As θ is rational-valued on 11'- elements, $\theta(u)$ is an integer.

Also, $[G:C(u)]\dfrac{\theta(u)}{\theta(1)}$ is an integer.

As 7 divides $\theta(1)$ but not $[G:C(u)]$, $\theta(u)=7z$ for some integer z.

As $\theta(1)=21$ and G is simple, $-2\leq z\leq 2$.

In particular, 7 does not divide :

$$[G:C(u)]\left(\frac{\theta(u)}{\theta(1)} - 1\right),$$

so that θ does not lie in $B_o^{(7)}(G)$.

By Lemma 1.2.14, there is a non-trivial character which belongs both to the principal 11-block and to the principal 7-block. As all the exceptional characters in $B_o^{(11)}(G)$ are algebraically conjugate, they all belong to the principal 7-block.

Thus no other irreducible character of the principal 11-block belongs to

the same 7-block as 0 does.

By Lemma 1.2.14, 49 cannot divide $|G|$. Let y be an 11-regular element of G. Then :

$$\#(\dot{x}\dot{x}=y) = \frac{|G|}{|C(x)|^2}\left(1+\frac{0(y)}{21}+9\frac{(0(y)-1)}{20}\right),$$

a class-algebra constant, and so in particular a non-negative integer.

Hence $0(y) \geq -1$ (because $0(y)$ is an integer).

Let S be a Sylow 5-subgroup of G and let s be a non-identity element of Z(S).

Then :

$$\#(\dot{s}\dot{s}=x) = \frac{|G|}{|C(s)|^2}\frac{(0(1)-0(s))^2}{21.20},$$

an integer, m say.

Then :

$$[G:C(s)] = \frac{420\, m\, |C(s)|^2}{(21-0(s))},$$

an integer not divisible by 5.

As $-1 \leq 0(s) \leq 20$, $(21-0(s))$ is not divisible by 25, so that as m is an integer and $[G:C(s)]$ is relatively prime to 5, $|C(s)|$ is not divisible by 25.

Thus $|S| = 5$, as s lies in Z(S).

Hence $|G| = 4.3^{k}.5.7.11.$ for some integer k.

Now $[G:N(P)] \equiv 1 \pmod{11}$ by Sylow's theorem, so that $k \equiv 1 \pmod{5}$.

Let W be a Sylow 3-subgroup of G and let w be a non-trivial element of Z(W).

Then:

$$\#(ww=x) = \frac{|G|}{|C(w)|^2} \frac{(21-0(w))^2}{20.21},$$

so that $[G:C(w)] = 420\, n \frac{|C(w)|}{(21-0(w))^2}$ for some integer n. As $[G:C(w)]$ is prime to 3 and $0 \leq (21-0(w)) \leq 22$, $|C(w)|$ is not divisible by 81.

As $W \leq C(w)$, 81 does not divide $|G|$ so that $k=1$ and $|G| = 3.4.5.7.11$. However, each exceptional character of the principal 11-block belongs to the principal 3-block, by Lemma 1.2.14, as 0 lies in a 3-block of defect 0, and all of the exceptional characters in the principal 11-block are algebraically conjugate.

This contradicts the fact that the principal 3-block only contains 3 irreducible characters. Thus the assumption that $[N(P):P] = 2$ is false.

As $O_{p'}(G) = 1$, $N(P) \neq P$. If $N(P)$ contains no element of order 5, then $[N(P):P] = 2$, contradicting the first part of the Lemma.

Section Three

In this section, we digress a little to examine the structure of finite irreducible primitive complex linear groups of degree $2q$, where q is a prime greater than 3. We are particularly interested in the case $q = 5$, which turns out to be the most difficult to treat.

We are able to use the results of this section to conclude that any proper subgroup of G which contains P and has order divisible by 25 must be irreducible.

Lemma 2.3.1

Let q be a prime greater than 3 and let H be a finite irreducible unimodular primitive complex linear group of degree $2q$.

Suppose that $Z(H) = 1$ and that $H = H'$.

Then the Sylow q-subgroups of H are elementary Abelian of order at most q^2. Also, if the order of H is divisible by q^2, then H contains a Sylow intersection of order q.

If q = 5 and 25 divides the order of H, then there is an element of H' which has a fixed-point space of codimension two.

Proof

We let $\theta(h)$ = trace(h) for all h in H, so that θ is a complex irreducible character of H.

We note that as H is primitive and Z(H) = 1, F(H) = 1 also. Thus when $q \neq 5$, Lemma 1.4.3 tells us that H has elementary Abelian Sylow q-subgroups.

Suppose then that q = 5, but that H has a non-Abelian Sylow 5-subgroup say S.

Let z be a non-identity element of $S' \cap Z(S)$. Then z has precisely two eigenvalues. Now as H is primitive and Z(H) = 1, there is a conjugate, y say, of z, which does not commute with z. Let $K = \langle z, y \rangle$.

By Lemma 1.3.19, all the irreducible constituents of $\theta|_K$ have degree one or two. Thus z and y both centralize $O_{5'}(K)$ by Lemma 1.2.10. Also, K has Abelian Sylow 5-subgroups so that z and y both centralize $O_5(K)$.

Hence $F(K) \leq Z(K)$, so that E(K) is non-trivial, and in fact neither z nor y centralizes E(K). Let E(K)=E.

As all irreducible constituents of $\theta|_E$ have degree 1 or 2, Lemma 1.3.1 tells us that E is isomorphic to SL(2,5). As Z(H) = 1, there is a linear constituent of $\theta|_E$ (otherwise the central involution of E would lie in the centre of H) which must of course be the trivial character of E, as $E = E'$.

Now, however, E contains an element of order six whose eigenvalues are $1, -w, -\bar{w}$ for a primitive cube root of unity, w. This contradicts Lemma 1.3.10, as H is primitive.

Thus the Sylow 5-subgroups of H are Abelian. Suppose then that S is a Sylow 5-subgroup of H, but that S contains an element, y say, of order

25 . We claim that y^5 only has two distinct eigenvalues.

As S is Abelian, [H:C(y)] is not divisible by 5. Since $\theta(1)=10$, there are integers a and b such that: $a\theta(1)+b[H:C(y)] = 2$. Hence

$$2\frac{\theta(y)}{\theta(1)} = a\theta(y) + b[H:C(y)]\frac{\theta(y)}{\theta(1)}$$

is an algebraic integer.

Thus $\theta(y) = 5d$ for some algebraic integer d . As y has order 25 and $\theta(1) = 10$, there are three possibilities to consider:

i) $\theta(y) = 5w_1 + 5w_2$, where w_1 and w_2 are 25-th roots of unity.

This situation cannot occur, for if it did, then y would have only two eigenvalues, so that in any reduction (mod 5) of H, we would certainly have $(y-1)^5 = 0$, so that y^5 would act trivially , and hence lie in $O_5(H)$. This would contradict the fact that y has order 25 and $O_5(H)=1$.

ii) $\theta(y)= 5w$ for some 25-th root of unity, w .

This case cannot occur, for suppose that it does . Then there is a 25-th

unity b such that y is similar to Diag (w,w,w,w,w,b,ab,a^2b,a^3b,a^4b), where a is a primitive 5th root of unity . Then y^5 has two eigenvalues only , and the argument used to show that H has Abelian Sylow 5-subgroups yields a contradiction.

iii) $\theta(y)=0$.

In this case there are two 25th roots of unity, w and b, say , such that y^5 has only the two eigenvalues w^5 and b^5 . Again , the argument used to prove that H has Abelian Sylow 5-subgroups supplies a contradiction.

Thus no such element y can exist, and H has elementary Abelian Sylow 5-subgroups . Hence , for any value of q, H has elementary Abelian Sylow q-subgroups.

We prove next that the Sylow q-subgroups of H have order q^2 or q. Let S be a Sylow q-subgroup of H,and let y be a non-identity element of S

Then q does not divide [H:C(y)],so that , as above, $\theta(y) = qa$ for some algebraic integer a.

Again,there are only three possibilities to consider:

i) $\theta(y) = q(w_1 + w_2)$ where w_1 and w_2 are q-th roots of unity.

Then y has only two eigenvalues which contradicts Lemma 1.4.3 if $q \neq 5$ and an argument above if $q = 5$. Hence this case cannot occur.

ii) $\theta(y) = qw$ for some q-th root of unity w.

iii) $\theta(y) = 0$.

Suppose then that the order of S is greater than q^2, and let A be a subgroup of order q^3 of S. We note that A has $1+q+q^2$ subgroups of order q.

Suppose that the generators of c cyclic subgroups of A satisfy the condition ii) above with $w=1$, that the generators of d cyclic subgroups of A satisfy the condition ii) above with $w \neq 1$, and that the generators of e cyclic subgroups of A satisfy the condition iii) above.

Then $c+d+e = 1+q+q^2$. Also, we have

$$|A|\ (\theta|_A, \theta|_A) = 4q^2 + (c+d)(q-1)4q^2.$$

As $|A| = q^3$, we see that q divides $(c+d)(q-1) + 1$, and $(c+d) \equiv 1 \pmod{q}$.

Now, a moment's thought reveals that $|A|\ (0|_A, 1_A) = 2q+cq(q-1)-dq$.

Hence $2+c(q-1)-d$ is divisible by q^2 and $c+d \equiv 2 \pmod q$, which contradicts the fact that we have already proved that $c+d \equiv 1 \pmod q$. Thus the order of S is at most q^2

Suppose now that the order of S is q^2. Then S has $q+1$ subgroups of order q.

Suppose that the generators of c cyclic subgroups of S satisfy the condition ii) above with $w=1$, that the generators of d cyclic subgroups of S satisfy the condition ii) above with $w \neq 1$, and that the generators of e cyclic subgroups of S satisfy the condition iii) above. Then $c+d+e = q-1$

Also, we see that :

$$|S|\ (0|_S, 1_S) = 2q+cq(q-1)-dq.$$

Thus $c+d \equiv 2 \pmod q$. As $0 \leq c+d \leq q+1$ we see that $c+d=2$.

Let A,B be the subgroups of order q of S which satisfy condition ii). We claim that A and B are conjugate in H. For, as q^2 divides the order of H and q^3 does not, 0 is in a q-block

of defect 1 .

As θ does not vanish identically on non-identity elements of A or B , both A and B are conjugate to a defect group of the block containing θ , so that they are also conjugate to each other.

We next claim that θ is q-rational . Suppose that this is not so.Then we may choose generators a,b of A ,B,respectively , such that $\theta(a)=\theta(b)=qw$,where w is a primitive q-th root of unity.We now prove that $a^{-1}b$ lies in $Z(N(S))$, contradicting the fact that $H = O^{q}(H)$,(since S is Abelian).

Let n be any element of N(S).Then either:

i) $A^{n} = A$ and $B^{n} = B$ or

ii) $A^{n} = B$ and $B^{n} = A$.

In the former case, $a^{n} = a$,and $b^{n} = b$ since θ assumes the same value on conjugate elements.Also,in the other case $a^{n} = b$ and $b^{n} = a$ for the same reason. In each case , n centralizes $a^{-1}b$, which verifies our assertion that $a^{-1}b$ lies in $Z(N(S))$.

This contradiction establishes

that θ is q-rational . We note that A and B are both Sylow intersections of order q as they are defect groups

Let A be a Sylow q-intersection of order q in H and let a be a non-identity element of A . We claim that for some irreducible character θ_1 of C(a) we have:

$\theta(ay) = \theta_1(y)$ for each q-regular element y of C(a).

As $\theta(a) \neq 0$, the q-block of H which contains θ must dominate some q-block of C(a) (in the sense of the Brauer homomorphism) . In fact , as θ lies in a q-block of defect 1 of H the q-block of H which contains θ can only dominate q-blocks of defect one of C(a).

In particular, some irreducible constituent of $\theta|_{C(a)}$ has a degree which is divisible by q . Now as a lies outside Z(H) and $\theta(1) = 2q$,any such constituent has degree q.Let θ_1 be one such constituent.

Since $\theta(a) = q$ and $\theta(1) = 2q$, θ_1 is the only irreducible constituent of $\theta|_{C(a)}$ which has degree divisible

by q . Now we can conclude, by using Brauer's second main theorem and the fact that the q-block of H which contains θ has defect one , that for any q-regular element y of C(a) , we have :

$\theta(ay) = w\,\theta_1(y)$, where w is a q-th root of unity with $\theta_1(a) = qw$. Since θ_1 is q-rational , we conclude that w = 1, so that, as desired, we have

$\theta(ay) = \theta_1(y)$.

Now suppose that q = 5. By a theorem of Gaschütz (or just by elementary transfer in this case), C(a) = $\langle a \rangle$ x K , for some subgroup K of C(a). Let $\theta_2 = \theta_1|_K$. Then θ_2 is an irreducible character of K.

Let $\theta|_{C(a)} = \theta_1 + \theta_3$. Since we know that $\theta(a) = q = \theta_1(a)$, we see that $\theta_3(a) = 0$. Since C(a) acts on the eigenspaces of a, we see that θ_3 is a sum of 5 linear characters.

For any 5-regular element of C(a), say y , we know that:

$\theta(ay) = \theta_1(y) = \theta_1(ay)$, so that $\theta_3(ay) = 0$. Consequently , all the linear constituents of θ_3 agree on y.

In particular, each 5-regular element of K' lies in the kernel of θ_3.

There are two cases to consider

Case 1: θ_2 is imprimitive

If θ_2 is imprimitive, then K has an Abelian normal subgroup A such that K/A is isomorphic to a subgroup of S_5.

Now let Q be a Sylow 5-subgroup of K. Then Q has order 5. Now the only primes which can divide the order of [A,Q] are 2, 3 and 7, as 11 divides the order of H to the first power only (if at all), by Lemma 1.2.6, and each element of [A,Q] has the eigenvalue 1 with multiplicity 5 or more (since $[A,Q] \leq K'$).

In any case, [A,Q] contains an elementary Abelian p-group of order p^4, B say, such that B = [B,Q]. As $B \leq K'$ and $\theta_1(1) = 5$, B contains an element, y say, of order p such that $\theta_1(y) = 3+w+\bar{w}$ for some p-th root of unity w. Then $\theta_1(y) = 8+w+\bar{w}$, so that y has a fixed-point subspace of codimension two.

Case 2 : θ_2 is primitive

In this case, we first note that θ_2 is faithful. Suppose that this is not the case. Then as $O_5(K) = 1$, (since $\langle a \rangle$ is a Sylow intersection) $\ker \theta_2$ contains an element x of order prime to 5. Then we have:

$\theta_3(x) = 5 + \theta_3(x) = 5 + 5w$, where w is a primitive $|\langle x \rangle|$-th root of unity. Then $(\det \theta_5)(x) = w \neq 1$, a contradiction, as $H = H'$. Thus θ_2 is faithful.

As θ_2 is faithful and primitive, K' is simple by Lemma 2.1.2. Also, $K' \leq \ker \theta_3$, as each 5-element of K' lies in $\ker \theta_3$. By Lemma 1.2.17, K' is isomorphic to one of:

A_5, A_6 or $PSU(4,2)$.

In any case, K' contains an involution t with $\theta_2(t) = 1$, so that $\theta(t) = 6$ and t has a fixed-point subspace of co-dimension two.

In both cases, K' contains an element with a fixed-point subspace of codimension two, and the proof of the Lemma is complete.

Remark

Lemma 2.3.1 may be useful for the classification of the finite complex quasi - primitive linear groups of degree 10 . The following argument gives an indication of how it might be used .

Let H be such a group of degree 10, and suppose that $O_5(H) = 1$. Let $K = O_2(H)$. If K is non-Abelian, then K is the central product of a cyclic group and a quaternion group . Then C(K) is isomorphic to subgroup of GL(5,ℂ) and H/C(K) is soluble .

If K is Abelian , then $K \leq Z(H)$ because H is quasi-primitive . Thus we may suppose that $E(H) \neq 1$. We may also suppose that E (= E(H)) is an irreducible quasi-primitive complex linear group of degree 10 .

If E is the product of more than one component, then each component is a complex linear group of degree n , where n = 2 or 5 . Thus we may assume that E is quasi-simple.

By Lemma 1.3.8 , we may suppose

that the only primes which divide [E:Z(E)] are 2,3 and 5 . If a Sylow 5-subgroup,R say,of E is non-Abelian then as in the previous Lemma, there is an element ,say x ,of R which has only two eigenvalues . Then x acts with quadratic minimum polynomial in any reduction (mod 5),of H (for we have assumed that $O_5(H) = 1$). By the results of J.G.Thompson on quadratic pairs , E/Z(E) is a simple group of Lie type in characteristic 5.

Thus we may suppose that E has Abelian Sylow 5-subgroups. If there is an element , y say , of order 25 in E , then y^5 acts with quadratic minimum polynomial in any reduction (mod 5) of H , so that E/Z(E) is a group of Lie type .Hence we may suppose that the Sylow 5-subgroups of E are elementary Abelian.

The later arguments of Lemma 2.3.1 may now be applied to E to deduce that, if 25 divides [E:Z(E)] , then E contains an element which has an eigenspace of codimension 2 .By the results of Huffman and Wales , [18], it is possible to determine E in

this case.

Thus we may suppose that 5 divides [E:Z(E)] to the first power only. Thus E/Z(E) is a simple group of order $2^a.3^b.5$, so that E/Z(E) is isomorphic to A_5, A_6 or PSU(4,2).

Corollary 2.3.2

Let p be a prime of the form 2q+1 where q is also prime and $q \geq 5$. Let H be a finite simple irreducible primitive complex linear group of degree p.

Let p be a Sylow p-subgroup of H and suppose that N(P) contains an element of order q.

Then :

i) If $q \geq 11$, H has elementary Abelian Sylow q-subgroups of rank at most 4 .

ii) If $q = 5$ and s is an element of order 5 in N(P), then C(s) has an Abelian Sylow 5-subgroup of rank at most three.

Proof

Let $\theta(h)$ = trace(h) for all h in H. Let x be an element of order p in P and let y be an element of order q in N(P).

Then $\theta(x) = 0$, as in Lemma 2.1.1. Now $\theta|_{P\langle y\rangle} = \theta_1 + \theta_2 + 1$, where θ_1 and θ_2 both are irreducible of degree q, (the fact that $H = O^q(H)$ forces the remaining character to be trivial).

Thus y has the eigenvalue 1 with multiplicity three , so has a fixed point subspace of dimension three. In particular , the fixed point subspace of y contains the one dimensional fixed point subspace of P.

i) When $q \geq 11$, we see that H has elementary Abelian Sylow q-subgroups by Lemma 1.4.3 . Let Q be a Sylow q-subgroup of H which contains y.

Now Q acts on the three dimensional fixed point subspace of y . Let K be the kernel of this action . We first prove that $[Q:K] \leq q^2$.

Let N be the subgroup of Q which acts as scalars on the above three dimensional subspace. Let $L = \langle P, N \rangle$. L is not an irreducible subgroup of H as the one dimensional fixed point

subspace of P is L-invariant.

Let M be the kernel of the action of L on the above one-dimensional subspace. Then $L = M\,N_L(P)$. We know that y lies in M, and that $N_L(P)$ has order divisible by q to the first power only, as $C(P) = P$ and $[N(P):P]$ divides 2q. Thus q does not divide $[N_L(P):N_M(P)]$, so that q does not divide $[L:M]$.

Hence N acts trivially on the above one-dimensional subspace, so that $N = K$. Now Q/K is an elementary Abelian q-group acting faithfully on the three-dimensional fixed-point subspace of y, and no non-trivial element of Q/K can act as a scalar in this action. Thus $[Q:K] \leq q^2$.

We next claim that $|K| \leq q^2$. Let $R = \langle P,K \rangle$. Once more, R is not an irreducible subgroup of H.

As H is simple, there are three possibilities by Lemma 2.1.3.

a) $R \leq N(P)$.

b) R has a normal subgroup, Y say, which is isomorphic to PSL(2,p) and which has index at most 2 in R.

c) E(R) is isomorphic to a primitive irreducible complex linear group of degree p-1 (= 2q).

In cases i) and ii), it is clear that q^2 does not divide $|R|$. We note that $Z(R) = 1$ as $C(P) = P$. To prove that $|K| \leq q^2$, we use Lemma 2.3.1 to conclude that q^3 does not divide $|E(R)|$. Let $E = E(R)$. We prove that q does not divide $[R:E]$.

Now $R = E\,N(P)$, so that R/E is cyclic. As H has elementary Abelian Sylow q-subgroups, we only need to prove that q divides $|N_E(P)|$. Suppose then that q does not divide $|N_E(P)|$, so that $[N_E(P):P] = 2$.

Since E is a simple group which has a faithful irreducible character of degree p-1 we conclude from Lemma 1.2.5 that p is a Fermat prime, and that E is isomorphic to SL(2,p-1), contrary to the fact that $p = 2q+1$ and q is odd. Thus q does not divide $[R:E]$, so that q^3 does not divide $|R|$.

ii) Suppose that $p = 11$. Then, as $\theta(y) = 1$ (we recall that y lies in

N(P) and has order 5) , y has the eigenvalue 1 with multiplicity three and each primitive 5th root of unity as an eigenvalue of multiplicity two.

In particular,as C(y) acts on the eigenspaces of y,all irreducible constituents of $\theta|_{C(y)}$ have degree 3 or less. Hence , C(y) has Abelian Sylow 5-subgroups. Let Q be a Sylow 5-subgroup of C(y), and let D be the subgroup of Q which is generated by the elements of order 5.

Now D acts on the three dimensional fixed-point subspace of y . Let K be the kernel of this action. A similar argument to that used above shows that $[D:K] \leq 25$.

Suppose that K has order 25 or more.Let $M = \langle P,K \rangle$. As K acts trivially on the fixed- point subspace of P, M is not irreducible. Let E = E(M).

We see again that E is an irreducible primitive complex linear group of degree 10 , and as in the proof of part i), we see that 5 does not divide [M:E]. As 25 divides $|K|$, 25 divides $|E|$.

Let V be the p-dimensional complex vector space on which H acts We may write $V = W \oplus Z$,where E acts irreducibly on W and on Z and where $\dim_{\mathbb{C}}(W) = 1$.

Lemma 2.3.1 allows us to conclude that there is an element of E which has a fixed-point subspace of dimension 8 in its action on Z so has a fixed - point subspace of dimension 9 in its action on V.

Lemma 1.3.14 now allows us to deduce that H is isomorphic to A_{12} .Part ii) of this Corollary is certainly valid for A_{12} ,so that the proof is complete

We note that part ii) of the above Corollary is valid for G.We conclude this section ,as promised , with the following result:

Corollary 2.3.3

i) Suppose that M is a subgroup of G which has order divisible by 11 and by 25.Then M is irreducible.

ii) Suppose that a Sylow 5-subgroup, S, of G, is Abelian of order 25 or

more. Then $(X|_S, 1_S) < 3$.

Proof

i) Suppose that the order of M is divisible by 11 and by 25, but that M is not irreducible. Then we may deduce, as in the previous corollary, that M contains an element with a fixed point subspace of dimension 9, contradicting Lemma 2.1.6.

ii) Suppose that S is Abelian of order 25 or more and that $(X|_S, 1_S) \geq 3$

By Lemma 2.2.1, we may suppose that S contains a non-identity element of N(P), say s. We know that X(s) = 1, so that s has the eigenvalue 1 with multiplicity 3.

Thus $(X|_S, 1_S) = 3$, and S acts trivially on the fixed-point space of s. However, s acts trivially on the fixed-point subspace of P. Thus S acts trivially on the fixed-point subspace of P, and $\langle S,P \rangle$ is not an irreducible subgroup of P, contrary to part i), as 25 divides $|\langle S,P \rangle|$.

Section Four

We have seen that N(P) contains an element of order 5, x say . In this section, we prove that the structure of C(x) is very restricted . We also examine the behaviour of X on the 5-section of x in G.

This information will be useful in determining the 5-local structure of G , and the character theoretic information will be helpful when we consider the case in which the order of G is divisible by 5 to the first power only.

Lemma 2.4.1

C(x) has an Abelian normal Sylow 5-subgroup of rank at most 3. Also, C(x) has a normal Sylow 3-subgroup of order at most 3 and cyclic Sylow 2-subgroups of order at most 2.

Furthermore, C(x) does not contain any element of order 6.

Proof

Let $K = P\langle x \rangle$ and let u be a non-trivial element of P.

As $X(u)=0$,it readily follows that $X|_K = \theta_1 + \theta_2 + 1$,where θ_1 , θ_2 are the non-linear irreducible characters of K (on using the fact that X is unimodular,we see that $X(x)=1$).

As $X(x) = 1$, x has the eigenvalue 1 with multiplicity 3, and all other 5th roots of unity as eigenvalues of multiplicity 2.By Lemma 2.1.5 , C(x) is a 7'-group.

By Lemma 1.4.5 ,C(x) contains no element of order 4,so that its Sylow 2-subgroups are elementary Abelian. We show that they are in fact cyclic

If this is not the case, then C(x) contains a subgroup A of type (2,2).By Lemma 1.5.1 , $X|_A$ contains either an irreducible constituent of multiplicity 10 , or else two linear constituents,each with multiplicity at least five.

However,in each case,A contains some non-trivial element with an eigenspace of dimension 10,contrary to Lemma 2.1.6 .

Thus the Sylow 2-subgroups of C(x) have order at most 2,and C(x) has a normal 2-complement.

Let T be a Sylow 5-subgroup of C(x). Then all of the irreducible constituents of $X|_T$ are linear, as every eigenvalue of x occurs with multiplicity at most 3, and T acts on the eigenspaces of x.

Thus T is Abelian. By Lemma 2.3.2, T has rank at most 3. Also, C(x) has a normal 2-complement, which is a $\{3,5\}$-group. Hence C(x) is soluble.

As no irreducible constituent of $X|_{C(x)}$ has degree greater than 3, T is normal in C(x) by Lemma 1.2.11.

We prove next that C(x) has cyclic 3-subgroups. Otherwise, C(x) has some subgroup B of type (3,3).

Now $X|_B$ has two irreducible constituents each of multiplicity 5 or more, so that as B is not cyclic, B contains a non-identity element with an eigenspace of dimension 10, contrary to the hypotheses on G.

Thus C(x) has cyclic Sylow 3-subgroups. As x has no eigenvalue of multiplicity 4 or more, the Sylow 3-subgroups of C(x) have order less than 9 by Lemma 1.5.2.

Suppose that R is a Sylow 3-subgroup of C(x) and that R≠1. We claim that R is normal in C(x) . It is sufficient to prove that [R,T]=1 as RT is the normal 2-complement of C(x).

Now RT acts on the eigenspaces of x , so that $X|_{RT}$ has at most one irreducible constituent of degree 3 or more (including multiplicities)

As RT has odd order,every other irreducible constituent of $X|_{RT}$ is linear , so contains [R,T] in its kernel.

Assume that [R,T]≠1.Then [R,T] contains a subgroup A=[A,T] of type (5,5)and $X|_{RT}$ contains an irreducible constituent of degree 3. As all the other irreducible constituents of $X|_{RT}$ contain A in their kernels , and A is not cyclic , A contains an element which has the eigenvalue 1 with multiplicity 9,contradicting Lemma 2.1.6 .Thus [R,T] = 1.

Now let t be an involution of C(x) (if there is one). Then tx has 10 distinct eigenvalues, so that if

y is an element of order 3 in C(xt) then y acts as a transvection in the reduction (mod 3), contrary to Lemma 1.4.5. Thus C(x) contains no element of order 6, and the proof of the Lemma is complete.

Corollary 2.4.2

i) Suppose that C(x) has even order. Then X(xt) = -1 for any involution t of C(x).

ii) Suppose that y is an element of order 3 in C(x). Then either:

a) X(y) = -4 and X(xy) = 1, or:

b) X(y) = 6w + 5 and X(xy) = w, for some primitive cube root of unity, w.

Case a) must occur when C(x) also has even order.

iii) The 5-block of G which contains X is invariant under any element of Gal ($\mathbb{Q}(X) / \mathbb{Q}$) when C(x) has even order, and is invariant under any element of Gal ($\mathbb{Q}(X)/\mathbb{Q}(w)$) in any case (where w is a primitive cube root of unity).

Proof

i) Suppose that t is an involution of C(x) . We saw in the proof of Lemma 2.4.1 that t has two eigenvalues of multiplicity 5 or more. As t lies in G', t has the eigenvalue -1 with even multiplicity , so that t must have the eigenvalue -1 with multiplicity 6 , and $X(t) = -1$.

Now we saw in Lemma 2.4.1 that in any reduction (mod 5) of G, x is similar to a matrix with two Jordan blocks of size 5 . As x acts on each eigenspace of t, x acts with minimum polynomial of degree five on both eigenspaces of t in any reduction (mod 5) of G . As t is a 5-regular element of G, an argument similar to that preceding Lemma 1.5.1 and Lemma 1.5.2 allows us to conclude that x has five distinct eigenvalues in its action on both (complex) eigenspaces of t.

As x has order 5, it quickly follows that $X(xt) = -1$.

ii) Let y be an element of order 3 in C(x) . A similar argument shows

that 2 of the eigenvalues of y have multiplicity 5 or more , and that x has five distinct eigenvalues in its action on either of the associated eigenspaces of y.

As y is unimodular,only two cases can occur:

a) y is similar to :

diag $(1,w,w,w,w,w,\bar{w},\bar{w},\bar{w},\bar{w},\bar{w})$, where w is a primitive cube root of unity. In this case , $X(y) = -4$ and $X(xy) = 1$.

b) y is similar to :

diag $(1,1,1,1,1,w,w,w,w,w,w)$, where w is a primitive cube root of unity.In this case , $X(y) = 6w+5$ and $X(xy) = w$.

When C(x) also has even order,y is conjugate to its inverse in C(x) ,so that X(y) is real , and case a) must occur.

iii) Let a be any element of $Gal(\mathbb{Q}(X)/\mathbb{Q}(w))$, where w is a primitive cube root of unity. Then by parts i) and ii), X and X^a agree, but do not vanish,on the 5-section of x in G.By Brauer's second main theorem , X and X^a both lie in the same 5-block of G which is consequently a-invariant.

When C(x) has even order, X is rational-valued on the 5-section of x in G, and a similar argument to the one above shows that the 5-block of G which contains X is a-invariant for any element a of Gal(Q(X)/Q).

Section Five

In this section, we show that for a prime divisor, q say, of the order of G, we can obtain a sharper bound on the power of q dividing the order of G, if we know that X is rational valued on q-elements.

The results which we prove here will be used repeatedly later on.

Lemma 2.5.1

i) Let R be a Sylow 2-subgroup of G. Then if $X|_R$ is rational-valued, the order of G is not divisible by 2^{16}.

ii) Let Q be a Sylow 3-subgroup of G. Then if $X|_Q$ is rational-valued, the order of G is not divisible by 3^6.

Proof

i) By Lemma 1.2.13, it is enough to prove that R has a rational-valued faithful character of degree eight.

It is easy to verify that $X|_R = \theta_1 + \theta_2$ where θ_1 and θ_2 are rational-valued characters (though not necessarily irreducible) of respective degrees eight and three. Furthermore, θ_1 is faithful, for otherwise, its kernel contains an involution which has the eigenvalue 1 with multiplicity nine, contradicting Lemma 2.1.6 .

ii) Again by Lemma 1.2.13, it suffices to show that Q has a rational-valued faithful character of degree eight.

A few moments' thought tells us that $X|_Q = \theta + \theta_1$, where θ and θ_1 are both rational valued characters and θ has degree eight . We only need to verify that θ is faithful.

Suppose then that θ is not faithful, and let y be an element of order three in ker θ .Then y has the eigenvalue 1 with multiplicity eight or more.However,as X(1) is odd and X(y) is real, y has the eigenvalue 1 with odd multiplicity.

Thus y has the eigenvalue 1 with multiplicity nine, which contradicts Lemma 2.1.6 .Hence θ is faithful,as required.

Lemma 2.5.2

Let Q be a Sylow 3-subgroup of G. Then:

i) If $X|_Q$ is real-valued, $|Q| \leq 3^{10}$.

ii) If $(X+\bar{X})|_Q$ is rational-valued, $|Q| \leq 3^{11}$.

Proof

i) Suppose that X_Q is real-valued. We first claim that Q has an Abelian normal subgroup of index at most 3.

Suppose that this assertion is false.Then certainly $X|_Q$ contains a non-linear irreducible constituent,θ say.As $X|_Q$ is real-valued,it contains θ and $\bar{\theta}$ with equal multiplicity.

Hence $\theta(1) = 3$ and $(X|_Q, \theta)_Q = 1$. Also, $X|_Q$ can contain no irreducible non-linear constituent apart from θ and $\bar{\theta}$ .Let $K = \ker \theta$ ($= \ker \bar{\theta}$).

As $\theta(1) = 3$, Q/K has an Abelian normal subgroup of index 3. Let D be the inverse image in Q of one such subgroup . By the definition of D,we

see that $D' \leq K$. As all irreducible constituents of $X|_Q$ apart from θ and $\overline{\theta}$ are linear, $D' \leq \ker X = 1$, so that D is Abelian . As $[Q:D] = 3$, the assumption that Q had no Abelian subgroup of index 3 was false.

Let A be an Abelian normal subgroup of Q with $[Q:A] = 3$. We claim that A has rank 4 or less .Let B be the subgroup of A generated by the elements of order 3.Suppose that $|B| \geq 3^5$.

Now the irreducible constituents (apart from the trivial character) of $X|_B$ occur in complex conjugate pairs, and as B has rank 5 , there are 5 such pairs. Furthermore, there is a non-identity element,b say,of B which lies in the kernel of 4 of the above pairs. As $X|_B$ is real-valued and $X(1) = 11$, b has the eigenvalue 1 with odd multiplicity , so with multiplicity 9 , contrary to Lemma 2.1.6 .

Hence A has rank 4 or less.By Lemma 2.1.8 , A has exponent dividing 27 ,so that to complete the proof of i) it is sufficient to prove that A has no subgroup of type (27,27) (for then $|A| \leq 27x9x9x9$, and $|Q| \leq 3^{10}$).

Suppose, on the contrary, that B is such a subgroup of A. Let b be any element of order 27 in B. Now b has 11 distinct eigenvalues, otherwise in any reduction (mod 3) of G, we see that $(b-1)^{10} = 0$, so that b^9 acts as a transvection, contradicting Lemma 2.1.7.

Now as $X|_B$ is real-valued, $X|_B$ contains the trivial character with odd multiplicity. However, for any non-trivial irreducible constituent θ of $X|_B$, $B/\ker\theta$ is cyclic, so that $\ker\theta$ contains an element, u say, of order 27. Thus u has the eigenvalue 1 with multiplicity 2 or more, which contradicts the fact that u has 11 distinct eigenvalues.

This contradiction completes the proof of i).

ii) As in the proof of Lemma 2.1.8, Q has an Abelian normal subgroup, A say, such that $[Q:A] \leq 27$. We prove that $|A| \leq 3^8$. Let $\theta = X+\overline{X}$.

As in the proof of Lemma 2.1.9, A has rank 8 or less. Suppose that A contains an element of order 27. Then $X1_A$ contains a linear constituent, say μ, such that $[A:\ker\mu] = 27$. As $\theta|_Q$ is rational valued, a further eight

algebraic conjugates of μ occur as constituents of $X|_A$. Then any element of $\ker \mu$ has the eigenvalue 1 with multiplicity 9 or more. Thus $\ker \mu = 1$ by Lemma 2.1.6.

In that case A is cyclic of order 27, so we assume from now on that A has exponent dividing 9. If A is elementary Abelian, we see that A has rank at most 8, so that

$$|Q| \leq 27\,|A| \leq 3^{11}.$$

As $\theta|_A$ is rational valued, we may write $X|_A = \beta_1 + \beta_2$, where β_1 and β_2 are characters of A which are invariant under Galois automorphisms of odd order, and where β_1 has degree 9 (so is faithful).

We may assume that A has exponent 9. Then there is a linear constituent, say μ, of β_1 such that $[A:\ker \mu] = 9$. As β_1 is invariant under Galois automorphisms of odd order, β_1 contains a further two algebraic conjugates of μ as constituents.

If β_1 contains another constituent, say γ with $[A:\ker \gamma] = 9$, distinct from the 3 above, then β_1 has two other algebraic conjugates of γ as constituents. There are in fact three possibilities to consider:

a) $\beta_1 = \theta_1 + \theta_2 + \theta_3$, where each θ_i is the sum of three algebraically conjugate characters and $[A:\ker\theta_i] = 9$

In this case, $|A| \leq 3^6$, since β_1 is faithful.

b) $\beta_1 = \theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5$, where θ_1 and θ_2 are both sums of three algebraically conjugate characters, with $[A:\ker\theta_1] = [A:\ker\theta_2] = 9$, but where θ_3, θ_4 and θ_5 are linear and $[A:\ker\theta_i] \leq 3$ for $i = 3,4,$ and 5

In this case, $|A| \leq 3^7$, as β_1 is faithful.

c) $\beta_1 = \theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5 + \theta_6 + \theta_7$,

where θ_i is linear with $[A:\ker\theta_i] \leq 3$ for $2 \leq i \leq 7$, but where θ_1 is the sum of three algebraically conjugate characters, and $[A:\ker\theta_1] = 9$.

$|A| \leq 3^8$ in this case, since β_1 is faithful.

In all cases, $|A| \leq 3^8$, as was to be proved. The proof of the Lemma is now complete.

Lemma 2.5.3

Let S be a Sylow 5-subgroup of G. Then if $X|_S$ is rational valued, S has order 5.

Proof

Suppose that $X|_S$ is rational valued. We know that $S \neq 1$, by Lemma 2.2.1 . We also note that S is Abelian , for if this were not the case, $X|_S$ would contain an irreducible constituent of degree 5, and for some non-trivial element y of Z(S) , X(y) would not be rational.

Now S is elementary Abelian , for a cyclic group of order 25 can have no faithful rational character whose degree is less than 20.

Suppose that the order of S is greater than 5 . As each non-trivial irreducible constituent of $X|_S$ has three other algebraic conjugates, and $X(1) = 11$, it readily follows that $X|_S$ contains the trivial character with multiplicity three.

We may suppose that $S \cap N(P) \neq 1$ by Lemma 2.2.1 . Let x be an element of order five in $S \cap N(P)$.

As x has the eigenvalue 1 with multiplicity three, S acts trivially on the fixed-point subspace of x. In particular , as x acts trivially on the (one-dimensional) fixed-point

subspace of P, S acts trivially on the fixed-point subspace of P.

This contradicts Lemma 2.3.3 .

Lemma 2.5.4

Let T be a Sylow 7-subgroup of Then if $X|_T$ is rational valued, $T=1_G$.

Proof

Suppose that $T\neq 1$, and that $X|_T$ is rational valued. Then any non-trivial irreducible constituent of $X|_T$ has a further five algebraic conjugates.

Thus $X|_T$ contains the trivial character with multiplicity five, and 6 non-trivial linear characters, each algebraically conjugate to the other

Hence $|T| = 7$. Now X is a non-exceptional character in some 7-block of G, since $X|_T$ is rational -valued.

Let u be a generator of T, and let $K = O_{7'}(C(T))$. We note that $X(u) = 4$, as $X(u) \equiv 4 \pmod 7$ and $(X|_T, 1_T)_T$ $(= 11 + 6X(u)) \geq 0$.

We let $K = O_{7'}(C(T))$.

Now we know that $[N(T):C(T)]$

divides 6 , and that as X is a non-exceptional character for the prime 7 , there is an ordinary irreducible character, θ say, of N(T) and a sign e such that $X(uz)=e\theta(z)$ for all z in K

In fact, as $X(u) = 4$, we see that $e = 1$ and $\theta(1) = 4$.

By Clifford's theorem, there are three cases to consider:

Case i) : $\theta|_K$ is irreducible

Let $\phi = \theta|_K$. As $X(uz)=\phi(z)$ for all z in K, it readily follows that there is a linear character θ_1 of K such that $X|_K = \phi + 70_1$.

We first claim that for any involution t of K, we have $\phi(t)=2$ and $\theta_1(t) = -1$. Suppose that this is not the case , and let y be an involution of K violating the above condition.

Suppose first that $\theta_1(y) = -1$ but that $\phi(y) \neq 2$. As $G=G'$, y has the eigenvalue -1 with even multiplicity so that $X(y) \equiv 3 \pmod 4$.

Hence, as $\theta_1(y) =-1$, $\phi(y)\equiv 2 \pmod 4$ so that $\phi(y) = -2$, and $X(y) = -9$. Thus y has the eigenvalue -1 with multiplicity 10, contradicting Lemma 2.1.6 .

Suppose then that $\theta(y) = 1$ Since $X(y) \neq 7$ by Lemma 2.1.6[1], and $X(y) \equiv 3 \pmod 4$, $\phi(y) = -4$.

Now u has the eigenvalue 1 with multiplicity 5, and y acts on the fixed-point subspace of u. In its action on this subspace, y has the eigenvalue -1 with multiplicity 4, the eigenvalue 1 with multiplicity 1

Now in any reduction (mod 2) of G, u still has a 5-dimensional fixed point subspace (as u has odd order) and y acts as a transvection on this subspace (to see this, let W denote the complex fixed-point subspace of u. Then $\dim_{\mathbb{C}}(W(1+y)) = 1$.)

Now all other eigenvalues of u have multiplicity 1, and the same is true in any reduction (mod 2) of G. As y is an involution, y must act trivially on the other eigenspaces of u in any reduction (mod 2) of G.

Thus y acts as a transvection in any reduction (mod 2) of G. This contradicts Lemma 2.1.7..

We claim now that K has cyclic

Sylow 2-subgroups. Suppose that x and z are distinct commuting involutions of K. Then xz is an involution and $\theta_1(xz) = 1$, contradicting the above result. Thus the Sylow 2-subgroups of K are either cyclic or generalized quaternion.

However, the Sylow 2-subgroups of K must in fact be cyclic, as for any involution t of K, we know that $\theta_1(t) = -1$, so that t lies outside K'.

As θ_1 is irreducible of degree four and does not vanish identically on 2-singular elements of K, there is an element, z say, of order 8 in K.

Now z commutes with u and u has one eigenvalue of multiplicity 5, six other eigenvalues of multiplicity 1 each. As u is 2-regular, we see that in any reduction (mod 2) of G, z is similar to a matrix with one Jordan block of size 5 and six Jordan block of size 1.

Thus z^4 is an involution which is a transvection in any reduction (mod 2) of G. This contradicts Lemma 2.1.7, so completes the elimination

of Case i).

Case ii)

In this case ,we assume that there are two irreducible characters, say θ_1, θ_2, of K, both conjugate under the action of $N(T)$, such that:

$$\theta_1|_K = \theta_1 + \theta_2 .$$

As $X(u) = 4$, we note that θ_1 and θ_2 both have degree 2. It is again easy to see that $X_K = \theta_1 + \theta_2 + 7\mu$ for some linear character, μ, of K.

As in Case i),we see that for any involution t of K, $\mu(t) = -1$, $\theta_1(t)+\theta_2(t) = 2$, and K has cyclic Sylow 2-subgroups. In particular,all involutions of K are conjugate.

Now let z be any involution of K.Then as θ_1 and θ_2 are conjugate under the action of $N(T)$,there is an element y of $N(T)$ such that :

$$\theta_2(z) = \theta_1(z^y).$$

As z and z^y are both conjugate in K,we see that $\theta_2(z) = \theta_1(z)$. This contradicts the fact that $\theta_1(z)$ is even , whereas we have already seen that $\theta_1(z)+ \theta_2(z) = 2$.

Case iii)

In this case, we assume that $\theta|_K = 2(\theta_1 + \theta_2)$, where θ_1 and θ_2 are linear characters of K.

This time $X|_K = 2\theta_1 + 2\theta_2 + 7\mu$, for some linear character μ, of K. In particular all irreducible constituents of $X|_K$ are linear, so that K is Abelian.

This contradicts the fact that N(T) has an irreducible character of degree 4, as the degree of a complex irreducible character of any finite group divides the index of any of its Abelian normal subgroups, whereas [N(T):K] is not divisible by 4.

The elimination of case iii) completes the proof of the Lemma.

Remark

Although the arguments of the previous two Lemmas may seem quite involved, it is worth noting that the irreducible character of degree 11 of the group A_{12} is rational-valued whereas the order of A_{12} is divisible both by 25 and by 7.

Section Six

In this section, we prove that the Sylow 5-subgroups of G are elementary Abelian of order at most 125.

Lemma 2.6.1

No 5-local subgroup of G is irreducible.

Proof

Suppose that the Lemma is false. Then we may choose a subgroup M of G which is maximal subject to :

$O_5(M) \neq 1$ and M is irreducible.

Certainly 11 divides $|M|$, so let P be a Sylow 11-subgroup of M. Let S be a Sylow 5-subgroup of M.

Case 1: When M is soluble

Let $F = O_{11'}(M)$. Then $F \geq O_5(M) \neq 1$. In this case $M = FN_M(P)$. Now $X|_F$ has 11 distinct irreducible constituents (as PF is a Frobenius group), each of them linear. Thus F is Abelian.

Let $W = O_5(M)$. Then $X|_W$ has 11

distinct constituents , so that by Lemma 1.5.2 , C(W) is an Abelian 5-group.

Now M = N(W) by the maximality of M.Thus C(W)=W =F.

We claim that W=J(S). Now ZJ(S) ⊴ M ,so M=N(ZJ(S)) by the choice of M.Let Z =ZJ(S).Then PZ is a Frobenius group,so that as above, C(Z) is an Abelian 5-group.Now J(S) is certainly contained in C(Z) , so that J(S) is Abelian and J(S)=Z.

As W is Abelian, W ≤ J(S),so that W=J(S) as claimed.Then S is a Sylow 5-subgroup of N(J(S)),so is a Sylow 5-subgroup of G.

As J(S) is Abelian and is weakly closed in S w.r.t. G, S ≤ M' by the Hall-Wielandt Theorem. Since M = W $N_M(P)$, W = S (otherwise M has a homomorphic image of order 5).

Thus S is Abelian,so that m(S)≤3 by Lemma 2.4.1 . This contradicts the fact that P acts fixed-point freely on S.

Case 2: M insoluble

We may assume that M is monomial.Let

$W = O_5(M)$. Then as above, $W = O_{11'}(M)$, so is the diagonal subgroup of M. Now M/W is isomorphic to a transitive permutation group of degree 11, which must be insoluble, as M is insoluble. By a result of W. Burnside, M/W must be isomorphic to a doubly-transitive permutation group of degree 11. Hence M/W has a subgroup that is isomorphic to PSL(2,11).

Let K be the inverse image in M of one such subgroup, and let V be the subgroup of exponent 5 of W.

As V admits P fixed-point freely, $|V| = 5^{5e}$, where e is some non-negative integer.

If e=2, then V contains an element with an eigenspace of co-dimension 1 (as, assuming V has been diagonalized V consists of all those diagonal unimodular matrices with eigenvalues all lying in the set of 5th-roots of unity.).

This contradicts Lemma 2.1.6 Hence e = 1, so K/W acts irreducibly and faithfully on V.

Now the absolutely irreducible

representations of PSL (2 , 11) in characteristic 5 have degrees 1,5,5, 10 , 11 and all are realizable over GF(5).Thus the action of K/W on V^* is absolutely irreducible,and afforded by the reduction (mod 5) of some absolutely irreducible $\mathbb{C}(K/W)$-module, say N (as [K:W] is divisible by 5 to the first power only).

Let L be a subgroup of index 11 in K,so that L/W is isomorphic to A_5.

Consideration of the character table of PSL(2,11) shows that L/W acts irreducibly on N,so that as 25 does not divide [L:W], L/W also acts irreducibly on the reduction of N (mod 5),which is just V^*.

However, $X|_V$ has 11 distinct constituents , permuted transitively by K/W , so one of them is fixed by L/W,and is not the trivial character, which contradicts the fact that L/W acts irreducibly on V^*.

This completes the elimination of Case 2,and the proof of the Lemma.

Corollary 2.6.2

i) No element of order 5 can act with minimum polynomial of degree 2 in any reduction (mod 5) of G.

ii) Let S be a Sylow 5-subgroup of G. Then for any characteristic subgroup Q of S, there is an element g of G-N(Q) such that $[S : S \cap S^{g}] \leq 25$.

Proof

i) Suppose that s is an element of S. which has order 5 and which acts with quadratic minimum polynomial in some reduction (mod 5) of G. Let W be the weak closure of s in S.

By Lemma 1.4.3 ,N(W) is irreducible contrary to the previous Lemma.

ii) Suppose that Q is characteristic in S ,but that $[S : S \cap S^{g}] > 25$ for any g in G-N(Q). We notice that N(Q) contains N(S).

By the previous Lemma , $X|_{N(Q)}$ is not irreducible.Then by Lemma 1.4.2 , there is an element g of G-N(Q) such that $[S: S \cap S^{g}] \leq X(1)^{2} = 121$ .Thus $[S : S \cap S^{g}] \leq 25$, contrary to our assumption.The proof of the corollary is complete.

Having established this Lemma, we can now proceed to prove that G has Abelian Sylow 5-subgroups.

Lemma 2.6.3

G has Abelian Sylow 5-subgroups.

Proof

Let S be a Sylow 5-subgroup of G and suppose that S is non-Abelian.

By Corollary 2.6.2, no element of order 5 can act with a quadratic minimum polynomial (mod 5) so that each non-identity element of S has 3 or more distinct eigenvalues Now $S' \cap Z(S) \neq 1$. Suppose that $X|_S$ has only one non-linear irreducible constituent, and let x be an element (not the identity) of $S' \cap Z(S)$. Then x has only two eigenvalues (for x belongs to the kernel of each linear character of S), a contradiction.

Thus $X|_S$ has two non-linear irreducible constituents, each having degree 5. Let these constituents be θ_1 and θ_2.

We claim that both are faithful. For suppose that θ_1 is not

faithful and let x be an element of order 5 in $Z(S) \cap \mathrm{Ker}\theta_1$. The unimodularity of X forces x to have only two eigenvalues, which we know is not the case.

We next claim that S is of maximal class. Every element of $Z(S)$ has at most three eigenvalues, so acts with cubic minimum polynomial in any reduction (mod 5) of G. Hence, as $O_5(G) = 1$, every element of $Z(S)$ has order 5. As θ_1 is faithful, $Z(S)$ is cyclic of order 5.

As S has a faithful irreducible character of degree 5, S has an Abelian normal subgroup, A, of index five. Let b be an element of S-A. There is an element a in $A - C_A(b)$. Hence $\langle a,b \rangle$ is non-Abelian, so that $\theta_1 |_{\langle a,b \rangle}$ is irreducible. In particular $Z(\langle a,b \rangle) = Z(S)$, so $|C_S(a) \cap C_S(b)| = 5$ Thus $|C_A(b)| = 5$, so $|C_S(b)| = 25$, and S has maximal class.

We also note that $A = J(S)$, unless $|A| \leq 25$, as this argument applies to any element of S-A. Let $J = J(S)$. We claim that if $|S| > 125$, then J is elementary Abelian. Let B be the

Frattini subgroup of J , and suppose that $B \neq 1$.

We note first that J is Abelian and is weakly closed in S with respect to G. By a well-known argument , two elements of C(J) are conjugate in G if and only if they are conjugate in N(J).In particular ,as J is Abelian, this applies to elements of J.

We use this fact to prove that Z(S) is weakly closed in S w.r.t. G. Let $Z = Z(S)$. As B is normal in S , $Z \leq B$. Also $B \leq S'$,as S has maximal class. Let z be a generator of Z,and suppose that some conjugate,y say,of z,lies in S-Z.

Then y has only 3 distinct eigenvalues , as z has , so that we cannot have $\theta_1(y)=0$. As θ_1 vanishes identically on S-J, y belongs to J.

Thus $y=z^h$ for some h in N(J) Now B is normal in N(J) so that y belongs to B.Thus y lies in S', so belongs to the kernel of the linear constituent of $X|_S$.

The only way that $\det \theta_1(y)$ could be 1 would be for y to lie in

Z (otherwise y would have precisely 2 eigenvalues in the representation affording θ_1 and thus could not be represented by a unimodular matrix). This contradicts the choice of y.

Thus Z is weakly closed in S with respect to G.

By Lemma 1.4.2 ,there is an element g in G-N(Z) such that $[S:S \cap S^g] \leq 25$.

Let $T = S \cap S^g$ .Then T is Abelian, otherwise Z(T) = Z, and $Z = Z^g$,which contradicts the fact that g does not lie in N(Z).Hence TZ is Abelian, and as T cannot contain Z, $|TZ| = |J|$.

Thus TZ = J,as J = J(S),so that Z is complemented in J , contradicting the fact that Z is contained in the Frattini subgroup of J.

Thus J is elementary Abelian if the order of S is greater than 125.

As θ_1 is faithful of degree 5, $|J| \leq 5^5$,so that $|S| \leq 5^6$ and S has class at most 5.

We claim that if S has class ≤ 4 , then Z is weakly closed in S w.r.t G

For $1 \neq z$ in Z it is enough by the above arguments to show that every

conjugate of z contained in S lies in S'.

Suppose first that S has class 3 or 4 . Let y be a conjugate of z which belongs to S . By the argument above , y lies in J . Suppose that y lies outside S'. Then we may choose an element b in S-J , and consider S as a subgroup of K , a subgroup of GL(5,$\mathbb{C}$) isomorphic to Z_5 wreath Z_5 , by extending the representation which affords θ_1 .

Then b lies outside J(K) and y lies outside K', so that $\langle yK', bK' \rangle = K/K'$, and $\langle y,b \rangle = K$, a contradiction as $S \neq K$.

Thus Z is weakly closed in S if S has class 3 or 4 .

If S has class 2, then θ_1 vanishes outside Z , so that z is not conjugate to any element of S-Z as z has only 3 eigenvalues .Thus Z is weakly closed in S wrt G in this case also.

Hence Z is weakly closed in S wrt G if S has class 4 or less.

If S has class 5, we let N=N(J), otherwise we let N=N(Z).

By Lemma 1.4.2 , there is an element g of G-N such that $[S:S\cap S^g]$ is at most 25. We proceed to derive a contradiction from this fact.

Let $T=S\cap S^g$, and suppose that S has class 3 or 4.

Then z lies outside T, so that T is Abelian. Also $T\cap Z_2(S)\neq 1$, as $TZ=J$ and $Z_2(S)\leq J$.

Let $1\neq y$ be an element of $T\cap Z_2(S)$. Then y lies in $Z_2(S)-Z(S)$, so that $\theta_1(y) = \theta_2(y) = 0$, and $X(y) = 1$. Hence y has the eigenvalue 1 with multiplicity 3 , all primitive 5-th roots of unity as eigenvalues of multiplicity 2.

By Lemma 1.4.5 , C(y) contains no element of order 4.

We claim that C(y) is soluble. Let L be the terminal member of the derived series of C(y), and suppose that $L\neq 1$. Then L has Abelian Sylow 2-subgroups, so that Z(L) has odd order . Thus L has no non-trivial character of degree less than 3.

As L acts on each eigenspace of y, $X|_L$ has precisely one non-linear irreducible constituent, which is of

degree 3.Then L contains an element with an eigenspace of co-dimension 2,contrary to Lemma 2.1.6 .

Thus C(y) is soluble,as claimed.Let R be a Sylow 5-subgroup of C(y) . By Lemma 1.2.10, R acts trivially on $O_{5'}(C(y))$. Since R is Abelian, R is normal in C(y).

However,J(S)=R,as [S:J(S)]=5 and y is not conjugate to any element of Z(S) (by consideration of X(y)).

Now $T = S \cap S^g$,and does not contain Z^g so that TZ^g is Abelian and $TZ^g = J^g$. Thus y belongs to J^g,so that we have $J = J^g = O_5(C(y))$, contrary to the fact that $T = S \cap S^g \neq J$.

Suppose that S has class 2. Then Z is not contained in T and so T is cyclic of order 5,as |S| =125.

Let T=<y>.Then X(y)=1, and as above , C(y) is 5-closed , which contradicts the fact that <y> is a Sylow 5-intersection.

Suppose that S has class 5 We claim that θ_1 can be extended to a faithful irreducible character of C(Z).Certainly , it can be extended

to an irreducible character of C(Z) as C(Z) acts on the eigenspaces of Z.

As θ_1 is a faithful character of S the kernel of the extension is a 5'-group.

Let $Z=\langle z\rangle$. Then z acts with cubic minimum polynomial (mod 5), so that as z has only three eigenvalues, all irreducible constituents of $X|_{C(Z)}$ lie in the same 5-block of C(Z) by Lemma 1.5.1.

Thus Ker θ_1, being a 5'-group, lies in the kernel of each of them, hence is trivial.

As 5^5 divides $[C(z):Z(C(z))]$, θ_1 is imprimitive by Lemma 1.3.4.

Thus C(z) has an Abelian normal subgroup A such that $C(z)/A$ is isomorphic to a subgroup of S_5.

As $O_{5'}(C(z)) = 1$, A is a 5-group. Also $[S:A] \leq 5$ so that, as A is Abelian, $A = J(S)$.

Now whenever z^h lies in S, z^h lies in J(S) as before, and $z^h = z^n$ for some n in N (= N(J)). Thus hn^{-1} belongs to $C(z) \leq N$, so $h \in N$.

Thus T does not contain Z, so

that $TZ=J$. Also , T does not contain Z^g , so that $TZ^g=J^g$.

As before, there is an element y in $(Z_2(S) \cap T)$ such that C(y) is 5-closed, so that $J = J^g = O_5(C(y))$, contradicting the fact that T does not contain Z.

Thus S is Abelian and the proof of the Lemma is complete.

Lemma 2.6.4

Let S be a Sylow 5-subgroup of G. Then S is elementary-Abelian and is of order at most 125.

Proof

We know that S is Abelian of rank at most 3.

Suppose that S is not elementary. Then let x be an element of order 25 in S . Now x has 11 different eigenvalues, otherwise we have:

$$(x-1)^5 = (x-1)^{10} = 0 \pmod 5,$$

whereas no element of order 5 acts with quadratic minimum polynomial (mod 5).

Suppose that S has a subgroup A of type (25,25).

Then $X|_A$ is multiplicity-free and contains two distinct irreducible constituents θ_1, θ_2.

Then $\mathrm{Ker}(\theta_1 \bar{\theta}_2)$ contains an element y of order 25.

Thus $\theta_1(y)=\theta_2(y)$, so that y has at most 10 distinct eigenvalues, a contradiction.

Let V be a complement to S in N(S). We claim that $|V|=4$.

We may write $S=T\times E$ where T is cyclic of order 25, E is elementary-Abelian, and V acts on both T and E.

As $X|_T$ has 11 distinct irreducible constituents, C(T) is an Abelian 5-group, so that S=C(T), and V acts faithfully on T. Thus $|V| \leq 4$.

By Lemma |.4.|, S is not cyclic, as X(1)=11. By the Smith-Tyrer theorem, $|V| \neq 2$, so that $|V|=4$, as claimed.

Now V acts Frobeniusly on T, and as X(1)=11, $X|_{VT}$ contains at least three linear constituents (including multiplicities) each of which has $T = [T,V]$ in its kernel.

This contradicts the

fact that $X|_T$ contains 11 distinct constituents , completing the proof of the Lemma.

Section Seven

Some Properties of Local Subgroups

Lemma 2.7.1

Let P be a Sylow 11-subgroup of G. Then P does not normalize any 2-subgroup of G or any 7-subgroup of G.

Proof

Suppose that P acts on a 2-group A. Then PA is a Frobenius group , and all irreducible constituents of $X|_A$ are linear,so A is Abelian.

Now A has rank 10 so (assuming A has been diagonalized) contains all those diagonal unimodular matrices which have all diagonal entries +1 or -1. Thus A contains some element which has the eigenvalue -1 with multiplicity 10 , contrary to our hypotheses on G.

Suppose that P acts on the 7-group B.

Then B is elementary-Abelian of rank 10, and contains an element of order 7 with only two eigenvalues, contrary to Lemma 2.1.5.

Lemma 2.7.2

Let y be an element of order 7 in G Then y centralizes any $\{3,5\}$-group which it normalizes.

Proof

Clearly y centralizes any 5-group which it normalizes, as G has Sylow 5-subgroups of order at most 125.

It thus suffices to prove that y centralizes every 3-group which it normalizes. Suppose that this is not so, and let B be a 3-group minimal subject to $B = [B,y] \neq 1$. Then B is a special 3-group.

Suppose that B is Abelian. Then $X|_{B\langle y\rangle}$ has only one non-linear irreducible constituent, say θ, which has degree 7 and multiplicity one. All linear constituents of $X|_{B\langle y\rangle}$ contain $B = [B,y]$ in their kernels Thus $(X|_B, 1_B{}_B) = 4$.

Now $|B| = 3^6$, so that B contains an element y with $\theta(y) = 5 + w + \bar{w}$, where w is a primitive cube root of unity

Then y has the eigenvalue 1 with multiplicity 9, which contradicts Lemma 2.1.6.

Thus B is a non-Abelian special 3-group. Now $X|_B$ has no irreducible constituent of degree 9. Let θ be an irreducible constituent of degree 3 of $X|_B$. As $X(1) = 11$, θ is y-invariant so $[B,y] \leq \ker\theta$ by Lemma 1.2.10, contrary to $B = [B,y]$.

This completes the proof of the Lemma.

Lemma 2.7.3

Let A be a non-cyclic 5-subgroup of G. Then A centralizes any $\{3,7\}$-group and any Abelian 2-group which it normalizes.

Furthermore, if A is a Sylow 5-subgroup of G, then A centralizes every 2-group which it normalizes.

Proof

Suppose that B is a 3-group minimal subject to $B = [B,A] \neq 1$.

Then B is a special 3-group. Suppose that B is non-Abelian. Then $X|_B$ contains some non - linear irreducible constituent, say θ.

Now θ is A-invariant as $X(1) = 11$, so that $[B,A] \leq \ker \theta$ by Lemma 1.2.10, contrary to $B = [B,A]$.

Thus B is Abelian of order 81, and some non-identity element of A, a say, acts trivially on B.

Let $K=BA$. Then $X|_K$ contains at least 2 non-linear constituents (counting multiplicity), otherwise B contains an element of order 3 having the eigenvalue 1 with multiplicity nine contrary to Lemma 2.1.6.

Hence each irreducible constituent of $X|_B$ has multiplicity at most two. Thus a acts with quadratic minimum polynomial (mod 5) by Lemma 1.5.1, contradicting Lemma 2.6.2.

A similar argument applies to any 7-group or any Abelian 2-group that is normalized by A.

Suppose then that A is a Sylow 5-subgroup of G, and that $1 \neq B$ is a 2-group minimal subject to $B=[B,A]$.

B is a non-Abelian special 2-group, A centralizes Z(B) and [B:Z(B)]=16

Now we may choose an element x of A which acts non-trivially on some Sylow 11-subgroup of G .

By Lemma 2.1.5 , $|C(x)|$ is not divisible by 4 , so Z(B) has order 2 and B is extra-special.

Let z be an element of order 2 in Z(B).Then,again by Lemma 2.1.5, -1 occurs with multiplicity 6 as an eigenvalue of z.

However,each linear character of B contains z in its kernel and the unique non-linear irreducible character of B has degree 4,so that z could not have the eigenvalue -1 with multiplicity 6,a contradiction

Thus no such subgroup B exists, completing the proof of the Lemma.

Section Eight

In this section, we prove that G contains no element of order 35 . We then use this fact to prove that if 7 divides $|G|$, then 25 does not divide $|G|$. We note that A_{12} contains an element of order 35.

Lemma 2.8.1

G contains no element of order 35.

Proof

Suppose that the lemma is false and that s is an element of order 5 in G such that C(s) contains some element, u say, of order 7. Let $C=C(s)$.

Let S be a Sylow 5-subgroup of G which contains s . Then $S \leq C$, as S is Abelian , and $[S, O_{5'}(C)] = 1$ by Lemma 2.7.3 .

Thus $O_{5'}(C)$ has order 2, 3 or 6 by Lemma 2.4.1, (and is not cyclic if it has order 6), so that $O_{5'}(C)$ is certainly centralized by u.

By Lemma 2.7.2, u centralizes $O_5(C)$, so that u centralizes F(C). We claim that C has a component L whose order is divisible by 35.

Certainly $E(C) \neq 1$, as u lies outside F(C), but centralizes F(C). As $O_{5'}(C)$ is soluble, 5 divides $|E|$. Suppose that E is a 7'-group.

Then E has a u-invariant Sylow 5-subgroup A, and $[A,u]=1$ by Lemma 2.7.2. Also, E has a Sylow 3-subgroup, B, which is centralized by u.

Now let R be a u-invariant Sylow 2-subgroup of E. Then $E = RC_E(u)$, as E is a $\{2,3,5\}$-group. Thus $[E,u]=[R,u]$ so is a 2-group. $[E,u]$ is a normal 2-subgroup of E, so $[E,u] \leq Z(E)$. Thus $[E,u,E] = [u,E,E] = 1$, so that $[E,E,u] = 1$ by the three subgroups lemma. As $E = E'$, $[E,u] = 1$.

Consequently, u centralizes $F^*(C)$ and u lies in $Z(F(C))$, contradicting the fact that u lies outside $O_{5'}(C)$

Thus C has a component, L say, of order divisible by seven. Now L has Abelian Sylow 5-subgroups and Abelian Sylow 7-subgroups, so that Z(L) is a $\{2,3\}$-group.

Thus $Z(L) \leq O_{5'}(C)$, so that Z(L) is cyclic of order 1, 2 or 3. As X is faithful, there is some non-trivial irreducible constituent of $X|_L$, say θ. As $|L|$ is divisible by 35, $\theta(1) \geq 4$ by Lemmas 1.3.1 and 1.3.2.

Also, $\theta(1) \leq 8$, as $L \leq C$ and s has no eigenvalue of multiplicity nine or more.

We eliminate the possible values of $\theta(1)$ individually, treating the case $\theta(1)=6$ last, as it is the most difficult.

Case 1: $\theta(1) = 4$

In this case, by Lemma 1.3.3, $L/Z(L)$ is isomorphic to A_7, and $Z(L)$ has order 2. Let t be an involution of $Z(L)$. By Lemma 2.4.1, $X(t) = -1$.

Now t has the eigenvalue -1 with multiplicity six, and L acts on the associated eigenspace. This contradicts the fact that $\theta(t) = -4$ and $X|_L$ cannot have an irreducible constituent of degree two.

Case 2: $\theta(1)=5$

This case cannot occur by Lemma 1.3.4, as 35 divides $[L:Z(L)]$

Case 3 : $\theta(1)=7$

In this case, as no non-identity element of $Z(L)$ has an eigenvalue of multiplicity greater than six, θ is faithful and $Z(L)=1$. Also, as $X|_L$ can have no non-trivial irreducible constituent of degree less than six

$X|_L = \theta + 4.1_L$.

Now as 35 divides $|L|$, L is isomorphic to A_8 or $Sp(6,2)$ by Lemma 1.3.6 .In either case , there is an involution t of L such that $\theta(t)=3$.Then $X(t)=7$, contrary to the hypotheses on G.

Case 4:$\theta(1)=8$

In this case ,as above,$Z(L)=1$ and θ is faithful.By Lemma 1.3.7 , L is isomorphic to A_9 , and so contains an involution t with $\theta(t)=4$.

As $X|_L = \theta+3.1_L$, $X(t)=7$,again contrary to the hypotheses on G.

Case 5:$\theta(1)=6$

In this case $X|_L = 5.1_L + \theta$,so that for each involution t of L-Z(L),we have $\theta(t) = -2$ (for $\theta(t)\equiv 2 \pmod 4$, as L=L'.Also $\theta(t)\neq 2$,as $X(t)\neq 7$.

As 35 divides [L:Z(L)] and $|Z(L)| = 2$ or 3 , we see from Lemma 1.3.5 that L/Z(L) is isomorphic to A_7 or HJ , the Hall-Janko simple group of order 604800.In the second case , we note that $|Z(L)| = 2$.

Case 5a): $|Z(L)| = 2$

In this case, we claim that L has generalized quaternion Sylow 2-subgroups. Let z be the involution of Z(L). Then, by Lemma 2.1.6, we know that $\theta(z) = -6$, so that for any other involution t of L, either $\theta(t) = 2$ or $\theta(zt) = 2$, which we know not to be the case. Thus there are no other involutions in L apart from z, and our claim is established, as $L = L'$.

In fact, as θ is faithful of degree 6, the Sylow 2-subgroups of L/Z(L) have exponent at most 8.

Thus, when Z(L) has even order, the Sylow 2-subgroups of L are of exponent at most 16, so have order at most 32.

By Lemma 1.3.5, L/Z(L) is isomorphic to A_7. Now S normalizes L, as no central product of 5 copies of L can have a faithful complex character of degree eleven.

In fact, S must induce inner automorphisms on L, and as S is

elementary Abelian , we may write LS = L x K ,for some 5-group K .Let b be an element of order 5 in K,and let s be an element of order 5 in S ∩ N(P),for some Sylow 11-subgroup P of G.

As b centralizes L and LK acts irreducibly on the 6 -dimensional eigenspace of t , b acts as scalars on this eigenspace . In particular, b ≠ s, as X(s) = 1 . Also , L acts trivially on the five-dimensional eigenspace of t ,so that s does not lie in L.

We may suppose that s = ab for some element a of order 5 in L .Now a is conjugate to all of its powers within L ,so that θ(a) is rational. Now θ extends to an irreducible character (which we still call θ) of L x K .

We know that θ(s) = 1, and it is easy to see that θ(a) = 1 .Thus we see that θ(b) = 6, so that a and s have the same fixed-points on the 6-dimensional eigenspace of t.Since a acts trivially on the other

eigenspace of t , a acts trivially on the fixed-point subspace of s.

As s acts trivially on the fixed-point subspace of P , we see that $\langle P,a,s \rangle$ acts trivially on the fixed-point subspace of P, so is not irreducible . However, the order of $\langle P,a,s \rangle$ is divisible by 11 and by 25 , contrary to Lemma 2.3.3 .

Case 5b) : $|Z(L)|$ is odd

Once more, $L/Z(L)$ is isomorphic to A_7 (by Lemma 1.3.5), so S induces inner automorphisms on L . Let b be an element of order 5 in L. Then b is conjugate to all its powers. Thus $X(b) = 6$.

Now we may write $LS = L \times C_S(L)$. Also , θ extends to an irreducible character of LS. There is an element, a say, of order 5 in S, with $X(a) = 1$ which normalizes P , some Sylow 11-subgroup of G.

Now $a = b^k c$, for some k and some c in $C_S(L)$. Since θ is irreducible, $\theta(c) = 6w$, for a 5-th root of unity w As $X(b) = 6$ and $X(b^k c) = 1$, we see

that w = 1.

Hence b acts trivially on the fixed point subspace of a , so that $\langle P,a,b \rangle$ is a proper subgroup of G which is not irreducible (as it acts on the one-dimensional fixed-point subspace of P) , but which has order divisible by 25 and by 11 , contrary to Lemma 2.3.3.

This contradiction completes the proof of the Lemma.

Corollary 2.8.2

If 7 divides $|G|$, then 25 does not divide $|G|$.

Proof

Suppose that 7 divides $|G|$ and that 25 divides $|G|$. Let T be a Sylow 7-subgroup of G and let S be a Sylow 5-subgroup of G .By Lemmas 2.5.4 and 2.5.5 , neither $X|_T$ nor $X|_S$ is rational-valued.

By Lemma 1.2.12, G contains an element of order 35,contrary to the previous Lemma.Consequently,if 7 divides $|G|$ then 25 does not.

Remark

It is worth noting at this point that G is a simple group whose order has the form :

$$2^a .3^b .5^c .7^d .11,$$

where $c \leq 1$ or $d = 0$.

Of the 26 presently known sporadic simple groups ,only M_{22} has an order of the correct form and does not appear in the list given in the main theorem of this thesis .However, M_{22} has no complex irreducible non-trivial character of degree less than 21.

. We also remark that at this point ,we are able to assert that G cannot be isomorphic to a group of Lie type . Suppose that G is isomorphic to a group of Lie type .

If G has characteristic 7,then since 11 divides $|G|$, $7^5 + 1$ must divide $|G|$, whereas

$7^5 + 1 = 88.191$ and 191 does not divide $|G|$.

If G has characteristic 3, then since 11 divides $|G|$, $3^5 - 1$ must divide $|G|$, whereas 121 divides $3^5 - 1$ but 121 does not divide $|G|$.

If G has characteristic 5, then since 11 divides $|G|$, $5^5 - 1$ must divide $|G|$, whereas

$$5^5 - 1 = 3124 = 44.71,$$

and 71 does not divide $|G|$.

If G has characteristic 2, then since 11 divides $|G|$, $2^5 + 1$ must divide $|G|$. Also, 2^{18} does not divide $|G|$, and $2^5 - 1$ cannot divide $|G|$, as $2^5 - 1 = 31$.

The only simple groups of Lie type in characteristic 2 which have the required properties are PSU(5,2) and PSU(6,2). We have assumed that G is not isomorphic to PSU(5,2). G is not isomorphic to PSU(6,2) because PSU(6,2) has no non-trivial irreducible character of degree less than 21.

Plainly , if the characteristic of G is 11 , G is isomorphic to PSL(2,11), since 11 divides $|G|$ to the first power only . This contradicts the assumption that G does not satisfy the conclusion of theorem A. Thus G cannot be of Lie type , since the only primes which divide $|G|$ are :

2,3 ,5 , 7 and 11.

For a list of the orders of the groups of Lie type , see page 492 of [14].

We note that G cannot be isomorphic to any alternating group by Lemmas 2.5.2 and 2.5.3.

We remark finally that we may (if necessary) assume that 2^{11} divides $|G|$ and that for a Sylow 2-subgroup , R of G ,we have $SCN_3(R) \neq \phi$.

By the results of Stingl [27] , any simple group whose order is not divisible by 2^{11} is of

'known' type , so G cannot be isomorphic to such a group. By the results of MacWilliams , and of Gorenstein and Harada, [15] , any simple group in which $SCN_3(2) = \emptyset$ is of known isomorphism type, so G cannot be isomorphic to such a group.

We will try to avoid quoting the above results , but there is one point later on where we need the Gorenstein-Harada result , and a few places where we need the results of Stingl.

Chapter Three

In this chapter, we shall prove that 25 does not divide the order of G . Let S be a Sylow 5-subgroup of G . We know already that S is elementary Abelian of order at most 125 .

We eliminate the possibilities $|S| = 25$ and $|S| = 125$ separately .

Section One

In this section , we prove that $|S| \neq 25$. Suppose then that S has order 25. We first prove :

Lemma 3.1.1

16 does not divide $[N(S):C(S)]$.

Proof

Let A be a Sylow 2-subgroup of $N(S) / C(S)$. Then A is isomorphic to a subgroup of $GL(2,5)$. We prove first that A contains no element of order 4 which acts Frobeniusly on S.

Suppose, on the contrary, that A contains such an element and let b be an element of N(S) which induces

such an automorphism on S.Then each irreducible constituent of $X|_{S\langle b\rangle}$ has degree 1 or 4.As X(1) = 11, $X|_{S\langle b\rangle}$ has at least three linear constituents (allowing for multiplicities) ,each of which contains S (= [S,b]) in its kernel.

Thus $(X|_S \; 1_S)_S \geq 3$, contrary to Lemma 2.3.3 Thus no such element b can exist.

Let B be the subgroup of Aut(S) which is isomorphic to SL(2,5).Then (identifying A with its image in Aut(S)), $|A \cap B| \leq 2$ (since B has a unique involution and $A \cap B$ does not contain an element of order 4).

Also we have:

$4|B| = |\text{Aut } S| \geq |AB| \geq |A||B|/2$, so that $|A| \leq 8$, as required.

Lemma 3.1.2

3 does not divide [N(S):C(S)].

Proof

Suppose that the Lemma is false and let x be an element of order 3 in N(S) which induces a fixed-point free automorphism of order 3 on S.

We claim first that C(S) = S. By Lemma 2.2.1, there is an element s of S which normalizes some Sylow 11-subgroup of G. By Lemma 2.4.2, X(s) = 1.

Now S has 6 subgroups of order 5 which fall into two orbits of size 3 under the action of x. Hence at least two other subgroups of order 5 in S are conjugate to $\langle s \rangle$. Let A be a subgroup of order 5 of S which is not conjugate to $\langle s \rangle$ under the action of x. Let $k = \sum_{a \in A^*} X(a)$. We claim that k = 9.

We note that :

$25\,(X|_S, 1_S) = 11 + 12 + 3k$ since X(b) = 1 whenever b is an element of S which lies in a subgroup conjugate to $\langle s \rangle$. Also, every irreducible constituent of $X|_{\langle x \rangle S}$ has degree 1 or 3 and each linear constituent of $X|_{S\langle x \rangle}$ contains S (= [S,x]) in its

kernel. As $(X|_S, 1_S) < 3$ by Lemma 2.3.3, and as $X(1) = 11$, $(X|_S, 1_S) = 2$ Hence $k = 9$ as claimed. In particular $(X|_A, 1_A) = 4$.

Let A be as above and let $z = \sum_{a \in A^*} |X(a)|^2$.

Then $25\,(X|_S, X|_S) = 121 + 12 + 3z$.

Hence $z \equiv 14 \pmod{25}$. Also, z is even, as $|X(a)|^2 = |X(a^{-1})|^2$ and both of these expressions are algebraic integers. Thus $z \equiv 14 \pmod{50}$.

We claim that $z = 64$, from which it will follow that $(X|_S, X|_S) = 13$. We note that $(X|_S, X|_S) \leq 19$. This is because S contains an element s of order 5 which normalizes some Sylow 11-subgroup of G, say P, and such that $X(s) = 1$. Then s has four eigenvalues with multiplicity 2 and one eigenvalue with multiplicity 3.

Now S cannot act as scalars on the 3-dimensional eigenspace of s, for otherwise, $\langle P, S \rangle$ acts as scalars on the fixed-point space of P, so is not irreducible, a contradiction, by Lemma 2.3.3. Thus $X|_S$ contains no constituent of multiplicity greater than 2. Hence $(X|_S, X|_S) \leq 21$. We also have :

$$25\,(X|_S, X|_S) = 121 + 12 + 3z,$$

so that $(X|_S, X|_S) \equiv 1 \pmod 3$, and

$(X|_S, X|_S) \leq 19$.

Thus $z \leq 114$. Also $(X|_S, X|_S) \geq 13$ as $(X|_S, 1_S) = 2$ and S is Abelian. Thus $z \geq 64$. Suppose that $z = 114$.

Now $5\,(X|_A, X|_A) = 121 + z$, so $(X|_A, X|_A) = 47$. As A has only 5 linear characters and $(X|_A, 1_A) = 4$, there are 4 non-negative integers, say t,u,v,w such that :

$47 = (X|_A, X|_A) = 16 + t^2 + u^2 + v^2 + w^2$ and $11 = X(1) = 4 + t + u + v + w$.

For any odd integer ,n say, $n^2 \equiv 1 \pmod 8$. Thus from the equation

$t^2 + u^2 + v^2 + w^2 = 31$,we may assume that $t \equiv 2 \pmod 4$ and that u,v and w are all odd . As t,u,v and w are non-negative and also

$t + u + v + w = 7$, we may assume that $t = 2$,$u = 3$, $v = w = 1$ .However $t^2 + u^2 + v^2 + w^2 = 15$ in that case.

This contradiction proves that $z = 64$ and so $(X|_S, X|_S) = 13$. Thus each non-trivial linear constituent of $X|_S$ occurs with multiplicity 1 and $(X|_S, 1_S) = 2$.

Suppose then that $C(S) \neq S$. Then $C(S)$ contains an element y of prime order q, where $q = 2$ or 3. As S is a q'-subgroup of $C(y)$, y acts as a transvection in any reduction (mod q) of G. This contradicts Lemma 1.4.5. Hence $C(S) = S$.

We next prove that $C(u) \leq N(S)$ for each non-identity element u of S. Suppose that this is not so and let v be a non-identity element of S such that $C(v) \not\leq N(S)$. Let $C = C(v)$. By Lemma 2.7.3, S centralizes $O_{5'}(C)$ so consequently $O_{5'}(C) = 1$. As S is not normal in C, $E(C) \neq 1$ (for S is Abelian and hence centralizes $F(C)$)

Let L be a component of C. As L has Abelian Sylow 5-subgroups and $O_{5'}(L)$ is trivial, L is simple. Since the order of L has the form $2^a 3^b 5$, L is isomorphic to A_5, A_6 or $PSU(4,2)$ by Lemma 1.2.17.

Now v is not conjugate to any power of s, as by Lemma 2.4.1, $C(s)$ has a normal Sylow 5-subgroup (we recall that s is an element of S which normalizes a Sylow 11-subgroup of G). Hence we may suppose that v belongs to the subgroup A above.

Now $\sum_{a \in A^*} |\chi(a)|^2 = 64$, so:

$(\chi|_A , \chi|_A) = 37$. Also:

$(\chi|_A , 1_A) = 4$.

Suppose then that w is a primitive 5th root of unity and that v has the eigenvalue w^i with multiplicity m_i for $1 \leq i \leq 4$.

Then we have:

$$4 + m_1 + m_2 + m_3 + m_4 = 11$$

$$16 + m_1^2 + m_2^2 + m_3^2 + m_4^2 = 37$$

Thus one of the m_i is 4, one of them is 2 , one of them is 1, and the other is 0.

Now L acts on the eigenspaces of v As L is simple , it acts trivially on the eigenspace of dimension 1 and on the eigenspace of dimension 2 . Also each element of order 5 in L is conjugate to its inverse within L , and so has the eigenvalue 1 with odd multiplicity.

We have already seen that each non-identity element of S has the eigenvalue 1 with multiplicity 3 or 4 , so that every element of order 5 in L has the eigenvalue 1 with multiplicity 3 .

Let u be any element of order 5 in $L \cap S$. Then u acts without fixed points on the 4-dimensional fixed point subspace of v, as u has the eigenvalue 1 with multiplicity 3 and u acts trivially on a 1-dimensional eigenspace of v and a 2-dimensional eigenspace of v. This contradicts the fact that $(X|_S, 1_S) = 2$.

Hence no such element v exists and S is normal in C(u) for every non-identity element u of S. We next prove that [N(S):C(S)] = 6.

As $X|_S$ is not real-valued, no element of N(S) can invert every non-identity element of S. From the structure of GL(2,5) it follows that 4 cannot divide [N(S):C(S)], so that [N(S):C(S)] = 3 or 6. As $C(s) \leq N(S)$ for each non-identity element of S, [N(S):C(S)] ≠ 3, for if it were, then N(S) would be a Frobenius group of order 75, contradicting Lemma 1.2.7, as X(1) = 11. Thus [N(S):C(S)] = 6.

We prove next that the order of G divides $2^{15} \cdot 3^5 \cdot 5^2 \cdot 11$. As N(S) contains no element of order 4 and S is normal in C(s) for every non-identity element s of S, G contains no element of order 20.

As $X|_S$ is not rational-valued, Lemma 1.2.12 tells us that $X|_T$ is rational-valued for any Sylow 2-subgroup T of G. Hence 2^{16} does not divide $|G|$ by Lemma 7.5.1 .

A similar argument shows that G contains no element of order 15, and Lemmas 1.2.12 and 2.5.1 allow us to conclude that 3^6 does not divide $|G|$. Hence $|G|$ divides $2^{15}.3^5.5^2.11$ as claimed.

As $S \cap S^g = 1$ for any g in G-N(S), $[G:N(S)] \equiv 1 \pmod{25}$. Also , we have $[N(S):S] = 6$,and it quickly follows that $[G:S] \equiv 6 \pmod{25}$.

We recall that for a Sylow 11-subgroup P of G , N(P) has order 55 or 110. Also $[G:N(P)] \equiv 1 \pmod{11}$ by Sylow's theorem .Thus we have :

a) $[G:P] \equiv 5$ or $10 \pmod{11}$.

We now have enough information to determine the order of G . Let $|G| = 2^a 3^b 5^2 11$. Then we know that $2^a 3^b 11 \equiv 6 \pmod{25}$. Hence we have

b) $2^a 3^b \equiv 21 \pmod{25}$.

Thus $2^a 3^{b-1} = 7 \equiv 32 \pmod{25}$,so that:

c) $2^{a-5} .3^{b-1} \equiv 1 \pmod{25}$.

We know that $1 \leq b \leq 5$ as 3 divides $[N(S):C(S)]$.

Case i) : b = 1

Then $2^{a-5} \equiv 1 \pmod{25}$. Hence $a \equiv 5 \pmod{20}$. As $a \leq 15$, $a = 5$. Thus $|G| = 2^5 .3.5^2 .11$ and also $[G:P] = 32.3.25 \equiv 2 \pmod{11}$, which contradicts a) above.

Case ii) : b = 2

Then $2^{a-5} 3 \equiv 1 \pmod{25}$

Thus $2^{a-5} \equiv -8 \pmod{25}$ and

$2^{a-8} \equiv -1 \pmod{25}$.

Hence $a \equiv 18 \pmod{20}$, contradicting the fact that $a \leq 15$.

Case iii) : b = 3

Then $2^{a-5} 3^2 \equiv 1 \pmod{25}$, so that $a \equiv 11 \pmod{20}$. Hence $a = 11$, as $a \leq 15$. Thus $|G| = 2^{11} 3^3 5^2 11$. Now $[G:P] = 2.27.25 \equiv 8 \pmod{11}$ which contradicts a) above.

Case iv) : b = 4

In this case $2^{a-5} 3^3 \equiv 1 \pmod{25}$, so that $2^{a-4} \equiv 1 \pmod{25}$ and we have:

$a \equiv 4 \pmod{20}$.

Thus $a = 4$, as $a \leq 15$. Consequently, $|G| = 2^4 .3^4 . 5^2 .11$, which we may assume not to be the case.

Case v) : b = 5

In this case $2^{a-5} 3^4 \equiv 1 \pmod{25}$, so that $a \equiv 17 \pmod{20}$. As $a \leq 15$, this is a contradiction.

This completes the proof of Lemma 3.1.2.

Corollary 3.1.3

N(S)/C(S) is Abelian of order 4 or 8 and of rank at most 2.

Proof

As N(S)/C(S) is isomorphic to a subgroup of GL(2,5) and has order not divisible by 5 or 3 , N(S)/C(S) is a 2-group . By Lemma 3.1.1 , the order of N(S)/C(S) is at most 8.

As G is simple , $[N(S):C(S)] \neq 2$ by the Smith-Tyrer theorem . Also we saw in the course of the proof of Lemma 3.1.1 that N(S)/C(S) had no subgroup of order 4 acting Frobeniusly on S. Thus no element of order 4 in N(S)/C(S) is conjugate to its inverse .

Suppose then that $[N(S):C(S)] = 8$ Then as N(S)/C(S) is isomorphic to a subgroup of GL(2,5) , it cannot be elementary Abelian . Thus N(S)/C(S)

contains an element of order 4, say u As u is not conjugate to its inverse in $N(S)/C(S)$ and $\langle u \rangle$ is normal in $N(S)/C(S)$, u lies in the centre of $N(S)/C(S)$, so that $N(S)/C(S)$ must be Abelian.

Remark

Before we can proceed we require the help of a Lemma.

Lemma 3.1.4

Let u be an element of order 5 in G which acts non-trivially on the 3-group B. Then :

i) C(u) has cyclic Sylow 2-subgroups

ii) B is Abelian .

Proof

Suppose that [B,u] is not Abelian. Then $X|_{[B,u]}$ contains an irreducible constituent ,θ ,which is non-linear. By Lemma 2.1.8, $\theta(1) = 3$. As $X(1) = 1$, $\theta = \theta^u$. By Lemma 1.2.10, $[B,u] \leq \ker\theta$, contrary to the fact that θ is not linear. Thus [B,u] is Abelian.

Now $X|_{\langle u \rangle [B,u]}$ contains two non-linear constituents, for otherwise, there is an element ,x, of order 3 in [B,u] with $X(x) = 8$, contrary to

Lemma 2.1.6. Hence $X|_{[B,u]}$ contains the trivial character precisely once so that B is Abelian (for [B,u] has been shown to lie in the kernel of any non-linear constituent of $X|_B$, so there can be no such constituent).

We now claim that in any reduction (mod 5) of G,u has 2 Jordan blocks of size 5 in its Jordan normal form. This readily follows, since <u>[B,u] is a Frobenius group and [B,u] has a fixed-point space of dimension 1 in any reduction (mod 5) of G (because [B,u] is a 5'-group with a complex fixed-point space of dimension 1).

Now we may apply the arguments of Lemma 2.4.1 to u in place of x, to conclude that C(u) has cyclic Sylow subgroups of order 2 or less.

Lemma 3.1.5

C(S) has odd order.

Proof

We note that the order of C(S) divides 6 |S| by Lemma 2.4.1 , and that C(S) contains no element of order 6 by the same Lemma.

Suppose then that C(S) contains an involution t . We first prove that $O_5(C(t)) \neq 1$. Let C = C(t).

Now S acts on $O_5(C)$,and in fact centralizes $O_{5'}(C)$ by Lemma 2.7.3 . Thus $O_{5'}(C) = \langle t \rangle$ .Suppose then that $O_{5'}(C) = 1$.Then S centralizes $F(C)$,so that $E(C) \neq 1$.

Let L be a component of C.We claim that 25 does not divide $|L|$. For L acts on the eigenspaces of t and by Lemma 2.4.2, X(t) = -1,so that t has the eigenvalue -1 with multiplicity 6 and , of course , the eigenvalue 1 with multiplicity 5 . Thus either L or L/Z(L) has a faithful irreducible character of degree 6 or less. As 7 does not divide the order of G , 25 does not divide the order of L by [10].

Suppose that L is the unique component of C.Then as $|L|$ is of the form $2^a 3^b 5$, $L/Z(L)$ is isomorphic to one of of : A_5 , A_6 or $Sp_4(3)$ .In particular , the outer automorphism group of L is a 5'-group.

However S acts on L ,so that $C_S(L) \neq 1$. Then $C_S(L)$ centralizes $F(C)$,so that $C_S(L) \leq Z(F(C))$ which contradicts the fact that $O_5(C) = 1$.

We may, and do, suppose that C has two components, say L_1 and L_2. We note that C is a $\{2,3,5\}$-group, so that the order of every component of C is divisible by 5. As C has Abelian Sylow 5-subgroups of order 25, L_1 and L_2 are the only components of C.

Now L_1 and L_2 both act on the 5-dimensional 1-eigenspace of t and as $Z(L_i) \leq \langle t \rangle$ for i = 1 and 2, we may suppose that L_1 acts trivially on the above space (because for each i, $L_i / Z(L_i)$ is simple and no non-Abelian simple group has a faithful complex character of degree 2 or 1.)

Suppose that L_1 acts irreducibly on the 6-dimensional -1-eigenspace of t. Then L_2 acts as scalars on the above space, and hence trivially, as L_2 is perfect. In particular, t does not belong to L_2 and L_2 is simple.

We claim that L_2 contains an involution u such that X(u) = 7, contradicting Lemma 2.1.6. Let θ be the character afforded by the action of L_2 on the 1-eigenspace of t. As L_2 acts trivially on the 6-dimensional -1-eigenspace of t, we only need to prove that L_2 contains an involution u with $\theta(u) = 1$.

Let v be any involution of L_2. As $L_2 = L_2'$, $\theta(v) \equiv \theta(1) \pmod 4$, so that $\theta(v) \equiv 1 \pmod 4$. Suppose then that $\theta(v) = -3$. By Glauberman's Z^*-theorem, there is a conjugate v^h of v such that v and v^h commute (where h lies in L_2). Then $\theta(v) = \theta(v^h) = -3$ and it quickly follows that $\theta(vv^h) = 1$. Thus in any case, we may choose some involution u of L_2 with $\theta(u) = 1$, as claimed.

We now prove that t is the only involution in L_1. Let the character afforded by the action of L_1 on the -1 -eigenspace of t be θ. Suppose that u is an involution of L_1 but that $u \neq t$.

Then $\theta(u) \equiv 2 \pmod 4$ and $\theta(u) \neq -6$ as $u \neq t$. Thus $\theta(u) = 2$ or -2. If $\theta(u) = 2$, then $X(u) = 7$ which contradicts Lemma 2.1.6. If $\theta(u) = -2$, then $X(tu) = 7$, which also contradicts Lemma 2.1.6. Thus no such involution u exists.

Thus the Sylow 2-subgroups of L_1 are generalized quaternion. Also each irreducible constituent of θ is of even degree. We have seen already that θ is not irreducible.

Suppose that θ is the sum of three (not necessarily distinct) irreducible constituents of degree 2 Then L_1 is isomorphic to SL(2,5) and contains an element, z say, of order 6 whose eigenvalues are $1, -w, -\bar{w}$, where w is a primitive cube root of unity This contradicts Lemma 1.3.10.

Thus $\theta = \theta_1 + \theta_2$, where θ_1 is irreducible of degree 2 and θ_2 is irreducible of degree 4. However, L_2 centralizes L_1, so that L_2 must act as scalars, and hence trivially, on the -1-eigenspace of t. As in the proof that θ was not irreducible, we may find an involution u of L_2 with $X(u) = 7$, contrary to Lemma 2.1.6. Thus $O_5(C) \neq 1$.

Now we let T be a Sylow 2-subgroup of G containing t. Suppose first that T has an elementary Abelian normal subgroup, A say, of rank at least 3 For any involution u of G, we define $\theta(u) = O_5(C(u))$. We prove that $\theta|_A$ is an A-signalizer functor.

Let a and b be two commuting involutions of G. We prove that $\theta(a) \cap C(b) \leq \theta(b)$. This proves that θ is balanced. We first show that $\theta(a) \cap C(b) \leq O_{2'}(C(b))$

Let $C = C(b)$. Let $\bar{C} = C/O_{2'}(C)$. Let u be an element of order 5 in $\theta(a) \cap C$. We only need to prove that $\bar{u}$ centralizes $F^*(\bar{C})$.

Now $\bar{u}$ lies in $O_{2'}(C_{\bar{C}}(\bar{a}))$ so $\bar{u}$ centralizes $O_2(\bar{C})$. It only remains to prove that $\bar{u}$ centralizes $E(\bar{C})$. Let $\bar{L}$ be a component of $\bar{C}$. If 25 divides $|C|$ then $O_5(C) \neq 1$ by an argument above, so that 25 does not divide $|\bar{C}|$. Certainly 25 does not divide $|\bar{C}|$ if 25 does not divide $|C|$, so that in any case 25 does not divide $|\bar{C}|$.

Thus $\bar{L}$ is the unique component of $\bar{C}$, and $|\bar{L}|$ has the form $2^a 3^b 5$. Hence $\bar{L}/Z(\bar{L})$ is isomorphic to one of:

$$A_5, A_6 \text{ or } Sp_4(3).$$

In particular, the outer automorphism group of $\bar{L}$ has order prime to 5 and $\bar{u}$ induces inner automorphisms on $\bar{L}$.

Thus $\bar{u}\,\bar{y}^{-1}$ centralizes $\bar{L}$ for some $\bar{y}$ in $\bar{L}$. Also, as $\bar{y}$ and $\bar{u}$ both centralize $O_2(\bar{C})$, $\bar{u}\,\bar{y}^{-1}$ must centralize $F^*(\bar{C})$. Hence $\bar{u}^{-1}\bar{y}$ lies in $Z(F(\bar{C}))$ and $\bar{u}$ lies in $F^*(\bar{C})$. As $\bar{u}$ is 2-regular and $F^*(\bar{C}) = \bar{L}\,O_2(\bar{C})$, $\bar{u}$ lies in $\bar{L}$. Suppose that $\bar{u} \neq 1$.

Then $\bar{a}$ centralizes a Sylow 5-subgroup of $\bar{L}$ (namely $\langle \bar{u} \rangle$) and (as $\bar{L}/Z(\bar{L})$ is isomorphic to one of the groups above), $\bar{a}$ centralizes $\bar{L}$ Thus $\bar{L}$ centralizes $O_5(C_{\bar{C}}(\bar{a})) = \langle \bar{u} \rangle$, a contradiction.

Thus $\theta(a) \cap C \leq O_{2'}(C)$. Let u be an element of order 5 in $\theta(a) \cap C$. Then u is centralized by the group $\langle a,b \rangle$ which is elementary Abelian of order 4. Then u centralizes every 3-group which it normalizes by Lemma 3.1.4. As $O_{2'}(C)$ is a $\{3,5\}$- group with Abelian Sylow 5-subgroups, u centralizes the Fitting subgroup of $O_{2'}(C)$. Hence u lies in $O_5(C)$ and we have : $\theta(a) \cap C(b) \leq \theta(b)$.

Let $K = \langle \theta(t) : t^2 = 1, t \text{ lies in } T \rangle$ We claim that K is a 5-group. This is proved by standard arguments, but we include as proof as this is as quick as quoting the necessary results. For any elementary Abelian subgroup, Y, of T of order 4 or more, we define $\theta(Y)$ to be $\langle \theta(y) : y \in Y \rangle$.

Next, let B be an elementary Abelian subgroup of T of order 8 or more. We prove that $\theta(B)$ is a 5-group.

Case 1: $\theta(b)$ cyclic for each b in B

Let x and y be any two elements of B, and suppose that $\theta(x)$ and $\theta(y)$ both have order 5 . Then as B acts on $\theta(x)$ and on $\theta(y)$, there is some involution z of B which centralizes both $\theta(x)$ and $\theta(y)$.Thus:

$\theta(x) = \theta(x) \cap C(z) \leq \theta(z)$,so that $\theta(x) = \theta(z)$, as $\theta(z)$ is cyclic . By a similar argument ,$\theta(y) = \theta(z)$,so that $\theta(y) = \theta(x)$.

Hence in this case $\langle \theta(b) : b \in B \rangle$ has order 1 or 5.

Case 2: $|\theta(b)| = 25$ for some b in B

Let b be an element of B such that $\theta(b)$ has order 25. Suppose that there is an element z of B with $\theta(z) \neq \theta(b)$ We claim that z may be chosen so that $|\theta(z)| = 25$.

Suppose that $\theta(z)$ has order 5.Then there is an involution x of B which centralizes $\theta(z)$ and such that :

$$\theta(b) \cap C(x) \neq 1 .$$

Now $\theta(z) = \theta(z) \cap C(x) \leq \theta(x)$ and : $\theta(b) \cap C x) \leq \theta(x)$. As $\theta(z) \neq \theta(b)$, $\theta(x)$ has order 25 and $\theta(x) \neq \theta(b)$. Thus we may replace z by x if need be ,and assume that $|\theta(z)| = 25$.

We claim next that we may assume that $\theta(z) \cap \theta(b) \neq 1$. Suppose, on the contrary that $\theta(z) \cap \theta(b) = 1$. Then there is an involution x of B such that $\theta(z) \cap C(x) \neq 1$ and such that $\theta(b) \cap C(x) \neq 1$.

Now $\theta(b) \cap C(x) \leq \theta(x)$ and $\theta(z) \cap C(x) \leq \theta(x)$. As $\theta(z) \cap \theta(b) = 1$ $\theta(x)$ has order 25 and $\theta(x) \neq \theta(b)$. Hence we may replace z by x if need be, and assume that $\theta(z) \cap \theta(b) \neq 1$.

Let $X = \theta(z) \cap \theta(b)$ and let $N = N(X)$. Then $\langle B, \theta(b), \theta(z) \rangle \leq N$. Also there is an involution x of B such that $\theta(z) \cap C(x) \not\leq X$ and such that $\theta(b) \cap C(x) \not\leq X$ (we obtain x by considering $\overline{N} = N/X$).

Now $\theta(z) \cap C(x) \leq \theta(x)$ and $\theta(b) \cap C(x) \leq \theta(x)$. Since $\theta(x)$ is an Abelian 5-group, the two groups $\theta(z) \cap C(x)$ and $\theta(b) \cap C(x)$ commute. Thus $\langle X, \theta(z) \cap C(x), \theta(b) \cap C(x) \rangle$ is a 5-group and so has order 25, as 125 does not divide $|G|$.

Hence we quickly see that:

$X(\theta(z) \cap C(x)) = X(\theta(b) \cap C(x))$

which contradicts the fact that $\theta(z) \neq \theta(b)$, but :

$$\theta(z) = X(\theta(z) \cap C(x)) \text{ and}$$

$$\theta(b) = X(\theta(b) \cap C(x)).$$

Thus we have established that $\theta(B)$ is a 5-group. This applies in particular to the group A chosen above.

Now let u be any involution of T Then as the rank of A is at least 3, the group $\langle u \rangle C_A(u)$ is elementary Abelian of order 8 or more .Now, as $C_A(u)$ is not cyclic,

$$\theta(u) = \langle \theta(u) \cap C(z) : z \in C_A(u) \rangle$$

$$\text{so } \theta(u) \leq \langle \theta(z) : z \in C_A(u) \rangle \leq \theta(A)$$

Hence $K \leq \theta(A) \leq K$, so that $K = \theta(A)$ and K is a 5-group .We now prove that whenever D is a subgroup of T which contains an elementary Abelian subgroup of order 4 , $N(K)$ contains $N(D)$. Again , the arguments used are standard.

Let D be such a subgroup of T and let B be an elementary Abelian subgroup of D of order 4 . From the definition of θ it is obvious that $\theta(u^g) = \theta(u)^g$ for any involution u of G.

Let x be any element of N(D). Then $B \leq D \leq T$. It suffices to prove that $\theta(B) = K = \theta(B^x)$, for then $K^x = \theta(B)^x = \theta(B^x) = K$ so that x lies in N(K).

Now let Y be a non-cyclic subgroup of T of order 4. Then:

$$K = \langle C_K(y) : y \in Y \rangle$$

Let $\theta(Y) = \langle \theta(y) : y \in Y \rangle$. Since T has an elementary Abelian normal subgroup of order 8, and K has order 25, $C_T(K) \neq 1$. Let z be an involution of $Z(T) \cap C(K)$. Then $K = \theta(z)$, clearly.

Thus

$$K = \langle \theta(z) \cap C(y) : y \in Y \rangle \leq \theta(Y) \leq K,$$

so that $K = \theta(Y)$. Consequently,

$$K = \theta(B) = \theta(B^x) = \theta(B)^x = K,$$ as required.

Now by Lemma 1.6.2, $T = T \cap G' = T \cap N(K)'$. However, (by Lemma 3.1.2 if K is not cyclic), $N(K) / C(K)$ is an Abelian 2-group. Thus $T \leq C(K)$. Hence $|K| = 5$, for if K has order 25, then K is a Sylow 5-subgroup of G and $N(K) = C(K)$, so that G has a normal 5-complement which contradicts the fact that G is simple.

Let u be any involution of N(K) We claim that $C(u) \leq N(K)$. We may suppose that u lies in T . Hence u lies in C(K).

Now $\emptyset(y)$ is cyclic for any involution y of G. As K is not trivial, there is an involution x of T such that $K = \emptyset(x)$. Let z be any involution in Z(T).Then :

i) $K = \emptyset(x) = \emptyset(x) \cap C(z) = \emptyset(z)$

ii) $K = \emptyset(z) = \emptyset(z) \cap C(u) = \emptyset(u)$.

Thus $C(u) \leq N(K)$ as $\emptyset(u) = O_5(C(u))$

This argument applies to the involution t which was assumed to lie in C(S) . As $C(S) = S \times \langle t \rangle$, we see that $N(S) \leq C(t) \leq N(K) = C(K)$. Hence $S \cap G' = S \cap C(K)'$, so that K lies outside G', a contradiction.

Thus T has no elementary Abelian normal subgroup of order 8 or more , contrary to the remarks at the end of chapter two.

Lemma 3.1.6

C(S) = S.

Proof

Suppose that $C(S) \neq S$. Then $C(S)$ contains an element, x say, of order 3 (by Lemmas 3.1.5 and 2.4.1). Let $C = C(x)$. We note that S centralizes $O_{5'}(C)$ by Lemma 2.7.3, so $\langle x \rangle = O_{5'}(C)$

By Lemma 2.4.2, either $X(x) = -4$, or $X(x) = 5 + 6w$, where w is a primitive cube root of unity We treat these two cases separately.

Case i) : $X(x) = -4$

In this case, x has the eigenvalue 1 with multiplicity 1, and has both the primitive cube roots of unity as eigenvalues of multiplicity 5.

Let θ be the complex character of C afforded by the action of C on one of the 5-dimensional eigenspaces of x. Then $(\det \theta)(x) \neq 1$, so that, in particular, x does not lie in C'.

We prove next that 3 divides $|G|$ to the first power only. To do this, it is enough to prove that 9 does not divide $|C|$.

Suppose that 9 divides $|C|$. Then as $N(S)/C(S)$ is a 2-group and 9 does not divide $|C(S)|$, S is not normal in C. As S centralizes both $O_5(C)$ and $O_{5'}(C)$, $E(C) \neq 1$.

Let L be a component of C. Then Z(L) is a 5'-group , as L has Abelian Sylow 5-subgroups. As x lies outside C' and $Z(L) \leq O_{5'}(C) = \langle x \rangle$, L is simple . As L acts non-trivially on one of the eigenspaces of x ,L has a faithful complex character of degree 5 or less , so L is isomorphic to one of : A_5 ,A_6 or PSU(4,2).

We claim that L = E(C).Suppose on the contrary that L_2 is another component of C.Then L_2 is simple. Now neither L nor L_2 can have a faithful complex character of degree less than 3. As L and L_2 act on the eigenspaces of x , one of them must act trivially on a 5-dimensional eigenspace of x.

We may suppose then that L_2 acts trivially on one of the 5-dimensional eigenspaces of x . Certainly L_2 acts trivially on the 1-dimensional fixed point subspace of x . Let θ be the character afforded by the action of L_2 on the remaining 5-dimensional eigenspace of x . Once more, as L_2 is simple , L_2 contains an involution t such that $\theta(t) = 1$. Hence $X(t) = 7$, contrary to Lemma 2.1.6.Thus L is the unique component of C.

Suppose that $O_5(C) = 1$, and let u be an element of order 5 in C-L. Then u induces inner automorphisms on L, so that uy^{-1} centralizes L for some y in L. As $F(C) = \langle x \rangle$, uy^{-1} centralizes $F^*(C)$. Hence uy^{-1} lies in $Z(F(C))$. This is a contradiction as $u \neq y$ and $Z(F(C)) = \langle x \rangle$. Thus $O_5(C) \neq 1$.

Let $K = O_5(C)$. We can now derive a contradiction by consideration of the action of K in any reduction (mod 5) of G. Certainly, L cannot act trivially on either 5-dimensional eigenspace of x, for if it did, then there would be an involution t of L with $X(t) = 7$ contrary to Lemma 2.1.6.

Neither A nor PSU(4,2) has a faithful complex character of degree less than 5. Thus $L \cong A_5$, for otherwise, as K centralizes L, K acts as scalars on each 5-dimensional eigenspace of x, so that by Lemma 1.5.2, K acts trivially in any reduction (mod 5) of G.

Suppose than that $L = A_5$. We exhibit a 5'-subgroup W of L such that $X|_{\langle x \rangle W}$ contains no irreducible constituent of multiplicity 3 or more. In fact, let W be a subgroup of L isomorphic to A_4. Let θ_1, θ_2 be the characters of W

afforded by its action on the two 5-dimensional eigenspaces of x.

As L acts non-trivially on each 5-dimensional eigenspace of x , θ_1 and θ_2 each have an irreducible constituent of degree 3 . Thus neither θ_1 nor θ_2 contains any irreducible constituent of multiplicity 3 . Hence $X|_{\langle x \rangle W}$ cannot contain any irreducible constituent of multiplicity 3 or more.

As K centralizes $\langle x \rangle W$, Lemma 2. . tells us that each element of K acts with minimum polynomial of degree at most 2 in any reduction (mod 5) of G. This contradicts Lemma 2.6.2 and so completes the elimination of case i).

Case ii) $X(x) = 6w + 5$

Suppose that S is normal in C.Then C divides $|N(S)|$, so that 9 does not divide $|C|$.Consequently,$\langle x \rangle$ is a Sylow 3-subgroup of G . However , x is not conjugate to its inverse in G, so that G has a normal 3-complement, whereas G is simple.Thus S is not normal in C.

As S centralizes F(C) , $E(C) \neq 1$. Let L be a component of C . As C has Abelian Sylow 5-subgroups , Z(L) is a

5'-group. Thus $Z(L) \leq O_{5'}(C) = \langle x \rangle$.

If C has another component, say L_2 then either L or L_2 acts trivially on the 5-dimensional eigenspace of x. We assume that L acts trivially on this space. Now L_2 acts non-trivially on the 6-dimensional eigenspace of x, for otherwise L_2 contains an involution t with $X(t) = 7$, contrary to Lemma 2.1.6. Of course L acts non-trivially on the 6-dimensional eigenspace of x. Let $E = E(C)$. Then $E = L L_2$. Let θ be the character afforded by the action of E on the 6-dimensional eigenspace of x. It readily follows that

$$\theta = \theta_1 + \theta_2$$

where θ_1 and θ_2 are both irreducible of degree 3, and also $L \leq \ker \theta_1$, $L_2 \leq \ker \theta_2$.

Now however, $X|_L = 8_{L_1} + \theta_{L_2}$, so that L contains an involution t with $X(t) = 7$, contrary to Lemma 2.1.6. Hence L is the unique component of C.

If L acts trivially on the 5-dimensional eigenspace of x, then $\theta(t) = -2$ for every involution, t of L. Let A be a subgroup of L of type

(2,2) (such a subgroup exists because Z(L) has odd order) . Then we note that $(X|_A, 1_A) = 5$, and that every other constituent of $X|_A$ occurs with multiplicity 2.

Since x acts trivially on the fixed-point space of A and x has only one eigenvalue on each of the other 'eigenspaces' of A , x must act trivially in any reduction (mod 3) of G, by the arguments which precede Lemma 1.5.1 .This contradiction shows that L acts non-trivially on the 5-dimensional eigenspace of x.

Then L has a non-trivial complex irreducible character of degree 5 or less ,so that 25 does not divide $|L|$ and $L/Z(L)$ is isomorphic to A_5 , A_6 or to PSU(4,2). In particular, L admits no outer automorphism of order 5.

Since $|S| = 25$ and $O_{5'}(C) \leq Z(C)$, it thus follows that $O_5(C) \neq 1$. Let $T = O_5(C)$. Suppose that L is not simple .Then $Z(L) \leq O_{5'}(C) = \langle x \rangle$, so that $Z(L) = \langle x \rangle$. In particular , L has non-Abelian Sylow 3-subgroups.

We note that $L/Z(L)$ is not isomorphic to A_5, as L has non-Abelian Sylow 3-subgroups, so that L acts irreducibly on the 5-dimensional fixed-point space of x. Thus each element of T acts as scalars on this space. As L has non-Abelian Sylow 3-subgroups, θ is either irreducible or is the sum of two irreducible characters of degree 3 (as $\theta(x) = 6w$, where w is a primitive cube root of unity). Thus each element of T has at most two eigenvalues on this space.

As x is a 5-regular element and and every element of T has at most two eigenvalues on any eigenspace of x, each non-identity element of T acts with quadratic minimum polynomial in any reduction (mod 5) of G, contrary to Lemma 2.6.2. Thus L is simple.

If L is not isomorphic to A_5, the same argument may be applied, as L has no non- trivial complex irreducible character of degree less than 5 and L acts non-trivially on each eigenspace of x. Thus L is isomorphic to A_5.

Let u be any element of order 3

in L . Then u has three eigenvalues on the 5-dimensional eigenspace of x , so ux has three eigenvalues , and cannot be conjugate to x . Now $S \leq LT$ so that $C = LN(S)$.

Since $\langle x \rangle$ is a Sylow 3-subgroup of N(S) , $L\langle x \rangle$ contains a Sylow 3-subgroup of C.Thus x is not conjugate to any other element of order 3 in C, (x is certainly not conjugate to its inverse , because X(x) is not real). As G is simple , this contradicts Lemma 1.6.5 , so the proof of this Lemma is complete.

Lemma 3.1.7

There is an element g of G-N(S) for which $S \cap S^g \neq 1$.

Proof

Suppose that $S \cap S^g = 1$ for all g in G-N(S).Then $[G:N(S)] \equiv 1 \pmod{25}$.Also S is normal in C(s) for any element s, of order 5 in G . Since 3 does not divide [N(S):C(S)] and C(S)= S , there is no element of order 15 in G.

By Lemma 2.5.3 , X is not 5-rational, so by Lemma 1.2.12 , X is

3-rational . Hence , by Lemma 2.5.1 ,
3^6 does not divide $|G|$. By the remarks
at the end of chapter two, we may also
suppose that 2^{11} divides $|G|$.

Since $[N(S):S] = 4$ or 8,
$[G:S] \equiv 4$ or $8 \pmod{25}$. Hence G
is of the form $2^a.3^b.5^2.11$, where

i) $11 \leq a \leq 17$.

ii) $0 \leq b \leq 5$.

iii) $11.2^a.3^b \equiv 4$ or $8 \pmod{25}$.

iv) $5^2.2^a.3^b \equiv 5$ or $10 \pmod{11}$.

Now $11.2^4 \equiv 1 \pmod{25}$, so that

v) $3^b.2^{a-6} \equiv 1$ or $2 \pmod{25}$.

Now $2^{13}.3 \equiv 1 \pmod{25}$, so that

vi) $a \equiv 13b + 6$ or $13b + 7 \pmod{20}$.

Since $2^a.3^b.5^2 \equiv 5$ or $10 \pmod{11}$,
we also have :

vii) $2^a.3^b \equiv 9$ or $7 \pmod{11}$, so that

viii) $a \equiv 2b+6$ or $2b+7 \pmod{10}$.

If $a \equiv 2b+6 \pmod{10}$, a is even, so
that $a \equiv 13b + 6 \pmod{20}$, and so

$$11b \equiv 0 \pmod{10} .$$

Thus $b = 0$ and $a \equiv 6 \pmod{20}$, contrary to the fact that $11 \leq a \leq 17$.

If $a \equiv 2b + 7 \pmod{10}$, then we have : $a \equiv 13b+7 \pmod{20}$, so again $11b \equiv 0 \pmod{10}$, which leads to the same contradiction.

Lemma 3.1.8

3^6 does not divide $|G|$.

Proof

Suppose that 3^6 divides $|G|$. Then X is not 3-rational, by Lemma 2.5.1. Also X is not 5-rational, by Lemma 2.5.3.

Let X^σ be a character distinct from, but 5-conjugate to, X. Let X^τ be a character distinct from, but 3-conjugate to, X. Then it is immediate that :

$$(X-X^\sigma, X-X^\tau) = 1$$

Thus there must be an element, u say, such that :

$$X(u) \neq X^\sigma(u) \text{ and } X(u) \neq X^\tau(u).$$

Then u must be 3-singular and 5-singular. Let z be the 5-part of u. Since $C(S) = S$ and S centralizes any

5'-group which it acts on, $O_{5'}(C(z)) = 1$

Let $C = C(z)$.

Since 3 divides $|C|$ and 3 does not divide $|N(S)|$, S is not normal in C. Let $E = E(C)$. Then $E \neq 1$, as S centralizes $F(C)$. We claim that E is isomorphic to A_5. Suppose that this is not the case.

As $|E|$ is of the form $2^a.3^b.5$, E is isomorphic to A_6 or to PSU(4,2). Since $O_{5'}(C) = 1$, E is simple. In either case, E has no faithful complex irreducible character of degree less than 5. We claim that $X|_E$ has an irreducible constituent of degree 5.

Suppose that this is not the case. We note that E acts on the eigenspaces of z. If E is isomorphic to A_6, then one of these eigenspaces must have dimension 8 or more, since $X|_E$ contains a faithful irreducible constituent of degree greater than 5. We claim that z has no eigenvalue of multiplicity 8 or more. Suppose that z has such an eigenspace.

As G is simple, there is a conjugate, y say, of z, such that $[z,y] \neq 1$. We let $K = \langle z,y \rangle$. Then $X|_K$ contains a linear

constituent of degree 5 or more . Now 25 does not divide $|K|$, for otherwise ,K must contain a Sylow 5-subgroup of G , whereas $X|_S$ contains no irreducible constituent of degree greater than 3 (because S contains an element s with X(s) = 1).

If z is conjugate to its inverse within K , complex conjugate eigenvalues of z occur with equal multiplicity . Thus the only eigenvalue which can occur with multiplicity greater than five is 1 . But 1 must occur with odd multiplicity as an eigenvalue of z , as X(1) is odd . Thus z has the eigenvalue 1 with multiplicity 9, contrary to Lemma 2.1.6 .

Thus z is not conjugate to its inverse within K . Since $\langle z \rangle$ is a Sylow 5-subgroup of K , K must have a normal 5-complement , R say. Let N = [R,z] . Then $(X|_N , 1)_N \geq 5$, because $X|_K$ contains a linear constituent of multiplicity 5 or more . Suppose that z does not centralize a $\langle z \rangle$-invariant Sylow 3-subgroup,W, of N. Then [W,z] is Abelian,otherwise $X|_{[W,z]\langle z \rangle}$ contains a linear constituent of degree 3 , θ say , and $[W,z,z] \leq \ker \theta$ by Lemma 1.2.10, a contradiction,as [W,z,z] = [W,z].

Then $X|_{[W,z]} = 6.1_{[W,z]} + \theta$, where θ is the sum of five non-trivial linear characters , permuted transitively by z.

Now W contains an element , n say, of order 3 ,such that $\theta(n) = 2$ .Then n has the eigenvalue 1 with multiplicity 9, contrary to Lemma 2.1.6.Suppose then that Q is a z-invariant Sylow 2-subgroup of N which is not centralized by z . Then an argument to that immediately above shows that [Q,z] is non-Abelian .

Now $X|_{[Q,z]} = \theta + 7\,1_{[Q,z]}$, where θ is an irreducible character of degree 4 and $\theta^z = \theta$. Since [Q,z] contains no involution t such that $X(t) = 7$, any involution , v ,of [Q,z] has $\theta(v) = -4$. Thus [Q,z] has a unique involution,which is central .

Now [Q,z] is generalized quaternion, so z centralizes [Q,z],a contradiction. Thus N = 1, so that z centralizes R. By a similar argument, y centralizes R .

Since $K = \langle z,y \rangle$, $R \leq Z(K)$ .However, R was the normal 5- complement of K, so K has a normal Sylow 5-subgroup , which contradicts the assumption that y and z do not commute . Thus z has no such

eigenspace, and E is not isomorphic to A_6 unless $X|_E$ contains a constituent of degree 5.

Suppose then that E is isomorphic to PSU(4,2), but that $X|_E$ contains no irreducible constituent of degree 5. Then $X|_E = 0 + 5\,1_E$, for an irreducible character, 0, of E, of degree 6.

Now E contains no involution t such that X(t) = 7. Thus 0(v) = -2 for any involution, v, of E. Let A be an elementary Abelian subgroup of E. Then $|A|\,(\,0|_A, 1_A) = 6 - 2\,(\,|A|-1)$, so that $|A| \leq 4$. However, PSU(4,2) has an elementary Abelian subgroup of order 8 so E cannot be isomorphic to PSU(4,2). Thus, as long as E is not isomorphic to A_5, $X|_E$ contains an irreducible constituent, say 0, of degree 5.

Since X(1) = 11 and C(S) = S, X lies in the principal 5-block of G. Thus, there are complex numbers $c_0, c_1, \ldots, c_n$ such that, for any 5-regular element, x of C(z), we have

$$X(xz) = \sum_{0_i \in B_0^{(5)}(C(z))} c_i\, 0_i(x).$$

As $\theta(1) = 5$, θ lies in a 5-block of defect one ,say B,of C(z) . Thus we have

$$\sum_{\mu \in B} (X|_{C(z)}, \mu)\ \mu(zx) = 0$$

for any such x.

In particular , we may set x = 1 in the above sum. This contradicts the fact that X(1) = 11 and 5 divides $\mu(1)$ for any μ in B,whereas at least one character from B,namely θ,occurs with non-zero multiplicity.

This contradiction shows that E is isomorphic to A_5 (and in fact it also shows that $X|_E$ cannot have any irreducible constituent of degree 5).

Now $C(z) = \langle z \rangle \times K$, for some subgroup K of C(z) .Also, we know that $K = E\ N_K(S \cap K)$,so $[K:E] \leq 2$, as K has a self-centralizing Sylow 5-subgroup .

If $[K:E] = 2$, then K is isomorphic to S_5 , so that any complex character of K is rational-valued . If K = E ,

then K has a self-centralizing Sylow 3-subgroup of order 3.

We recall that there is a 3-singular u , of G , with 5-part z , such that X(u) is not 5-rational or 3-rational. This contradicts the fact that K acts on the eigenspaces of z and any complex character of K is rational-valued on 3-singular elements of K ,whereas there is a 3-singular element , h say , of K such that X(u)= X(zh) is not 3-rational

This contradiction proves that 3^6 does not divide $|G|$.

Remark

We have in fact proved that for any element s of order 5 in S such that S is not normal in C(s) , E(C(s)) must be isomorphic to A_5 and furthermore , $X|_E$ contains no irreducible constituent of degree 5, where E = E (C(s)).

Lemma 3.1.9

i) S has two weakly closed cyclic subgroups, W and Y say ,such that ,for for any s in S - (W $\cup$ Y), C(s) = S .

ii) [G:N(S)] $\equiv$ 6 or 11 (mod 25).

Proof

By Lemma 3.1.2, N(S)/S is Abelian of order 4 or 8.We saw in the proof of that that Lemma that no element of order 4 in in N(S) can act Frobeniusly on S. Thus N(S)/S is not cyclic of order 8.

Let A be a complement to S within N(S) .Then we may regard A as a subgroup of GL(2,5) acting on the 2-dimensional 'vector space',S . Since A is Abelian of exponent 2 or 4, A may be assumed to be a group of diagonal matrices .

In that case, the subgroups W,Y of S corresponding,respectively,to the spaces generated by $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$,are normalized by A , so are normal in N(S) , and hence are weakly closed in S with respect to G We note that W is not conjugate to Y in N(S), so not in G either.

For any element s of S-(W∪Y) , $A \cap C(s) = 1$, so that C(s) has a normal 5-complement. Since S centralizes every 5'-group which it normalizes , and since C(S) = S, we see that C(s) = S.

ii) By Lemma 3.1.7, there is an element s of order 5 in S such that S is not normal in C(s) . By i), s lies either in W , or in Y.

Suppose that s lies in Y.Then as E(C(s)) is isomorphic to A_5 , we see that E (N(Y)) is isomorphic to A_5. In particular, N(Y) has 6 Sylow 5-subgroups.

If Y is the only non-trivial Sylow intersection contained in S , then S permutes the Sylow 5-subgroups of G that are not contained in N(Y) in cycles of length 25 (under conjugation).In that case , $[G:N(S)] \equiv 6 \pmod{25}$.

If W is also a Sylow 5-intersection, then N(W) also has 6 Sylow 5-subgroups . S is the only Sylow 5-subgroup of G which lies in N(Y) and N(W) . Also , S permutes the Sylow 5-subgroups of G which lie outside (N(W)∪N(Y)) in cycles of length 25,so that $[G:N(S)] \equiv 11 \pmod{25}$ in this case.

Lemma 3.1.10

N(S)/ S is non-cyclic of order 4.

Proof

We assume that 2^{11} divides $|G|$.

i) Suppose that $[N(S):C(S)] = 8$.

Let $G = 2^a.3^b.5^2.11$. Then we know that $11.2^{a-3}.3^b \equiv 11$ or $6 \pmod{25}$, so that either :

$$2^{a-3}.3^b \equiv 1 \pmod{25}$$

or :

$$2^{a-8}.3^{b-1} \equiv 1 \pmod{25}$$

Then either :

1) $a \equiv 13b + 3 \pmod{20}$ or

2) $a \equiv 13b-5 \pmod{20}$.

Case 1) : $a \equiv 13b + 3 \pmod{20}$

We know that $b \leq 5$. If $b = 1$, then $a = 16$, and we have:

$$|G| = 2^{16}.3.5^2.11$$

Let P be a Sylow 11-subgroup of G. Then $[G:N(P)] \equiv 1 \pmod{11}$, and

$$|N(P)| = 55 \text{ or } 110$$

whereas $3.5.2^{16} \equiv 2^{18} \equiv 3 \pmod{11}$, a contradiction.

If $b = 2$, then $a \equiv 9 \pmod{20}$, contrary to the fact that $11 \leq a \leq 17$. If $b = 3$, then $a \equiv 2 \pmod{20}$, contrary

to the fact that $1 \leq a \leq 17$. If $b = 4$, then $a \equiv 15 \pmod{20}$, so $a = 15$. If $b=5$ then $a \equiv 8 \pmod{20}$, a contradiction, as $11 \leq a \leq 17$.

In this case, then, we see that

$$|G| = 2^{15} \cdot 3^{4} \cdot 5^{2} \cdot 11.$$

Case 2) : $a \equiv 13b-5 \pmod{20}$

If $b = 1$, then $a \equiv 8 \pmod{20}$, a contradiction . If $b = 2$, then we see that $a \equiv 1 \pmod{20}$, a contradiction. If $b = 3$, then $a \equiv 14 \pmod{20}$, so that

$$|G| = 2^{14} \cdot 3^{3} \cdot 5^{2} \cdot 11$$

Now for a Sylow 11-subgroup, P, of G , we have:

$[G:P] \equiv 9 \pmod{11}$, contrary to Sylow's theorem and the fact that N(P) has order 55 or 110.

If $b = 4$, then $a \equiv 7 \pmod{20}$, a contradiction. If $b = 5$, $a \equiv 0 \pmod{20}$, a contradiction. Hence this case cannot occur .

We conclude that $|G| = 2^{15} \cdot 3^{4} \cdot 5^{2} \cdot 11$, and that $[G:N(S)] \equiv 11 \pmod{25}$. Then for Y and W , the subgroups of order 5 defined in the previous Lemma , we see

that N(W) and N(Y) both have six Sylow 5-subgroups .

Let A be a complement to S in N(S) Since we have assumed that A has order 8 , A contains an element of order 4 which acts as $\begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$ on S (when A is regarded as a subgroup of GL(2,5) . We know that A is isomorphic to $Z_4 \times Z_2$) Let this element be x .

We see that x transitively permutes the remaining four subgroups of order 5 of S . Let b be an element of order 5 in $S \cap N(P)$, for a Sylow 11-subgroup, P of G . Let $B = \langle b \rangle$.

By Lemma 2.4.1 , $N(B) \leq N(S)$, so that B is neither W nor Y . By Lemma 2.7.3 , $C(b) = S$. Thus N(P) must have order 55, (for N(P) contains no element of order 10) . Then we have :

$$[G:N(P)] = 2^{15} \cdot 3^{4} \cdot 5 \equiv 2 \pmod{11},$$ a contradiction.

Thus $[N(S):C(S)] = 4$. Suppose that $N(S)/S$ is cyclic . Let A be a Sylow 2-subgroup of N(S). A is generated by an element , a , of order 4 which acts like $\begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$ on S (when A is .

regarded as a subgroup of GL(2,5)).

Let W and Y be the subgroups of S ,defined in the previous Lemma. Let b be an element of order 5 in S n N(P), where P is some Sylow 11-subgroup of G. We claim that $\langle b \rangle = W$, (recall that W is the subgroup of S generated by the element $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$).

Suppose that $\langle b \rangle$ is not weakly closed in S with respect to G.Then the 4 subgroups of order 5 in S distinct from Y and W are all conjugate to $\langle b \rangle$ by the action of A .For any non-identity element , z say , of one of these subgroups,we have :

$$X(z) = X(b) = 1.$$

. We also note that any element w, say , of W is conjugate to all of its non-trivial powers ,and that each element of y is conjugate to its inverse. Thus :

$$25 \ (X|_S , 1_S) = 11 + 16 + 4r + 2t,$$

where $r = X(w)$ for any w in $W^{\#}$, and

$t = X(y) + X(y^2)$ for any y in $Y^{\#}$.

(We note that r and t are both integers).Now $(X|_S , 1_S)$ is

odd ,since r and t are integers . By Lemma 2.3.3, $(X|_S, 1_S) = 1$, so that

$$4r + 2t = -2.$$

Since r = X(w) for some w which is conjugate to all of its powers , r = 1 or 6 . If r = 6 ,then t = -13, so that $5\,(X|_Y, 1_Y) = -15$, which is absurd . Thus r = 1, and t = -3. Now X(w) = 1 , so w has the eigenvalue 1 with multiplicity 2 and has each primitive cube root of unity as an eigenvalue of multiplicity 2.

As in the proof of Lemma 2.4.1 , C(w) has a normal Sylow 5-subgroup. Thus N(W) has a normal Sylow 5-subgroup , so [G:N(S)] ≡ 6 (mod 25).

Now let $|G| = 2^a.3^c.5^2.11$ .Then

$$2^{a-7}.3^{b-1} \equiv 1 \pmod{25}\ ,\ \text{so}$$

$$a \equiv 13c-6 \pmod{20}..$$

If c = 1, then a ≡ 7 (mod 20), a contradiction, as 11 ≤ a ≤ 17. If c = 2, a≡ 0 (mod 20),a contradiction If c = 3 , then a ≡ 13 (mod 20), so that

$$|G| = 2^{13} \cdot 3^{3} \cdot 5^{2} \cdot 11.$$

However, we note that $C(b) = S$ by Lemma 3.1.9, so that $|N(P)| = 55$, and $[G:N(P)] \equiv 2 \pmod{11}$, contrary to Sylow's theorem. Thus $c \neq 3$.

If $c = 4$, then $a \equiv 6 \pmod{20}$, a contradiction. If $c = 5$, then we see that $a \equiv 9 \pmod{20}$, a contradiction.

This contradiction proves that $\langle b \rangle$ is weakly closed in S wrt G, so that $\langle b \rangle = Y$ or W. We note that C(W) has a normal 5-complement, so that $C(W) = S$. Thus S is not normal in N(Y) so that $Y \neq \langle b \rangle$ (for S is normal in C(b)). Hence $\langle b \rangle = W$.

We see, as above, that $[G:N(S)] \equiv 6 \pmod{25}$, so that again we have $|G| = 2^{13} \cdot 3^{3} \cdot 5^{2} \cdot 11$. Again, we see that $C(b) = S$, so that N(P) has order 55 for a Sylow 11-subgroup P of G, and $[G:N(P)] \equiv 2 \pmod{11}$, a contradiction.

Lemma 3.1.11

$|S| \neq 25$.

Proof

Given the assumption that $|S| = 25$, we have the following information:

i) For some s of order 5 in S, $E(C(s))$ is isomorphic to A_5.

ii) $N(S)/S$ is elementary Abelian of order 4, and $C(S) = S$.

We use this information to derive a contradiction. It is easy to see that, for the element s in i) $C(s)$ is isomorphic to $Z_5 \times A_5$.

We first claim that s cannot have the eigenvalue 1 with multiplicity seven. Suppose that it does. Let $E = E(C(s))$, let b be an element of order 5 in E, and let u be an element of order 5 in $S \cap N(P)$, for some Sylow 11-subgroup, P, of G.

Since $X(u) = 1$, u is not a power of s. Since L acts on each eigenspace of s, and L has no non-trivial complex character of degree less than 3, L acts trivially on all the eigenspaces of s, apart from the 7-dimensional fixed-point subspace of s (for s is conjugate to its inverse in N(S), so all eigenvalues

of s, apart from 1, occur in complex conjugate pairs). Thus b has the eigenvalue 1 with multiplicity 4 or more, so that u is not a power of b either.

We may suppose then, that u = sb. Now we may suppose that s and b are both diagonal , and that

s = diag $(\alpha, \bar{\alpha}, \beta, \bar{\beta}, 1, 1, 1, 1, 1, 1)$

b = diag $(1, 1, 1, 1, *, *, *, *, *, *)$

where α and β are primitive 5-th roots of unity (though they need not be distinct).

Since u = ab , and u has the eigenvalue 1 with multiplicity 3, b acts trivially on the fixed-point space of u , so that $\langle P, u, b \rangle$ acts trivially on the fixed-point space of P, but has order divisible by 11 and by 25, contrary to Lemma 2.3.3 .

Thus s cannot have the eigenvalue 1 with multiplicity 7. By Lemma 2.1.6, s cannot have the eigenvalue 1 with multiplicity 9.

Let x be an element of order 3 in E . Let C = C(x) . We prove that 9 does not divide |C|. Suppose then that 9 divides |C| .Then as 9

does not divide $|N(\langle s\rangle)|$, C does not have a normal Sylow 5-subgroup.

We note that $X|_E$ has 2 or more non-linear constituents since E contains no element with an eigenspace of co-dimension 2. Since $X|_E$ cannot contain any irreducible constituent of degree 5, as in Lemma 3.1.8 , the multiplicity of w as an eigenvalue of x is just the number of non-linear constituents of $X|_E$, (where w is a primitive cube root of unity).

Suppose that there are just two non-linear constituents of $X|_E$. Then x has the eigenvalue 1 with multiplicity 7 and the eigenvalues w and $\bar{w}$ with multiplicity 2 each.

Now s centralizes $O_{5'}(C)$, for let $R = O_{5'}(C)$. Then [R,s] acts trivially on both 2-dimensional eigenspaces of x. If $[R,s] \neq 1$, it is easy to see that [R,s] contains an element with a fixed-point space of dimension 9 , contrary to Lemma 2.1.6 .

Since $C(sx) = C(s) \cap C(x)$, we

conclude that $O_{5'}(C) = \langle x \rangle$. Since $\langle s \rangle$ is not normal in $C(x)$, $C(x)$ has a component , L say .

Now L acts trivially on each two-dimensional eigenspace of x . We may suppose that :

$x = \mathrm{diag}(w, w, \bar{w}, \bar{w}, 1, 1, 1, 1, 1, 1, 1)$

$s = \mathrm{diag}(1, 1, 1, 1, *, *, *, *, *, *, *)$.

Since x is an element of E , the component of $C(s)$, we deduce that both non-linear constituents of $X|_E$ come from the action of E on the fixed-point space of s.This fixed-point space must therefore have dimension 6 or more. Since s is conjugate to its inverse in G , this space has odd dimension.

However,we have already seen that the fixed-point space of s cannot have dimension 7 (or 9) , a contradiction .

We conclude that x has the eigenvalue w with multiplicity 3 or more , so exactly 3, since $X|_E$ has at most 3 non-linear constituents.

Again, we see that $O_{5'}(C) = 1$, and that C has a component , L say.

The same argument as above allows us to deduce that s acts non-trivially onone of the 3-dimensional eigenspaces of x.

We see that $[N_L(\langle s\rangle):C_L(\langle s\rangle)] = 2$ and that $C = L\langle x\rangle$. We observe that $L/Z(L)$ is isomorphic to A_5 or A_6, and that $Z(L) = 1$ in the former case, but $Z(L) \neq 1$ in the latter case (for L has a non-trivial complex character of degree 3).

We also note that C has a self-centralizing Sylow 3-subgroup . Thus G has a self-centralizing Sylow 3-subgroup, so X is in the principal 3-block of G, as 3 does not divide X(1)

Let θ be the irreducible character of degree 3 of C which is afforded by the action of C on one of the 3-dimensional eigenspaces of x . We claim that θ does not lie in the principal 3-block of C(x). This is certainly true if L is isomorphic to A_5 (for θ lies in a 3-block of defect 1 in that case).Suppose then that $L/Z(L)$ is isomorphic to A_6.

We note that L must act

non-trivially on the 5- dimensional fixed-point space of x,for otherwise s would have the eigenvalue 1 with multiplicity 7, which we have shown not to be the case . Let t be an involution of C(s) which inverts x (there is such an involution, since C(s) has a component isomorphic to A_5).

Then t lies in the extended centralizer of x . Since L acts irreducibly on the five-dimensional fixed-point space of x , and since t centralizes <s>,a Sylow 5-subgroup of L , t acts as a scalar on the 5-dimensional fixed-point space of x.

Now t inverts x,and x has the eigenvalues w , $\overline{w}$ with multiplicity three each (where w is a primitive cube root of unity) . Now t must interchange these eigenspaces. Since t acts as a scalar on the other eigenspace of x , we conclude that X(t) = 5 or -5 .

As G = G' and X(1) = 11,we must in fact have : X(t) = -5 ,so that t has the eigenvalue -1 with multiplicity

8 . We recall,however,that t lies in E, the component of C(s), and that E is isomorphic to A_5.

We have seen that $X|_E$ contains three non-linear constituents , and (of course),any linear constituent of $X|_E$ is trivial.It readily follows that t has the eigenvalue 1 with multiplicity 4 or more , contrary to the fact that X(t) = -5. Thus L/Z(L) is not isomorphic to A_6.

Hence 0 does not lie in the principal 3-block of C(x) ,as was to be proved. Let B be the 3-block of C(x) which contains 0.Then B is a 3-block of defect 1.Now C(x) has self-centralizing Sylow 3-subgroups, so G has also.Thus G has only one 3-block of full defect,which must contain X so that X is in the pricipal 3-block of G.

It follows from Brauer's second and third main theorems that :

$$(*) \qquad \sum_{\mu \in B} (X|_C , \mu)\ \mu(xy) = 0$$

for any 3-regular element,y, of C.

Since x has no eigenvalue of

multiplicity 6 or more, no constituent of $X|_C$ can have degree 6. Since B is a block of defect 1, $X|_C$ contains three constituents from B, each of degree 3, one of which contains x in its kernel (we consider (*) when y = 1 to derive this fact).

We now claim that X(xs) = 2. The constituents from B make no contribution to X(xs), by (*). Since L, the component of C, is isomorphic to A_5, we now see that $X|_L$ has three non-linear constituents and that $X|_L$ contains the trivial character twice (both times coming from the action of L on the fixed-point space of x).

Hence X(xs) = 2, as s lies in L. Since X is not rational-valued (by Lemma 2.5.3), there is an algebraic conjugate, X^*, of X, which also lies in the principal 5-block of G but is different from X. Then $X^*(xs) = 2$.

Now as C(s) = <s>E, there are 20 characters in the principal 5-block of C(s) :

5 of degree 1.

10 of degree 3.

5 of degree 4.

For any irreducible character θ of degree three in the principal 5-block , $\theta(sx) = 0$ whilst for any irreducible character ,θ,of degree 4 in the principal 5-block of $C(s)$,

$|\theta(sx)|^2 = 1$,so:

$$\sum_{\theta \in B_0^{(5)}(C(s))} |\theta(sx)|^2 = 10.$$

By Brauer's second main theorem

$$\sum_{\mu \in B_0^{(5)}(G)} |\mu(sx)|^2 = 10.$$

We have already seen that $X(sx) = X^*(sx) = 2$. Hence , apart form the trivial character , there can only be one further character, θ say, for which $\theta(sx) \neq 0$, and for that θ , $|\theta(sx)|^2 = 1$.

Hence the character table of G has a fra gment of the form:

	1	sx
1	1	1
X	11	2
X^*	11	2
θ	c	b

However, we also know that :

$$\sum_{\mu \in B_0^{(5)}(G)} \mu(sx)\,\mu(1) = 0,$$

since sx is a 5-singular element, Thus $c = 45$ and $b = -1$, a contradiction, as $|S| = 25$.

This contradiction shows that $\langle s \rangle$ is normal in $C(x)$, so that 9 does not divide $|C(x)|$ and 9 does not divide $|G|$.

Now we have :

i) $|G| = 2^k .3.5^2 .11$, $k \leq 17$.

ii) $[N(S) : C(S)] = 4$.

iii) $[G:N(S)] \equiv 6$ or $11 \pmod{25}$.

If $[G:N(S)] \equiv 6 \pmod{25}$, then

$2^{k-2} .3.11 \equiv 6 \pmod{25}$, so that :

$2^{k-7} \equiv 1 \pmod{25}$ and $k = 7$,

contrary to the remarks at the end of chapter two.

If $[G:N(S)] \equiv 11 \pmod{25}$, then

$2^{k-2} .3 \equiv 1 \pmod{25}$, so that :

$k \equiv 15 \pmod{20}$, and $k = 15$.

Then $|G| = 2^{15}.3.5^{2}.11$, and for a Sylow 11-subgroup, P , of G, we have :

$[G:P] \equiv 2 \pmod{11}$, contrary to the fact that

$[G:N(P)] \equiv 1 \pmod{11}$ and

$|N(P)| = 55$ or 110.

This contradiction completes the proof of this Lemma , and so concludes this section.

Section Two

In this section ,we assume that S , a Sylow 5-subgroup of G, has order 125 . By Lemma 2.1.5 and by Lemma 1.4.2, there is an element g of G-N(S) such that $S \cap S^{g} \neq 1$. We will first exploit this fact , and we will produce a Sylow intersection of order 25.

Lemma 3.2.1

S contains a Sylow 5-intersection of order 25.

Proof

Suppose that $B \leq S$ is a maximal Sylow intersection of order 5 .Since S is elementary Abelian , there is a subgroup , C , of C(B) such that :

$$C(B) = C \times B .$$

By the maximality of B, $O_5(C) = 1$, and the Sylow 5-subgroups of C have trivial intersection with each other. Let $T = S \cap C$, so that T is a Sylow 5-subgroup of C of order 25.

By Lemma 2.7.3, S centralizes $O_{5'}(C)$ so that $E(C) \neq 1$ (because S does not centralize $F^*(C)$) .

Suppose that C has two components L_1 and L_2 , say . As $|C|$ is of the form $2^a .3^b .5^2$, L_1 and L_2 both have order divisible by 5 to the first power only.

Now $T \cap T^c = 1$ for all c in $C-N_C(T)$. However , L_2 centralizes $L_1 \cap T$, and $L_1 \cap T$ has order 5. Thus $L_2 \leq N_C(T)$, a contradiction. Hence C has a unique component, L, say.

Now $|L|$ has the form $2^a.3^b.5^2$, and by Lemma 1.2.7, there is an element u say, of order 5 in T such that $C_L(u) \neq TZ(L)$. By Lemma 1.2.16, L contains a Sylow 5-intersection of order 5, a contradiction.

Lemma 3.2.2

i) $C(S) = S$.

ii) Let A be a Sylow 5-intersection of G of order 25 with $A \leq S$. Then: $C(A) = A \times K$, and $E(K)$ is isomorphic to A_5.

Proof

Since S is elementary Abelian, $C(A) = A \times K$ for some subgroup K of $C(A)$. As A is a Sylow intersection, $O_5(K) = 1$. Also, by Lemma 2.7.3, S centralizes $O_{5'}(K)$. Thus $E(K) \neq 1$.

Since $|K|$ is of the form $2^a.3^b.5$, $E(K)$ is quasi-simple. Let $L = E(K)$ and let $T = S \cap L$.

Suppose first that $Z(L) = 1$. Then L is isomorphic to A_5, A_6 or to $PSU(4,2)$. If L is isomorphic to $PSU(4,2)$, then L has no faithful

irreducible character of degree less than 5 . Also , L has no faithful irreducible character of degree 8 , and $X|_L$ contains no constituent of degree 9 or 10, because L acts on the eigenspaces of a for any $a \neq$ in A, and a has no eigenspace of dimension 9 or 10.

Suppose that $X|_L$ contains only one non-linear constituent, 0 say . If $0(1) = 6$, then L contains an involution t with $0(t) = 2$,so that $X(t) = 7$, contrary to Lemma 2.1.6. If $0(1) = 5$, then L contains an involution t with $0(t) = 1$,so that $X(t) = 7$, contrary to Lemma 2.1.6.

Thus $X|_L$ contains two non linear constituents, which both have degree 5.Thus $X|_A$ must contains two linear constituents,say 0_1 and 0_2, each with multiplicity 5 or more . Since a is not cyclic,there is an element a of order 5 in A with $0_1(a) = 0_2(a)$, so that a has an eigenspace of dimension 10 , contrary to Lemma 2.1.6 . Thus L is not isomorphic to PSU(4,2).

Suppose that L is isomorphic to A_6. Then a slight variation of the argument above allows us to conclude that $X|_L = \theta + 3\,1_L$, where θ is irreducible of degree 8. Hence $X|_A$ must contain a linear constituent of multiplicity 8 or more. As A is not cyclic, A contains some element of order 5 which has an eigenspace of dimension 9 or more, contrary to Lemma 2.1.6. Consequently, L is not isomorphic to A_6.

We claim that $Z(L) = 1$. Suppose that this is not the case. Then S centralizes Z(L). By Lemma 2.4.2, any element x of $Z(L)^\#$ has only two eigenvalues, one of multiplicity 6 and one of multiplicity 5 (the case $X(x) = -4$ cannot arise, since L acts on the 5-dimensional eigenspaces of x which forces x to lie outside L').

We claim that for any 5'-subgroup B of K, $X|_B$ contains an irreducible constituent of degree 4 or more, or else $X|_B$ must contain 2 irreducible constituents of multiplicity 3.

No non-identity element of A can act with quadratic minimum polynomial in any reduction (mod 5) of G, so that by Lemma 1.5.1, $X|_B$ contains an irreducible constituent, μ say of multiplicity 3 or more. Suppose that $(X|_B, \mu) = 3$ and that no other constituent of $X|_B$ has multiplicity 3

As A is not cyclic, there is an element a of order 5 in A which has only 2 eigenvalues in its action on the homogeneous CB-module which affords the character 3μ. Now a acts with quadratic minimum polynomial in any reduction (mod 5) of G by Lemma 1.5.1, since $X|_B$ has no irreducible constituent of degree 3 or more, apart from μ. This contradicts Lemma 2.6.2. Hence either $(X|_B, \mu) > 3$, or else $X|_B$ contains some other irreducible constituent of multiplicity 3.

Suppose that L/Z(L) is isomorphic to PSU(4,2). If Z(L) has order 3, then L acts irreducibly on the eigenspace of dimension 6 of x. Let B be a Sylow 3-subgroup of L. Then $X|_B$ contains no constituent of multiplicity 3, as L acts non-trivially on the other eigenspace of x (otherwise there is

an involution in L with X(t) = 7). Thus contradicts the above remarks.

Thus Z(L) has order 2 .L acts irreducibly on the 6-dimensional -1 eigenspace of x in this case , as L has no irreducible character of degre 2 . Thus A acts as scalars on this space . Thus each element of A has at least three eigenvalues on the other eigenspace of t (otherwise there is an element which acts with quadratic minimum polynomial in any reduction (mod 5) of G) .

Thus L can have no irreducible constituent of degree 5 or more in its action on the 5-dimensional fixed point subspace of x,so that as L/Z(L) has no non-trivial complex character of degree 4 or less, L acts trivially on the 5-dimensional eigenspace of x.

Since L contains no involution t such that X(t) = 7 , x is the only involution in L , so that the Sylow 2- subgroups of L are generalized quaternion (for if z were another involution of L , either X(z) = 7 or X(zx) = 7). However

PSU(4,2) does not have dihedral Sylow 2-subgroups, a contradiction. Thus $L/Z(L)$ is not isomorphic to PSU(4,2).

Suppose that L/Z(L) is isomorphic to A_6. Then if x has order 2, then L acts irreducibly on the 6-dimensional eigenspace of x. Then any element of A acts as scalars on this space. If L acts irreducibly on the 5-dimensional eigenspace of x, then every element of A acts as scalars on this space also, so that every element of A must act trivially in any reduction (mod 5) of G. Thus L acts trivially on the 5-dimensional eigenspace of x.

Let b be an element of S which normalizes some Sylow 11-subgroup, P of G. Then we know that X(b) = 1. Thus $b = wy$, where w lies in $L^{\#}$ and y lies in $A^{\#}$. Let θ be the character afforded by the action of L on the eigenspace of dimension 6 of t. Then θ is a non exceptional irreducible character for the prime 5, so that $\theta(w) = 1$. We also know that b has five eigenvalues in its action on the 5-dimensional fixed point space of x by Lemma 2.4.1. Thus y has 5 eigenvalues on this

space, and since y acts as a scalar on the 6-dimensional eigenspace of x, there is a 5-th root of unity, a say, such that $X(wy) = a$. Since $b = wy$, we see that $a = 1$. Hence, y acts trivially on the eigenspace of x of dimension 6. Also, y acts trivially on the 3-dimensional fixed-point space of b (for w and b must now have the same fixed-point space).

Then $\langle P, b, y \rangle$ acts on the fixed-point space of P, so is not irreducible, whereas its order is divisible both by 11 and by 25, which is contrary to Lemma 2.3.3. Thus $|Z(L)| \neq 2$.

If Z(L) has order 3, then we claim that L acts trivially on the 5-dimensional eigenspace of x. Either L acts irreducibly on the 6-dimensional eigenspace of x, or else this space is the direct sum of two irreducible L-spaces, of dimension 3 each. In either case, each element of A has at most 2 eigenvalues on this space, so by Lemma 1.5.2, each element of order 5 in A has at least three eigenvalues on the other eigenspace

of x .Thus L cannot act irreducibly on this space, so must act trivially on it .

Now L has an elementary Abelian subgroup of order 4, say B .Let θ be the character of L afforded by the action of L on the 6-dimensional eigenspace of x. Then $\theta(b) = -2$ for any involution , b , of B (for we cannot have $X(b) = 7$).We then have:

$$4\,(\theta|_B, 1_B) = 6-2-2-2 = 0.$$

Now x centralizes B , but on any homogeneous $\mathbb{C}B$-submodule of the restriction to B of the $\mathbb{C}G$-module on which G acts in the given representation, x can only have one eigenvalue (for the fixed-point space of x is the same as the fixed-point subspace of B ,and x has only one other eigenvalue).By Lemma 1.5.1, x acts trivially in any reduction (mod 3) of G ,a contradiction.

Thus L/Z(L) is not isomorphic to A_6 ,so L/Z(L) must be isomorphic to A_5 and Z(L) must have order 2.

We claim that L acts trivially on the fixed-point space of x . Suppose that this is not the case . Let B be a subgroup of L that is isomorphic to SL(2,3) . Then the six-dimensional eigenspace of x is the sum of three (maybe isomorphic) 2-dimensional $\mathbb{C}B$-modules.

However, since L acts non-trivially on the 5-dimensional eigenspace of x by assumption , the 5-dimensional eigenspace of x is the sum of two 1 - dimensional $\mathbb{C}B$-modules and one 3-dimensional $\mathbb{C}B$-module . Thus $X|_B$ has at most one constituent with multiplicity 3 ,none of multiplicity greater than 3 . This contradicts an earlier remark in this Lemma. Thus L acts trivially on the 5-dimensional eigenspace of x.

Let θ be the character afforded by the action of L on the eigenspace of dimension six of x . The argument used to eliminate the possibility $|Z(L)| = 2$, $L/Z(L)$ isomorphic to A_6 may be used again to eliminate the possibility that θ is irreducible.

If θ is the sum of three irreducible characters of degree 2,

then L contains an element , u say , with eigenvalues $1, -\bar{w}$ and $-w$, where w is a primitive cube root of unity contrary to Lemma 1.3.10.

Thus $\theta = \theta_1 + \theta_2$, where θ_1 is irreducible of degree 4 , and where θ_2 is irreducible of degree 4 . We note that the character degrees for the 5-block of L which contain θ_1 and θ_2 are 2,2,4 and 6 ,so that θ_2 is a rational-valued character .

Let y be an element of order 5 in L.Then $\theta_2(y) = -1$ and $\theta_1(y) = w+\bar{w}$, where w is a primitive 5-th root of unity . Thus y has no fixed-points on the 6-dimensional eigenspace of x The other way about , there is no eigenspace of y on which x has more than one eigenvalue . By Lemma 1.5.1, x acts trivially in any reduction (mod 2) of G , a contradiction.

This contradiction establishes at last that $Z(L) = 1$, so that L is isomorphic to A_5 . As L is isomophic to A_5 , $O_{5'}(C(S)) \leq O_{5'}(K)$.Suppose

that x is a non-identity element of $O_{5'}(K)$. Then $[L,x] = 1$, so L acts on the eigenspaces of x. Let B be a subgroup of L which is isomorphic to A_4.

We have seen that $X|_{B\langle x\rangle}$ must contain an irreducible constituent of multiplicity four, or else two of multiplicity 3. Thus L must act trivially on one of the eigenspaces of x of dimension five or six.

If L acts trivially on a 6-dimensional eigenspace of x, then $X|_L$ contains at most one non-trivial constituent (of degree 3,4 or 5) as L acts on the other eigenspace of x. Then L contains an involution t with $X(t) = 7$, contrary to Lemma 2.1.6

If x has three eigenvalues, the same argument may be applied (for by Lemma 2.4.1, the eigenvalues of x have multiplicity 1, 5 and 5. Thus we may suppose that x has one eigenvalue of multiplicity 6, one of multiplicity 5, and that L acts trivially on the 5-dimensional eigenspace of x.

Let θ be the character of L which is afforded by its action on the six dimensional eigenspace of x .Suppose that x has order 2.

Then for an involution t, of L , we see that : $\theta(t) = 2$ (since $X(t) \neq 7$).Hence, we see that $X(xt) = 7$,a contradiction.

Thus x has order 3.We claim that x acts trivially in any reduction (mod 3) of G,which contradicts Lemma 2.1.1 .Let D be a Sylow 3-normaliser of L ,and let $R = A \times D$ .Let θ be the character of L afforded by the action of L on the 6-dimensional eigenspace of x.

Then as L contains no involution with $X(t) = 7$, $\theta(t) \neq 2$ for any involution of L.Thus $\theta = \theta_1 + \theta_2$,where θ_1 and θ_2 are both irreducible of degree 3 .

Then $\theta|_D$ does not contain the trivial character . Hence $X|_R$ is multiplicity free (for S contains an element with 5 distict eigenvalue on the fixed-point space of x) .Thus

x acts trivially in any reduction (mod 3) of G , by Lemma 1.5.1 .

This contradiction completes the proof of the Lemma.

Lemma 3.2.3

Let A be a Sylow intersection of order 25 in S, and let u be an element of order 3 in C(A) . Then 9 does not divide $|C(u)|$, so 9 does not divide $|G|$.

Proof

We first claim that X(u) = 5. Let L be the component of C(A) . We first prove that $X|_L$ contains just two non-linear constituents .If $X|_L$ contains only one such constituent then L contains an involution, t say with X(t) = 7.

Suppose then that $X|_L$ contains three non-linear constituents.Let B be a Sylow 2-normalizer in B, and 0 be the irreducible character of B of degree 3. Then it is not hard to see that $X|_B = 3\,0 + 2\,1_B$, and as

B is a 5'-group, an argument used in the previous Lemma leads to a contradiction.

Hence $X|_L$ contains just two non-linear constituents. We next claim that neither of these have degree 5. Suppose that one of them does, say θ_1. Let θ_2 be the other non-linear constituent. Then as A centralizes L and $\theta_1(1) + \theta_2(1) \geq 8$, there is an element, a say, of order 5 in A which has an eigenspace of dimension 8 or more (as A is not cyclic). By Lemma 2.1.6, we may suppose that the dimension is 8.

Since G is simple, there is a conjugate, b say, of a, which does not commute with a. Let $M = \langle a, b \rangle$. Since a and b have an eigenspace of dimension 8, the intersection of the eigenspaces has dimension 5 or more

Since S contains an element s such that $X(s) = 1$, S cannot be contained in M. Suppose that 25 does not divide $|M|$. Then $\langle a \rangle$ is a Sylow 5-subgroup of M. Now a cannot be conjugate to its inverse in M,

for otherwise , the only eigenvalue a could have of multiplicity 5 or more would be 1,and a would have the eigenvalue 1 with odd multiplicity, whereas by Lemma 2.1.6 , a can have no eigenvalue of multiplicity 9.

Thus if 25 does not divide $|M|$, then M has a normal 5-comp lement. We claim that a centralizes $O_{5'}(M)$.

Let R be a Sylow 3-subgroup of $O_{5'}(M)$ Suppose that a does not centralize R.Then [R,a] is Abelian by Lemma 3.1.4, so that (as $X|_M$ contains a linear character of multiplicity 5),$X|_{[R,a]}$ contains the trivial character with multiplicity 5 or more . Then R must contain an element of order 3 with a fixed-point subspace of dimension 9, a contradiction. A similar argument applies if a is assumed to act non-trivially on an Abelian 2-subgroup of R,whereas if a acts non-trivially on some non-Abelian special 2-group, K =[K,a], of R, we see easily that :

$X|_K = 7\,1_K + \theta$, where θ is an irreducible character of degree 4 of K, so that K contains an involution

t with $X(t) = 7$, contrary to Lemma 2.1.6.

Thus a must centralize $O_{5'}(M)$, and hence so does b. Since a and b do not commute, M does not have a normal 5-complement, so that 25 divides $|M|$.

Since a and b do not commute but both centralize $O_{5'}(M)$, $E(M) \neq 1$. Let $E = E(M)$. We remark that 125 does not divide $|M|$, because $X|_M$ has a linear constituent of multiplicity 5 or more, whereas $X|_S$ can have no constituent of multiplicity greater than 3, because S contains an element s such that $X(s) = 1$.

Suppose that 25 divides $|E|$. Since 7 does not divide $|E|$ and E has a faithful complex character of degree 6 or less (because E acts trivially on a 5-dimensionalspace), E is not quasi-simple, by Lindsey's classification of linear groups of degree 6, [20].

Then $E = L_1 L_2$, for two components L_1 and L_2. This is not

possible, because L_1 and L_2 both act trivially on the same subspace of dimension 5 ,and for each i, $X|_{L_i}$ has at least two non-linear constituents (otherwise there is an element with an eigenspace of codimension 2) and one of these constituents must have degree 3 or more (otherwise there is an element of order 6 which has eigenvalues contradicting Lemma 1.3.10).

Thus E is quasi-simple. As 25 divides $|M|$ and a and b both centralize $O_5(M)$, it quickly follows that $O_5(M) \neq 1$. Let $T = O_5(M)$ and let z be an element of order 5 in T.

We claim that z acts with quadratic minimum polynomial in any reduction (mod 5) of G, contrary to Lemma 2.6.2. There is a subspace of dimension 5 on which z acts as scalars and E acts trivially (for $X|_M$ contains a linear character of multiplicity 5 or more).

If $X|_E$ contains an irreducible constituent of degree 6 , then z

has two eigenvalues only , so acts with quadratic minimum polynomial in any reduction (mod 5) of G.

Since E contains no element with an eigenspace of dimension 9 , we conclude that $X|_E$ contains two non-linear constituents, one of which has degree greater than two.

If E/Z(E) is isomorphic to A_6 , let B be a Sylow 3-subgroup of E . If E/Z(E) is isomorphic to A_5 , let B be a Sylow 2-normalizer of E (note that we cannot have E/Z(E) isomorphic to PSU(4,2) because $X|_E$ has a non-linear constituent of degree 3 or less).

It readily follows that $X|_B$ contains no irreducible constituent of multiplicity 3 or more, and that $X|_B$ contains the trivial character with multiplicity 5 or 6.

Since z has an eigenvalue of multiplicity 5 on the fixed-point space of B, and since B is a 5'-group, z acts with quadratic minimum polynomial in any reduction of G (mod 5), the required contradiction.

Thus A contains no element with an eigenspace of dimension 8. and $X|_L$ contains no irreducible constituent of degree 5 .Since L is isomorphic to A_5 and $X|_L$ contains two non-linear constituents only, $X(u) = 5$.

Thus u has the eigenvalue 1 with multiplicity seven, and the two primitive cube roots of unity with multiplicity 2 each . We prove now that A is normal in C(u) . Suppose that this is not the case.

Let C = C(u).It is easy to see that A must centralize $O_{5'}(C)$ (for otherwise , there is an element with an eigenspace of dimension 9 in $O_{5'}(C)$). Since A is a Sylow 5-subgroup of C , there is a component ,E say of C.

We claim that E is simple. If E is not simple , then A centralizes Z(E) . Since C(A) = A x K where E(K) is isomorphic to A_5 ,and K has a self centralizing Sylow 5- subgroup ,we must conclude that K is isomorphic to S_5 , and that Z(E) = $\langle t \rangle$ for some involution , t .

We claim however, that t does not lie in C' . To do this ,it is sufficient to observe that t has two different eigenvalues on the two dimensional w-eigenspace of u, where w is a primitive cube root of unity (for C acts on this space but t is not unimodular in this action).

We know that $X|_L$ cannot have two constituents of degree 4 , and that $X|_L$ has two non-linear constituents, so that $X|_K$ has an irreducible constituent of degree 6 and

$$X|_L = \theta_1 + \theta_2 + 5\,1_L \quad , \text{ where}$$

θ_1 and θ_2 are irreducible of degree 3 , and are interchanged by t.

Now K has one irreducible character only,of degree 6,say θ,and $\theta(tu) = 0$ (because θ vanishes off L) for this character.It follows easily that t has two different eigenvalues on the w-eigenspace of u , so that t lies outside C',contrary to the fact that t lies in Z(E). Thus E must be simple.

As E is simple, E acts trivially on both 2-dimensional eigenspaces of u . Since 7 does not divide $|E|$, E has a faithful irreducible character of degree 6 or less (for E acts non trivially on the fixed-point space of u , which has dimension 7) . Now no simple group which has a faithful complex character of degree 6 or less has order divisible by 25 , (see [20]) so that 25 does not divide $|E|$.

Suppose that C has another component , H say . Then $X|_E$ and $X|_H$ both have at least two non-linear constituents, which is easily seen to be a contradiction (as they centralize each other and both act trivially on the two -dimensional eigenspaces of u).

Thus E is the only component of C . Since E is isomorphic to A_5 , A_6 or PSU(4,2), and 25 divides $|C|$, it readily follows that $O_5(C) \neq 1$

Let $T = O_5(C)$, and z be an element of order 5 in T.

Let θ be the character afforded by the action of E on the 7-dimensional eigenspace of u. Then θ contains either two non-linear constituents, or else an irreducible constituent of degree 6 (otherwise there is an element of E which has an eigenspace of dimension 9). In the latter case, z has only two eigenvalues in its action on the 7-dimensional fixed-point space of u Since the other eigenspaces of u are of dimension 2, z acts with quadratic minimum polynomial in any reduction (mod 5) of G, contrary to Lemma 2.6.2

In the former case, E must be isomorphic to A_5. Let B be a Sylow 2-normalizer of E. As θ contains two non-linear constituents, $X|_{B\langle u\rangle}$ contains no irreducible constituent of multiplicity three or more. Since $B\langle u\rangle$ is a 5'-group centralized by z, z must act with quadratic minimum polynomial in any reduction (mod 5) of G, contrary to Lemma 2.6.2.

This contradiction establishes that A is normal in C(u) . We are trying to prove that 9 does not divide $|C(u)|$ .Since $\langle u \rangle$ is a Sylow 3-subgroup of C(A) , it only remains to prove that $[N_{C(u)}(A) : C_{C(u)}(A)]$ is not divisible by 3.

Suppose that 3 divides $[N_{C(u)}(A) : C_{C(u)}(A)]$, and let v be an element of order 3 in $N_{C(u)}(A) - C_{C(u)}(A)$. Now $\langle v \rangle A$ is a Frobenius group, and $X|_A$ contains either two irreducible constituents of degree 3 or more, or else one of degree 6 or more (because $L \leq C(A)$, and $X|_L$ has two or more non-linear constituents)

The only way that this can happen is that $X|_A = 2\,1_A + 3(\theta_1 + \theta_2 + \theta_3)$ where the θ_i are linear characters which are transitively permuted by v

This is not possible, since $\langle v \rangle A \leq C(u)$, and u has one eigenvalue of multiplicity 7 and 2 eigenvalues of multiplicity 2 each . Thus 9 does not divide $|C(u)|$, from which it easily follows that 9 does not divide $|G|$.

Lemma 3.2.

$|S| \neq 125$.

Proof

Under the hypothesis that $|S| = 125$, we have proved that 3 divides $|G|$ to

the first power only. Hence there is an integer x such that :

i) $x \equiv 1 \pmod 3$.

ii) $x(x+1)$ divides $|G|$.

iii) The character degrees in the principal 3-block of G are :

$1, x, x+1$

iv) 11 divides $x(x+1)$ (since the principal 11- block cannot contain characters of degree x and x+1).

Case i) : 11 divides x+1

In this case, $x \equiv -1 \pmod{11}$, so that x is even , (because 5 is a quadratic residue (mod 11) .If x is a power of 2 , say 2^k , then k is odd, as $x \equiv -1 \pmod{11}$. This contradicts the fact that $x \equiv 1 \pmod 3$. Thus 5 divides x.

Then x+1 is prime to 2, 3 and 5, so that x+1 = 11 , and x = 10 , which contradicts Lemma 2.3.2 , since 125 divides $|G|$.

Case ii) : 11 divides x

Since $x+1 \equiv 1 \pmod{11}$, 2 divides x+1 to an even power. Since

$x+1 \equiv -1 \pmod 3$, 5 divides $x+1$. If $x = 11$, then G has a rational-valued character of degree 11, contrary to Lemma 1.3.9. Thus x is even, so that $x+1$ is odd and must be a power of 5 . This is not possible , since 5^5 does not divide $|G|$, whereas :

$$x+1 \equiv 1 \pmod{11}.$$

Thus $|S| \neq 125$.

Chapter Four

In this chapter , we consider the possibility that the order of G is not divisible by 25 . We will let S denote a fixed Sylow 5-subgroup of G for the remainder of this chapter . As might be expected , the arguments used are of a character-theoretic nature.

In Section One,we will dispose of the easiest case and we will prove that [N(S) : C(S)] ≠ 2 .We remark here that a Sylow 5-normalizer in PSL(2,11) is dihedral of order 10.After this section we assume that [N(S):C(S)] = 4.

In Section Two ,we will prove that C(S) ≠ S .We note that M_{11} has a self-centralizing Sylow 5-subgroup of order 5 .In Sections Three,Four, and Five, we prove that 7 divides |G| .

In Section Three ,we assume that 7 does not divide |G|,and we prove that C(S) has even order.We remark here that PSU(5,2) has a Sylow 5-centralizer of order 15.

In Section Four,we continue to assume that 7 does not divide |G| , and we prove that the character degrees for the principal 5-block are :

1,66,99,144,176

and that the order of G is either

$$2^{12}.3^{6}.5.11 \quad \text{or} \quad 2^{14}.3^{7}.5.11 .$$

We also show that a Sylow 11-normalizer of G has order 55.

In Section Five, we prove that 7 must divide $|G|$, by proving that unless 7 divides $|G|$, it is not possible to find a consistent set of character degrees for the principal 11-block, given the information about G which we already have.

In Section Six, we prove that 49 must divide $|G|$. In Section Seven, we derive a contradiction by proving that 7 does not divide $|G|$ to the second power. This final contradiction completes the proof of the main theorem of this thesis.

Section One

We assume during this section that $[N(S):C(S)] = 2$. Thus the principal 5-block consists of two exceptional characters, the trivial character, and another non-exceptional character, which is rational valued.

Let the degree of the non-trivial non-exceptional character be x. Then there is a sign e such that $x \equiv e \pmod 5$ and $x(x+e)$ divides $|G|$ (for the exceptional characters each have degree $x+e$). In particular , both x and $x+e$ are integers of the form $2^a.3^b.7^c.11^d$.

Lemma 4.1.1

11 divides $x(x+e)$.

Proof

As G has a self-centralizing Sylow 11-subgroup, P say ,each irreducible character of G which has degree prime to 11 lies in the principal 11-block of G. As N(P) has order 55 or 110,each irreducible character in principal 11-block of G has degree congruent (mod 11) to one of:

$$1, -1, 5, \text{or } -5.$$

Also,each irreducible character of the principal 5-block is rational valued on 5-regular elements and so certainly on 11-singular elements . Hence no irreducible character which is in the principal 5-block can also be an exceptional character in the principal 11-block.

Thus 11 must divide x(x+e), for the principal 11-block of G cannot contain characters of degrees x and x+e which are non-exceptional.

Lemma 4.1.2

$x \neq 11$

Proof

Suppose that x = 11.Then G has a rational-valued irreducible character of degree 11,so that G has a subgroup of index 11 or 12 by Lemma 1.3.9 and G is no counterexample to Theorem A.

Corollary 4.1.3

i) C(S) has order 10,15,or 30.

ii) If C(S) has order 15,no element of order 3 in C(S) is conjugate to its inverse in G.

Proof

i) As $x \neq 11$,X does not lie in the principal 5-block of G. As 5 does not X(1) we may conclude that G has more than one 5-block of full defect , so that $C(S) \neq S$.By Lemma 2.4.1 ,C(S) has one of the orders listed above.

ii) Suppose that C(S) has order 15, and let u be an element of order 3 in C(S). By Lemma 2.4.2 , we have only two cases to consider.

a) $X(s) = X(su) = X(su^2) = 1$

$X(u) = -4.$

b) $X(su) = w$, where w is a primitive cube root of unity.

$X(u) = 6w + 5.$

However , case a) cannot occur, for otherwise X is constant and non-zero on 5-singular elements, so lies in the principal 5-block of G , which is not the case.

Hence case b) occurs, so that u is not conjugate to its inverse in G.

Lemma 4.1.4

Either: $x = 99$ and $e = -1$.

or: $x = 21$ and $e = 1$.

Proof

The proof is completely arithmetical, and is broken into several parts.

Case i): When 11 divides x

There are six subcases to consider, depending on the prime factors of x .

a) $x = 11.2^a$, $x+e = 3^b.7^c$.

Now a is even, as $x \equiv e \pmod 5$.

Clearly, $x \neq 44$, so that $a \geq 4$.

If $c \neq 0$, then $2^{a+2} \equiv e \pmod 7$ so that $e = 1$, as a is even and -1 is not a quadratic residue (mod 7). Thus $3^b 7^c \equiv 1 \pmod{11}$, so that c is even, as 3 is a quadratic residue (mod 11) and 7 is not.

Thus $7^c \equiv 1 \pmod{16}$, and as $3^b 7^c \equiv x+e = 1 \pmod{16}$, b is also even. Now however, we see that :

$3^b 7^c \equiv 1$ or $-1 \pmod 5$, whereas

$x+e \equiv 2e \equiv 2 \pmod 5$.

Thus $c = 0$.

Now $3^b \equiv 2e \pmod 5$, so b is odd. As a is even, $11\ 2^a \equiv 2 \pmod 3$, so $e = 1$, as $11\ 2^a + e = 3^b$. Now we see that $3^b \equiv 1 \pmod 4$ as a is even, so that b is even, a contradiction.

b) $x = 11.3^a$, $x+e = 2^b 7^c$.

Now a is even , as $x \equiv e \pmod 5$. In particular $x \equiv 3 \pmod 4$. If $b \geq 2$ then $x + e \equiv 0 \pmod 4$, so $e = 1$. Then $2^b \equiv 1 \pmod 3$ as $a \neq 0$, and hence b is even.

As $2^b 7^c \equiv 2e \pmod 5$, c is then odd. Then, however, $x \equiv -1 \pmod 7$, which contradicts the fact that a is even and $x = 11.3^a$. Thus $b \leq 1$, so $b = 1$, as x is odd and $x+e = 2^b 7^c$.

As $11.3^a + e = 2.7^c$, $c \neq 0$. Also $e = -1$, as $e \equiv 2 \pmod 3$. Hence $2.7^c \equiv -1 \pmod{11}$, so $c \equiv 2 \pmod{10}$. By Lemma 2.1.4, 7^{12} does not divide $|G|$, so that $c = 2$ and $x = 99$ in this case.

c) $x = 11.7^a$, $x + e = 2^b 3^c$

Now $a \neq 0$, and a is even, for we know that $7^a \equiv e \pmod 5$. Consequently, $x \equiv 3 \pmod 8$, so $x + e \not\equiv 0 \pmod 8$. Thus $b = 1$ or 2.

If $b = 1$, then $e = -1$ (otherwise $x \equiv 0 \pmod 4$). Thus we have:

$2.3^c \equiv -1 \pmod 7$, so that c is odd (as -1 is not a quadratic residue (mod 7)).

However, $x + e \equiv -2 \pmod 5$, so that $3^c \equiv -1 \pmod 5$, a contradiction as c is odd.

If $b = 2$, then $e = 1$, so that $4.3^c \equiv 1 \pmod 7$. In particular, c is even, as 3 is not a quadratic residue (mod 7). However, in this case, $x + e \equiv 2 \pmod 5$, a contradiction, as c is even and $x+e = 4.3^c$.

d) $x = 11.2^{a}.3^{b}$, $x+e = 7^{c}$.

Now c is odd, as $7^{c} \equiv 2e \pmod 5$. Also, $7^{c} \equiv e \pmod{11}$, so that $e = -1$ as 7 is not a quadratic residue (mod 11). Thus we see that:

$x = 7^{c} + 1 \equiv 8 \pmod{16}$ as c is odd. Hence $a = 3$. Furthermore, we see that $x = 7^{c} + 1 \equiv 2 \pmod 3$, so $b = 0$.

Thus $x = 88$, a contradiction.

e) $x = 11.2^{a}.7^{b}$, $x+e = 3^{c}$.

In this case, $e = 1$, since 3 is a quadratic residue (mod 11) and $3^{c} \equiv e \pmod{11}$. Also, c is odd, as $3^{c} = x + e \equiv 2 \pmod 5$.

Hence $x = 3^{c} - 1 \equiv 2 \pmod 4$, so that $a = 1$. Clearly $x \neq 22$, so that $b \neq 0$ and $3^{c} \equiv 1 \pmod 7$. However this contradicts the fact that c is odd and 3 is not a quadratic residue (mod 7).

f) $x = 11.3^{a}.7^{b}$, $x+e = 2^{c}$.

As $2^{c} \equiv 2e \pmod 5$, c is odd. Also, as $2^{c} \equiv e \pmod{11}$ and c is odd, we see that $e = -1$, as 2 is a quadratic non-residue (mod 11).

Now b = 0, for otherwise we have $2^c \equiv -1 \pmod 7$, a contradiction, as 2 is a quadratic residue (mod 7) but -1 is not.

As $x = 11.3^a \equiv -1 \pmod 5$, a is even. Thus $x \equiv 3 \pmod 8$ and also $2^c = x-1 \equiv 2 \pmod 8$. Hence c = 1, a contradiction.

The elimination of case f) completes the exhaustion of all possibilities when $x \equiv 0 \pmod{11}$. When $x \not\equiv 0 \pmod{11}$, the arguments are of a similar nature. We know in this case that $x + e \equiv 0 \pmod{11}$.

Case ii) : $x+e \equiv 0 \pmod{11}$.

Once more, we must consider six possibilities.

a) $x = 2^a$, $x+e = 11.3^b.7^c$.

As $2^a \equiv e \pmod 5$, a is even. Also, as $2^a \equiv -e \pmod{11}$ and a is even, we see that e = -1 and $a \equiv 0 \pmod{10}$.

Then, however, we see that $2^{10} - 1$ divides x+e, a contradiction, as 31 divides $2^{10} - 1$.

b) $x = 3^a$, $x+e = 11.2^b.7^c$.

As above , a is even e = -1 and $a \equiv 0 \pmod{10}$. In particular, we see that $3^5 - 1$ divides $x+e$, which is a contradiction ,as 121 divides $3^5 - 1$.

c) $x = 7^a$, $x+e = 11.2^b.3^c$

As above,a is even, e = -1 and $a \equiv 0 \pmod{10}$ .This contradicts the fact that 7^{10} does not divide $|G|$.

d) $x = 2^a 3^b$, $x+e = 11.7^c$

As $11.7^c \equiv 2e \pmod 5$, c is odd Thus $x+e \equiv 5 \pmod 8$,so that 8 does not divide x and $a \leq 2$ .Hence $b \neq 0$. Now $x+e = 11.7^c \equiv 2 \pmod 3$, so that e = -1 , as $x \equiv 0 \pmod 3$.

Since $x \equiv -e \pmod{11}$,a is even,as 2 is not a quadratic residue (mod 11),but 3 is .Now $x = 11.7^c + 1$ so that $x \equiv 6 \pmod 8$,contradicting the fact that a is even.

e) $x = 2^a.7^b$,$x + e = 11.3^c$

As $11.3^c \equiv 2e \pmod 5$,c is odd. Now $x \equiv 2^a \pmod 3$, and $c \neq 0$, so $2^a \equiv -e \pmod 3$. Hence if a is even, e = -1. In that case , as c is odd , $x = 11.3^c + 1 \equiv 2 \pmod 8$, contrary to the fact that a is even.

Thus a is odd and e = 1. Now b = 0, otherwise $11.3^c \equiv 1 \pmod 7$, which contradicts the fact that c is odd and 3 is not a quadratic residue (mod 7).

As b = 0, we now have:

$$2^a + 1 = 11.3^c.$$

Also, $11.3^c \equiv 2 \pmod 5$, so that $c \equiv 3 \pmod 4$ and $11.3^c \equiv 9 \pmod{16}$ Thus $a \leq 3$, a contradiction.

f) $x = 3^a.7^b$, $x + e = 11.2^c$.

As $11.2^c \equiv 2e \pmod 5$, c is odd. If $e = -1$, then $x \equiv 2 \pmod 3$, so a=0 Furthermore, in that case, b = 0, as 11.2^c is a quadratic residue (mod 7) and -1 is not. This contradiction shows that e = 1.

Hence $x \equiv -1 \pmod{11}$, so that b is odd, as 3 is a quadratic residue (mod 11), but 7 and -1 are not. Also $x \equiv 1 \pmod 5$, so that $a \equiv b \pmod 4$ and a is also odd.

Thus $x \equiv 1 \pmod 8$, so that $x + 1 = 11.2^c \equiv 2 \pmod 8$ and c = 1. Hence x = 21, x + e = 22.

Lemma 4.1.5

$x \neq 21$

Proof

Suppose on the contrary that $x = 21$ and let θ be the character of degree 21 in the principal 5-block Then θ is rational-valued. Let T be a Sylow 7-subgroup of G and let u be an element of $T^{\#}$.

Then as 7 does not divide $[G : C(u)]$ and $[G:C(u)]\,\theta(u)/\theta(1)$ is an algebraic integer, we see that $\theta(u) = 7z$ for some integer z . Also, $|z| < 3$, as G is simple.

Thus $[G:C(u)] \not\equiv [G:C(u)]\theta(u)/\theta(1) \pmod 7$, so that θ lies outside the principal 7-block of G. As G contains no element of order 35 , Lemma 1.2.14 tells us that there is a non-trivial character of G which lies in both the principal 5-block of G and the the principal 7-block of G . As the two exceptional characters agree on 5-regular elements of G they must agree on 7-singular elements of G

Hence both exceptional characters of the principal 5-block lie in the principal 7-block of G .Lemma 1 .2.14 allows us to conclude that θ lies in a 7-block of defect 0 of G.

Hence T has order 7.As $X|_T$ is not rational-valued by Lemma 2.5.4 , $[N(T):C(T)] \neq 6$.Now both exceptional characters of the principal 5-block are non-exceptional characters of the principal 7-block . Hence there are at least three non-exceptional characters in the principal 7-block of G , so that $[N(T): C(T)] \neq 2$.

As G is simple,we are forced to conclude that $[N(T):C(T)] = 3$. Now however , the two non-principal non- exceptional characters of the principal 7-block of G cannot be rational - valued , as they are both exceptional characters lying in the principal 5-block of G .As the order of G is even and G is simple , this contradicts Lemma 1.6.1 .

Lemma 4.1.7

G has a self-centralizing Sylow 7-subgroup of order 49.

Proof

Let T be a Sylow 7-subgroup of G. Then by Lemma 2.1.8, T is elementary

Abelian . Let u be any non-identity element of T , and let θ_1 and θ_2 be the exceptional characters of the principal 5-block of G.Both of these characters have degree 98 and are rational-valued on 5-regular element

As 7 does not divide [G:C(u)], and $[G:C(u)]\,\theta_1(u) / \theta_1(1)$ is an algebraic integer,it quickly follows that $\theta_1(u) = 49z$ for some integer z. Thus $[G:C(u)]\theta_1(u)/\theta_1(1) \not\equiv [G:C(u)] \pmod 7$, as $|z| < 2$.In particular,θ_1 does not belong to the principal 7-block of G (and neither does θ_2).

By Lemma 1.2.14 , $|T| \leq 49$,so that $|T| = 49$, as $\theta_1(1) = 98$.Furthermore, we claim that $T = C(T)$.Suppose first that C(T) contains an involution ,t. As $G = G'$, $\theta_1(t) \equiv \theta_1(1) \pmod 4$, so that $\theta_1(t) \equiv 2 \pmod 4$ .Also, 7 does not divide $[G:C(t)]$, so that, as $[G:C(t)]\,\theta_1(t)/\theta_1(1)$ is an integer , $\theta_1(t) = 49z$ for some integer z.

As $\theta_1(t) \equiv 2 \pmod 4$, $z \equiv 2 \pmod 4$ whereas $|z| < 2$,as G is simple. This contradiction shows that the order of C(T) is odd . Suppose then that C(T) contains an element, x say ,of order three.

As above, $\theta_1(x) = 49z$ for some integer z. Furthermore, as x has order three, $\theta_1(x) \equiv \theta_1(1) \pmod 3$, so that $\theta_1(x) \equiv 2 \pmod 3$. As G is simple, we conclude that $\theta_1(x) = -49$.

Now let s be an element of order 5 in S. Let $K = O_{5'}(C(s))$. We calculate the sum of class algebra constants

$$\sum_{k \in K} \#(s \cdot x = sk) .$$

This expression is a sum of class algebra constants, so a non-negative integer, n.

By Brauer's second main theorem, for any character θ of the principal 5-block of G, $\theta(sk) = \theta(s)$ for each k in K. By the same theorem, for any irreducible character θ outside the principal 5-block of G, we have:

$$\sum_{k \in K} \theta(sk) = 0.$$

Thus $$n = \frac{|K|\,|G|}{|C(s)|\,|C(x)|}\left(1 - \frac{48}{99} - \frac{49.3}{98}\right)$$

which is certainly negative, contrary to the fact that n is non-negative.

Hence 3 does not divide $|C(T)|$. As G contains no element of order 35, $C(T) = T$.

Lemma 4.1.7

$|C(S)| \neq 15$

Proof

Suppose that C(S) has order 15.We note that G contains no element of order 10 , so that $|N(P)| = 55$ for a Sylow 11-subgroup P of G.

We know that the order of G is of the form $2^a.3^b.5.7.11^2$, and that $[G:N(P)] = 2^a.3^b.7^2 \equiv 1 \pmod{11}$ .As 3 is a quadratic residue (mod 11) but 2 is not,we see that a is even.

Now let u be an element of order 3 in C(S) and let s be an element of order 5 in S.By Lemma 4.1.3,u is not conjugate to its inverse in G, so su is certainly not conjugate to its inverse in G.

Let t be any involution of G.By a well-known argument t is conjugate to an involution of N(S)-C(S) as [N(S):C(S)] = 2 and S is cyclic.

Now N(S) has only one conjugacy class of involutions ,as |N(S)| = 30 and N(S) contains only 5 involutions as u is central in N(S).Consequently

$$\sum_{i=0}^{2} \#(tt = su^i) = 5.$$

Now if θ is an irreducible character of G and θ does not lie in the principal 5-block of G ,

$$\theta(s) + \theta(su) + \theta(su^2) = 0,$$

whilst if θ lies in the principal 5-block of G,

$$\theta(s) = \theta(su) = \theta(su^2).$$

Hence $$3\frac{|G|}{|C(t)|}^2\frac{(99-\theta(t))^2}{99.98} = 5$$

where θ is the character of degree 99 in the principal 5-block of G. This contradicts the fact that 2 divides $|G|$ to an even power.

Lemma 4.1.8

G possesses only one conjugacy class of involutions.

Proof

Let B denote the 5-block of G which contains X. By Lemma 2.5.4, X is not 7-rational and by Lemma 2.4.2, B is invariant under 7-conjugation. Hence B contains an irreducible character, X^*, of degree 11 which is 7-conjugate to, but different from, X.

As $[N(S):C(S)] = 2$, B contains two exceptional characters, which each must have degree 22, say X_1 and X_2.

Let t ,u be any two involutions of G. Let $X(t) = a$, $X(u) = b$. Then $X^*(t) = a$,$X_1(t) = X_2(t) = 2a$ and $X^*(u) = b$,$X_1(u) = X_2(u) = 2b$.

Hence:

$$\sum_{\theta \in B} \frac{\theta(t)\theta(u)\theta(y)}{\theta(1)} = 0$$ for any 5-singular element y of G.

We know that C(S) has order 10 or 30 and we consider these two cases separately .

Case i) : $|C(S)| = 10$

In this case,G has only two 5-blocks of full defect, which must be B and the principal 5-block.

Let t,u be as above ,and let s be an element of order 5 in S.We wish to evaluate $\#(tu = s)$. By the remarks above ,only the principal 5-block can make a non-zero contribution to the character theoretic evaluation of the above expression .

The contribution from the principal 5-block is :

$$\frac{|G|}{|C(t)| \cdot |C(u)|} \cdot \frac{(99-\theta(t))(99-\theta(u))}{99.98}$$

where θ is the character of degree 99 in the principal 5-block of G. As

G is simple , this expression is not zero . Hence we may suppose that tu has order 5 so that t is conjugate to u in G.

Case 2 : $|C(S)| = 30$

Here $C(S) = S \times K$ where K is isomorphic to S_3 .Also,each involution of G is conjugate to an involution of $N(S)-C(S)$,so that $N(S) = L \times K$ where L is isomorphic to D_{10} .

It follows that N(S) has three 5-blocks of full defect,and so has G. Thus there is another 5-block, B^*, of full defect which is different from B and the principal 5-block.

Let x be an element of order 3 in C(S) and let s be an element of order 5 in S . Then for any irreducible character θ of the principal 5-block of G , $\theta(s) = \theta(sx) = \theta(sx^2)$ .Also,by Lemma 2.4.2,$X(s) = X(sx) = X(sx^2) = 1$

Now the three 5-blocks of N(S) correspond to the three irreducible characters of K . K has the following character table (z is an involution of K).

	1	x	z
1	1	1	1
ϕ_1	1	1	-1
ϕ_2	2	-1	0

This is reflected in the fact that for any irreducible character, θ, of B, $\theta(sx) = \theta(s) = -\theta(sz)$ (for X has this property by Lemma 2.4.2) and that for any irreducible character, μ, of B^*, $\mu(sz) = 0$, $\mu(s) = -2\mu(sx)$

We calculate,

$$\#(t\,u = s) + 2\,\#(t\,u = sx) \quad (= m, \text{say})$$

By the above remarks, B^* makes no contribution to the above calculation By the remarks earlier in this Lemma, B makes no contribution to the above calculation.

It follows that we may restrict our attention to the principal 5-block of G and that :

$$m = \frac{|G|}{|C(t)|\,|C(u)|} \cdot \frac{(99-\theta(t))(99-\theta(u))}{99.98}$$

(where θ is the character of degree 99 in the principal 5-block). As G is simple, $m \neq 0$.

Hence we may suppose that tu has order 5 or 15, so that t and u are conjugate in G.

Thus G has only one conjugacy class of involutions in any case.

Lemma 4.1.9

i) $|G|$ divides $2^8.3^5.5.7^2.11$.

ii) G contains no element of order 14.

Proof

As $|C(S)| = 10$ or 15, we may conclude from Lemma 2.4.2 that the 5-block of G which contains X is invariant under algebraic conjugation . We saw in the proof of the previous Lemma that this block only contains two characters of degree 11 which are 7-conjugate to each other.

Let R be a Sylow 3-subgroup of G. Then $X|_R$ must be rational-valued by the above remarks. Hence $|R| \leq 3^5$ by Lemma 2.5.1 .

Let t be an involution of G. As G has one conjugacy class of involution $[G : C(t)]$ is odd . Also, as the order of C(S) is even , 5 divides $|C(t)|$.

Let s be an element of order 5 in S and let θ be the character of degree 99 in the principal 5-block of G . Then $\theta(st) = \theta(s) = -1$, so that $\theta(t) \equiv -1 \pmod 5$. Also, as $G = G'$, $\theta(t) \equiv \theta(1) \equiv -1 \pmod 4$, so that $\theta(t) \equiv -1 \pmod{20}$.

We prove next that $-19 \leq \theta(t) \leq 19$

We may suppose that $\langle t \rangle S$ is dihedral of order 10. Let λ be the non-trivial linear character of $\langle t \rangle S$. Then :

$$0 \leq 10\,(\theta|_{\langle t \rangle S}, \lambda)_{\langle t \rangle S} = 99 - 4 - 5\,\theta(t)$$

so that $\theta(t) \leq 19$. Also we have:

$$0 \leq 10\,(\theta|_{\langle t \rangle S}, 1)_{\langle t \rangle S} = 99 - 4 + 5\,\theta(t)$$

so that $\theta(t) \geq -19$.

As $\theta(t) \equiv -1 \pmod{20}$, we conclude that either $\theta(t) = -1$ or $\theta(t) = 19$. Now let $K = O_5(C(S))$. Then by similar arguments to those used in earlier Lemmas,

$$(*) \sum_{k \in K} \#(\dot{t}\dot{t} = sk) = \frac{|K|\,|G|}{|C(t)|^2} \frac{(99-\theta(t))^2}{99.98}$$

Now $|K| = 2$ or 6 and $\theta(t) = -1$ or 19 so that 7 does not divide the order of $C(t)$. As G has only one conjugacy class of involutions, G contains no element of order 14.

From (*) we also see that:

$$[\,G:C(t)\,] = \frac{m\,|C(t)|\;99.98}{|K|\,(99-\theta(t))^2}$$, where m is the integer: $\sum_{k \in K} \#(\dot{t}\dot{t} = sk)$

Now $[G:C(t)]$ is odd, as G has one conjugacy class of involutions. As $|K| = 2$ or 6 and $\theta(t) = 19$ or -1, we conclude from the equation above that 2^9 does not divide $|C(t)|$, so 2^9 does not divide $|G|$.

Hence the order of G divides $2^8 .3^5 .5.7^2 .11$ and the proof of the Lemma is complete.

Now we let T denote a Sylow 7-subgroup of G.

Lemma 4.1.10

The assumption that $[N(S):C(S)] = 2$ leads to a contradiction.

Proof

We first prove that $T \cap T^g = 1$ for any g in G-N(T) and that N(T) has odd order.

Let u be an element of order 7 in T Then C(u) is a $\{3,7\}$- group by Lemmas 2.4.1 and 4.1.9 . Also,T centralizes $O_3(C(u))$ by Lemma 2.7.2 . As T is Abelian, we deduce that $C(u) \leq N(T)$. Since u was an arbitrary element of order 7 in T , it follows that T has trivial intersection with all of its distinct conjugates.

Suppose that N(T) contains an involution,t say.Then t inverts each non-identity element of T, as G does not contain any element of order 14.

However, we know that there is just one other irreducible character of G which is distinct from X and is 7-conjugate to X. This character must agree with $\overline{X}$ on T. However, as every element of T is conjugate to its inverse, $X|_T$ is real-valued. This contradiction completes the proof of our assertion that the order of N(T) is odd.

As $T \cap T^g = 1$ for all g in G-N(T), $[G:N(T)] \equiv 1 \pmod{49}$. Also, as T is elementary Abelian of rank 2 and N(T) has odd order, [N(T):C(T)] divides 9. Since C(T) = T and G has no normal 7-complement, [N(T):T] = 3 or 9.

Now $|G|$ divides $2^8 \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$. We deal separately with each possible value of [N(T):T].

Case i): [N(T):T] = 3

In this case, [G:T] = 3 [G:N(T)], so that $[G:T] \equiv 3 \pmod{49}$.

Let $|G| = 2^a \cdot 3^b \cdot 5^2 \cdot 7 \cdot 11$. Then we see that $[G:T] = 2^a \cdot 3^b \cdot 55$. Hence:

(*) $2^{a+1} \cdot 3^b \equiv 1 \pmod{49}$. Now we know that $2^4 \cdot 3 \equiv -1 \pmod{49}$. As 2 is a quadratic residue (mod 7) and 3 is not, b is even. Furthermore, $b \geq 2$, as G has an irreducible character of degree 99.

If b = 2 ,then a = 7 ,from (*),so that $|G| = 2^7 .3^2 .5.7^2 .11$.Let P be a Sylow 11-subgroup of G . Then N(P) has order 55 or 110,and [G:N(P)] is congruent to 7 (mod 11) or 9 (mod 11) respectively , contradicting Sylow's theorem.

If b = 4,then a ≡ 15 (mod 42) from (*), contradicting the fact that a ≤8

Case ii) :[N(T):T] = 9

In this case,[G:T] ≡ 9 (mod 49). Let $[G:T] = 2^a .3^b .5.11$. Then we see that $2^{a+1} .3^{b-1} \equiv 1 \pmod{49}$.

As 2 is a quadratic residue (mod 7) but 3 is not, b is odd (and 3 ≤b≤ 5). If b = 5,then a ≡ 15 (mod 42) ,again contrary to the fact that a ≤ 8 . If b = 3,then a = 7 , $|G| = 2^7 3^3 5 7 11^2$. Then for P as above , [G:N(P)] ≡ -1 or 5 (mod 11), contradicting Sylow's theorem.

This contradiction completes the proof of this Lemma .

Remark

We close this section by noting that we may assume from now on that [N(S) : C(S)] = 4 .

Section Two

In this section, we prove that $C(S) \neq S$. In fact, we prove a slightly stronger result (Lemma 4.2.1). We prove that the principal 5-block can contain at most one character of degree 11, so that if X lies in the principal 5-block, then X is rational-valued. Lemma 1.3.9 allows us to exclude this possibility.

Lemma 4.2.1

X does not lie in the principal 5-block of G.

Proof

Suppose that X belongs to the principal 5-block of G. Then, as X is not rational-valued, the principal 5-block of G contains at least one more irreducible character of degree 11 which is algebraically conjugate to X.

As $[N(S):C(S)] = 4$, the principal 5-block of G contains 5 irreducible characters, each of degree congruent to +1 or -1 (mod 5). At least one of these characters has a degree, x say, with $x \equiv -1 \pmod 5$. It follows that the character degrees for the

principal 5-block are either:

1 , 11 , 11, x ,x-23.

or: 1 , 11, 11 ,x, 23-x .

The second case cannot occur, for $x \equiv -1 \pmod 5$ and $x(23-x)$ must divide $|G|$ so that $x = 9$ or 14 ,

whereas the character of degree x lies in the principal 11-block and each character of the principal 11-block has degree congruent to one of $1,-1,5$ or $-5 \pmod{11}$.

By an argument similar to that of Lemma 4.1.| , we can deduce that 11 divides $x(x-23)$.

Case i): 11 divides x

a) $x = 11.2^{a}$, $x-23 = 3^{b}.7^{c}$

Here, $3^{b}.7^{c} \equiv -1 \pmod{11}$, so that c is odd, as 3 is a quadratic residue (mod 11), but 7 and -1 are not. Also, $3^{b}.7^{c} \equiv 1 \pmod 5$, as $x \equiv -1 \pmod 5$ Hence b is also odd.

Thus $3^{b}.7^{c} \equiv 5 \pmod 8$, so that $x \equiv 4 \pmod 8$ and $a = 2$. Hence $x = 44$ and $x-23 = 21$.

Let 0 be the character of degree 21 in the principal 5-block of G

and let u be an element of order 7 in G . We note that 0 is rational-valued as it is the only character of degree 21 in the principal 5-block. As the Sylow 7-subgroups of G are Abelian , 7 does not divide [G:C(u)].

As [G:C(u)]0(u)/0(1) is an integer, 0(u) = 7z for some integer z with |z| < 3 (as G is simple).Thus [G:C(u)]0(u)/0(1) $\not\equiv$ [G:C(u)] (mod 7) so that 0 lies outside the principal 7-block of G.

As G contains no element of order 35 , Lemma 1.2.14 forces us to conclude that 0 lies in a 7-block of defect 0 and that all of the other characters of the principal 5-block lie in the principal 7-block.

However,the character of degree 44 in the principal 5-block must be rational-valued as it is the unique character of degree 44 which lies in the principal 5-block of G . As 49 does not divide |G| ,every rational-valued character in the principal 7-block has degree congruent to +1 or -1 (mod 7).

This contradiction eliminates case a).

b) $x = 11.3^{a}$, $x-23 = 2^{b}.7^{c}$.

As $x \equiv 1 \pmod 5$, a is even. Hence $x \equiv 3 \pmod 8$, so $x-23 \equiv 4 \pmod 8$ and $b = 2$. Then c is also even , as $x-23 \equiv 1 \pmod 5$. However, we see that $4.7^{c} \equiv -1 \pmod{11}$, which contradicts the fact that -1 is not a quadratic residue (mod 11).

c) $x = 11.7^{a}$, $x-23 = 2^{b}.3^{c}$.

As $x \equiv -1 \pmod 5$, a is even. As above, $b = 2$. Then $4.3^{c} \equiv -1 \pmod{11}$, a contradiction , as 3 is a quadratic residue (mod 11), but -1 is not.

d) $x = 11.2^{a}.3^{b}$, $x-23 = 7^{c}$.

As $x-23 \equiv 1 \pmod 5$, $c \equiv 0 \pmod 4$. However , $7^{c} \equiv -1 \pmod{11}$, contrary to the fact that -1 is a quadratic non-residue (mod 11).

e) $x = 11.2^{a}.7^{b}$, $x-23 = 3^{c}$.

Here, 3 is a quadratic residue (mod 11), but -1 is not , so that the equation $3^{c} \equiv -1 \pmod{11}$ has no integer solution .

f) $x = 11.3^{a}.7^{b}$, $x-23 = 2^{c}$.

Once more, c is even, and an argument similar to that of part d) yields a contradiction.

Case ii) : 11 divides x - 23

a) $x = 2^{a}$, $x - 23 = 3^{b}.7^{c}$

As $x \equiv -1 \pmod 5$, a is even . Thus $x \equiv 1 \pmod 3$, so b = 0 . Also c is divisible by 4 , as $7^{c} \equiv 1 \pmod 5$.

Thus $7^{c} \equiv 1 \pmod{16}$, and $x \equiv 8 \pmod{16}$. Consequently, a = 3, a contradiction.

b) $x = 3^{a}$, $x-23 = 11.2^{b}.7^{c}$

As $x \equiv -1 \pmod 5$, $a \equiv 2 \pmod 4$. Thus $x \equiv 1 \pmod 4$ and b = 1 . Hence : $22.7^{c} \equiv 1 \pmod 5$, and c is odd. Thus $7^{c} \equiv -1 \pmod 8$, so $22.7^{c} \equiv 10 \pmod{16}$

However, as $a \equiv 2 \pmod 4$, we have $3^{a} \equiv 9 \pmod{16}$, so $x-23 \equiv 2 \pmod{16}$ contradicting the equation: $x - 23 = 22.7^{c}$.

c) $x = 7^a$, $x - 23 = 11.2^b.3^c$.

Here, $x \equiv 1 \pmod 3$, so that $c = 0$. Also, a is even, so that $x \equiv 1 \pmod 4$ Hence $x - 23 \equiv 2 \pmod 4$ and $b = 1$, a contradiction, as $x-23 \neq 22$.

d) $x = 2^a.3^b$, $x-23 = 11.7^c$

As $x-23 \equiv 1 \pmod 5$, c is even. Thus $x - 23 \equiv 3 \pmod 8$, and $a = 1$. Also, $2.3^b \equiv -1 \pmod 5$, so b is odd.

Now $c \neq 0$, as $x \neq 34$, so that $2.3^b \equiv 2 \pmod 7$. Hence $3^b \equiv 1 \pmod 7$ a contradiction, as b is odd and 3 is notq quadratic residue (mod 7).

e) $x = 2^a.7^b$, $x - 23 = 11.3^c$

In this case, c is even, as $x-23 \equiv 1 \pmod 5$. Now $x-23 \equiv 3 \pmod 4$ so that $a = 1$. As $2.7^b \equiv -1 \pmod 5$, b is odd.

Now, however, $11.3^c \equiv 5 \pmod 7$, which contradicts the fact that c is even, whereas 5 is a quadratic non-residue (mod 7).

f) $x = 3^a.7^b$, $x-23 = 11.2^c$.

In this case, c is even, so that $x - 23 \equiv 2 \pmod 3$ and a = 0. Hence b is even , as $x \equiv -1 \pmod 5$. Thus $x \equiv 1 \pmod 4$, so that c = 1 , which is a contradiction.

Now $|G|$ is of the form:

$$2^r.3^s.5.7.11^t.$$

Also x(x-23) divides the order of G and 11 divides x(x-23) .Thus we have eliminated every possible form for the prime factorizations of x and of x-23 . Hence the proof of the Lemma is complete.

Corollary 4.2.2

i) $C(S) \neq S$.

ii) If $|C(S)| = 15$ and x is an element of order three in C(S), then there is a primitive cube root of unity, w, such that X(xs) = w for any element, s, of order 5 in S , and such that X(x) = 6w + 5.

Proof

i) If C(S) = S, then G has only one 5-block of full defect , namely the principal 5-block . As 5 does not divide X(1) , X must then lie in the principal 5-block , contrary to the above Lemma.

ii) Suppose that $|C(S)| = 15$ but that the conclusion of part ii) is false. Let s be an element of order 5 in S and let x be an element of order 3 in C(S).

By Lemma 2.4.2 ,we must conclude that : $X(s) = X(sx) = X(sx^2) = 1$. Hence X assumes the constant value 1 on all 5-singular elements , so must lie in the principal 5-block of G, contradicting the previous Lemma.

Corollary 4.2.3

i) If $|C(S)| = 15$, then 27 divides $|G|$, and unless 81 divides G ,the Sylow 3- subgroups of G are elementary Abelian of order 27.

ii) If $|C(S)| = 15$ and 7 divides $|G|$, then G contains an element of order 21.

Proof

i) Let R be a Sylow 3-subgroup of G. and suppose that $|C(S)| = 15$.

Let x be an element of order 3 in C(S).By the previous corollary, $X(x) = 6w + 5$ for some primitive cube root of unity,w.In particular , x is not conjugate to its inverse in G.

Suppose that R is Abelian of rank at most 2. Then as $G = G'$, $R \leq N(R)'$. Now as R has rank 2, $N(R) = RK$ for some 2-group K. Furthermore, we also have : $R = [R,K]$, $C_R(K) = 1$.

Let T be the subgroup of R which is generated by the elements of order 3. Then $N(R)/C(R)$ acts faithfully on T. As $T = [T,K]$, it quickly follows (from the structure of $GL(2,3)$ when T is not cyclic) that each element of T is conjugate to its inverse in $N(R)$

However, x is conjugate to an element of T but x is not conjugate to its inverse in G, a contradiction. This argument certainly applies when $|R| \leq 9$.

Suppose that R is non-Abelian of order 27 and that x lies in R. Then $X|_R$ contains a non-linear irreducible constituent, θ say, and in fact $\theta(1)=3$ As $|R| = 27$, θ is faithful.

Now $\theta(y) = 0$ for any y in $R-Z(R)$. As x has only two eigenvalues, $\theta(x) \neq 0$ Thus x lies in $Z(R)$ and x cannot be conjugate in G to any element of

R-Z(R).Now x is not conjugate to its inverse in G , and Z(R) is cyclic of order 3.Thus x is not conjugate in G to any other element of R.

As x has only two eigenvalues,x has quadratic minimum polynomial in any reduction (mod 3) of G . Now we see that Lemma 1.6.5 contradicts the simplicity of G.

ii) Suppose that $|C(S)| = 15$,and that 7 divides $|G|$ .Let x be an element of order 3 in C(S) . Then X(x) is not rational.

Let T be a Sylow 7-subgroup of G. Then $X|_T$ is not rational-valued , so that by Lemma 1.2.12 , G contains an element of order 21.

Remark

We close this section with some observations about the 5-blocks of G. We know that C(S) has order 10,15 or 30.

Case i) : $|C(S)| = 10$

Let t be an involution of C(S) and s be an element of order 5 in S.

G has two 5-blocks of full defect, the principal 5-block , and another 5-block of full defect , B say,which contains five characters.

For any irreducible character θ in the principal 5-block of G ,there is a sign e such that

$$\theta(s) = \theta(st) = e .$$

For any irreducible character θ in B ,there is a sign e such that :

$$\theta(s) = e = -\theta(st) .$$

We note that X is in B.

Let a and b be any elements of G. Consider :

$$\#(a\,b = s) + \#(a\,b = st) .$$

This may be evaluated from the expression :

$$\frac{|G|}{|C(a)|\,|C(b)|} \sum_{\theta \in I(G)} \frac{\theta(a)\,\theta(b)\,(\theta(s)+\theta(st))}{\theta(1)}$$

Unless θ lies in the principal 5-block of G , $\theta(s) + \theta(st) = 0$, whilst if θ does lie in the principal 5-block , $\theta(s) = \theta(st)$.

Hence :

$$2\,\frac{|G|}{|C(a)|\,|C(b)|} \sum_{\theta \in A_5^5(G)} \frac{\theta(a)\,\theta(b)\,\theta(s)}{\theta(1)}$$

is a sum of class algebra constants,

Similarly,

$$\#(a\,b = s) - \#(a\,b = st) = \frac{|G|}{|C(a)|\,|C(b)|} \sum_{\theta \in \mathrm{Ir}(G)} \frac{\theta(a)\,\theta(b)\,(\theta(s)-\theta(st))}{\theta(1)}$$

$$= 2\,\frac{|G|}{|C(a)|\,|C(b)|} \sum_{\theta \in \mathcal{B}} \frac{\theta(a)\,\theta(b)\,\theta(s)}{\theta(1)} \quad ,$$

and this is a difference of class algebra constants, so is certainly an integer.

Case ii) : $|C(S)| = 15$

In this case , since the element of order 3 in C(S) is not conjugate to its inverse in G , G has three 5-blocks of full defect :

i) The principal 5-block.

ii) B , the 5-block containing X .

In this block, for an element s of order 5 in S and an element x of order 3 in C(S) , and for any character ,θ of B, there is a sign e and a primitive cube root of unity , w , such that :

$$\theta(s) = e.$$

$$\theta(sx) = w\,e.$$

$$\theta(sx^2) = w^2\,e.$$

For a given choice of x, the value of w depends only on B, not on θ.

iii) $\bar{B}$, the 5-block containing $\bar{X}$.

In this block, for the same s of order 5 in S and the same x of order 3 in C(S), and for any character θ of B, there is a sign e such that :

$$\theta(s) = e.$$

$$\theta(sx) = w^2 e.$$

$$\theta(sx^2) = w e,$$

where w is the same as in ii).

By arguments similar to those of case i), we find that, for any a and b in G :

$$\sum_{i=0}^{2} \#(a\,b = sx^i)$$

$$= \frac{3|G|}{|C(a)|\,|C(b)|} \sum_{\theta \in B_0^{(S)}} \frac{\theta(a)\,\theta(b)\,\theta(s)}{\theta(1)}.$$

$$\sum_{i=0}^{2} \bar{w}^i \#(a\,b = sx^i)$$

$$= \frac{3|G|}{|C(a)|\,|C(b)|} \sum_{\theta \in B} \frac{\theta(a)\,\theta(b)\,\theta(s)}{\theta(1)}.$$

$$\sum_{i=0}^{2} w^{i} \qquad (a\,b = s x^{i})$$

$$= \frac{3\,|G|}{|C(a)|\;|C(b)|} \sum_{\theta \in \overline{B}} \frac{\theta(a)\;\theta(b)\;\theta(s)}{\theta(1)}.$$

Each of these expressions is an algebraic integer.

Case iii) : $|C(S)| = 30$

In this case , C(S) is isomorphic to $S \times S_3$. Let x be an element of order 3 in C(S) and let t be an involution of C(S) .

This time , S has three 5-blocks of full defect :

i) The principal 5-block.

ii) The 5-block,B,of G that contains X . For any irreducible character,θ say , of B , there is a sign e such that :

$$\theta(s) = \theta(sx) = e = -\theta(st)$$

for any element ,s, of order 5 in S.

iii) Another 5-block, B^{*} say. For any irreducible character,θ in B, there is a sign e , such that :

$$\theta(s) = 2e$$
$$\theta(sx) = \theta(sx^{2}) = -e.$$
$$\theta(st) = 0.$$

Let $K = O_{5'}(C(s))$.

For any irreducible character θ of G which is not in the principal 5-block of G, we see that

$$\sum_{y \in K} \theta(sy) = 0 \text{ , whereas}$$

for any irreducible character θ of G which is in the principal 5-block of G, we see that

$$\sum_{y \in K} \theta(sy) = 6\,\theta(s).$$

Thus for any a and b in G

$$\sum_{y \in K} \#(a\,b = sy)$$

$$= \frac{6\,|G|}{|C(a)|\,|C(b)|} \sum_{\theta \in B_e^{(5)}} \frac{\theta(a)\,\theta(b)\,\theta(s)}{\theta(1)},$$

is an integer.

For any irreducible character θ of G which does not lie in B, we see that

$$\theta(s) + 2\,\theta(sx) - 3\,\theta(st) = 0$$

whilst for any irreducible character θ of G which does lie in B, we see that :

$$\theta(s) + 2\,\theta(sx) - 3\,\theta(st) = 6\,\theta(s).$$

It quickly follows that :

$$\#(a\,b = s) + 2\,\#(a\,b = sx) - 3\,\#(a\,b = st)$$

$$= \frac{6\,|G|}{|C(a)|\;|C(b)|} \sum_{\theta \in \mathcal{B}} \frac{\theta(a)\;\theta(b)\;\theta(s)}{\theta(1)}.$$

which is again an integer .

These remarks may be summarized by the following Lemma , which will be very useful later.

Lemma 4.2. 4

For any elements a and b of G , and any element , s of order 5 in G , both

$$\frac{6\,|G|}{|C(a)|\;|C(b)|} \sum_{\theta \in \mathcal{B}_0^{(5)}} \frac{\theta(a)\;\theta(b)\;\theta(s)}{\theta(1)}.$$

and

$$\frac{6\,|G|}{|C(a)|\,|C(b)|} \sum_{\theta \in \mathcal{B}} \frac{\theta(a)\,\theta(b)\,\theta(s)}{\theta(1)}$$

are algebraic integers .

Section Three

Until we state otherwise, we will assume that 7 does not divide $|G|$. For the rest of this section, we assume that $|C(S)| = 15$. We will derive a contradiction from this assumption.

Lemma 4.3.1

The possible orders for G are :

i) $2^4 .3^7 .5.11$.

ii) $2^{12} .3^{11} .5 .11$.

iii) $2^{16} .3 .5.11$.

iv) $2^{10} .3^5 .5.11$.

v) $2^6 .3^{13} .5.11$.

Proof

We first note that as $|C(S)| = 15$, G contains no element of order 10, so that, in particular, $|N(P)| = 55$ for a Sylow 11-subgroup, P, of G.

Now $|G|$ has the form :

$2^a .3^b .5.11$, where :

i) $3 \leq a \leq 17$

ii) $3 \leq b \leq 13$

iii) $2^a .3^b \equiv 1 \pmod{11}$.

iv) $2^{a-2} .3^{b-1} \equiv 1 \pmod{5}$.

From iii), we have: $a \equiv 2b \pmod{10}$, so that a is even . We then conclude from iv) that b is odd . Also , we have : $a \equiv b+1 \pmod 4$. We consider each possible value of b separately.

a) If $b = 3$, then $a \equiv 16 \pmod{20}$, so that $a = 16$.

b) If $b = 5$, then $a \equiv 10 \pmod{20}$, so that $a = 10$.

c) If $b = 7$, then $a \equiv 4 \pmod{20}$, so that $a = 4$.

d) If $b = 9$, then $a \equiv 18 \pmod{20}$, a contradiction, as $a \leq 17$.

e) If $b = 11$, then $a \equiv 12 \pmod{20}$, so that $a = 12$.

f) If $b = 13$, then $a \equiv 6 \pmod{20}$, so that $a = 6$.

Hence the only possible values of G are those given in the statement of this Lemma.

Lemma 4.3.2

$|G| \neq 2^{16} .3^3 .5.11$

Proof

Suppose that $|G| = 2^{16} .3^3 .5.11$. Then the Sylow 3-subgroups of G are elementary Abelian by Corollary 4.3.2 Let x be an element of order three in C(S). Let C = C(x) and let K = O (C).

5'

Now S acts without non-identity fixed points on $K/\langle x\rangle$, so that K is nilpotent. As $|O_3(C)| \leq 27$, S must centralize $O_3(C)$, so that $O_3(C) = \langle x\rangle$ as 9 does not divide $|C(S)|$. Suppose that $O_2(C) \neq 1$. Let $M = O_2(C)$.

As C(S) contains no element of order 6, S acts Frobeniusly on M. By Corollary 4.2.2, x has only two distinct eigenvalues, one of which occurs with multiplicity 6, while the other occurs with multiplicity 5. As SM acts on each eigenspace of x, M is Abelian (for $X^*|_{SM}$ has no irreducible constituent of degree greater than 5)

Now M has rank 4, for otherwise M would have rank 8 (as S acts without non-trivial fixed points on M) and M would contain an involution with a fixed-point space of co-dimension two, contrary to Lemma 2.1.6. For the same reason, M cannot act trivially on the 5-dimensional eigenspace of x.

Now C acts on the 5-dimensional fixed-point subspace of x. Let T be the kernel of this action. Now T does not contain S by Corollary 4.2.2. Thus $T \leq K$, so that K is nilpotent. As M

has rank 4 , $T \cap M = 1$ (for S acts Frobeniusly on $T \cap M$ and M is not contained in T).Thus $T = \langle x \rangle$.

Let $\overline{C} = C/T$ and θ be the irreducible character of C afforded by the action of C on the 5-dimensional eigenspace of x . Then $\theta|_{SM}$ is irreducible and $\theta|_{M}$ contains 5 distinct constituents As M is a normal subgroup of C , θ is induced from a linear character of a subgroup of C of index 5.Consequently $\overline{C}$ has an Abelian normal subgroup , A say ,such that $\overline{C}/A$ is isomorphic to a subgroup of S_5 .

If 5 divides $|A|$, then $\overline{C}$ has a normal Sylow 5-subgroup , and C has also. As 9 does not divide $|N(S)|$, 9 does not divide $|C|$,contrary to Lemma 4.2.3 . Thus A is a 5'-group.Let B be the inverse image in C of A . Then B is a 5'-group,so that $B \leq M \times \langle x \rangle$ and 9 does not divide $|B|$. As 9 does not divide $[C:A]$,27 does not divide $|C|$, contrary to Lemma 4.2.3 .

We conclude that $O_2(C) = 1$. Now S is not normal in C , as 9 does not divide $|N(S)|$, and so $F(C) = \langle x \rangle$.

Thus $E(C) \neq 1$. As C is a $\{2,3,5\}$-group and 25 does not divide $|C|$, C has a unique component, L say. As 81 does not divide $|G|$, $L/Z(L)$ is isomorphic to A_5 or A_6.

Now $N(S) \leq C$, so that $C = LN(S)$ Now 27 divides $|C|$ by Lemma 4.2.3 and $Z(L) \leq \langle x \rangle$, so that 9 divides $[L:Z(L)]$ and $L/Z(L)$ is isomorphic to A_6. Now we claim that x does not commute with any of its other conjugates.

We know that S acts non-trivially on each eigenspace of x, so that L must certainly act non-trivially on these spaces. Let y be an element of order 3 in $L-\langle x \rangle$. Let $\bar{L} = L/Z(L)$. We note that $\bar{L}$ acts faithfully on the 5-dimensional fixed-point subspace of x

Now $\bar{y}$ is conjugate to its inverse within $\bar{L}$, so that y has three distinct eigenvalues in its action on the 5-dimensional fixed-point subspace of x Also xy and x^2y both have 3 distinct eigenvalues in their action on this space. As x has only two eigenvalues x cannot be conjugate to y, xy, or to x^2y.

Now $L\langle x \rangle$ contains every Sylow 3-subgroup of C, and x is certainly not conjugate to its inverse in G, so that no conjugate of x, apart from x itself, lies in C. Since x acts with

quadratic minimum polynomial in any reduction (mod 3) of G , Lemma 1.6.5 now contradicts the simplicity of G.

The proof of Lemma 4.3.2 is now complete.

Lemma 4.3.3

$$|G| \neq 2^{12}.3^{11}.5.11$$

Proof

Suppose that $|G| = 2^{12}.3^{11}.5.11$ and let x be an element of order 3 in C(S).Let C = C(x).We first claim that 3^8 divides $|C|$. Let R be a Sylow 3-subgroup of G which contains x.

We may suppose that R consists of monomial matrices.Let D be the normal subgroup of R which consists of all the diagonal matrices in R . As each irreducible constituent of $X|_R$ has degree 1 or 3 , [R:D] ≤ 27 , so that $|D| \geq 3^8$. We claim that x lies in D , which will suffice to prove that 3^8 divides $|C|$,as D is Abelian.

Let Θ be an irreducible constituent of degree 3 of $X|_R$ (if there is one) As x has only 2 eigenvalues, Θ(x) ≠ Θ Thus x is represented by a diagonal matrix in any monomial representation of R which affords Θ .Hence x lies in D , as required.

We next claim that $O_3(C)$ has order 3^9. Suppose first that $\langle x \rangle = O_3(C)$. Suppose that L is a component of C^3. Then as 5 divides $|C|$ to the first power only, L is the unique component of C. As $N(S) \leq C$, $C = LN(S)$.

Now $L/Z(L)$ is isomorphic to one of : A_5, A_6 or $PSU(4,2)$. As 9 does not divide $|Z(L)|$, 3^6 does not divide $|L|$, so that 3^7 does not divide $|C|$, a contradiction. Thus if $O_3(C) = \langle x \rangle$, then $E(C) = 1$.

Let $T = O_{5'}(C)$. Then S acts fixed-point freely on $T/\langle x \rangle$, so that T is nilpotent. Now S is not normal in C, as 9 does not divide $|N(S)|$. As $E(C) = 1$ and $O_3(C) = \langle x \rangle$, we deduce that $O_2(C) \neq 1$. Let $M = O_2(C)$.

As S acts Frobeniusly on M, and M contains no involution with an eigenspace of codimension 2, we deduce as in the previous Lemma that M is Abelian of rank 4 and that M acts non-trivially on the 5-dimensional fixed-point subspace of x.

Let θ be the character afforded by the action of C on the fixed-point subspace of x and let $T = \ker \theta$. As

in the previous Lemma we find that $T = \langle x \rangle$ .Let $\overline{C} = C/\langle x \rangle$ .Again we find that $\overline{C}$ has an Abelian normal subgroup A say, such that $\overline{C}/A$ is isomorphic to a subgroup of S_5 . As we have assumed that $O_3(C) = \langle x \rangle$,we find ,just as we did in the previous Lemma , that 27 does not divide $|C|$,a contradiction.

Thus we conclude that $O_3(C) \neq \langle x \rangle$. Let $W = O_3(C)$. By Lemma 3.1.4 , W is Abelian . Now S acts Frobeniusly on [W,S] ,so that [W,S] has rank 4 (for if it had rank 8,then W would contain an element with a fixed-point space of co-dimension two) . Thus S acts indecomposably on [W,S] , and [W,S] is homocyclic. As 3^{12} does not divide $|G|$, [W,S] has exponent 3 or 9.

Let K = [W,S]. Then SK acts on each eigenspace of x . As SK is a Frobenius group , we conclude that

$$X|_{SK} = 1 + \theta_1 + \theta_2 ,$$

where θ_1 and θ_2 are both irreducible of degree 5 , though they need not be distinct characters (if $X|_{SK}$ did not have this form , then K would contain an element with a fixed-point subspace of co-dimension two).

As $W = K \times \langle x \rangle$, it is easy to see that $X|_W$ has 11 distinct constituents By Lemma 1.5.1, $C(W)$ is an Abelian 3-group. As $C(W) \leq C$, we see that $C(W) = W$. In particular, $O_2(C) = 1$. We claim that 9 does not divide $[C:W]$.

Let θ be the character afforded by the action of C on the fixed-point subspace of x and let $T = \ker \theta$. We find once more that $T = \langle x \rangle$. Again we find that θ is induced from a linear character of a subgroup of index 5 of C, so that $\bar{C}$ $(= C/\langle x \rangle)$ has an Abelian normal subgroup, A say, such that $\bar{C}/A$ is isomorphic to a subgroup of S_5. As $\bar{C} = C/\langle x \rangle$, 9 does not divide $[C:W]$, as claimed.

If W is elementary Abelian, then $|W| = 3^5$, so that 3^7 does not divide $|C|$, a contradiction. Thus $|W| = 3^9$. Let $M = N(W)$ and let $U = O_{5'}(M)$.

Now S normalizes some Sylow 3-subgroup, say Y, of U. Also, $W \leq Y$. By Lemma 3.1.4, Y is Abelian, so that $Y = [Y,S] \times C_Y(S)$. By the argument used above for W, $[Y,S]$ is homocyclic of rank 4 and of exponent 3 or 9. Since $C_Y(S) = \langle x \rangle$ and $W \leq Y$, we deduce that $Y = W$.

Now $N(S) \leq M$ as $N(S) \leq C$. Suppose that M is soluble .Then $M = U\ N(S)$, so that 3 does not divide $[M:U]$ (for x lies in U) . Thus W is a Sylow 3-subgroup of $N(W)$, and hence of G , whereas 3^{11} divides $|G|$ and $|W| = 3^{9}$ a contradiction.Thus M is insoluble.

Let R be a Sylow 3-subgroup of M. We claim that $ZJ(R)$ is normal in M and that ,in fact, $J(R) = W$. Now as $C(W) = W$, $R \neq W$, since $M = N(W)$ and W is not a Sylow 3-subgroup of G.

Suppose that $W = O_{5'}(M)$ .Then as M is insoluble , M/W has a component L,say, which is a simple group whose order has the form $2^{a}.3^{b}.5$. Thus L is isomorphic to one of :

$$A_5\ ,\ A_6 \text{ or } PSU(4,2).$$

As $|W| = 3^{9}$,

L cannot be isomorphic to $PSU(4,2)$. We claim that,in fact,L is isomorphic to A_5.

We note that L permutes the 11 linear constituents of $X|_W$. If L has an orbit of size 5 in this action , then L has a subgroup of index 5 ,and

L is isomorphic to A_5, so we assume that L has no such orbit. As $X(1) = 11$ and S has two orbits of size 5 on the constituents of $X|_W$, we see that L has an orbit of size 10 on the linear constituents of $X|_W$.

If L is isomorphic to A_6, then the action of L on the orbit of size 10 is doubly transitive. Let B be the stabilizer in L of μ, a character in the orbit of length 10. Then B acts transitively on the nine remaining characters in the orbit of size 10. Let D be a Sylow 3-subgroup of B. Then D acts transitively on the above set of nine characters.

As D is a 3-group, D centralizes a non-identity element of W, say w. Let u be a constituent of $X|_W$ which lies in the orbit of size 9 under the action of D. Then $X(w) = 9\,\mu(w) + \lambda_1(w) + \lambda_2(w)$ where λ_1 and λ_2 are the constituents of $X|_W$ which lie outside the orbit of size 9 under the action of D. Thus w has an eigenspace of codimension 2 or less, contrary to Lemma 2.1.6. Thus L is not isomorphic to A_6.

Thus L is isomorphic to A_5, as claimed . As 25 does not divide [M:W] , L = E(M/W) .As F(M/W) = 1 9 does not divide [M:W] , and M has Sylow 2-subgroups which are either Abelian or are dihedral of order 8 Thus M is 3-stable . As C(W) = W , M is 3-constrained . Hence ZJ(R) is normal in R .

If S centralizes ZJ(R) , then ZJ(R) = $\langle x \rangle$ and [M: C(x)] $\leq$ 2 (we know that C(x) $\leq$ M , as M = N(W) and W = O_3 (C(x))) . Certainly R is a Sylow 3-subgroup of N (ZJ(R)) and so of G , contrary to the fact that R has order 3^{10} , whereas 3^{11} divides |G|.

If S does not centralize ZJ(R) ,then C_M (ZJ(R)) $\leq$ $O_{5'}$ (M) = W (as we are still working under the assumption that $O_{5'}$ (M) = W) . In particular , J(R) $\leq$ W . As W is Abelian, W = J(R) as claimed.

Now however , R is a Sylow 3-subgroup of N(J(R)) and so of G , contrary to the fact that $|R| = 3^{10}$ and 3^{11} divides |G| . Thus we may suppose that $O_{5'}$ (M) has even order.

We recall that $U = O_{5'}(M)$. Now W is not contained in $Z(U)$, so $\chi|_W$ contains an irreducible constituent which is not linear, and which does not contain W in its kernel (otherwise we would have $[W,U] \leq \ker \chi$). Let θ be such a constituent. Then $\theta(1)$ is a power of 2, as W is an Abelian normal subgroup of U and $[U:W]$ is a power of 2.

If $\theta(1) \geq 4$, then θ is S-invariant, as $\chi(1) = 11$. Then the irreducible constituents of $\theta|_W$ are permuted by S. However, S has two orbits of size 5 and an orbit of size 1 on the linear constituents of $\chi|_W$ (which are all distinct). As $\theta(1)$ is a power of 2, we cannot reconcile these facts, and we are forced to conclude that $\theta(1) = 2$.

Then θ^{SW} must be irreducible, for again θ cannot be S-invariant. Also, θ^{SW} occurs as a constituent of $\chi|_{SW}$. As 11 does not divide $|M|$, $\chi|_M$ is not irreducible. Thus θ^{SW} must extend to an irreducible character, say θ^*, of M, which occurs as a constituent of $\chi|_M$.

Now $X|_M = \theta^* + \mu$, where μ is a linear character of M. As $\theta^*(s) = 0$ for any element, s, of order 5 in S, we see that $S \leq \ker \mu$ by the unimodularity of X. Thus $[S,U] \leq \ker \mu$. As S acts Frobeniusly on a Sylow 2-subgroup of U and as $[W : [W,S]] = 3$, we see that $[U : [S,U]] \leq 3$.

Now SW acts on the eigenspaces of x and x has the eigenvalue 1 with multiplicity five and a primitive cube root of unity as an eigenvalue with multiplicity 6. It follows that $\theta|_{SW}$ contains two irreducible constituents of degree 5 and that x lies outside $\ker \mu$.

Let $Q = [S,U]$. Then x lies outside Q, so that S acts without non-trivial fixed-points on Q, and Q is nilpotent. Now $Q = \ker \mu \cap U$, so that Q is normal in M. Hence $O_2(Q)$ is normal in M. As $C(W) = W$ and $W = O_3(M)$, we conclude that $O_2(Q) = 1$, contrary to the fact that U has even order and Q contains a Sylow 2-subgroup of U.

This contradiction completes the proof of Lemma 4.3.3.

We conclude this section with:

Lemma 4.3.4

$|C(S)| \neq 15$.

Proof

We have proved that 2^{11} does not divide $|G|$ if $C(S)$ has order 15 .The result now follows from the remarks at the end of chapter two.

Corollary 4.3.5

3^{12} does not divide $|G|$ if 7 does not divide $|G|$.

Proof

We know now that $|C(S)|$ is even,when 7 does not divide $|G|$.Hence the 5-block of G which contains X is invariant under all algebraic conjugation . Since this block only contains 5 characters , either X is real-valued on 3-elements , or else $X + \overline{X}$ is rational-valued on 3-elements .

In the former case, 3^{10} does not divide $|G|$ by Lemma 2.5.2 and in the other case , 3^{11} does not divide $|G|$ by Lemma 2.5.2 .

Section Four

In this section, we still assume that 7 does not divide $|G|$ and that $|C(S)|$ is even. We prove that the only possible set of character degrees for the principal 5-block is :

1, 66, 99, 144, 176.

Lemma 4.4.1

The principal 5-block of G contains an irreducible character of degree 66 or 16.

Proof

If $X \neq \overline{X}$, let $X^* = X$. If $X = \overline{X}$, we may choose X^* to be an algebraic conjugate of X different from X, since we know that X is not rational-valued.

Now XX^* assumes the constant value 1 on 5-singular elements. Also, as $X^* \neq \overline{X}$, $(XX^*, 1_G) = 0$. Since XX^* assumes the constant value 1 on 5-singular elements there is an irreducible constituent θ of XX^*, lying in the principal 5-block of G, with $\theta(1) \equiv 1 \pmod 5$. Also, $\theta(1) \leq 120$

We also know that $\theta(1)$ is congruent to one of : 0, 1, -1, 5, or -5 (mod 11). As

$\theta(1)$ divides $|G|$, $\theta(1)$ is one of :

1, 6 , 11 , 16 , or 66.

As G is simple, $\theta(1) \neq 1$. As $G/Z(G)$ is not isomorphic to PSL(2,11), $\theta(1) \neq 6$ If $\theta(1) = 11$, then θ is rational-valued by the arguments of Lemma 4.2.1 , so that G is no counterexample to the theorem by Lemma 1.3.9 . Hence $\theta(1) = 16$ or 66.

Lemma 4.4.2

The possible sets of character degrees in the principal 5-block are:

i) 1 , 16, 16, 66, 99

ii) 1,66,66,891,1024

iii) 1,66,99,1024,1056

iv) 1,66,99,144,176

v) 1,66,176,7776,8019

Proof

Let θ be the character described in the previous Lemma. There are 2 cases to consider:

Case i) : $\theta(1) = 16$

In this case, θ is an exceptional character in the principal 11-block. Thus the principal 11-block contains another exceptional character of degree 16 . This

character is algebraically conjugate to 0, so also lies in the principal 5-block.

It quickly follows that there is an integer x and a sign e such that:

a) $x \equiv -1 \pmod 5$.

b) The character degrees in the principal 5-block are : 1 , 16 , 16 , x , e(x-33).

If e = -1, then $x \leq 33$. As x and 33-x divide $|G|$, we may suppose that x = 9. Now however , the character of degree 9 must lie in the principal 11-block , which contradicts the fact that every irreducible character of the principal 11-block has degree congruent to one of: 1, -1, 5, or -5 (mod 11).

Thus e = 1.

We need now to find x find x such that :

i) x and x-33 both divide $|G|$.

ii) $x \equiv -1 \pmod 5$.

Either x or x-33 is odd. If x is odd , then 3 divides x to an even power, since $x \equiv -1 \pmod 5$. As $x \neq 11, 9$ divides x and so 3 divides x-33 to the first power only . Thus 2 divides x-33 to an odd power , as $x-33 \equiv 1 \pmod 5$.

If 4 divides x-33 , then $x \equiv 1 \pmod 4$ so that 11 does not divide x (for if it did, then x would be of the form 11.3^{2k} and $x \equiv 3 \pmod 4$).In that case , x is the degree of a non-exceptional characte of the principal 11-block , and so :

$x \equiv 1 \pmod{11}$,as x is a power of 3 Then also, $x-33 \equiv 1 \pmod{11}$,contrary to the fact that $x - 33 = 2^{r}.3^{c}$ for some odd integer r. Thus 4 does not divide x-33 and $x - 33 = 66$, $x = 99$,in this case.

If x-33 is odd , then 3 divides x-33 to an even power , so that 3 divides x to the first power only . Certainly , we cannot have x= 3 ,33 or 66 in this case, so that 4 divides x,and $x-33 \equiv 3 \pmod 4$ Thus 11 divides x-33 (for otherwise , $x-33$ has the form 3^{2d} for some integer d , so $x-33 \equiv 1 \pmod 4$.).

Thus $x - 33$ has the form 11.3^{2d} , so that $x-33 \equiv 3 \pmod 8$ and $x \equiv 4 \pmod 8$ Thus x = 132,a contradiction.

Case ii) : $\theta(1) = 66$

Let the character degrees for the principal 5-block be: 1 , 66, x , y , z. We note the following facts:

a) At least one of x,y,z is odd.

b) At least one of x,y,z is prime to 3.

c) At least one of x,y,z is prime to 11

d) Any character in the principal 5-block has degree congruent (mod 11) to one of : 0,1,-1,5 or -5.

e) $x \neq 11, y \neq 11, z \neq 11$ (for otherwise, the principal 5-block would contain a rational-valued character of degree 11).

We may suppose that $x \equiv -1 \pmod 5$. We claim that we may also suppose that $y \equiv 1 \pmod 5$. For otherwise:

$$x \equiv y \equiv z \equiv -1 \pmod 5$$ and :

$$x + y + z = 67.$$

as x,y and z all divide $|G|$, it is easy to see that ,without loss of generality:

$x = 54, y = 9, z = 4$

This contradicts d) above.

Thus we assume that $y \equiv 1 \pmod 5$ and that $x \equiv -1 \pmod 5$. Now there is a sign e such that $1 + 66 - x + y + ez = 0$ and $z \equiv e \pmod 5$.

Suppose first that the principal 5-block contains an exceptional character of the principal 11-block . Then it contains two such characters of equal degree . Hence either $x = z$ or $y = z$.

Suppose that $x = z$ and that 6 divides x Then $1 + 66 - 2x + y = 0$, so that y is prime to 6 .As y is prime to 5 and divides the order of G , $y = 11$, contrary to e).

Thus we may suppose that either:

i) $x = z = p^a$ where $p = 2$ or 3 or :

ii) $y = z = p^a$ where $p = 2$ or 3.

We note that in all cases , a is even , as $x = -1 \pmod 5$ and $y \equiv 1 \pmod 5$.

As a is even, p^a is a quadratic residue (mod 11) . Since p^a is the degree of an exceptional character in the principal 11-block , $p^a \equiv 5 \pmod{11}$ (5 is a quadratic residue (mod 11), but -5 is not).

In the first case , we have:

$$1 + 66 - 2x + y = 0 .$$

As $x \equiv 5 \pmod{11}$, $y \equiv -2 \pmod{11}$, contrary to e) above.

In the second case , we have:

$$1 + 66 + 2y - x = 0.$$

Hence $y \equiv 0 \pmod{11}$. Suppose that $p = 2$. Then $2^a \equiv 5 \pmod{11}$ and $2^a \equiv 1 \pmod 4$. Hence $a \equiv 4 \pmod{20}$ and $a = 4$, as $a \leq 17$ Thus $x = 99$, and the character degrees in this case are 1, 16, 16, 66, 99 . Suppose that $p = 3$. Then :

$$1 + 66 - x + 2.3^{a} = 0.$$

Hence x is prime to 3 and is odd . Since x is prime to 5 , we are forced to conclude that x = 11 , contrary to e) above.

We suppose from now on that x,y and z are each congruent (mod 11) to 0 , -1 or 1 . We consider several cases:

i) Suppose that x is a power of 3.

In this case , $x = 3^{b}$,where $b \neq 0$ As $x \equiv -1 \pmod 5$, $b \equiv 2 \pmod 4$. Also , $x \equiv 1 \pmod{11}$ as 3 is a quadratic residue (mod 11) but -1 is not.Hence $b \equiv 0 \pmod 5$ so that b = 10, as 3^{20} does not divide |G|.

Now $1 + 66 - x + y + ez = 0$, so that $y + ez \equiv 14 \pmod{81}$. Also $y + ez \equiv 0 \pmod{11}$,as $x = 1 \pmod{11}$. Suppose that 11 does not divide yz. Then either y or z is a power of 2.

If $y = 2^{c}$,then $c \equiv 0 \pmod 4$,as $y = 1 \pmod 5$. Hence 2^{c} is a quadratic residue (mod 11) so that $2^{c} \equiv 1 \pmod{11}$ .Thus 10 divides c,so that $c \equiv 0 \pmod{20}$, whereas 2^{20} does not divide |G| and $c \neq 0$.

Hence z is a power of 2,and the same argument applies unless $z \equiv -1 \pmod 5$.In that case , we use a similar argument to conclude that $z = 2^{10}$. We now have:

$$1 + 66 - 3^{10} - 2^{10} + y = 0.$$

It quickly follows that $y \equiv 2 \pmod 4$,

$y \equiv 6 \pmod 9$ and $y \equiv 1 \pmod{11}$. As y is an integer of the form $2^r.3^s$, we have a contradiction.

Thus 11 divides both y and z. Also , 3 does not divide both y and z. If $y = 11.2^r$,then $r \equiv 0 \pmod 4$,as $y \equiv 1 \pmod 5$. Thus $y \equiv 2 \pmod 3$. Now:

$$1 + 66 - 3^{10} + 11.2^r + ez = 0.$$

Thus 3 divides z. Also,$ez \equiv 6 \pmod 8$ so that 2 divides z but 4 does not .Thus $z = 22.3^k$ for some integer k . As $z \equiv e \pmod 5$, k is odd. Thus $z \equiv 2 \pmod 8$, so that $e = -1$ and $k \equiv 3 \pmod 4$.

Hence $11.2^r \equiv 14 \pmod{27}$.Certainly then $2^{r+1} \equiv 5 \pmod 9$ and $r \equiv 4 \pmod 6$. As $r \equiv 0 \pmod 4$) and 2^{18} does not divide $|G|$, we must have $r = 16$. However ,as $2^{18} \equiv 1 \pmod{27}$, $2^{16} \equiv 7 \pmod{27}$, so that $11.2^{16} \equiv -4 \pmod{27}$,a contradiction

Thus $z = 11.2^r$,and a similar argument applies unless $z \equiv -1 \pmod 5$. Thus we assume that $z \equiv -1 \pmod 5$.

Now $1 - 3^{10} - 11.2^r + y = 0$

As $z \equiv -1 \pmod 5$, r is even , so that $11.2^r \equiv 2 \pmod 3$ and $y \equiv 1 \pmod 3$. Hence $y = 11.2^s$ for some integer s . As $y \equiv 1 \pmod 5$,s is even,and $y \equiv 2 \pmod 3$,

a contradiction.

This disposes of the possibility that x is a power of 3. An analagous argument allows us to conclude that z is not a power of 3 unless $z \equiv 1 \pmod 5$.

ii) Suppose that y is a power of 3.

In this case, let $y = 3^b$

Then $b \equiv 0 \pmod 4$, as $y \equiv 1 \pmod 5$. Also $y \equiv 1 \pmod{11}$, so that $b \equiv 0 \pmod 5$. As 3^{20} does not divide $|G|$ and $y \neq 1$, this case cannot arise.

Similarly, z cannot be a power of 3 when $z \equiv 1 \pmod 5$. Thus none of x, y or z is a power of 3.

Also, a similar argument shows that if y is a power of 2, then 2^{20} divides y, contradicting the fact that 2^{20} does not divide $|G|$. This argument applies when z is a power of 2 and $z \equiv 1 \pmod 5$.

iii) Suppose that x is a power of 2.

Let $x = 2^a$. Then $a \equiv 2 \pmod 4$ as $x \equiv -1 \pmod 5$. Thus 2^a is a quadratic residue $\pmod{11}$, so that $2^a \equiv 1 \pmod{11}$

Hence $a \equiv 0 \pmod{10}$, so that $x = 2^{10}$, as 2^{20} does not divide $|G|$.

Now we have:

$1 + 66 - 1024 + y + ez = 0.$

Hence $y + ez \equiv 6 \pmod 9$.

$y + ez \equiv 5 \pmod 8$.

It quickly follows that 3 divides both y and z (otherwise, both are prime to 3 and at least one is odd, so either $y = 11$ or $z = 11$), but that 9 cannot divide both y and z.

Thus one of y,z has the form 33.2^r, the other has the form 11.3^s, where r is odd and s is even. If $r = 1$, then the character degrees are 1, 66, 66, 891, 1024. Hence we assume that $r \geq 3$.

In that case, either 11.3^s or $e\,11.3^s$ is congruent to 5 (mod 8). As s is even, $11.3^s \equiv 3 \pmod 8$. Hence $e = -1$ and $z = 11.3^s$. Thus $11.3^s \equiv -1 \pmod 5$, so that $s \equiv 2 \pmod 4$. Also $33.2^r \equiv 1 \pmod 5$ so that $r \equiv 1 \pmod 4$.

We now have:

$$1 + 66 - 1024 + 33.2^r - 11.3^s = 0.$$

Thus $2^r - 3^{s-1} = 29$. If $s > 2$, then we have: $2^r \equiv 2 \pmod{27}$ (for $s \equiv 2 \pmod 4$ so that $s \geq 6$). Hence $r \equiv 1 \pmod{18}$. As 2^r divides $|G|$ and $r > 1$, this is not possible. Hence $s = 2$, and the character degrees are : 1, 66, 99, 1024, 1056.

A similar argument applies if

z is a power of 2 ,and $z \equiv -1 \pmod 5$.We may now assume that one of x,y or z has the form : 11.2^a , that another has the form 11.3^b , and that the other has the form $2^c.3^d$ (where abcd $\neq 0$, a is even and b is even).

As $1 + 66 - x + y + ez = 0$ it follows that if $2^c.3^d \equiv u \pmod 5$, then $2^c.3^d = -u \pmod{11}$ (where u = 1 or -1) We may suppose that $x = 2^c.3^d$ if u = -1, or that $y = 2^c.3^d$ if u = 1.

iv) $x = 2^c.3^d$

As $x \equiv -1 \pmod 5$, $c-d \equiv 2 \pmod 4$. Also $x \equiv 1 \pmod{11}$, so that c is even, as 2 is not a quadratic residue (mod 11), but 3 is . Hence c and d are both even.

Now $1 + 66 - x + y + ez = 0$, so that

$$y + ez \equiv 1 \pmod 4 \quad \text{and}$$

$$y + ez \equiv 5 \pmod 9.$$

As a and b are both even, $11.2^a \equiv 0 \pmod 4$ and $11.3^b \equiv 3 \pmod 4$. Thus e = -1 and $z = 11.3^b$ .As $z \equiv -1 \pmod 5$, $b \equiv 2 \pmod 4$

Now $1 + 66 - 2^c.3^d + 11.2^a - 11.3^b = 0$.

Hence $11.2^a \equiv 5 \pmod 9$, and $a \equiv 4 \pmod 6$

As $11.2^a \equiv 1 \pmod 5$, $a \equiv 0 \pmod 4$. Thus $a \equiv 4 \pmod{12}$. As $a \leq 17$, a = 4 or 16.

If a = 4 , then:

$1 + 66 + 176 - 2^c.3^d - 11.3^b = 0$. Hence $11.3^b < 243$, so that $b = 2$, and the character degrees are : 1, 66, 99, 144, 176.

If $a = 16$, then $11.2^{16} \equiv -4 \pmod{27}$. As $1 + 66 + 11.2^{16} - 2^c.3^d - 11.3^b = 0$, we see that either $b = 2$ or $d = 2$. If $d = 2$, then $c \equiv 0 \pmod 4$ and $c \equiv 4 \pmod{10}$ (as $2^c.3^d \equiv -1 \pmod 5$ and $2^c.3^d \equiv 1 \pmod{11}$) so that $c = 4$, as $c \leq 17$. Then the degrees are $1, 66, 144, 11.2^{16}, 11.3^b$ where :

$1 + 66 - 144 + 11.2^{16} = 11.3^b$.

Now $2^8 \equiv 256 \equiv 13 \pmod{243}$, so that $2^{16} \equiv 169 \pmod{243}$ and $11.2^{16} \equiv 158 \pmod 3$. Hence $11.3^b \equiv 81 \pmod{243}$, and $b = 4$, which is a contradiction.

iv) $y = 2^c.3^d$

In this case, $2^c.3^d \equiv 1 \pmod 5$, so that $c \equiv d \pmod 4$. Also, $y \equiv -1 \pmod{11}$, so that c is odd, as 3 is a quadratic residue but 2 and -1 are not. Consequently, c and d are both odd.

If $d = 1$, then $c \equiv 1 \pmod 4$. Furthermore, $3.2^c \equiv -1 \pmod{11}$, so that $c = 7 \pmod{10}$. Hence $c \equiv 17 \pmod{20}$, so that $c = 17$. Let θ be the character of degree 3.2^{17}. Then θ is in a 2-block of defect 0 and vanishes on 2-singular elements. However, as $|C(S)|$ is

even, there is an element s of S and an involution t of C(S) such that :

$0(st) = 0(s) = -1$, a contradiction.

If $c = 1$, then $d \equiv 3 \pmod 5$, as $2.3^d \equiv -1 \pmod{11}$. Also, $d \equiv 1 \pmod 4$ Thus $d \equiv 13 \pmod{20}$, a contradiction, as 3^{13} does not divide $|G|$. Hence $c \geq 3$ and $d \geq 3$.

Now $1 + 66 + 2^c.3^d - x + ez = 0$. Thus:

$x - ez \equiv 13 \pmod{27}$.

$x - ez \equiv 3 \pmod 8$.

Now either x or z has the form 11.2^r other has the form 11.3^S, where r and s are even. Thus $11.2^r \equiv 2 \pmod 3$, so that $x = 11.3^s$, $z = 11.2^r$ and $e = 1$.

Now $s \geq 2$, so that $z \equiv 5 \pmod 9$ and $r \equiv 4 \pmod 6$. As $z \equiv 1 \pmod 5$, $r \equiv 0 \pmod 4$ Hence $r \equiv 4 \pmod{12}$. If $r = 16$, then $z \equiv -4 \pmod{27}$, as before. Now:

$$1 + 66 + 11.2^{16} - 11.3^s + 2^c.3^d = 0.$$

As $d \geq 3$, we see that $11.3^s \equiv 9 \pmod{27}$, a contradiction, as $99 = 18 \pmod{27}$. Thus $r = 4$.

We now have:

$$1 + 66 + 176 + 2^c.3^d - 11.3^s = 0$$

Consequently, $11.3^s - 2^c.3^d = 243$. Since $s \equiv 2 \pmod 4$, $11.3^s = 3 \pmod{16}$. Certainly $243 \equiv 3 \pmod{16}$, so that $c \geq 4$. As c is odd,

$c \geq 5$.

Consequently, $11.3^{s} \equiv 19 \pmod{32}$ so that $s \equiv 6 \pmod{8}$. As $s \leq 13$, we see that $s = 6$.

Now the character degrees are :

1, 66 , 176, 7776, 8019.

The proof of the Lemma is complete.

Corollary 4.4.3

i) 32 divides $|G|$.

ii) If there is a character of degree 1024 in the principal 5-block of G then 2^{11} divides $|G|$.

iii) If $|C(S)| = 30$, then 27 divides $|G|$.

Proof

In each of the possible sets of degrees for the principal 5-block , there is a character of degree divisible by 16 , say θ . We know that θ does not vanish at all 2-singular elements, because there is an involution t of $C(S)$ and an element s of s such that $\theta(st) = \theta(s) \neq 0$.

Thus θ does not lie in a 2-block of defect 0, so that 32 divides $|G|$.

A similar argument shows that 2^{11} divides $|G|$ if the principal 5-block of G contains an irreducible character of degree 1024.

iii) Each possible set of character degrees contains a character of degree divisible by 9 ,say 0.If C(S) has order 30, then G contains an element , x , of order 15 with $0(x) \neq 0$. Thus 0 does not lie in a 3-block of defect 0 , so that 27 divides $|G|$.

Lemma 4.4.4

The character degrees 1,16,16,66,99 do not occur.

Proof

Suppose that these degrees do occur. Let 0_1 be one of the characters of degree 16,and let t be an involution of G which is central in a Sylow 2-subgroup of G.

Then as G is simple and

$([G:C(t)], 0_1(1)) = 1$, $0_1(t) = 0$.

Now the character table of G has a fragment of the form:

	1	t	s
1	1	1	1
0_1	16	0	1
0_2	16	0	1
0_3	66	a	1
0_4	99	1+a	-1

Now let u be an involution of C(S) and s be an element of order 5 in S . We know that $\theta_1(us) = \theta_1(s) = 1$. Consequently, $\theta_1(u) \equiv 1 \pmod 5$. As $G=G'$, $\theta_1(u) \equiv 0 \pmod 4$ Thus $\theta_1(u) \equiv 16 \pmod{20}$. As G is simple we conclude that $\theta_1(u) = -4$.

We note ,in particular,that u and t are not conjugate in G,so that G has at least 2 conjugacy classes of involutions .Let R be a Sylow 2-subgroup of G. We claim that $|R| = 64$ .We already know that $|R| \geq 32$.

As the principal 11 - block of G contains characters of degree 16 , we see that $|N(P)| = 55$ for a Sylow 11-subgroup P of G. Let $|R| = 2^a$ .Then $[G:N(P)] = 2^a.3^b$ so that a is even by Sylow's theorem,as 2 is not a quadratic residue (mod 11),but 3 is a quadratic residue (mod 11).

We next claim that $1,\theta_3$ and θ_4 lie in the principal 2-block of G,but that θ_1 and θ_2 do not.First,let t be as above. $[G: C(t)]\theta_1(t)/\theta_1(1) \not\equiv [G:C(t)] \pmod 2$ as $[G:C(t)]$ is odd.Thus θ_1 does not lie in the principal 2-block of G and a similar

argument applies to θ_2.

As t is not conjugate to any involution of C(S), Lemma 1.2.14 tells us that there is a non-trivial character of odd degree which lies in both the principal 2-block and the principal 5-block. This character must be θ_4. Suppose then that θ_4 does not lie in the principal 2-block of G. Then Lemma 1.2.14 tells us that :

$$1 + \theta_4(s)\,\theta_4(t) = 0 \quad (s \text{ is as above})$$

Thus $\theta_4(t) = 1$, whereas $\theta_4(1) \equiv 3 \pmod 4$ so that t lies outside G', a contradiction.

Now θ_1 and θ_2 are 11-conjugate characters so that they agree on 2-singular element As they do not vanish on all 2-singular elemnets, they lie in the same 2-block.

Let z be an element of R which is not conjugate to any element of C(S). Then Lemma 1.2.14 tells us that :

$$\theta_1(s)\,\theta_1(1) + \theta_2(s)\,\theta_2(z) = 0.$$

Consequently, $\theta_1(z) = \theta_2(z) = 0$.

Thus θ_1 assumes the following values on R

i) $\theta_1(1) = 16$

ii) $\theta_1(y) = -4$ if y is an involution of R conjugate to some involution of C(S).

iii) $\theta_1(z) = 0$ if z is any other element of R.

Suppose that case ii) occurs k times. Then

$$0 \leq |R|\,(\theta_1, 1_R) = 16 - 4k .$$

As $|C(S)|$ is even, $k \neq 0$, so that $k = 4$.

Also, we have :

$$|R|\,(\theta_1, \theta_1) = 256 + 64 \text{ , so that}$$

$|R| = 64$.

Now let $|G| = 2^6 . 3^b . 5 . 11$. By Sylow's theorem , $2^6 . 3^b \equiv 1 \pmod{11}$, so that we have: $b = 3 \pmod 5$.

If $b = 3$, then $|G| = 2^6 . 3^3 . 5 . 11$ and $|N(S)| = 40$, by Sylow's theorem . Thus G contains no element of order 15.

Now θ_4 lies in a 3-block of defect 1 and no other character of the principal 5-block lies in a 3-block of defect 1 . By Lemma 1.2.14, we see that $\theta_4(s)\,\theta_4(x) = 0$ for any non-trivial 3-element x of G . As $\theta_4(s) \neq 0$, θ_4 lies in a 3-block of defect 0 of G , a contradiction.

As $b \leq 11$, we conclude that $b = 8$, so that $|G| = 2^6 . 3^8 . 5 . 11$, contrary to the remarks at the end of chapter two.

Lemma 4.4.5

The character degrees 1,66,99,1024,1056 cannot occur.

Proof

Suppose that the degrees above do occur. Let t be a central involution of a Sylow 2-subgroup of G. Let θ_1 be the character of degree 1024 and let θ_2 be the character of degree 1056.

As [G: C(t)] is odd, 1024 divides $\theta_1(t)$. As G is simple, $\theta_1(t) = 0$. We next claim that t inverts an element of order 5. If it does not, then t can invert no 5-singular element.

The character table of G has a fragment of the form:

	1	s	t
1	1	1	1
θ_1	1024	-1	0
θ_2	1056	1	a
θ_3	66	1	b
θ_4	99	-1	1+a+b

As t inverts no 5-singular element, we have:

$$1 + \frac{a^2}{1056} + \frac{b^2}{66} - \frac{(1+a+b)^2}{99} = 0.$$

We find , after multiplying through by 99 that 3 divides $(1 + a + b)^2$, so that 9 divides $(1 + a + b)^2$ .Let $(1 + a + b)^2 = 9u$

Then : $1 + \frac{a^2}{1056} + \frac{b^2}{66} = \frac{u}{11}$.

Multiplication by 1056 yields : $1056 + a^2 + 16b^2 = 96$.Consequently,3 must divide $a^2 + b^2$. The only way that this can happen is that 3 divides a and 3 divides b whereas 3 divides 1+a+b.

Thus t inverts an element of order 5, s say.Now :

$10\,(\emptyset_3, 1)_{<t>S} = 66 + 4 + 5\,\emptyset_3(t)$, so that $\emptyset_1(t) \geq -14$. A similar argument shows that $\emptyset_3(t) \leq 14$.By similar reasoning, we deduce that $-19 \leq \emptyset_4(t) \leq 19$.

Now 32 divides $\emptyset_2(t)$,as [G:C(t)] is odd and 32 divides $\emptyset_2(1)$. However, we know that $\emptyset_2(t) = \emptyset_2(t)^2 - (1 + \emptyset_4(t))$.We also know that $|\emptyset_3(t)| \leq 14$ and $|\emptyset_4(t)| \leq 19$ In fact,as G = G', $\emptyset_4(t) \equiv 3 \pmod 4$.

There are three possibilities :

i) $\theta_2(t) = 0$, $\theta_4(t) = 1 + \theta_3(t)$.

ii) $\theta_2(t) = 32$, $\theta_4(t) = 19$, $\theta_3(t) = -14$.

iii) $\theta_2(t) = -32$, $\theta_4(t) = -17$, $\theta_3(t) = 14$.

By Lemma 4.2.4,

$$\frac{6\,|G|}{|C(t)|^2}\left(1 + \frac{a^2}{1056} + \frac{b^2}{66} - \frac{(1+a+b)^2}{99}\right)$$

is an integer, z say . Let $u = \dfrac{z\,|C(t)|^2}{6\,|G|}$

As $[G:C(t)]$ is odd and 2^{11} divides $|G|$, it is not difficult to see that $u = 2^{10} r / s$ where r and s are integers and s is odd.

Now 32 divides a , and $b \equiv 2 \pmod 4$ Let $b = 4c + 2$ .Then, in the 2-adic integers we have:

$$1 + 2\,\frac{(2c+1)^2}{33} - \frac{(4c+3)^2}{99} \equiv 0 \pmod{32}$$

or : $1 + 8c^2 + 8c + 2 \equiv 3 + 8c + 16c^2 \pmod{32}$

Thus $8c^2 \equiv 0 \pmod{32}$ and c is even . In other words, $b \equiv 2 \pmod 8$.

As $b \equiv 2 \pmod 8$, case iii) above does not occur. Let $b = 8d + 2$. Suppose that case ii) above occurs, so that a=32 and b= -14 .Then on substitution of these values , we have:

$$u = 1 + \frac{32}{33} + \frac{98}{33} - \frac{361}{99} = \frac{128}{99}$$, contrary

to the fact that $u \equiv 0 \pmod{1024}$. Thus case i) must occur, and $a = 0$. Now we have:

$$u = 1 + \frac{2(4d+1)^2}{33} - \frac{(8d+3)^2}{99}$$

Thus $99u = 99 + 6 + 48d + 96d^2 - (64d^2 + 48d + 9)$

so $99u = 96 + 32d^2 \equiv 0 \pmod{2^{10}}$.

Thus $3 + d^2 \equiv 0 \pmod{32}$, a contradiction as $d^2 \equiv 1 \pmod 8$ if d is odd. The proof of this Lemma is complete.

We assume for the rest of this section that 2^{11} divides $|G|$.

Lemma 4.4.6

The possible orders of G are :

i) $2^{11}.3^5.5.11$

ii) $2^{12}.3^6.5.11$

iii) $2^{13}.3^6.5.11$

iv) $2^{13}.3^{11}.5.11$

v) $2^{14}.3^7.5.11$

vi) $2^{17}.3^3.5.11$.

Proof

We know that 2^{13} does not divide $|G|$. Let P be a Sylow 11-subgroup of G.

Case i) : $|N(P)| = 55$, $|N(S)| = 60$

In this case , $|G| = 2^a.3^b.5.11$, where

$2 \leq b \leq 11$, $11 \leq a \leq 17$ and where

i) $2^a.3^b \equiv 1 \pmod{11}$, so $a \equiv 2b \pmod{10}$.

ii) $2^{a-3}.3^b \equiv 1 \pmod{5}$, so $a \equiv b+3 \pmod{5}$

Hence a is even and b is odd

a) $a \neq 16$, for otherwise , $b \equiv 13 \pmod{20}$.

b) Suppose that $a = 14$. Then $b \equiv 7 \pmod{20}$, so that $|G| = 2^{14}.3^7.5.11$.

c) Suppose that $a = 12$. Then $b \equiv 1 \pmod{20}$, a contradiction as $2 \leq b \leq 11$.

Case ii) : $|N(P)| = 55$, $|N(S)| = 120$.

This time, $|G| = 2^a.3^b.5.11$, where $11 \leq a \leq 17$

$3 \leq b \leq 11$ and :

i) $2^a.3^b \equiv 1 \pmod{11}$, so $a \equiv 2b \pmod{10}$

ii) $2^{a-3}.3^{b-1} \equiv 1 \pmod{5}$, so $a \equiv b+2 \pmod{4}$

Thus a and b are both even.

a) If $a = 12$, then $b \equiv 6 \pmod{20}$, so that $b=6$ and $|G| = 2^{12}.3^6.5.11$.

b) $a \neq 14$, for otherwise $b \equiv 12 \pmod{20}$.

c) $a \neq 16$, for otherwise $b \equiv 18 \pmod{20}$.

Case iii) : $|N(P)| = 110$, $|N(S)| = 40$

In this case , $|G| = 2^a.3^b.5.11$, where

$11 \leq a \leq 17$, $3 \leq b \leq 11$ and :

i) $2^{a-1}.3^b \equiv 1 \pmod{11}$, so $a \equiv 2b+1 \pmod{10}$

ii) $2^{a-3}.3^b \equiv 1 \pmod{5}$, so $a \equiv b+3 \pmod{4}$

Thus a is odd and b is even.

a) If $a = 11$, then $b \equiv 0 \pmod{20}$, contrary the fact that 3^{20} does not divide $|G|$.

b) If $a = 13$, then $b \equiv 6 \pmod{20}$, so $b = 6$ and $|G| = 2^{13} \cdot 3^{6} \cdot 5 \cdot 11$

c) If $a = 15$, then $b \equiv 12 \pmod{20}$, contrary to the fact that $b \leq 11$.

d) If $a = 17$, then $b \equiv 18 \pmod{20}$, contrary to the fact that $b \leq 11$.

Case iv) : $|N(P)| = 110$, $|N(S)| = 120$

In this case , $|G| = 2^{a} \cdot 3^{b} \cdot 5 \cdot 11$, where $11 \leq a \leq 17$, $3 \leq b \leq 11$ and :

i) $2^{a-1} \cdot 3^{b} \equiv 1 \pmod{11}$, so $a \equiv 2b+1 \pmod{10}$

ii) $2^{a-3} \cdot 3^{b-1} \equiv 1 \pmod{5}$, so $a \equiv b+2 \pmod{4}$

Thus a and b are both odd.

a) If $a = 11$, then $b \equiv 5 \pmod{20}$, so $b = 5$ and $|G| = 2^{11} \cdot 3^{5} \cdot 5 \cdot 11$

b) If $a = 13$, then $b \equiv 11 \pmod{20}$, so $b = 11$ and $|G| = 2^{13} \cdot 3^{11} \cdot 5 \cdot 11$

c) If $a = 15$, then $b \equiv 17 \pmod{20}$, contrary to the fact that $b \leq 11$.

d) If $a = 17$, then $b \equiv 3 \pmod{20}$, so $b = 3$ and $|G| = 2^{17} \cdot 3^{3} \cdot 5 \cdot 11$.

Lemma 4.4.7

$|G| \neq 2^{17} \cdot 3^{3} \cdot 5 \cdot 11$

Proof

Suppose that $|G| = 2^{17} \cdot 3^{3} \cdot 5 \cdot 11$. Then C(S)

has order 30 (from the previous Lemma) . Let x be an element of order 3 in C(S) and let C = C(x). Now S centralizes $O_3(C)$, and so $\langle x \rangle = O_3(C)$ by Lemma 2.4.1 .

Also S acts fixed-point freely on on $O_{5'}(C)/\langle x \rangle$, so that $O_{5'}(C)$ is nilpotent and $O_{5'}(C) = \langle x \rangle \times O_2(C)$.

Now x has both primitive cube roots of unity as eigenvalues of multiplicity 5 , so that as C acts on each eigenspace of x , x lies outside C' . Let L be a component of C (if one exists) . As L = L' and the Sylow 5-subgroups of L are Abelian, $Z(L) \leq O_2(C)$.

Now 5 divides |L|, so that $S \leq L$ Thus S centralizes $O_2(L) \times \langle x \rangle$ and $O_2(C) = 1$ by Lemma 4.2.1 . Hence L is simple . As 81 does not divide |G| , L is isomorphic to A_5 or A_6 . Suppose that L is isomorphic to A_5 . Then as $C = LN_C(S)$, 27 does not divide |C| so that G has non-Abelian Sylow 3-subgroups

Let R be a Sylow 3-subgroup of G which contains x . Then $\theta(x) = 0$ for each non-linear irreducible character θ of R. Since x has the eigenvalue 1 with multiplicity 1, we conclude that $X|_R$ contains precisely one non-linear irreducible constituent , with multiplicity 1, say θ_1 .

Let u be an element of order 3 in Z(R). Then $X(u) = 8 + 3w$ for some primitive cube root of unity , w. In particular , u is not conjugate to its inverse in G. As $\theta_1(y) = 0$ for any y in R-Z(R),u is not conjugate in G to any element of R-Z(R) . Thus u is not conjugate in G to any other element of R.

As G is simple and u acts with quadratic minimum polynomial in any reduction (mod 5) of G,we have a contradiction to Lemma 2.6.2, Thus L is isomorphic to A_6 . We note that $\langle x \rangle$ is a maximal Sylow intersection of C(x) Let R be a Sylow 3-subgroup of C(x) and let $W = \langle x \rangle$.

We claim that W is weakly closed in R with respect to G. Now X(x) = -4,so that it is sufficient to prove that $X(y) \neq -4$ if y lies in R-W.As S acts non-trivially on both of the 5-dimensional eigenspaces of x and L has no irreducible character of degree less than 5 , we deduce that $X|_L = 1 + \theta_1 + \theta_2$, where θ_1 and θ_2 both have degree 5.

Let y be any element of order 3 in L.Then y is conjugate to its inverse within L .Thus $\theta_1(y) = 2$ or -1 and $\theta_2(y) = 2$ or -1 Certainly , $\theta_1(y) \neq -4$. Also we have:

$X(xy) = 1 + w\theta_1(y) + w^2\theta_2(y)$, where w is a primitive cube root of unity , so we see

quickly that $X(xy) \neq -4$. Also, $X(x^2y) \neq -4$. As $R = \langle x \rangle \times (R \cap L)$, we conclude that x is not conjugate in G to any element of R-W. Thus W is weakly closed in R with respect to G .

Now $N(R) \leq N(W)$ by the weak closure of W in R . By Sylow's theorem, we have: $[G:N(R)] \equiv [N(W):N(R)] \equiv 1 \pmod 3$, and so $[G:N(W)] \equiv 1 \pmod 3$. Now $[G:N(W)]$ has the form 11.2^k for some integer k, so that k is odd . Also, $N(S) \leq N(W)$, as $W = O_3(N(S))$, so that $[G:N(W)] \equiv 1 \pmod 5$ by the argument above. However , since k is odd , 11.2^k is not congruent to 1 (mod 5), a contradiction

Suppose then that C has no component. As 27 divides $|G|$, 9 divides $|C|$, so that S is not normal in C , as N(S) has order 120 Since $E(C) = 1$, $F^*(C) = F(C)$, so that $O_2(C) \neq 1$ Let $K = O_2(C)$. As C(S) contains no element of order 6 , S acts Frobeniusly on K. Since SK acts on each eigenspace of x , $X|_{SK}$ has no irreducible constituent of degree larger than 5, so that K is Abelian.

Now K must act non-trivially on one of the 5-dimensional eigenspaces of x , and SK acts irreducibly on this space . Thus $X|_C$ has an irreducible constituent of degree 5,

say θ . Now $\ker\theta \leq O_2(C)$. Let $H = C/\ker\theta$. Then θ is a faithful irreducible character of H of degree 5 and is imprimitive since $\theta|_{O_2(H)}$ contains 5 distinct constituents.

Thus H has an Abelian normal subgroup ,M say, such that H/M is isomorphic to a subgroup of S_5 . If 5 divides $|M|$, then H is soluble, and so is C, so $C = O_{5'}(C)N_C(S)$, and 9 does not divide $|C|$, a contradiction as 9 divides $|G|$. If 5 does not divide $|M|$, then T, the inverse image of M in C , is contained in $O_{5'}(C)$. As 9 does not divide [H:M] , and [H:M] = [C:T], we conclude that 27 does not divide $|C|$. Thus the Sylow 3-subgroups of G are non-Abelian, and we may use an argument from an earlier part of this Lemma to derive a contradiction . The proof of this Lemma is complete.

Lemma 4.4.8

The character degrees for the principal 5-block of G are not:

1,66,176,7776,8019

Proof

As 3^6 divides 8019, $|G|$ must be one of :

i) $2^{12}.3^6.5.11$

ii) $2^{13}.3^{6}.5.11$

iii) $2^{14}.3^{7}.5.11$

Case i) : $|G| = 2^{12}.3^{6}.5.11$

In this case , $|C(S)| = 30$. Let θ be the character of degree 8019 in the principal 5-block of G . Then θ lies in a 3-block of defect 0, so must vanish on each 3-singular element of G. However, there is an element x of order 3 in C(S) and an element s of order 5 in S , such that : $\theta(sx) = \theta(s) = -1$. This contradiction shows that $|G| \neq 2^{12}.3^{6}.5.11$

Case ii) : $|G| = 2^{13}.3^{6}.5.11$

In this case , $|C(S)| = 10$. Let θ be the character of degree $7776 = 32.243$. Then θ is in a 3-block of defect 1 of G, so is the only character of its 3-block which also lies in the principal 5-block .

Lemma 1.2.14 now tells us that : $\theta(1)\,\theta(s) \equiv 0 \pmod{3^{6}}$ where s is an element of order 5 in S . This is a contradiction as $\theta(s) = -1$.

Case iii) : $|G| = 2^{14}.3^{7}.5.11$

In this case , $|C(S)| = 10$, so that once more

G contains no element of order 15 .The above argument, this time used with the character of degree 8019 (= 11.3^6), yields a contradiction

Hence these degrees cannot occur and the proof of this Lemma is complete.

Lemma 4.4.9

If 2^{12} divides $|G|$, then the character degrees for the principal 5-block are not

1, 66, 66, 891, 1024

Proof

Suppose that the above degrees do occur in the principal 5 -block . Let θ be the character of degree 1024 in the principal 5-block and let t be an involution which is central in some Sylow 2-subgroup of G. Then $[G:C(t)]$ and $\theta(1)$ are coprime so that $\theta(t) = 0$ .We claim that t inverts an element of order 5 . Suppose that this is not the case.

The character table of G has a fragment of the form :

1	t	s
1	1	1
66	a	1
66	b	1
891	-(1+a+b)	1
1024	0	-1

As t inverts no element of order 5, t inverts no 5-singular element, so:

$$1 + \frac{a^2}{66} + \frac{b^2}{66} + \frac{(1+a+b)^2}{891} = 0 ,$$

a contradiction.

Thus t inverts some element of order 5, so that we may suppose that t lies in N(S). By considering the restriction of one of the irreducible characters above of degree 66 to the group $\langle t \rangle S$, we see that $-14 \leq a \leq 14$, $-14 \leq b \leq 14$.

By Lemma 4.2.4,

$$\frac{6|G|}{|C(t)|^2}\left(1 + \frac{a^2}{66} + \frac{b^2}{66} + \frac{(1+a+b)^2}{891}\right)$$

is an integer, m say. Let $r = \frac{m|C(t)|^2}{6|G|}$.

Then since $[G:C(t)]$ is odd, and 2^{12} divides G, we see that (in the 2-adic integers), $r \equiv 0 \pmod{2^{11}}$.

Since $G = G'$, both a and b are congruent to 2 (mod 4). Let $a = 2u$, and Let $b = 2v$. Then we note that :

$$r = 1 + \frac{2u^2}{33} + \frac{2v^2}{33} + \frac{(1 + 2u + 2v)^2}{891}$$

so that we have:

$$891r = 891 + 54(u^2 + v^2) + (1+2u+2v)^2$$

As $r \equiv 0 \pmod{2^{11}}$, we have :

$$27 + 22(u^2 + v^2) + (1+2u+2v)^2 \equiv 0 \pmod{32}$$

Since u and v are odd, both u^2 and v^2 are congruent to 1 (mod 8). Thus

$11 + 12 + (1+2u+2v)^2 \equiv 0 \pmod{16}$ and

$(1 + 2u + 2v)^2 \equiv 9 \pmod{16}$.

Consequently, $u + v \equiv 2 \pmod 4$, so that $u \equiv v \pmod 4$.

Now $u^2 + v^2 \equiv 2 \pmod 8$, so that $22(u^2 + v^2) \equiv 12$ or $28 \pmod{32}$. In the first case, we see that :

$(1+ 2u + 2v)^2 \equiv 25 \pmod{32}$, so that

$1 + 2u + 2v \equiv 5$ or $-5 \pmod{16}$.

Since $u+v \equiv 2 \pmod 4$, we conclude that $1 + 2u + 2v \equiv 5 \pmod{16}$, so that $u+v \equiv 2 \pmod 8$. In the second case, we have: $(1 + 2u + 2v)^2 \equiv 9 \pmod{32}$.

Since $u + v \equiv 2 \pmod 4$, we see that $1 + 2u + 2v \equiv -3 \pmod{16}$, so that

$u + v \equiv 2 \pmod 8$ in this case also.

Since $-14 \leq u+v \leq 14$, there are only four cases to consider:

Case i) : $u + v = -14$

In this case, $u = v = -7$. Thus we have:

$891r = 891 + 54.98 + 729$, so that

$27r = 33 + 196 + 27 = 256$, contrary to the fact that $r \equiv 0 \pmod{2048}$.

Case ii) : $u + v = -6$

In this case, we have:

$$891r = 891 + 54\,u^2 + 54(6+u)^2 + 121$$

Since $r \equiv 0 \pmod{2^{11}}$, we conclude that

$$54\,(u^2 + (6+u)^2) \equiv -12 \pmod{1024},$$

so $9\,(u^2 + (6+u)^2) \equiv -2 \pmod{512}$.

Now $9.398 = 7.512 - 2$, so that

$u^2 + (6+u)^2 \equiv 398 \pmod{512}$, contrary to the fact that $-7 \leq u \leq 7$.

Case iii) : $u + v = 2$

In this case, we have:

$$891r = 891 + 54\,(u^2 + (u-2)^2) + 25,$$

so that, as $r \equiv 0 \pmod{2^{11}}$, we have:

$$54\,(u^2 + (u-2)^2) \equiv 108 \pmod{1024}.$$

Thus $u^2 + (u-2)^2 \equiv 2 \pmod{512}$. Since $-7 \leq u \leq 7$, we see that $u = 1$. Hence,

$891r = 1024$, a contradiction ,as $r \equiv 0 \pmod{2^{11}}$.

Case iv) : $u + v = 10$

In this case,we have :

$$891r = 891 + 54\,(u^2 + (u-10)^2) + 441$$

Hence we have :

$$54\,(u^2 + (u-10)^2) \equiv 716 \pmod{1024}$$

and: $27\,(u^2 + (u-10)^2) \equiv 358 \pmod{512}$

Thus $u^2 + (u-10)^2 \equiv 146 \pmod{512}$ (for $27.146 = 358 + 7.512$) . Since $-7 \leq u \leq 7$ and $-7 \leq u-10 \leq 7$, we see that $u^2 + (u-10)^2 = 146$ .However, 146 can only be represented in one way as a sum of two squares, that is :

$$146 = 11^2 + 5^2,$$

so that the equation

$u^2 + (u-10)^2 = 146$ has no solution in integers ,a contradiction.

This final contradiction completes the proof of this Lemma.

Corollary 4.4.10

$|G| \neq 2^{13}.3^{6}.5.11$

Proof

Suppose that $|G| = 2^{13}.3^{6}.5.11$.

The degrees in the principal 5-block are

1,66,99,144,176.

Also, $|N(P)| = 110$ for a Sylow 11-subgroup P of G and $|N(S)| = 40$.

We may suppose that $S \leq N(P)$. Let t be an involution of $N(P) \cap C(S)$. We calculate the sum of class algebra constants :

$$n = \#(tt = s) + \#(tt = st)$$

For any irreducible character ,0, of G which does not lie in the principal 5-block of G, $0(s) + 0(st) = 0$ by Brauer's second main theorem. Thus only characters from the principal 5-block can make any non-zero contribution to the character-theoretic expression for the above sum.

The character table of G has a fragment of the form:

	1	t	s	st
1	1	1	1	1
0_1	66	a	1	1
0_2	99	b	-1	-1
0_3	144	c	-1	-1
0_4	176	d	1	1

where $1 + a + d = b + c$

We claim that $a = 6$, $b = -1$ and $c = 4$ Now $a \equiv 2 \pmod 4$, as $G = G'$. Also, $a \equiv 1 \pmod 5$, as $\theta_1(st) = 1$. Thus $a \equiv 6 \pmod{20}$ However,

$$(\theta \Big|_{\langle t \rangle P}, 1)_{\langle t \rangle P} = 66 + 11a \geq 0$$

so that $a \geq -6$. Similarly, $a \leq 6$. Thus $a = 6$.

Now $b \equiv 3 \pmod 4$ and $b \equiv -1 \pmod 5$, so that $b \equiv -1 \pmod{20}$. An argument similar to that above shows that $-9 \leq b \leq 9$, so that $b = -1$.

Similarly, $c \equiv 4 \pmod{20}$ and $|c| \leq 14$, so that $c = 4$. We conclude that $d = -4$.

Now we may substitute these values in the character-theoretic expression for the above sum to conclude that:

$$n = \frac{2|G|}{|C(t)|^2}\left(1 + \frac{36}{66} - \frac{1}{99} - \frac{16}{144} + \frac{16}{176}\right)$$

so that $n = \dfrac{100|G|}{33|C(t)|^2}$.

In particular as 2^{13} divides $|G|$ but 2^{14} does not, 2 divides n to an odd power

Now if t_1, t_2 are two conjugates of t whose product is s or st, then t_1 and t_2 both lie in $N(S)$. We may thus evaluate n inside $N(S)$.

As a conjugate of t inverts s ,we may write $N(S) = \langle t \rangle \times B$,where B is a Frobenius group of order 20.Let u be an involution of B . Then u and tu are not conjugate to each other in N(S) (though they might be conjugate in G) , and any involution of N(S) which inverts s must be conjugate in S to u or tu.Hence t is conjugate in G to u or to tu.

Case i):u and tu are not conjugate in G

Suppose that t is conjugate in G to u. Then as u and tu are not conjugate in G , $\#(t^{\cdot} t = st) = 0$ .Also,we see that $\#(t^{\cdot} t = s) = 5$, as each conjugate of t which lies in N(S) must lie in B above, and there are 5 such conjugates . Thus $n = 5$ in this case.

A similar argument shows that $n = 5$ if t is conjugate in G to tu .

Case ii) : u and tu are conjugate in G

This time , N(S) contains 10 conjugates of u , 5 which are conjugate in N(S) to u ,and 5 which are conjugate in N(S) to tu.

Thus $\#(t\dot{t} = s) = 10$, for the first conjugate of t may be any of the above 10 conjugates of u, and then the second is uniquely determined. Similarly, we see that $\#(t\dot{t} = st) = 10$. Thus $n = 20$ in this case.

In either case, 2 divides n to an even power, contrary to our earlier finding. Thus $|G| \neq 2^{13}.3^{6}.5.11$.

Lemma 4.4.11

$|G| \neq 2^{11}.3^{5}.5.11$

Proof

Suppose that $|G| = 2^{11}.3^{5}.5.11$. Thus $|C(S)| = 30$. Let x be an element of order 3 in $C(S)$. Let $C = C(x)$.

We first prove that $\langle x \rangle = O_3(C)$. Suppose that this is not the case. Then as S acts non-trivially on $O_3(C)$, we must conclude that $O_3(C)$ is elementary Abelian of order 243. Thus C is soluble. In fact, as $C(y)$ is a $\{2,3\}$-group for any 3-element, y, of G which is not conjugate to $1, x$ or x^{-1}, we may conclude that $C(u)$ is soluble for any element u of order 3 in G.

Let R be a Sylow 3-subgroup of G. If $O_{3'}(C(u)) = 1$ for each element u of order 3 in G, then $[G:N(R)] \equiv 1 \pmod 5$ a contradiction, as $[G:N(R)]$ divides $2^{11}.11$ (for 5 divides $|C(u)|$ and R is normal in C(u) in this case). However, if $O_{3'}(C(u)) \neq 1$ for some u in R, then $\langle O_{3'}(C(u)) : u \in R \rangle$ is a soluble 3'-group by the results of [13]. Let us call this group T, and let M = N(T). By well-known arguments (see for example [12]), we may deduce that $C(u) \leq M$, for every element u of order 3 in M. Certainly, $N(R) \leq M$, so that $R \cap R^g$ is a 3'-group for any g in G-M. Thus $[G:M] \equiv 1 \pmod 5$ a contradiction, once more, since $[G:M]$ divides $2^{11}.11$ (for $S \leq C(x) \leq M$). Thus $\langle x \rangle = O_3(C)$.

We now prove that $O_2(C) = 1$. Suppose that $O_2(C) \neq 1$. Then as in the proof of Lemma 4.4.7, we conclude that 27 does not divide $|C|$. Let R be a Sylow 3-subgroup of G which contains x. Then $|C_R(x)| = 9$. As R has at least 9 linear characters, we conclude that $\theta(x) = 0$ for any non-linear irreducible character θ of R.

Since x has the eigenvalue 1 with multiplicity 1 , $X|_R$ has precisely one non-linear irreducible constituent, with multiplicity 1 .We claim that [R,x] is cyclic of order at most 9.Since $X|_R$ has 8 linear constituents, each non-identity element of [R,x] has the eigenvalue 1 with multiplicity 8 or more.If [R,x] is not cyclic , it contains an elementary Abelian subgroup A of order 9.Since $X|_A$ contains the principal character with multiplicity 8 or more , A contains an element of order 3 with a fixed-point space of dimension 9, contrary to Lemma 2.1.6 . Thus [R,x] is cyclic.

Each non-identity element of [R,x] has at most 4 distinct eigenvalues , so acts with minimum polynomial of degree at most 4 in any reduction (mod 3) of G As $O_3(G) = 1$, [R,x] has order 9 or less Then $|R| \leq |C_R(x)|\,|[R,x]| \leq 81$, contrary to the fact that $|R| = 243$. Thus $O_2(C) = 1$

Now S acts fixed-point freely on $O_{5'}(C)/\langle x\rangle$. Hence $O_{5'}(C)$ is nilpotent , so that $O_{5'}(C) = \langle x\rangle$. As 9 divides $|C|$, but 9 does not divide $|N(S)|$, $O_{5'}(C) = 1$. Thus C has a unique component $O_5(C)$, L say , and Z(L) = 1 (as x lies outside C') .

We claim that L is isomorphic to PSU(4,2) . L is certainly isomorphic to one of: A_5 , A_6 or PSU(4,2).Suppose that L is isomorphic to A_5 . Then as $C=LN_C(S)$ 27 does not divide $|C|$,so we may derive a contradiction in a similar fashion to that used when we assumed that $O_2(C) \neq 1$ earlier in this Lemma.

Suppose then that L is isomorphic to A_6 .Then let R be a Sylow 3-subgroup of C.An argument similar to one used in Lemma 4.3.2 allows us to conclude that x is not conjugate in G to any element of R-<x>. Let T be a Sylow 3-subgroup of N(R).Then $T \leq C(x)$ as <x> is weakly closed in R with respect to G.Thus R is a Sylow 3-subgroup of G.

However,since $C = LN_C(S)$ 81 does not divide |C|,a contradiction, since 243 divides |G|.Consequently,L is isomorphic to PSU(4,2). Let M = N(<x>). Then $N(S) \leq M$,so that $[G:M] \equiv 1 \pmod 5$ L has order $2^6 .3^4 .5$,and M = LN(S).As $|N_L(S)| = 20$, and $|N(S)| = 120$, we see that M has order $2^7 .3^5 .5$. Consequently, [G:M] = 176 . Let θ be the permutation character obtained from the permutation

action of G on the right cosets of M in G and let t be an involution of N(P) (where P is a Sylow 11-subgroup of G. That N(P) has order 110 in this case is clear from the proof of Lemma 4.4.6)

We prove that $\theta(t) = 16$. Clearly, $\theta(t) \geq 0$. As $G = G'$, $\theta(t) \equiv 0 \pmod 4$. We may suppose that $S \leq N(P)$ and that t lies in C(S). As $N(S) \leq M$, S fixes no right coset of M in G except M itself. Hence $\theta(s) = \theta(st) = 1$ for any element s of order 5 in S. Thus $\theta(t) \equiv 1 \pmod 5$ As M contains no conjugate of P, we see that θ vanishes on elements of order 11

Now $(\theta|_{P\langle t\rangle}, 1_{P\langle t\rangle}) = 176+11\,\theta(t)$,

so that $\theta(t) \geq -16$. A similar argument, with the other linear character of $P\langle t\rangle$ allows us to conclude that $\theta(t) \leq 16$. As $\theta(t) \equiv 16 \pmod{20}$ and $\theta(t) \geq 0$, we see that $\theta(t) = 16$.

Now θ contains the trivial character with multiplicity 1 and θ vanishes on all 11-singular elements of G. Thus we may write $\theta = \theta_1 + \theta_2$, where θ_1 and θ_2 are ordinary characters of G such that:

i) $\theta_1(1) \equiv -1 \pmod{11}$.

ii) θ_1 is irreducible

The possible values for $\theta_1(1)$ are :

10, 32, 54, 120.

(for $\theta_1(1)$ divides $|G|$ in any case).

a) If $\theta_1(1) = 10$, then $\theta_1(t) = 0$ since t lies in $N(P)$. This contradicts the fact that $G = G'$.

b) If $\theta_1(1) = 54$, then $\theta_1(t) \equiv 2 \pmod 4$ as $G = G'$. Also θ_1 assumes the value -1 on each non-identity element of P , so that $-4 \leq \theta_1(t) \leq 4$ as t inverts each such element. Thus $\theta_1(t) = 2$ or -2.

Now $\theta_2(t) = 16 - \theta_1(t)$, as $\theta(t) = 16$. Also, θ_2 assumes the value 1 on each non identity element of P, so $-12 \leq \theta_2(t) \leq 12$ (as θ_2 is an ordinary character of G and $P\langle t\rangle$ is a dihedral group), contrary to the fact that $\theta_2(t) = 16 - \theta_1(t)$.

c) If $\theta_1(1) = 120$, then $\theta_1(t) \equiv 0 \pmod 4$ Also, θ_1 vanishes on 5-singular elements of G , so that for an element s of order 5 in S we have: $\theta_1(s) = \theta_1(st) = 0$. Thus $\theta_1(t) \equiv 0 \pmod 5$.

Now θ_1 assumes the value -1 on each non-identity element of P, so that as θ_1 is an ordinary character of G and $P\langle t\rangle$

is dihedral , $-10 \leq \theta_1(t) \leq 10$. Since $\theta_1(t) \equiv 0 \pmod{20}$, we see that $\theta_1(t)=0$. Consequently , $\theta_1(t) = 16$, whereas we know that θ_2 is an ordinary character of degree 56 which assumes the value 1 on non-identity elements of P , and we also know that $P\langle t\rangle$ is dihedral.

This is a contradiction ,and the proof of this Lemma is complete.

Lemma 4.4.12

$|G| \neq 2^{13}.3^{11}.5.11$

Proof

Suppose that $|G| = 2^{13}.3^{11}.5.11$. Then $|C(S)| = 30$. Let x be an element of order 3 in C(S) . Let $C = C(x)$ and let $K = O_{5'}(C)$. We prove first that 3^7 does not divide $|C|$.

S acts fixed-point freely on $K/\langle x\rangle$ so that K is nilpotent . We know that $X(x)= -4$ and that x has the eigenvalue 1 with multiplicity one,each primitive cube root of unity as an eigenvalue of multiplicity 5.Suppose that $O_3(C) \neq \langle x\rangle$ and let $T = O_3(C)$.

By Lemma 2.4.1 ,S acts non-trivially on T , so that T is Abelian by Lemma

3.1.4. Let M = [S,T]. Now SM acts on each eigenspace of x.

If SM acts trivially on one of the 5-dimensional eigenspaces of x, then M contains an element of order 3 with a fixed-point subspace of co-dimension 2 contrary to Lemma 2.1.6 (for let θ be the irreducible character of degree 5 afforded by the action of SM on the 5-dimensional eigenspace of x. Then as M has rank 4 or more , and M = [M,S], M contains an element , y, of order 3 with $\theta(y) = 3 + w + \bar{w}$, where w is a primitive cube root of unity).

Thus SM acts non-trivially on each 5-dimensional eigenspace of x.Thus $X|_T$ has 11 distinct constituents, so that C(T) is an Abelian 3-group by Lemma 1.5.1 .As $C(T) \leq C(x)$,$T = C(T)$. Hence $T = F^*(C)$.

Now M has rank 4 or 8,as S acts fixed-point freely on M and X(1) = 11. If M had rank 8, then it would contain an element of order 3 with a fixed-point subspace of co-dimension 2,contrary to Lemma 2.1.6 .Thus M has rank 4.

Let θ be the character of C of

degree 5 afforded by the action of C on the w-eigenspace of x (where w is a primitive cube root of unity) . Since $\theta(s) = 0$, ker θ is a 5'-group . Also, $T \cap \ker \theta = 1$, so that θ is faithful.

θ is certainly irreducible, for SM is a Frobenius group , and SM $\leq$ C. Since T is normal in C and $\theta|_T$ contains five distinct constituents , θ is not primitive . As θ is faithful, C has an Abelian normal subgroup , A say , such that C/A is isomorphic to a subgroup of S_5 and such that $T \leq A$.

As $C(T) = T$, we conclude that A=T Thus 9 does not divide [C:T] .Since M has rank 4,S acts indecomposably on M, so that M is homocyclic.Also, T= M $\langle x \rangle$ If M is elementary Abelian, then T has order 3^5 ,so that 3^7 does not divide |C| Suppose then that M is homocyclic of exponent 9 (M cannot be homocyclic of exponent larger than 9 , since 3^{12} does not divide |G|).

Let $N = N(\langle x \rangle)$. Then $N(S) \leq N$, since $\langle x \rangle = O_3(N(S))$. Also, N acts on T.Now C(S) contains an involution, t say.Also t acts on [T,S] = M . Now S acts on $C_M(t)$,so that $C_M(t) = 1$.Thus S x $\langle t \rangle$

acts Frobeniusly on M.

Consequently, $X|_{SM} = 1 + \theta + \overline{\theta}$, for some irreducible character θ of SM (since $X1_M$ is real-valued). As M is homocyclic of exponent 9 and rank 4, and since $M = [M,S]$, M contains an element, y say, of order 9 such that $\theta(y) = 3 + w + \overline{w}$, for some primitive 9-th root of unity, w. Thus y has only 3 distinct eigenvalues, so that y acts with minimum polynomial of degree at most 3 in any reduction (mod 3) of G and y^3 lies in $O_3(G)$, contrary to the fact that $O_3(G) = 1$ and y has order 9.

Thus 3^7 does not divide $|C|$ when $O_3(C) \neq \langle x \rangle$. We may thus suppose that $O_3(C) = \langle x \rangle$. Suppose that $O_3(C) \neq 1$ and let $R = O_2(C)$. As $C(S)$ contains no element of order 6, SR is a Frobenius group. Since SR acts on each eigenspace of x, $X|_{SR}$ contains no irreducible constituent of degree 10 so that R is Abelian.

Similar arguments to those used for T above allow us to deduce that $X|_C$ contains an irreducible constituent of degree 5 which is faithful, but is

not primitive. Again , C possesses an Abelian normal subgroup,A, containing R , such that C/A is isomorphic to a subgroup of S_5 . Since $O_3(C) = \langle x \rangle$, 9 does not divide $|A|$, so that 27 does not divide $|C|$ in this case.

We may thus suppose that $O_{5'}(C) = \langle x \rangle$

If S is normal in C , then 9 does not divide $|C|$, since 9 does not divide $|N(S)|$ .We may suppose that $F(C) = \langle x \rangle$ so that $E(C) \neq 1$.As 25 does not divide $|C|$ and C is a $\{2,3,5\}$- group,C has a unique component,L say.

Now L/Z(L) is isomorphic to one of : A_5 , A_6 or PSU(4,2).As $Z(L) \leq F(C)$ $|Z(L)| \leq 3$. Thus 3^6 does not divide $|L|$ .As $C = LN_C(S)$, 3^7 does not divide $|C|$ (for $Z(L) \leq N(S)$) . In any case 3^7 does not divide $|C|$,as claimed.

Let Q be a Sylow 3-subgroup of G which contains x. We may suppose that Q consists of monomial matrices . As each irreducible constituent of $X|_Q$ has degree 1 or 3 and X(1) = 11 , the diagonal subgroup , D, of Q has index at most 27 in Q.Thus $|D| \geq 3^8$,so that x lies outside D.

Let θ be irreducible constituent of degree 3 of $X|_Q$ such that x is not represented by a diagonal matrix in the corresponding representation. Then $\theta(x) = 0$. As x has the eigenvalue 1 with multiplicity 1, there is at most one such constituent.

Thus $X|_{\langle x \rangle D}$ contains precisely 8 linear constituents. As 3 does not divide $|C(x)|$ and x lies outside D, 3 does not divide $|C_D(x)|$. We may conclude that $|[D,x]| \geq 27$.

However, $X|_{[D,x]}$ contains the trivial character with multiplicity 8 or more, so that [D,x] is cyclic, for if A were a subgroup of type (3,3) of D, then A would contain an element of order 3 with a fixed-point subspace of co-dimension 2, contrary to Lemma 2.1.6. Each element of [D,x] has at most 4 distinct eigenvalues, so acts with minimum polynomial of degree at most 4 in any reduction (mod 3) of G. As $O_3(G) = 1$ and [D,x] is cyclic, we conclude that $|[D,x]| \leq 9$, contrary to the fact that $|[D,x]| \geq 27$.

This final contradiction completes the proof of the Lemma.

Corollary 4.4.12

If 2^{11} divides $|G|$ then $|G|$ is either $2^{12}.3^{6}.5.11$ or $2^{14}.3^{7}.5.11$. In both cases $|N(P)| = 55$ where P is a Sylow 11-subgroup of G.

Proof

It is immediate from Lemma 4.4.6 and the above Lemma that the orders above are the only possible orders for G. Now in either case, $[G:N(P)] = 2^{a}.3^{b}$, where a is even, so that $|N(P)| = 55$ in both cases.

Section Five

We can now see that the principal 11-block of G contains 5 non-exceptional characters and 2 exceptional characters Also the character of degree 144 in the principal 5-block lies in the principal 11-block.

We may decompose the character $X\bar{X}$ to conclude that the principal 11-block contains an irreducible character, θ, of degree less than 121 such that either:

i) $\theta(1) \equiv -1 \pmod{11}$ or:

ii) $\theta(1) \equiv 5 \pmod{11}$.

In case ii) $\bar{\theta}$ also occurs as a constituent of $\bar{X}\bar{X}$ and $\bar{\theta} \neq \theta$.

The possibilities for $\theta(1)$ are : 10,60,120,16,27,32,54 .We have omitted the possibility $\theta(1) = 5$ as $C(S)$ has even order . We prove that there is no set of degrees for the principal 11-block consistent with this information.

Lemma 4.5.1

$\theta(1) \neq 10$.

Proof

Suppose that $\theta(1) = 10$.As $C(S)$ has As $C(S)$ has even order,we may choose an involution t of $C(S)$. Certainly 5 cannot divide $[G:C(t)]$.

As $[G:C(t)]\theta(t)/\theta(1)$ is an integer,we conclude that 5 divides $\theta(t)$. Certainly $\theta(t)$ is even,so that 10 divides $\theta(t)$. As G is simple and $\theta(1) = 10$, we are forced to conclude that $\theta(t) = 0$, contradicting the fact that $G = G'$.

We note that this argument shows that G possesses no irreducible character of degree 10.

Lemma 4.5.2

$\theta(1) \neq 16$

Proof

We know that θ cannot lie in the principal 5-block of G. Certainly θ lies in a 5-block of defect 1.

If $|G| = 2^{14}.3^{7}.5.11$, then $|C(S)| = 10$ and G has only two 5-blocks of defect 1. As X is not in the principal 5-block of G, X and θ lie in the same 5-block of G.

If $|C(S)| = 30$, then G possesses three 5-blocks of full defect : the principal block, the 5-block containing X, and one further 5-block, B say. However, every irreducible character of B has degree congruent to 2 or -2 (mod 5), because each character of B agrees up to sign on 5-singular elements with the unique irreducible character of degree 2 of C(S) which contains S in its kernel. As θ lies outside the principal 5-block we conclude that in any case, θ and X both lie in the same 5-block of G.

This 5-block is invariant under algebraic conjugation and so contains at least two characters of degree 11 as X is not rational-valued . This block also contains two characters of degree 16, as 0 is an exceptional character for the prime 11.

As the block contains five irreducible characters , the degrees must be :

11, 11, 16, 16, 54.

The character of degree 54 lies in the principal 11-block of G.

Now the character degrees for the principal 11-block are :

1, 54, 144, x, e(x-75), 16, 16

where $x \equiv -1 \pmod{11}$ and $e = 1$ or -1.

If $e = -1$, then $x \leq 75$ and $x(75-x)$ divides $|G|$. As $x \equiv -1 \pmod{11}$, this is quickly seen to be impossible. Thus $e=1$

As $x \equiv -1 \pmod{11}$, x is even, for otherwise $x = 3^a.5^b$, whereas 3 and 5 are both quadratic residues (mod 11) , but -1 is not. Thus x-75 is odd , so that 3 divides x-75 (for $x \neq 80$).

As $x-75 \equiv 1 \pmod{11}$ and x-75 has the form $5^a.3^b$ where a = 0 or 1 , we see that $b \geq 2$. Thus 3 divides x but 9

does not . If 5 does not divide x, then $x = 3.2^{c}$ for some integer c. As $x \equiv -1 \pmod{11}$, $c \equiv 7 \pmod{10}$. Thus c = 7 as 2^{15} does not divide $|G|$.

Then x - 75 = 309, a contradiction as 103 does not divide $|G|$. Thus 5 divides x and x-75. Let $x = 15.2^{d}$. Then $d \equiv 3 \pmod{10}$ as $x \equiv -1 \pmod{11}$. Thus d = 3 or d = 13.

If d = 13, then $2^{d} \equiv 2 \pmod{9}$, so that $x-75 \equiv 9 \pmod{27}$. Thus 27 does not divide x-75, so that x-75 = 45 and $x = 120$, a contradiction, as $x = 15.2^{13}$.

If d = 3, then x = 120, so that x-75= 45 and the character degrees for the principal 11-block are :

1, 45, 54, 120, 144, 16, 16

Let y be a non-identity element of P, a Sylow 11-subgroup of G. Then as G contains no element of order 22,

$$\sum_{\theta \in B_0^{(2)}(G) \cap B_0^{(11)}(G)} \theta(y)\theta(1) \equiv 0 \pmod{2^{k}},$$

where 2^{k} is the order of a Sylow 2-subgroup of G.

Now neither character of degree 16 above can lie in the principal 2-block of G (as they both vanish at elements which are central in a Sylow 2-subgroup

of G). It quickly follows that :

$$\sum_{0 \in B_o^{(2)}(G) \cap B_o^{(ii)}(G)} \theta(y)\,\theta(1) \neq 0 \quad .$$

However, $\left| \sum_{0 \in B_o^{(2)}(G) \cap B_o^{(ii)}(G)} \theta(y)\,\theta(1) \right| < 500$, a contradiction as 2^{12} divides $|G|$.

Thus $\theta(1) \neq 16$.

Lemma 4.5.3

$\theta(1) \neq 27$

Proof

Suppose that $\theta(1) = 27$. Then θ does not lie in the principal 5-block of G . Now θ is a constituent of $X\bar{X}$, and $X\bar{X}$ assumes the constant value 1 on all 5-singular elements of G. Consequently, if

$$\mu = \sum_{\phi \in B} (X\bar{X}, \phi)\phi$$

where B is the 5-block of G containing θ, then μ vanishes at every 5-singular element of G . We also note that every character of B has degree congruent to 2 or -2 (mod 5).

Thus $X\bar{X}$ must contain an irreducible constituent , β, from B such that : $\beta(s) = -2$ for any element s of order 5 in S. Then $\beta(1) \equiv 3 \pmod 5$. Also $\beta(1) \leq 66$

As $\beta(1)$ divides $|G|$ and $\beta(1)$ is congruent to one of: 0, -1 or 1 (mod 11), $\beta(1) = 33$. Thus the character degrees for B are : 27,27,33,x,e(x-21), where $e = 1$ or -1 and $x \equiv -2 \pmod 5$.

In fact, as x divides $|G|$, we cannot have $e = -1$ (otherwise $x \leq 21$). Now 11 must divide x(x-21), as the principal 11 block of G cannot contain irreducible characters of degrees x and x-21.

Case i) : 11 divides x

If x is even in this case, then as x-21 divides $|G|$, x-21 is a power of 3. Thus 3 divides x, $x = 33.2^a$ and $x-21 = 3^b$. Now $3^b \equiv 1 \pmod{11}$, as 3 is a quadratic residue (mod 11). Thus $b \equiv 0 \pmod 5$, so that $b = 5$ as 3^{10} does not divide $|G|$.

Thus $x = 264$, a contradiction as $x \equiv -2 \pmod 5$. Hence x is odd. Since $x \equiv -2 \pmod 5$, 3 divides x.

If 9 divides x, then $x-21 = 3.2^a$. Now $a \equiv 2 \pmod 4$ as $x-21 \equiv 2 \pmod 5$. Also $a \equiv 2 \pmod{10}$, as $x-21 \equiv 1 \pmod{11}$. Thus $a = 2$ so that $x = 33$, a contradiction as we have assumed that 9 divides x. Thus $x = 33$.

Case ii) : 11 divides x-21

If x-21 is even, then x is a power of 3, a contradiction, as $x \equiv -1 \pmod{11}$ Thus x-21 is odd. As $x-21 \equiv 2 \pmod{5}$, 3 divides x-21.

If 9 divides x-21, then $x = 3.2^{s}$. As $x \equiv 3 \pmod{5}$, s is even. This contradicts the fact that $x \equiv -1 \pmod{11}$.

Thus the character degrees for the 5-block B are : 27,27,33,33,12 . Hence the character degrees for the principal 11-block are: 1,12,144,x,e(130-x),27,27 where $x \equiv -1 \pmod{11}$ and e = 1 or -1.

If e = 1, then $x \leq 130$, and the only possible set of degrees is :

1,10,12,120,144,27,27.

This contradicts the fact that G has no irreducible character of degree 10.

Thus e = -1. Suppose that 5 does not divide x , then 5 does not divide x-130. If 3 does not divide x-130 , then x-130 is a power of 2. Thus $x = 2.3^{k}$ for some integer k. As $2.3^{k} \equiv -1 \pmod{11}$, $k \equiv 3 \pmod{5}$. As 3^{8} does not divide $|G|$, k = 3, so that x = 54, a contradiction as

$x > 130$. Thus 3 divides $x-130$, so that 3 does not divide x, and x is a power of 2. Let $x = 2^k$. As $x \equiv -1 \pmod{11}$, $k \equiv 5 \pmod{10}$ Thus $k = 5$, as 2^{15} does not divide $|G|$. This contradicts the fact that $x > 130$. Thus 5 divides x.

Now x and $x-130$ must both be even, as 3 cannot divide both of them. One of them must be of the form 10.3^k, as 4 cannot divide them both. Also, $k \neq 0$, as G has no irreducible character of degree 10. It is x that is of the form 10.3^k, as 10.3^k is a quadratic non-residue (mod 11), whereas $x - 130 \equiv 1 \pmod{11}$.

As $x \equiv -1 \pmod{11}$, $k \equiv 0 \pmod{5}$, so that $k = 5^{10}$, as 3^{10} does not divide $|G|$ We now see that : $x = 2430$, $x-130 = 2300$ whereas 23 does not divide $|G|$.

This contradiction completes the proof of the Lemma.

Lemma 4.5.4

$0(1) \neq 54$.

Proof

Suppose that $0(1) = 54$. Then 0 does not lie in the principal 5-block of G. As in the proof of Lemma 4.5.3, 0 lies in the same 5-block as X.

As $X\bar{X}$ assumes the constant value 1 on all 5-singular elements of G , there is an irreducible constituent, μ, of $X\bar{X}$ which belongs to the same 5-block as θ and such that $u(1) \equiv 1 \pmod 5$.

As $\mu(1) \leq 66$, we conclude that $\mu(1) = 11$, 16 or 66 . If $\mu(1) = 16$, then the character degrees for this 5-block are: 11, 11, 16, 16, 54 , a possibility that was disposed of in Lemma 4.5.2 .

If $\mu(1) = 66$, then the character degrees for this 5-block are : 11, 11, 54, 66, 34 a contradiction, as 17 does not divide $|G|$.

If $\mu(1) = 11$, we claim that $\mu = X = \bar{X}$. We note that the 5-block of G containing X contains just one other irreducible character of degree 11, for otherwise the character degrees are : 11, 11, 11, 54 , 21 whereas 7 does not divide $|G|$.

Thus $\mu = X$ or $\bar{X}$. As $X\bar{X}$ is real-valued X and $\bar{X}$ occur with equal multiplicity as constituents of $X\bar{X}$. If $X \neq \bar{X}$, then $X\bar{X} = 1 + \theta + a(X + \bar{X}) + \beta$, and as $X\bar{X}$ is constant on 5-singular elements, β contains another irreducible constituent θ_1 , say, from the 5-block of X such that $\theta_1(1) \equiv -1 \pmod 5$, and $\theta_1(1) \leq 44$.

The only possibility is: $\theta_1(1) = 44$. Thus the character degrees for the 5-block of G which contains X are: 11,11,54,44,76 , a contradiction, as 19 does not divide $|G|$. Thus $X = \bar{X}$.

By Lemma 2.5.1 , $X|_R$ is not rational-valued, for a Sylow 3-subgroup, R, of G , as 3^6 divides $|G|$. As $X = \bar{X}$, there are 3^k irreducible characters of G which are 3-conjugate to X (including X itself) for some integer $k > 0$. This contradicts the fact that the 5-block of G which contains X contains only two characters of degree 11 and is invariant under all algebraic conjugation . The proof of this Lemma is now complete.

Lemma 4.5.5

$\theta(1) \neq 32$.

Proof

If $\theta(1) = 32$, then $|G| = 2^{12}.3^6.5.11.$, for if $|G| = 2^{14}.3^7.5.11$, then $|C(S)| = 10$ and the degree of every irreducible character of G is congruent to 0, 1 or -1 (mod 5).

The character degrees for the principal 11-block are :

$$1, 144, 32, x, y, z, z \quad .$$

One (at least) of x,y or z is odd,so is of the form $5^a.3^b$,where a = 0 or 1 and $1 \leq b \leq 6$

Also, both 5 and 3 are quadratic residues (mod 11),so that $5^a.3^b \equiv 1$ or 5 (mod 11).

We have the following possibilities:

i) a = 0 ,b = 5.

ii) a =0 ,b = 3.

iii) a = 1, b = 2.

iv) a = 1,b = 5.

Case i) : a = 0,b = 5.

Let θ_2 be the character of degree 243 in the principal 11-block.Now θ_2 belongs to the same 5-block as θ does . Let s be an element of order 5 in S and let u be an element of order 11 in P.

Then $\theta(u) = -1$,$\theta(s) = 2$ and $\theta_2(u) = 1$,$\theta_2(s) = -2$. Thus we see that

$$\theta(u)\theta(s) + \theta_2(u)\theta_2(s) = -4.$$

By Lemma 1.2.14 , there must be another irreducible character θ_3 , which lies both in the principal 11-block of G and in the same 5-block as θ does.As $\theta_3(s) = 2$ or -2 a moment's thought persuades us that x ,y and z are each degrees of characters which lie in the same 5-block as θ , so none of them is divisible by 5.

From the degree equation for the principal 11-block , one of x, y or z is a power of 2, say 2^k. As $2^k \equiv 2$ or $-2 \pmod 5$ k is odd. Thus $2^k \equiv -1$ or $6 \pmod{11}$.

If $2^k \equiv -1 \pmod{11}$, then $k \equiv 5 \pmod{10}$ so that k = 5 and the degrees are :

1, 144, 32, 32, 243, 324, 324

a contradiction, as the characters of degree 324 cannot lie in the same 5-block as 0.

If $2^k \equiv 6 \pmod{11}$ then $k = 9$, and the degrees are : 1, 144, 32, 243, 868, 512, 512,

a contradiction

ii) a = 0, b = 3

In this case the degrees are :

1, 144, 32, x, e(x - 86), 27, 27

where $x \equiv -1 \pmod{11}$ and e = 1 or -1 .

If e = 1, then as $x - 86 \equiv 1 \pmod{11}$ 2 divides x - 86 to an even power (since 3 and 5 are quadratic residues (mod 11) but 2 is not). As $x \equiv -1 \pmod{11}$, 2 divides x to an odd power. The only way that this can happen is that 2 divides x to the first power only. If 5 does not divide x then $x = 2.3^r$ and $r \equiv 3 \pmod 5$. As $r \leq 6$ r = 3 and x = 54, a contradiction , as we have assumed that e = 1 , so $x \geq 86$. Thus 5 divides x and $x = 10.3^s$. As $x \neq 10$, we conclude that s = 5 and that x = 2430.

Then $x - 86 = 8.293$, so that $x - 86$ does not divide $|G|$, a contradiction.

If $e = -1$, then $x \leq 86$, and the only possible set of degrees is :

1, 144, 32, 32, 54, 27, 27.

Now the character of degree 54 does not lie in the principal 5-block of G. Neither does it lie in the 5-block of G which contains 0, as every character of that block has degree congruent to 2 or -2 (mod 5). Thus no other character of the principal 11-block of G lies in the same 5-block as 0 does. As G contains no element of order 55, this contradicts Lemma 1.2.14.

iii) a = 1, b = 5

In this case, the degrees for the principal 11-block of G are :

$1, 144, 32, x, e(x-1102), 1215, 1215$

where $x \equiv 1 \pmod{11}$.

If $e = 1$, then $x - 1102 \equiv -1 \pmod{11}$, so that 2 divides $x-1102$ to an odd power. As $x \equiv 1 \pmod{11}$, 2 divides x to an even power. Thus 2 divides $x-1102$ to the first power only. As $x-1102 \neq 2$ or 10, 3 must divide $x - 1102$, so that 3 does not divide x. Then $x = 5.2^k$, and $k \equiv 6 \pmod{10}$, so $k = 6$ as $k \leq 12$. Thus $x = 320$, whereas $x \geq 1102$, a contradiction.

If e = -1 ,then $x \leq 1102$,and $1102-x \equiv 1 \pmod{11}$.As $x \equiv 1 \pmod{11}$, 2 divides x to an even power.Similarly,since $1102-x \equiv 1 \pmod{11}$, 2 divides 1102 - x to an even power.As 4 does not divide 1102,we conclude that x and 1102-x are both odd.As 3 does not divide 1102,either x or 1102-x is prime to 3 . As 11 does not divide x or 1102 - x,we are conclude that either x = 5 or 1102-x = 5 (for both divide $|G|$). This contradicts the fact that x and 1102-x are both congruent to 1 (mod 11).

iv) a = 1 ,b = 2

In this case ,the character degrees for the principal 11-block are :

1,144,32,45,y, z,z

If $y \equiv 1 \pmod{11}$,then z = e(158+y) for some sign e .Thus e = 1 as $z \geq 0$. Hence $z \equiv 5 \pmod{11}$.Thus 2 divides y to an even power (as 3 and 5 are quadratic residues (mod 11) but 2 is not).Also , 2 divides z to an even power. As z = y+158,we conclude that y and z are both odd .As at least one of y or z is prime to 3 ,we conclude that either y = 5 or z = 5 .As $y \equiv 1 \pmod{11}$, we see that z = 5 , a contradiction ,since $y \geq 0$ and z = y+158.

Thus $y = -1 \pmod{11}$. The character degrees are now:

$$1, 144, 32, 45, y, e(158-y), e(158-y).$$

If $e = 1$, then $y \leq 158$ and as both y and $158-y$ divide $|G|$, we have a contradiction. Thus $e = -1$. Since $y \equiv -1 \pmod{11}$ and $y-158 \equiv -5 \pmod{11}$, 2 divides y to an odd power and divides $y - 158$ to an odd power also. Thus one of them is divisible by 2 to the first power only.

If 4 does not divide y, then 5 divides y for otherwise $y = 2.3^k$, so that $k = 3$, since $k \leq 6$, whereas $y > 158$, a contradiction. Thus $y = 10.3^k$ in this case. As $y \equiv -1 \pmod{11}$, $k \equiv 0 \pmod{5}$, so that $k = 5$ as $y \neq 10$. Thus $y = 2430$, $y-158 = 2272 = 32.71$, whereas 71 does not divide $|G|$, a contradiction. Thus 4 divides y.

Hence 4 does not divide $y-158$. Since $y-158 \neq 2$ or 10, 3 divides $y-158$. Thus 3 does not divide y. If 5 does not divide y then $y = 2^t$, so that $t \equiv 5 \pmod{10}$, since $y \equiv -1 \pmod{11}$. As 2^{15} does not divide $|G|$ $t = 5$, a contradiction, as $y > 158$. Thus 5 divides y. Hence $y-158 = 2.3^r$. Also, since $y-158 \equiv 6 \pmod{11}$, $r \equiv 1 \pmod{5}$. Since 5 divides y, $y-158 \equiv 2 \pmod{5}$, so consequently

$r \equiv 0 \pmod 4$. Thus $r \equiv 16 \pmod{20}$, whereas $r \leq 6$, a contradiction.

The proof of this Lemma is complete

Lemma 4.5.6

$0(1) \neq 120$

Proof

Suppose that $0(1) = 120$. Then the degrees for the principal 11-block are :

$1, 120, 144, x, y, z, z$ where

i) $z \equiv 5$ or $-5 \pmod{11}$

ii) $y \equiv 1$ or $-1 \pmod{11}$

iii) $x \equiv 1$ or $-1 \pmod{11}$.

iv) At least one of x, y or z is odd and at least one of them is prime to 3.

Case i) : z odd

Then $z = 5^a.3^b$, where $a = 0$ or 1. Thus z is a quadratic residue (mod 11), so that $z \equiv 5 \pmod{11}$. If $a = 0$, then $b \equiv 3 \pmod 5$ so that $b = 3$, as 3^8 does not divide $|G|$. The character degrees are then:

$1, 120, 144, x, x+2, 27, 27$

where $x \equiv -1 \pmod{11}$. As 3 and 5 are both quadratic residues (mod 11), 2 must divide x to an odd power, and 2 divides $x + 2$ to an even power. The only way that this can happen is that 2 divides x but

that 4 does not.

Now $x \neq 2$ or 10, so that 3 divides x. Thus 3 does not divide $x+2$. If 5 does not divide $x+2$, then $x+2 = 2^a$ for some integer a. As $x+2 \equiv 1 \pmod{11}$, $a \equiv 0 \pmod{10}$, so that $a = 10$, as 2^{20} does not divide $|G|$. Now $x = 1022$, a contradiction as 1022 does not divide $|G|$. Thus 5 divides $x+2$ and 5 does not divide x.

Now x has the form 2.3^k. As $x \equiv -1 \pmod{11}$ $k \equiv 3 \pmod{5}$, and $k = 3$ as 3^8 does not divide $|G|$. Now $x = 54$ and $x+2 = 56$, whereas 7 does not divide $|G|$, a contradiction. We conclude that $a = 1$, so that $z = 5.3^b$.

Now $b \equiv 0 \pmod{5}$, so that $b = 5$, as G has no irreducible character of degree 5 and $b \leq 5$. Thus $z = 1215$. The degrees for the principal 11-block are :

$$1, 144, x, 120, e(1190-x), 1215, 1215,$$

where $x \equiv 1 \pmod{11}$ and $e = 1$ or -1.

If $e = 1$, then $x \leq 1190$, and $1190-x \equiv 1 \pmod{11}$. Since $x \equiv 1 \pmod{11}$, 2 divides both x and $x-1190$ to an even power. Since 4 does not divide 1190, both x and $1190-x$ are odd. At least one of them is prime to 3, so that the other is prime both to 3 and to 2. The latter character

degree must be 5 ,a contradiction as both x and 1190-x are congruent to 1 (mod 11).

Thus e = 1,so that $x \geq 1190$ and $x-1190 \equiv -1 \pmod{11}$. Hence 2 divides x-1190 to an odd power .Also, 2 divides x to an even power as $x \equiv 1 \pmod{11}$.Thus 2 divides x-1190 to the first power only. Now $x-1190 \neq 2$ or 10 , so that 3 divides x-1190.Hence 3 does not divide x,and x is of the form $5^r.2^s$,where $r \leq 1$.

If r = 0,then $2^s \equiv 1 \pmod{11}$,so that $s \equiv 0 \pmod{10}$ and s = 10 , since 2^{20} does not divide |G|.However, $x \geq 1190$ and $2^{10} = 1024$,a contradiction . If r = 1,then $5.2^s \equiv 1 \pmod{11}$,so that $s \equiv 6 \pmod{10}$ and s=6.This contradicts the fact that x >1190 Thus z must be even.

Case ii) : x or y odd

We may as well suppose that x is odd. This time ,$x = 5^a.3^b$, where $a \leq 1$. We may also suppose that z is even . We note that $x \equiv 1 \pmod{11}$ since 3 and 5 are quadratic residues (mod 11).

a) If a = 0

If a = 0,then $b \equiv 0 \pmod{5}$,so that b = 5 as 3^{10} does not divide |G| .Consequently, the character degrees for the principal

11-block are :

1, 120, 144, 243 , y, z, z.

We note that in this case , $|C(S)| = 30$, and $|G| = 2^{12} . 3^{6} .5.11$.

If $y \equiv -1 \pmod{11}$, then 2 divides y to an odd power. Also $z = e(268-y)$ for some sign e .If $e = 1$, then $y \leq 268$ and we have a contradiction, as y and z must both divide $|G|$. Thus $e = -1$, so that $z = y-268$,and $z \equiv 6 \pmod{11}$. Hence 2 divides z to an odd power. As 8 does not divide 268 ,but 4 does, y and z are both divisible by 2 to the first power only . Then 5 divides y,for otherwise, $y = 2.3^{s}$ so that $s \equiv 3 \pmod{5}$ and $s = 3$,contrary to the fact that $y \geq 268$.As 5 divides y, z has the form 2.3^{t} .Since $z \equiv 6 \pmod{11}$ $t \equiv 1 \pmod{5}$.As $z = y-268$ and 5 divides y , $z \equiv 2 \pmod{5}$ .Thus $t \equiv 0 \pmod{4}$,so that $t \equiv 16 \pmod{20}$,a contradiction,as $t \leq 7$.Thus $y \equiv 1 \pmod{11}$.

As $y \equiv 1 \pmod{11}$,the character degrees are :

1, 120, 144, 243, y, y+268, y+268.

If 3 does not divide z ,then z has the form $5^{a}.2^{b}$ where $a \leq 1$.As $z \equiv 5 \pmod{11}$ b is even.If $a = 1$, then $z \equiv 2 \pmod{3}$,so

that $y \equiv 1 \pmod 3$ (as $y = z-268$). Now however, y must be a power of 2 ,so that $y = 2^{10}$,as $y \equiv 1 \pmod{11}$ and 2^{20} does not divide $|G|$.Then $z = 1292$,contrary to the assumption that 5 divides z . Thus z is a power of 2,say 2^d .As $z \equiv 5 \pmod{11}$ $d \equiv 4 \pmod{10}$. Since $|G| = 2^{12}.3^6.5.11$ and $z > 268$,we have a contradiction.

Thus 3 divides z,so that as $z = y+268$, $y \equiv 2 \pmod 3$. Thus 5 divides y , for otherwise $y = 2^r$,where r is even , since $y \equiv 1 \pmod{11}$,so that $y \equiv 1 \pmod 3$.Let $y = 5.2^s$ .Now $s \equiv 6 \pmod{10}$,as $y \equiv 1 \pmod{11}$ Thus $s = 6$,$y = 320$ and $z = 588$.

However,7 divides 588 but 7 does not divide $|G|$,a contradiction.Thus $a \neq 0$.

b) If $a = 1$

If $a = 1$,then $b \equiv 2 \pmod 5$. If $b = 2$,then the character degrees are :

$$1,45,120,144,y,z,z$$

If $y \equiv 1 \pmod{11}$, then $z = 70 + y$ and $z \equiv 5 \pmod{11}$.Thus 2 divides z to an even power and y to an even power.As z is even, and $70 \equiv 2 \pmod 4$,we have a contradiction Thus $y \equiv -1 \pmod{11}$,and 2 divides y to an odd power.Also, $z = e(70-y)$ for some sign e. As y and z both divide $|G|$ and $y \neq 10$,

we see that if e = 1, then y = 54 and the degrees are: 1,45,54,144,120,16,16.

It has already been demonstrated in Lemma 4.5.2 that this set of character degrees cannot occur. Thus e = -1 and $z \equiv 6 \pmod{11}$. Now as z = y-70, either y or z is prime to 3. Also, y and z cannot both be divisible by 4. Now $y \neq 10$ and $z \neq 10$, so that whichever one of y,z is not divisible by 4, the other is prime to 3.

If z is prime to 3, then $z = 5^r.2^s$ where s = 0 or 1. If r = 0, then $s \equiv 9 \pmod{10}$, as $z \equiv 6 \pmod{11}$. Thus s = 9 and z = 512. Then y = 582 = 2.291, so that y does not divide |G|, a contradiction. If r = 1, then $s \equiv 5 \pmod{10}$, so that s = 5, since 2^{15} does not divide |G|. Then z=160 and y=230, whereas 23 does not divide |G|, a contradiction. Thus 3 must divide z, so that y is prime to 3.

If y is a power of 2, say 2^t, then t = 5 since $y \equiv -1 \pmod{11}$ and 2^{15} does not divide |G|. This contradicts the fact that $y \geq 70$. Thus $y = 5.2^d$ for some integer d. Now since $y \equiv -1 \pmod{11}$, $d \equiv 1 \pmod{10}$. As $y \neq 10$, we see that d = 11. The character degrees are: 1,120,144,45,10240,10170,10170.

However, 1017 = 9.113, so that z does divide |G|, a contradiction. Thus $b \neq 2$. As

3^{12} does not divide $|G|$, and $b \equiv 2 \pmod 5$, we conclude that $b = 7$. Thus $x = 10935$.

Now the character degrees are :

$$1, 144, 120, 10935, y, z, z$$

If $y \equiv -1 \pmod{11}$, then $z = e(10960-y)$, where $e = 1$ or -1. If 3 does not divide y, then 5 divides y, for otherwise, $y = 2^k$, and $k = 5$, as $y \equiv -1 \pmod{11}$ and 2^{15} does not divide $|G|$. However, $|G| = 2^{14}.3^7.5.11$ as 3^7 divides x. Thus $|C(S)| = 10$, and each irreducible character of G has degree which is congruent to one of: $0, -1$ or $1 \pmod 5$. This contradicts the fact that $y = 32$. Thus 5 divides y in this case, so that $y = 5.2^t$ for some integer t. As $y \equiv -1 \pmod{11}$, we conclude that $t \equiv 1 \pmod{10}$. As $y \neq 10$, we are forced to conclude that $t = 11$, so that the character degrees are :

$$1, 120, 144, 10240, 10935, 720, 720.$$

As G contains no element of order 22, we see that each irreducible character of G in the principal 11-block must also lie in the principal 2-block of G (by Lemma 1.2.14).

We derive a contradiction by proving that 0, the character of degree 10240 above, does not lie in the principal 2-block of G. For suppose that it does, and let t be a central

involution in some Sylow 2-subgroup of G. Then $[G:C(t)]$ is odd and 2^{11} divides $\theta(1)$ so that 2^{11} divides $\theta(t)$.

As θ lies in the principal 2-block of G, $[G:C(t)]\ \theta(t)/\theta(1)$ is odd, so that $\theta(t) \neq 0$. Thus $\theta(t) \geq 2^{11}$, so that $|C(t)| > 2^{22}$. Now 5 does not divide $|C(t)|$, for otherwise: $([G:C(t)], \theta(1)) = 1$, so $\theta(1)$ divides $\theta(t)$ a contradiction, as $\theta(t) \neq 0$ and G is simple Also, 11 does not divide $|C(t)|$, so that $|C(t)| = 2^{14} \cdot 3^{b}$ for some integer b.

As $|C(t)| \geq 2^{22}$, $3^{b} \geq 2^{8}$, so that $b \geq 6$ Let θ^* be the permutation character afforded by the action of G on the right cosets of $C(t)$ in G. As $2^{14} \cdot 3^{6}$ divides $|G|$, we see that $\theta^*(1) = 55$ or 165. We note that θ^* vanishes on all 11-singular elements and on all 5-singular elements, since $|C(t)|$ is not divisible by 11 or by 5.

Now suppose that $\theta^*(1) = 55$. Then $\theta^* - 1$ is an ordinary character of G of degree 54 which assumes the constant value -1 on all 11-singular elements of G. Thus θ^* contains a non-trivial constituent which lies in the principal 11-block, a contradiction, as the principal 11-block contains no irreducible non-trivial character of degree less than 120, and $\theta^*(1) = 55$.

Suppose then that $\theta^*(1) = 165$. This time we can conclude that $\theta^*(1)$ contains some non-trivial irreducible constituent from the principal 11-block (which must be non-exceptional , as the exceptional characters have degree 720). As $\theta^*(1) - 1$ assumes the constant value -1 on 11-singular elements, we may in fact conclude that $\theta^* - 1$ contains an irreducible constituent which lies in the principal 11-block and has degree which is congruent to -1 (mod 11) . The character of degree 120 is the only possibility . Let us denote this character by θ_1 .

Now $\theta^* - \theta_1 - 1$ is an ordinary character of G which assumes the constant value -1 on all 5-singular elements of G. We deduce that this character contains some irreducible constituent from the principal 5-block with degree congruent to -1 (mod 5) . This is a contradiction, since $\theta^*(1) - \theta_1(1) - 1 = 44$ and the character degrees for the principal 5-block are : 1,66,99,144,176 .

This contradiction finally establishes that the character degrees :

1,120,144,10240,10935,720,720

do not occur.

Suppose that $y \equiv 1 \pmod{11}$.

Then $z = 10960 + y$. If y and z are both prime to 5, then one of them is a power of 2. If y is a power of 2, then $y = 2^{10}$ since $y \equiv 1 \pmod{11}$ and 2^{20} does not divide $|G|$. Then $y \equiv 1 \pmod 3$, so that $z \equiv 2 \pmod 3$, a contradiction ($z = 1024 + 10960$, so that 32 does not divide z). If z is a power of 2 then $z = 2^s$, where $s \equiv 4 \pmod{10}$, since $z \equiv 5 \pmod{11}$. As $z > 10960$, we conclude that $s = 14$. Then $z \equiv 4 \pmod 9$, so that $y \equiv 6 \pmod 9$ (as $y = z - 10960$). Also, $y \equiv 16 \pmod{32}$ as $10960 = 16.685$). Hence $y = 48$, a contradiction, as $y \equiv 1 \pmod{11}$.

Consequently, 5 divides both y and z. Suppose that 3 does not divide z, so that $z = 5.2^r$ for some integer r. Then r is even, as $z \equiv 5 \pmod{11}$. Thus $z \equiv 2 \pmod 3$, so that $y \equiv 1 \pmod 3$, as $y = z - 10960$. Now y is of the form 5.2^k, where k is even, since we know that $y \equiv 1 \pmod{11}$. Now, however, we have : $y \equiv 2 \pmod 3$, a contradiction. Thus 3 divides z, but not y.

Now y has the form 5.2^m where m is an integer congruent to 6 (mod 10), since we know that $y \equiv 1 \pmod{11}$. As 2^{16} does not divide $|G|$, $m = 6$ and $y = 160$. Consequently $z = 11280 = 5.3.16.47$, a contradiction, as 47 does not divide $|G|$. The proof of this Lemma is now complete.

Lemma 4.5.7

$\theta(1) \neq 60$

Proof

Suppose that $\theta(1) = 60$. Then the degrees for the principal 11-block are :

$$1, 144, x, y, z, 60, 60 .$$

We may assume that 2 does not divide x. Since $x \equiv 1$ or $-1 \pmod{11}$, and 3 and 5 are both quadratic residues (mod 11), we conclude that $x \equiv 1 \pmod{11}$.

As 3^8 does not divide $|G|$, we conclude that x is one of: 45, 243 or 5.3^7. We deal separately with each of these cases.

Case i) : $x = 45$

There are signs e_1, e_2 such that $1 + 144 + 45 + e_1 y + e_2 z - 60 = 0$. Thus we may suppose that 4 does not divide y. If y is odd, then so is z. In that case, either y or z is prime to 3, so either $y = 5$ or $z = 5$, a contradiction since $y \equiv e_1 \pmod{11}$ and $z \equiv e_2 \pmod{11}$. Thus y is even, so that $y \equiv 2 \pmod 4$.

It follows that $y \equiv -1 \pmod{11}$, since 3 and 5 are quadratic residues (mod 11) but 2 and -1 are not. If 5 divides y, then $y = 10.3^s$, where $s \equiv 0 \pmod 5$. Since G

has no irreducible character of degree 10 and 3^{10} does not divide $|G|$, we deduce that $s = 5$ and that $y = 2430$. Then the degrees for the principal 11-block are:

$$1, 144, 45, 2430, 2300, 60, 60$$

a contradiction, as 2300 does not divide G. Thus 5 does not divide y.

Hence y must have the form 2.3^r, where $r \equiv 3 \pmod 5$, as $y \equiv -1 \pmod{11}$. Since $r \leq 7$ (for y divides $|G|$), we conclude that $r = 3$ and $y = 54$. The degrees for the principal 11-block must be :

$$1, 144, 45, 54, 76, 60, 60$$

a contradiction, as 76 does not divide $|G|$. Thus $x \neq 45$.

Case ii) : $x = 243$

In this case, $|G| = 2^{12}.3^6.5.11$, for if $|G| = 2^{14}.3^7.5.11$, then $|C(S)| = 10$ and each irreducible character of G has degree congruent to 0, 1 or -1 (mod 5) The irreducible character of degree 243 must lie in a 3-block of defect 1 of G.

By Lemma 1.2.14, as G contains no element of order 33, there is some other irreducible charaacter in the principal 11-block which lies in the same 3-block as the character of degree 243. Thus we may assume that $y = 243t$, where 3 does not divide t.

Now the character degrees for the principal 11-block are :

1, 144 , 243 , 243t , z , 60 , 60.

Now z must have the form $2^a.5^b$ where b = 0 or 1 . As $z \equiv 1$ or $-1 \pmod{11}$ and $z \neq 10$, 16 certainly divides z.

Now there are signs e and d such that:

$1 + 144 + 243 + e\,243t + dz - 60 = 0.$

As 16 divides z ,we see that 8 divides 243t ,but 16 does not.

It follows that $243t \equiv -1 \pmod{11}$ since 2 is a quadratic non-residue (mod 11) .However , t = 8 or 40, since t divides |G| , and t is prime to 3 . Thus 243t = 8 or 7 (mod 11) , contrary to the fact that $243t \equiv -1 \pmod{11}$. Thus $x \neq 243$.

Case iii) : $x = 5.3^7$

In this case, $|G| = 2^{14}.3^7.5.11$,as x divides |G| . The character degrees for the principal 11-block are :

1, 144 ,10935 ,y,z,60,60.

There are signs e and d such that :

$1 + 144 + 10935 + ey + dz - 60 = 0.$

Thus we may suppose that e = -1 and $y \equiv -1 \pmod{11}$.

As $y \equiv -1 \pmod{11}$, 2 divides y to an odd power. Thus y and z are even. Now $dz-y \equiv 4 \pmod 8$ as $5.3^7 \equiv 7 \pmod 8$. If 8 divides y, then 4 divides z, but 8 does not. In that case 3 divides z, as $z \neq 4$ or 20. Then 3 does not divide y, so that $y = 5^a.2^b$ where $a = 0$ or 1. If $a = 0$, then $2^b \equiv -1 \pmod{11}$, so that $b \equiv 5 \pmod{10}$. As 2^{15} does not divide $|G|$, $b = 5$ and $y = 32$, contradicting the fact that $y \equiv 0, 1$ or $-1 \pmod{11}$. If $a = 1$, then $b \equiv 1 \pmod{10}$, so that $b = 11$ (as $y \neq 10$) and $y = 10240$. The character degrees for the principal 11-block are thus:

1, 144, 10935, 10240, 780, 60, 60

a contradiction, as 780 does not divide $|G|$. Thus 8 does not divide y, so that 2 divides y to the first power only.

As $dz-y \equiv 4 \pmod 8$, 2 also divides z to the first power only. As 3 cannot divide both y and z, we see that either $y = 10$ or $z = 10$, contrary to the fact that G has no irreducible character of degree 10.

This completes the elimination of case iii), and so completes the proof of this Lemma.

Remark

Given the assumptions that $C(S)$ has even order and 2^{11} divides $|G|$, but 7 does not, we have eliminated every possible value for $\emptyset(1)$.

By the remarks at the end of chapter two, we may conclude that 7 divides $|G|$.

Section Six

For the remainder of this section, we will assume that T is a Sylow 7-subgroup of G and that T has order 7.

Lemma 4.6.1

$[N(T):C(T)] = 3$.

Proof

By Lemma 2.5.4 , $X|_T$ is not rational valued.Thus $[N(T):C(T)] \neq 6$. Hence as $[N(T):C(T)]$ divides 6 and $N(T) \neq C(T)$ we need to prove that $[N(T):C(T)] \neq 2$

Suppose then that $[N(T):C(T)] = 2$ Then the principal 7-block consists of the trivial character,one further non-exceptional character of degree x ,say, where $x \equiv e \pmod 7$ for some sign e, and 3 exceptional characters of degree x+e.

Thus $x(x+e)$ divides $|G|$.We claim that 55 divides $x(x+e)$.As G contains no element of order 35 , we conclude that some non-principal character of the principal 7-block lies in the principal 5-block of G.

As [N(S):C(S)] = 4, each irreducible character of the principal 5-block of G has degree congruent to +1 or to -1 (mod 5) . Hence the principal 5-block cannot contain a character of degree x as well as a character of degree x + e . Thus there is a character in the principal 7-block which does not lie in the principal 5-block of G.

We note that the exceptional characters of the principal 7-block agree on 7-regular elements, so they agree on 5-singular elements . Hence they either vanish identically on 5-singular elements ,or they all lie in the same 5-block . If they vanish identically on 5-singular elements, then 5 divides x+e.

Suppose then that the exceptional characters of the principal 7-block all lie in the same 5-block , B say

If B is the principal 5-block of G then the non-exceptional character of degree x is the only character of the principal 7-block which does not lie in the principal 5-block. Since

this character assumes the constant value e on 7-singular elements , we conclude from Lemma 1.2.14 that $ex \equiv 0 \pmod 5$, so 5 divides x.

If B is not the principal 5-block a similar argument tells us that $-e(x+e) \equiv 0 \pmod 5$, so that x+e is divisible by 5 , which contradicts the assumption that the exceptional characters do not vanish on all 5-singular elements.

Hence 5 divides x(x+e).As the principal 11-block cannot contain a character of degree x as well as a character of degree x+e ,there is a character in the principal 7-block which does not lie in the principal 11-block of G. As every irreducible character outside the principal 11-block has degree divisible by 11, 11 divides x(x+e).

Thus 55 divides x(x+e).Also ,7 does not divide x(x+e). We can now prove the Lemma by eliminating each possible prime factorization of x.

a) $x = 55.2^{a}$, $x+e = 3^{b}$

In this case , e = 1, as 3 is a quadratic residue (mod 11) and -1 is not (for $3^{b} \equiv e \pmod{11}$) . Also, $b \equiv 0 \pmod{5}$ as $3^{b} \equiv 1 \pmod{11}$ so that $3^{5} - 1$ divides $3^{b} - 1$. Thus 121 divides x, a contradiction.

b) $x = 55.3^{a}$, $x+e = 2^{b}$

Here the characters of degree x+e all lie in the principal 5-block so have degree congruent to 1 or -1 (mod 5). Hence b is even, and e = 1 as e is a quadratic residue (mod 11).

Thus $b \equiv 0 \pmod{10}$, as $2^{b} \equiv 1 \pmod{11}$. Hence $2^{5} - 1$ divides $2^{b} - 1$, a contradiction as $x = 2^{b} - 1$.

c) $x = 55$, $x+e = 2^{a}.3^{b}$

Here of course, e = -1 and x+e = 54 Thus the 3 exceptional characters of degree 54 all lie in the principal 5-block of G . It readily follows that the character degrees for the principal 5-block are 1, 54, 54, 54, 161 a contradiction , as 161 = 7.23 and 23 does not divide $|G|$.

d) $x = 11.2^{a}$, $x+e = 5.3^{b}$

Here , e = 1, as 5 and 3 are both quadratic residues (mod 11) but -1 is not. Thus $5.3^{b} \equiv 2 \pmod 7$, so that b is odd , as 2 is a quadratic residue (mod 7) but 3 and 5 are not.

Thus $5.3^{b} \equiv 7 \pmod 8$, so that $x = 5.3^{b} - 1 \equiv 6 \pmod 8$. Hence a = 1, a contradiction.

e) $x = 11.3^{a}$, $x+e = 5.2^{b}$

This time, e = -1, because 5.2^{b} is a quadratic non-residue (mod 7) and $5.2^{b} \equiv 2e \pmod 7$.

Now $11.3^{a} \equiv 1 \pmod 5$, so that a is even. However $11.3^{a} \equiv -1 \pmod 7$ a contradiction as -1 is a quadratic non-residue (mod 7).

f) $x = 5.2^{a}$, $x+e = 11.3^{b}$

As $11.3^{b} \equiv e \pmod 5$, b is even. Thus 11.3^{b} is a quadratic residue (mod 7), so e = 1, as $x+e \equiv 2e \pmod 7$ Now, however, $5.2^{a} \equiv 1 \pmod 7$ which yields a contradiction as 5 is not a quadratic residue (mod 7), but 2 is.

g) $x = 5.3^{a}$, $x+e = 11.2^{b}$

Here , $x \equiv -e \pmod{11}$, so $e = -1$, as 5 and 3 are both quadratic residues (mod 11) but -1 is not .Now,however, $11.2^{b} \equiv -2 \pmod{7}$, a contradiction as 11 and 2 are quadratic residues (mod 7),but -1 is not.

h) $x = 2^{a}$, $x+e = 55.3^{b}$

$2^{a} \equiv e \pmod{7}$ and 2 is a quadratic residue (mod 7),so $e = 1$. Also, a is even,as $2^{a} \equiv -1 \pmod{5}$ .Now,however, $2^{a} \equiv -1 \pmod{11}$, a contradiction, as a is even and -1 is not a quadratic residue (mod 11).

i) $x = 3^{a}$, $x+e = 55.2^{b}$

As $3^{a} \equiv -e \pmod{5}$, a is even. Thus $e = 1$, as $3^{a} \equiv e \pmod{7}$.However, now we have $3^{a} \equiv -1 \pmod{11}$, which contradicts the fact that -1 is not a quadratic residue (mod 11), but 3^{a} is.

j) $x = 2^{a}.3^{b}$, $x+e = 55$

Here $55 \equiv 2e \pmod{7}$, contrary to the fact that $e = 1$ or -1.

We have now considered every possible prime factorization of x , so the Lemma is proved.

Lemma 4.6.2

$C(T) \neq T$.

Proof

Suppose that $C(T) = T$ .Then by Lemma 4.2.3 ,we know that $C(S) \neq 15$,where S is a Sylow 5-subgroup of G.Also,we know that $C(S) \neq S$, so that there is an involution t in $C(S)$. By Lemma 2.4.2 ,$X(t) = -1$.

As $C(T) = T$ and $X(1) \equiv -3 \pmod 7$,X is an exceptional character in the principal 7- block . Let u be an element of T.Then $1+X(u)+\overline{X}(u) = 2$,so that there is a character in the principal 7-block,whose degree,y say is congruent to $-1 \pmod 7$.

Then the character degrees for the principal 7-block are:

1,y,12-y,11,11 or 1,y,y-12,11,11.

In the former case,$y = 6$.

Case i) : $y = 6$

In this case ,the character table of G has a fragment of the form:

1	t	u
1	1	1
6	a	-1
6	-a	-1
11	-1	b
11	-1	1-b

where t and u are as above.

As [N(T):C(T)] = 3 , t cannot invert any 7-singular element.Thus:

$$1 - \frac{a^2}{6} - \frac{a^2}{6} + \frac{1}{11} = 0 \quad \text{,so that}$$

$36 = 11a^2$,a contradiction.

Case ii)

In this case,the character table of G has a fragment of the following form:

1	t	u
1	1	1
y	a	-1
y-12	a	1
11	-1	b
11	-1	1-b

This time, we have:

$$1 - \frac{a^2}{y} + \frac{a^2}{y-12} + \frac{1}{11} = 0.$$

Hence: $$\frac{12}{11} + \frac{12a^2}{y(y-12)} = 0$$

a contradiction. Thus C(T) ≠ T.

Lemma 4.6.3

C(T) is Abelian of order 14 or 21.

Proof

As [N(T):C(T)] = 3 and $X|_T$ is not rational-valued, X is an exceptional character for the prime 7.

Consequently, there is an irreducible character θ of $N(T)$ and a sign e such that:

$X(y) = e\,\theta(y)$ for any 7-singular y any y in $N(T)$, and $\theta(1) = 3$.

Since $X(1) = 11$, $e = -1$.

Then $X|_{C(T)} = \theta_1 + \theta_2 + \ldots \theta_7 + \theta_8$,

where $\theta_1 \ldots\ldots \theta_7$ are all linear and $X(y) = \theta_8(y)$ for any 7-singular element of $C(T)$.

Let x be an element of order 7 in T. Then we may suppose that $\theta_i(x) = w^{i-1}$ for $1 \leq i \leq 7$, where w is a primitive 7-th root of unity, and that $\theta_8(x) = 1 + w^3 + w^5 + w^6$.

Then for any 7-regular element, z of $C(T)$, we have :

$$\theta_1(xz) + \ldots\ldots + \theta_7(xz) = 0,$$

so that $\theta_1(z) = \ldots\ldots = \theta_7(z)$.

We note that each irreducible constituent of $X|_{C(T)}$ is linear, for $N(T)$ fixes the constituent of θ_8 which contains T in its kernel,.

Thus C(T) is Abelian. Let μ be the constituent of $\theta_8 \mid C(T)$ which contains T in its kernel .Then the 7-block of C(T) that contains μ is invariant under N(T) .

Consequently , for any 7-regular element , z of C(T) , we have :

$$\theta_8(z) = (1 + w + w^3 + w^5)\,\mu(z),$$

and :

$$X(z) = 7\,\theta_1(z) + 4\,\mu(z).$$

Let z be an element of order p in C(T) , (where p = 2 or 3). Then xz has 11-distinct eigenvalues, so that C(xz) is a $\{7,p\}$- group by Lemma 1.5.2 . As C(T) is Abelian, C(T) is a $\{7,p\}$-group.

Now x has no eigenvalue of multiplicity 3 or more , so that C(T) contains no element of order 4 and no element of order 9 .Thus C(T) has elementary Abelian Sylow p-subgroups . If they are not cyclic , then there is an element of order p in $\ker(\bar{\theta}_1 \mu)$, and this element is central in G, a contradiction.

The proof of the Lemma is complete.

Lemma 4.6.4

i) 2^{16} does not divide $|G|$.

ii) 3^{12} does not divide $|G|$.

iii) If $|C(S)|$ is even, then $C(T)$ has order 14.

iv) If $|C(S)| = 15$, then $|C(T)| = 21$.

Proof

We claim that B, the 5-block of G which contains X, can only contain one further character of degree 11 that is algebraically conjugate to X

B certainly contains the other character of degree 11 which is 7-conjugate to X, and only one such 7-conjugate of X. If B contains any other algebraic conjugates of X, it must contain 4 characters of degree 11 and one of degree 44.

As G contains no element of order 35, Lemma 1.2.14 tells us that all characters of B lie in the same 7-block, a contradiction as $|T| = 7$ and each character of degree 11 in B is exceptional for the prime 7.

i) If $C(S)$ has even order, then B is invariant under any algebraic automorphism, so that X is 2-rational and 3-rational. By Lemma 2.5.1, 2^{16} does not divide $|G|$, and 3^{6} does not divide $|G|$.

Suppose that $C(T)$ has order 21. Then $C(T)$ contains an element y, of order 3 such that $X(y) = 7\alpha + 4\beta$, for some cube roots of unity α and β. In that case, $X(y)$ is not 3-rational, a contradiction. Since $C(T)$ has order 14 or 21, we see that $C(T)$ must in fact have order 14 in this case.

ii) If $|C(S)| = 15$, then X is not 3-rational. As X is not 7-rational, G contains an element of order 21 by Lemma 1.2.12. Thus $|C(T)| = 21$ in this case. Also, B is invariant under any Galois automorphism which fixes cube roots of unity, so that X is 2-rational and $X + \overline{X}$ is 3-rational.

By Lemmas 2.5.1 and 2.5.2, 2^{16} does not divide $|G|$, and 3^{12} does not divide $|G|$.

Lemma 4.6.5

The only possible order of G is: $2^{15} .3^{11} .5.7.11$

Proof

We have enough information about Sylow normalizers of G to be able to prove this Lemma using Sylow's theorem alone . We consider several cases separately though . We may suppose that 2^{11} divides $|G|$.

Case i) : $|C(S)| = 15$

In this case, $|G| = 2^{a} .3^{b} .5.7.11$ where $11 \leq a \leq 15$, $3 \leq b \leq 11$.

Also, $|N(S)| = 60$ and $|N(P)| = 55$ and $|N(T)| = 63$.

By Sylow's theorem,we see that:

a) $2^{a-2} .3^{b-1} .7 \equiv 1 \pmod 5$

b) $2^{a} .3^{b} .7 \equiv 1 \pmod{11}$.

c) $2^{a} .3^{b-2} .5.11 \equiv 1 \pmod 7$.

These three equations yield :

d) $a \equiv b \pmod 4$

e) $(a+7) \equiv 2b \pmod{10}$

f) $2a + b + 1 \equiv 0 \pmod 6$

From equation f) , b is odd. From equation d) , a is odd . From e) $b \equiv 3a+1 \pmod 5$. From f) , we also see that $b \equiv a+2 \pmod 3$.

As $b-a \equiv 0 \pmod 4$,we see that: $b-a \equiv 8 \pmod{12}$

Now $11 \leq a \leq 15$ and $3 \leq b \leq 11$,so that $-12 \leq b-a \leq 8$. Thus $b-a = 8$ or -4.

If $b-a = 8$,then $b = 11$ and $a = 3$, and $b \not\equiv 3a + 1 \pmod 5$,a contradiction If $b-a = -4$, then as $b \equiv 3a +1 \pmod 5$ we see that $a \equiv 0 \pmod 5$.

As a is odd , $a = 15$. Thus $a = 15$ and $b = 11$ is the only possibility so: $|G| = 2^{15} .3^{11} .5.7.11$ in this case.

Case ii): $|C(S)| = 10$

In this case, $|G| = 2^{a} .3^{b} .5.7.11$,and $11 \leq a \leq 15$, $1 \leq b \leq 5$. Also, N(S) has order 40 and N(T) has order 42 .Again by Sylow's theorem:

a) $2^{a-3} .3^{b} .7 \equiv 1 \pmod 5$

b) $2^{a-1} .3^{b-1} . 55 \equiv 1 \pmod 7$.

Thus we have:

c) $a-b \equiv 2 \pmod 4$.

d) $2a + b \equiv 0 \pmod 6$.

Hence a and b are both even.

Let P be a Sylow 11-subgroup of G. Then $|N(P)| = 110$, for otherwise $[G:N(P)] = 2^a.3^b.7 \equiv 1 \pmod{11}$ which contradicts the fact that a and b are both even but 7 is not a quadratic residue (mod 11).

Thus $2^{a-1}.3^b.7 \equiv 1 \pmod{11}$, and:

e) $a+6 = 2b \pmod{10}$.

From c) and d), we deduce that $a - b = 6 \pmod{12}$. Also, as a and b are both even, $12 \leq a \leq 14$, $2 \leq b \leq 4$ Thus $a-b = 6$. From e), we conclude that $b \equiv 2 \pmod 5$, so that $a \equiv 8 \pmod{10}$, a contradiction.

Case iii): $|C(S)| = 30$

In this case, $|N(T)| = 42$ and $|N(S)| = 120$. Also $|G| = 2^a.3^b.5.7.11$ where $11 \leq a \leq 15$, $1 \leq b \leq 5$.

By Sylow's theorem,

a) $2^{a-3}.3^{b-1}.7 \equiv 1 \pmod 5$.

b) $2^{a-1}.3^{b-1}.55 \equiv 1 \pmod 7$.

Thus we see that:

c) $a \equiv b + 1 \pmod 4$

d) $2a + b \equiv 0 \pmod 6$

Thus b is even and a is odd.

Also $a-b \equiv 9 \pmod{12}$. Now $2 \leq b \leq 4$ and $11 \leq a \leq 15$, so that $a-b = 9$.

Now let P be a Sylow 11-subgroup of G. Then $|N(P)| = 55$, for otherwise $[G:N(P)] = 2^{a-1}.3^{b}.7$ which contradicts the fact that a is odd, b is even, 7 is not a quadratic residue (mod 11), but $[G:N(P)] \equiv 1 \pmod{11}$.

Thus $[G:N(P)] = 2^{a}.3^{b}.7$, so that $2^{a}.3^{b}.7 \equiv 1 \pmod{11}$ and :

e) $a + 7 \equiv 2b \pmod{10}$

As $a-b = 9$, we see that $b \equiv 6 \pmod{10}$ a contradiction as $b \leq 4$.

Lemma 4.6.6

$\cdot |G| \neq 2^{15}.3^{11}.5.7.11$

Proof

Suppose that $|G| = 2^{15}.3^{11}.5.7.11$.

Then we have:

a) $|C(S)| = 15$

b) $|C(T)| = 21$

c) $|N(P)| = 55$

Also, by Lemma 4.6.3, C(T) contains an element x of order 3 such that :

$X(x) = 4w + 7\bar{w}$, where w is a primitive

cube root of unity. Let $C = C(x)$.

We claim that 27 does not divide $|C|$. This is certainly true if $C \leq N(T)$, so suppose that T is not normal in C. Let $K = O_{7'}(C)$ and let θ be the character afforded by the action of C on the 4-dimensional w-eigenspace of x. We note that $\ker \theta \leq K$. Also $[K,T] \leq \ker \theta$ by Lemma 1.2.10. As $K = C_K(T)[K,T]$, we see that $K = \langle x \rangle \ker \theta$.

By Lemma 2.7.2, T centralizes a Sylow 3-subgroup of K, so that $\langle x \rangle$ is a Sylow 3-subgroup of K. Hence 9 does not divide $|K|$ and 3 does not divide $|\ker \theta|$. We only need to prove that 27 does not divide $[C:\ker \theta]$.

Let $B = C / \ker\theta$. We note that $\bar{x}$, the image of x in B, lies outside B', for $(\det \theta)(\bar{x}) = w^4 \neq 1$. Also $O_{7'}(B) = \langle \bar{x} \rangle$, as $O_{7'}(C) = \langle x \rangle \ker \theta$.

Now $\bar{T}$ centralizes $F(B)$. If $\bar{T}$ is normal in B, then 27 does not divide $|B|$. Thus we may suppose that $\bar{T}$ is not normal in B. Then $E(B) \neq 1$. Let $E = E(B)$.

Now $\bar{x}$ lies outside B', so outside E. Thus $O_{7'}(E) = 1$. As E has Abelian Sylow 7-subgroups, $O_7(E) = 1$. Thus E is simple

As $\theta|_E$ is a faithful complex character of degree 4, E is isomorphic to PSL(2,7)

Now $\bar{T} \leq E$, and $B = E\,N(\bar{T})$. Since 3 divides $|N(\bar{T}) \cap E|$ and 27 does not divide $|N(\bar{T})|$, we see that 27 does not divide $|B|$, as claimed.

Let R be a Sylow 3-subgroup of G which contains x. We know that $|R| = 3^{11}$, and by Lemma 2.5.1, R has an Abelian normal subgroup of index at most 27. We derive a contradiction by showing that this subgroup may be assumed to contain x.

We may suppose that R is represented by monomial matrices. Let D be the subgroup of R which is represented by diagonal matrices. Clearly D is Abelian. As $X|_R$ contains no irreducible constituent of degree 9, $[R:D] \leq 27$. It thus suffices to prove that x lies in D.

As x has only two eigenvalues, $\theta(x) \neq 0$ for any irreducible constituent θ of $X|_R$. As R is represented by monomial matrices and each irreducible constituent of $X|_R$ has degree 1 or 3, x is represented by a diagonal matrix, so x lies in D.

As D is Abelian and 27 does not divide the order of $C(x)$, $|R| \leq 3^5$, contrary to the fact that $|R| = 3^{11}$.

We conclude this section with:

Lemma 4.6.7

49 divides $|G|$.

Section Seven

In this section, we assume that 49 divides $|G|$, and eventually derive a contradiction. Let B be the 5-block of G which contains X. By Lemma 2.8.1, B is invariant under 7-conjugation. Also, by Lemma 2.5.4, X is not 7-rational. The results of this section divide into two cases, depending on whether B contains more than one other character which is 7-conjugate to X. By Lemma 2.5.4, there is at least one other character in B which is 7-conjugate to X.

We assume for the moment that B only contains one other character which is 7-conjugate to X. Let T be a Sylow 7-subgroup of G (we recall that T is elementary Abelian). Then $(X + \overline{X})|_T$ is

rational-valued and for any non-trivial linear constituent , μ, of $X|_T$,a further two algebraic conjugates of μ occur as contituents of $X|_T$.

As $X(1) = 11$, it easily follows that $(X|_T , 1_T) \equiv 2 \pmod 3$ and that $|T| \leq 7^3$ (as algebraically conjugate characters have the same kernel).

Lemma 4.7.1

i) $|T| = 49$.

ii) $C(T) = T$.

iii) $[N(T):T] = 3,6,9$ or 18.

Proof

We first prove that T contains no non-identity element with a fixed-point space of co-dimension 3. Suppose that x is such an element.

As G is simple, there is a conjugate y of x such that $[x,y] \neq 1$. Let $K = \langle x,y \rangle$. As $X(1) = 11$ and x and y each have a fixed-point subspace of dimension 8 , K has a fixed-point subspace of dimension 5 or more . Thus 5 does not divide K .

As x and y do not commute , K does not have a normal Sylow 7-subgroup. As x at most four distinct eigenvalues , x centralizes any 7'-subgroup of G which it normalizes (and so does y) . Thus

$O_{7'}(K) \leq Z(K)$. As K has Abelian Sylow 7-subgroups, $O_7(K) \leq Z(K)$.

Thus $F(K) \leq Z(K)$, so that $E(K) \neq 1$. Let L be a component of K . As $(X|_K, 1_K) \geq 5$, L has a faithful complex character of degree 6 or less . We may write $X|_L = 5\,1_L + \theta$, where θ is an ordinary character of L . We also note that as 7 divides [L:Z(L)] , L has no non- trivial irreducible character of degree less than 3.

As 5 does not divide |L| , there are four possible decompositions of θ to be considered.

Case a)

We assume in this case that $\theta = \theta_1 + \theta_2$ where θ_1 and θ_2 are both irreducible of degree three. We note that $\theta_i^x = \theta_i$ for $i = 1,2$ as x has order 7, and similarly $\theta_i^y = \theta_i$ for $i = 1,2$. Thus each θ_i can be extended to an irreducible character of K (as $K = \langle x,y \rangle$).

As x has the eigenvalue 1 with multiplicity 8 , we may suppose that x lies in $\ker \theta_1$. Thus $[x,y] \leq \ker \theta_1$, so that $K / \ker \theta_1$ is Abelian , contrary to the fact that θ_1 is irreducible of degree 3.

Case b)

In this case ,we assume that $\theta = \theta_1 + 3\,1_L$, where θ_1 is irreducible of degree 3. Then L contains an element with a fixed-point space of dimension 9 as $X|_L = 8\,1_L + \theta_1$ (any involution of L will do).This contradicts Lemma 2.1.6.

Case c)

In this case ,we assume that $\theta = 2\,1_L + \theta_2$,where θ_2 is irreducible of degree 4 .Then $X|_L = \theta_2 + 7\,1_L$.

Let t be any involution of L. Then $\theta_2(t) \equiv 0 \pmod 4$ as $L = L'$. If $\theta_2(t) = 0$,then $X(t) = 7$, contrary to Lemma 2.1.6 .Thus $\theta_2(t) = -4$.

Let u be an element of order 7 in L Then u has the eigenvalue 1 with multiplicity 8 , and three eigenvalues of multiplicity one each .

As $X1_L = 7\,1_L + \theta_2$ and $\theta_2(t) = -4$, t has the eigenvalue 1 with multiplicity 7 on the 8-dimensional fixed-point subspace of u.As the other eigenvalues of u have multiplicity 1 each , t acts as a transvection in any reduction (mod 2) of G ,contrary to Lemma 2.1.7.

Case d)

In this case, we assume that θ is irreducible, and we extend θ to an irreducible character of K. By Lemma 1.2.6, $[K : O_7(K)] \leq 7$. However, as $O_7(K) \leq Z(K)$, $O_7(K) = 1$, for as $X|_K = 5\,1_K + \theta$ and θ is irreducible, any element of $O_7(K)^{\#}$ has at most two eigenvalues, a contradiction as we know that $X + \bar{X}$ assumes a rational value on any element of order 7.

Thus 49 does not divide $|K|$, so that x and y both lie in L. Since $K = \langle x, y \rangle$, we see that $K = L$. Let $R = \langle x \rangle$. Then as L has no normal 7-complement, $[N_L(R) : C_L(R)] = 3$, (for $\theta(x) = 3 + w_1 + w_2 + w_3$, where the w_i are primitive 7-th roots of unity).

As θ is irreducible, but does not assume rational values on R, θ is an exceptional character of K (for the prime 7). Let $M = O_{7'}(C(R))$. Then there is an ordinary irreducible character, say μ, of M, and a sign e such that, for any element, m, of M we have: $\theta(xm) = e(w + w^2 + w^4)\mu(m)$ where w is some primitive 7-th root of unity.

Then $\theta(x) = e\mu(1)(w + w^2 + w^4)$ a contradiction, since we already know that $\theta(x) = 3 + w_1 + w_2 + w_3$, where w_1, w_2 and w_3 are primitive 7-th roots of unity.

Thus T contains no element with a fixed-point space of codimension 3

i) Suppose that $|T| \geq 7^3$. Then we may write $X|_T = \theta_1 + \theta_2 + \theta_3 + 2\,1_T$, where each θ_i is the sum of three non-trivial linear characters which are all algebraically conjugate.

Then $[T:\ker \theta_i] = 3$ for each i, so that $|T| = 7^3$. As $|T| = 7^3$, there is an element, x say, of order 7 in T which lies in both $\ker \theta_1$ and $\ker \theta_2$. Thus x has the eigenvalue 1 with multiplicity 8, which we have shown to be impossible. Thus $|T| = 49$.

ii) We claim first that the trivial character is the only constituent of $X|_T$ which occurs with multiplicity greater than 1, and that it occurs with multiplicity 2.

Now $(X|_T, 1_T) \equiv 2 \pmod 3$. Certainly we know that $(X|_T, 1_T) \neq 8$. Suppose that $(X|_T, 1_T) = 5$. Then we may write

$X|_T = 5\,1_T + 0_1 + 0_2$, where each 0_i is the sum of three algebraically conjugate linear characters.

As T is not cyclic, there is an element of order 3 in $\ker 0_1$, say x. Then x has the eigenvalue 1 with multiplicity 8, a contradiction.

Suppose that $X|_T$ contains some non-trivial linear character with multiplicity greater than 1. Then we have:

$X|_T = 2\,1_T + 0_1 + 2\,0_2$, where each 0_i is the sum of 3 algebraically conjugate linear characters.

As T is not cyclic, there is an element of order 7 in $\ker 0_2$, say x. Then x has the eigenvalue 1 with multiplicity 8, a contradiction.

Thus $X|_T$ contains the trivial character with multiplicity two and 9 other linear characters, each with multiplicity 1. Suppose then that $C(T) \neq T$.

Then C(T) contains an element of order p, where p = 2 or 3. Let y be such an element. By the arguments preceding Lemma 1.5.1, y acts as a transvection in every reduction (mod p) of G (as T is a p'-subgroup of C(y)). This contradicts Lemma 2.1.7. Thus C(T) = T.

iii) As $X|_T$ is not real-valued, not every element of T is conjugate to its inverse within T. Since T is elementary Abelian of order 49, N(T)/T is isomorphic to a subgroup of GL(2,7).

Since no element of N(T)/T can induce an automorphism corresponding to $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ on T, N(T)/T has cyclic Sylow 2-subgroups of order at most 2.

Thus [N(T): T] = 3,6,9 or 18.

Lemma 4.7.2

i) $T \cap T^g = 1$ for all g in G-N(T).

ii) [N(T): T] ≠ 3.

Proof

i) It is sufficient to prove that T is normal in C(v) whenever v is an element of order 7 in T.

Suppose then that v is an element of order 7 in T, but that T is not normal in C(v). Let C = C(v) and let $K = O_{7'}(C)$. Suppose that T does not centralize K.

There is a constituent ,0 say, of $X|_{TK}$ such that $[T,K] \not\leq \ker 0$. By Lemma 1.2.10, $0(1) \geq 7$ .As TK acts on the eigenspaces of v , v has an eigenvalue of multiplicity 7 or more

However , as $X + \overline{X}$ is rational valued on 7-elements , v must have the eigenvalue 1 with multiplicity 7 or more.As $(X|_{\langle v \rangle}, 1_{\langle v \rangle}) \equiv 2 \pmod 3$ v must have the eigenvalue 1 with multiplicity 8 , a contradiction, as in the previous Lemma.

Thus T centralizes K , so that T centralizes F(C). Since T is not normal in C , $E(C) \neq 1$. Let L be a component of C . Then L has no non-trivial complex character of degree less than 3 (for $O_{7'}(C) \leq C(T) = T$ so that $O_{7'}(C) = 1$ and 7 divides $[L: Z(L)]$). Also $Z(L) \leq O_7(L) = 1$, as $L = L'$ and L has Abelian Sylow 7-subgroups . Thus L is simple.

Now v has no eigenvalue of multiplicity 6 or more .As L acts on the eigenspaces of v , L must have a faithful complex character of degree

5 or less . Thus L is isomorphic to PSL(2,7) (as 5 does not divide $|L|$, or alternatively, as $Z(L) = 1$) .

Consequently , each non-linear constituent has degree 3, for L acts on the eigenspaces of v . If $X|_L$ has only one non-linear constituent, then $X|_L = 8\,1_L + 0$, and L contains an involution with a fixed-point space of co-dimension 2 ,contrary to Lemma 2.1.6 .

Thus v has at least 2 eigenvalues of multiplicity 3 or more . Since $X(v)+\bar{X}(v)$ is rational and v has the eigenvalue 1 with multiplicity 5 or less , v has the eigenvalue 1 with multiplicity 2 and, without loss of generality , v has the eigenvalues w^2 , w^4 and w with multiplicity 3 each (where $w = \exp(2\pi i / 7)$).

Let $M = \langle v \rangle \times L$. Then $X|_M = 0_1 + 0_2 + 0_3 + 2\,1_M$, where 0_1 and 0_2 are irreducible of degree 3 and $0_3(v) = 3w$,without loss of generality .

Then there is an element y , of

order 7 in L , such that

$$\theta_1(vy) = 1 + w^5 + w^3$$

(we have assumed ,as we may ,that $\theta_2(v) = 3w^2$) . Thus vy has the eigenvalue 1 with multiplicity 3 or more . In fact, we quickly see that vy has the eigenvalue 1 with multiplicity 5,and the eigenvalues w^3, w^6, w^5 with multiplicity 2 each (since $X(vy) + \bar{X}(vy)$ is rational).

For i = 1,2 ,vy has three distinct eigenvalues in the representation of M affording the character θ_i .Thus θ_i must also be irreducible (for otherwise vy could not have the eigenvalue 1 with multiplicity 5).

Now L contains a dihedral subgroup of order 6 , D say . For $1 \leq i \leq 3$, $\theta_i|_D$ is the sum of the only irreducible character of degree 2 of D and the non-trivial linear character of D . Thus $X|_D$ does not contain any irreducible constituent of multiplicity 4 or more.

Since D is a 7'-subgroup of C(V) ,v acts with minimum polynomial

of degree 3 or less in any reduction (mod 7) of G by Lemma 1.5.1 . This contradicts Lemma 2.1.5 , and so the proof of part i) is complete.

ii) Suppose that [N(T):T] = 3 . Then as T ≤ G', N(T) is a Frobenius group of order 147. Thus C(u) has a normal 7-complement for any element u of order 7 in T . In fact , since T is normal in C(u),for any such u, we see that C(u) ≤ C(T) . We know that C(T) = T ,so that C(u) = T for any element u of order 7 in T.

By Lemma 1.2.7 , G has no faithful irreducible complex character of degree less than 24,a contradiction as X(1) = 11 . Thus [N(T):T] ≠ 3.

Lemma 4.7.3

i) 2^{16} does not divide |G|.

ii) 3^{12} does not divide |G|.

ii) If |C(S)| is even , then 3^{6} does not divide |G|.

Proof

We prove that B contains only one other algebraic conjugate of X. Suppose that this is not the case. As

B contains just one other 7-conjugate of X and B contains five characters, we conclude that B contains 3 other algebraic conjugates of X.

The character table of G must have a fragment of the form :

	1	u	s
X	11	a	1
X_1	11	$\bar{a}$	1
X_2	11	a	1
X_3	11	$\bar{a}$	1
X_4	44	$2(a + \bar{a})$	-1

where X_1 is 7-conjugate to X, and X_2 is algebraically conjugate to X by some Galois automorphism which fixes 7-th roots of unity.

By Lemma 4.2.4,

$$\frac{6|G|}{|C(u)|^2}\left(2\frac{(a^2 + \bar{a}^2)}{11} - 4\frac{(a + \bar{a})^2}{44}\right)$$

is an integer.

As T is Abelian, 7 does not divide $[G:C(u)]$. Since 49 divides $|C(u)|$,

we conclude that $(a - \bar{a})^2$ is an integer divisible by 49.

As $X(u)$ is not rational, we see that $a \neq \bar{a}$. Since $X(u) + \overline{X}(u)$ is rational, there are three uniquely determined non-negative integers, say q, r and s, such that :

$$X(u) = q + r(w+w^2+w^4) + s(w^3 + w^5 + w^6)$$

and $q + 3(r+s) = 11$

where $w = \exp(2\pi i / 7)$.

As $a = X(u)$, we see that

$$(a - \bar{a})^2 = -7(r-s)^2$$

Since $(a - \bar{a})^2$ is divisible by 49 we conclude that 7 divides (r-s).

Since $q + 3(r+s) = 11$, and q, r and s are all non-negative, we conclude that $r = s$. Then we have

$$X(u) = q - r$$

contrary to the fact that $X(u)$ is not rational. This contradiction completes the proof of the assertion that B contains only one other character which is 7-conjugate to X.

i) We claim that X is 2-rational. By Lemma 2.4.2, B is invariant under 2-conjugation. Since B contains only

one other algebraic conjugate of X which is, in fact, 7-conjugate to X , X is fixed by any Galois automorphism which fixes 7-th roots of unity , so is certainly 2-rational.

By Lemma 2.5.1 , 2^{16} does not divide |G|.

ii) By Lemma 2.4.2, B is invariant under any Galois automorphism which fixes exp(2πi / 3), and an argument similar to that above , X is fixed by any such Galois automorphism which also fixes 7-th roots of unity .Hence $X + \overline{X}$ is 3-rational , so that 3^{12} does not divide |G| by Lemma 2.5.2 .

iii) If |C(S)| is even , then B is invariant under algebraic conjugation Thus X must be invariant under every Galois automorphism which fixes 7-th roots of unity, so X is 3-rational, and 3^{6} does not divide |G| by Lemma 2.5.1

We are now in a position to derive a contradiction from the assumption that B contains only one other character that is 7-conjugate to X .

Lemma 4.7.4

B contains at least two other characters which are 7-conjugate to X.

Proof

Under the hypothesis that this Lemma is false, we have the following information :

i) A Sylow 7-subgroup ,T , of G has order 49 and $[G:N(T)] \equiv 1 \pmod{49}$ Also $[N(T):T] = 6, 9$ or 18.

ii) $|G|$ divides $2^{15}.3^{11}.5.7^{2}.11$, and if $|C(S)|$ is even for a Sylow 5-subgroup ,S, of G then $|G|$ divides $2^{15}.3^{5}.5.7^{2}.11$ (we recall also that $|N(S)| = 40$, 60 or 120) .

Case a) : $|N(S)| = 60$

In this case , G contains no element of order 10 ,so $|N(P)| = 55$ for a Sylow 11-subgroup, P, of G.

Now $|G| = 2^{a}.3^{b}.5.7^{2}.11$, where $3 \leq a \leq 15$ (we cannot have a = 2 as N(S) contains an element of order 4 and G is simple) and $2 \leq b \leq 11$ (we cannot have b = 1 , since C(S) contains an element of order 3 which is not conjugate to its inverse ,and G is simple).

By Sylow's theorem ,we have :

1) $2^{a}.3^{b}.7^{2} \equiv 1 \pmod{11}$

2) $2^{a-2}.3^{b-1}.7^{2} \equiv 1 \pmod{5}$.

From 1) , we conclude that $a \equiv 2b + 6 \pmod{10}$, and from 2),we conclude that $a \equiv b-1 \pmod{4}$. Thus a is even and b is odd.

If $b = 3$, then $a \equiv 2 \pmod{20}$ a contradiction ,as $3 \leq a \leq 15$ .If $b = 5$,then $a \equiv 16 \pmod{20}$,contrary to the fact that $3 \leq a \leq 15$.

If $b = 7$, then $a \equiv 10 \pmod{20}$ so that $a = 10$ and

$$|G| = 2^{10}.3^{7}.5.7^{2}.11$$

Thus $[G : T] = 2^{10}.3^{7}.55$,so that $[G:T] = 2^{3}.3^{6} \equiv 1 \pmod{49}$ (we note that $3.2^{4} \equiv -1 \pmod{49}$).

However , $[G : N(T)] \equiv 1 \pmod{49}$, and $[N(T):T] = 6, 9$ or 18 ,so that $[G : T] \equiv 6, 9$ or $18 \pmod{49}$, a contradiction.

If $b = 9$, then $a \equiv 4 \pmod{20}$,so $a = 4$ and $|G| = 2^{4}.3^{9}.5.7^{2}.11$ .Then $[G:T] = 2^{4}.3^{9}.55 \equiv 39 \pmod{49}$,a contradiction , since $[G:T]$ must be congruent to $6,9$ or $18 \pmod{49}$.

If $b = 11$, then $a \equiv 18 \pmod{20}$, contrary to the fact that $3 \leq a \leq 15$ Thus Case a) does not occur.

Case b) : $|N(S)| = 40$

In this case, $|G| = 2^{a} .3^{b} .5.7^{2} .11$, where $3 \leq a \leq 15$ and $1 \leq b \leq 5$ .By Sylow's theorem, we have:

$$2^{a-3} .3^{b} . 7^{2} \equiv 1 \pmod 5$$

so that $a \equiv b+1 \pmod 4$.

Suppose first that $|N(P)| = 55$ for a Sylow 11-subgroup ,P, of G . Then $2^{a} .3^{b} . 7^{2} \equiv 1 \pmod{11}$, so that $a \equiv 2b+6 \pmod{10}$. Then a must be even , and b must be odd.

If $b = 1$,then $a \equiv 18 \pmod{20}$, a contradiction . If $b = 3$, then $a \equiv 12 \pmod{20}$,so that

$$|G| = 2^{12} .3^{3} .5.7^{2} .11 .$$

Then $[G : T] = 2^{12} .3^{3} .55$,so that $[G:T] \equiv -6 \pmod{49}$,a contradiction, as $[G:T] \equiv 6, 9$ or $18 \pmod{49}$.

If $b = 5$, then $a \equiv 6 \pmod{20}$, so that $a = 6$ and

$$|G| = 2^{6} .3^{5} .5.7^{2} .11 .$$

Then $[G:T] \equiv 16 \pmod{49}$,contrary to the fact that $[G:T]$ is congruent to 6,9 or 18 (mod 49).

Thus we may suppose that,in this case, $|N(P)| = 110$.Now we have:

$2^{a-1} \cdot 3^{b} \cdot 7^{2} \equiv 1 \pmod{11}$, so that $a \equiv 2b + 7 \pmod{10}$. We recall that $a \equiv b + 1 \pmod{4}$ in this case. Then a is odd, and b is even.

As 3 divides $|N(T)|$, $b \neq 0$. If $b = 2$ then $a \equiv 11 \pmod{20}$, so that

$$|G| = 2^{11} \cdot 3^{2} \cdot 5 \cdot 7^{2} \cdot 11 .$$

Then $[G : T] = 2^{12} \cdot 3^{3} \equiv -1 \pmod{49}$ a contradiction.

If $b = 4$, then $a \equiv 5 \pmod{20}$, so that $|G| = 2^{5} \cdot 3^{4} \cdot 5^{2} \cdot 7^{2} \cdot 11$. It readily follows that $[G:T] \equiv 19 \pmod{49}$, a contradiction.

Thus case b) cannot occur.

Case c) : $|N(S)| = 120$

In this case, $|G| = 2^{a} \cdot 3^{b} \cdot 5 \cdot 7^{2} \cdot 11$, where $3 \leq a \leq 15$, and $1 \leq b \leq 5$.

By Sylow's theorem,

$$2^{a-3} \cdot 3^{b-1} \cdot 7^{2} \equiv 1 \pmod{5},$$

so that $a \equiv b \pmod{4}$.

Suppose first that $|N(P)| = 55$ for a Sylow 11-subgroup, P, of G. Then

$2^{a} \cdot 3^{b} \cdot 7^{2} \equiv 1 \pmod{11}$, so that $a \equiv 2b + 6 \pmod{10}$. Thus both a and b are even.

If $b = 2$, then $a \equiv 10 \pmod{20}$, so that $|G| = 2^{10}.3^{2}.5.7^{2}.11$. Hence $[G:T] \equiv 24 \pmod{49}$, a contradiction. If $b = 4$, then $a \equiv 4 \pmod{20}$, so that $|G| \equiv 2^{4}.3^{4}.5.7^{2}11$, and we see that $[G : T] = 34 \pmod{49}$, which is a contradiction. Thus $|N(P)| \neq 55$.

Suppose then that $|N(P)| = 110$. Then $2^{a-1}.3^{b}.7^{2} \equiv 1 \pmod{11}$, so that $a \equiv 2b + 7 \pmod{10}$. Hence a and b are both odd.

If $b = 1$, then $a \equiv 9 \pmod{20}$, so that $a = 9$ and $|G| = 2^{9}.3.5.7^{2}.11$. Then $[G:T] \equiv 4 \pmod{49}$, a contradiction. If $b = 3$, then $a \equiv 3 \pmod{20}$, so that $a = 3$ and $|G| = 2^{3}.3^{3}.5.7^{2}.11$. Then $[G:T] \equiv 22 \pmod{49}$, a contradiction. If $b = 5$, then $a \equiv 17 \pmod{20}$, which contradicts the fact that $a \leq 15$.

Thus case c) does not occur, so that none of the possible values for $|N(S)|$ can occur, a contradiction which proves the Lemma.

We may suppose from now on that B contains 2 more irreducible characters which are 7-conjugate to X. Let T be a Sylow 7-subgroup of G.

Lemma 4.7.5

i) 2^{16} does not divide $|G|$

ii) 3^{12} does not divide $|G|$.

iii) If $|C(S)|$ is even, then 3^{6} does not divide $|G|$.

Proof

We first prove that B contains only three characters of degree 11. Suppose that this is not the case .Then B must contain precisely four characters of degree 11 , and one of them ,say 0 , must be 7-rational. The arguments used so far in this thesis may be applied to deduce that 0 cannot be 7-rational, just as we proved in Lemma 2.5.4 that X could not be 7-rational . Thus B can only contain 3 irreducible characters of degree 11.

i) As all irreducible characters of degree 11 in B are 7-conjugate and B is invariant under 2-conjugation, X is 2-rational. By Lemma 2.5.1 , 2^{16} does not divide $|G|$.

ii) As B is invariant under any Galois automorphism which fixes cube roots of unity, and as all characters of degree 11 in B are 7-conjugate, $X + \overline{X}$ must be rational-valued on 3-elements , so that 3^{12} does not divide $|G|$ by Lemma 2.5.2 .

iii) If C(S) has even order, then B is invariant under algebraic conjugation , so that X is 3-rational, and 3^6 does not divide |G| by Lemma 2.5.1 .

Remark

We wish to prove that T has order 49 We first need to consider the possible sets of character degrees in B .

Lemma 4.7.6

The possible sets of character degrees for B are :

i) 11,11,11,66,99.

ii) 11,11,11,264,241.

iii) 11,11,11,924,891.

Proof

As B contains three characters of degree 11 and each character of B has degree congruent to 1 or -1 (mod 5) , there is an integer , x say, such that $x \equiv -1 \pmod 5$ and the degrees for B are : 11,11,11 , x , e(x-33) , where e = 1 or -1.

As x and x - 33 must both divide G and G is simple , it is easy to see that e = 1 .

Case 1 : 11 does not divide x

In this case , $x \equiv 1$ or $-1 \pmod{11}$, as the character of degree x must lie in the principal 11-block (and must be non - exceptional , as the exceptional characters in the principal 11-block lie in the same 5-block) . We recall that $x \equiv -1 \pmod{5}$ and that both x and x-33 divide $|G|$. There are several cases to consider.

Subcase 1 a) : $x = 2^a$

In this case , x-33 is prime to 2, 3, 5 and 11, so that $x-33 = 7^b$. Now as $x \equiv -1 \pmod{5}$,a is even , so that $x \equiv 1 \pmod{11}$, since -1 is not a quadratic residue (mod 11) . Hence $a \equiv 0 \pmod{10}$, so $x-33 \equiv 7 \pmod{8}$.

Now $x-33 \equiv 1 \pmod{5}$,so that b is even . Now however, $7^b \equiv 1 \pmod{8}$, a contradiction .

Subcase 1 b) : $x = 2^a.3^b$

In this case, $x-33 = 3^c.7^d$. If $c > 1$,then $b = 1$, so $a \equiv 2 \pmod{4}$, as $x \equiv -1 \pmod{5}$. Then $x = 2^a.3$,so that $x \equiv 1 \pmod{11}$ and $a \equiv 2 \pmod{10}$ Thus $a \equiv 2 \pmod{20}$ and $a = 2$, since x divides $|G|$.Then $x-33 < 0$, contrary to the fact that x-33 is a character degree. Thus $c = 1$.

Then d is odd , since $3.7^d \equiv -1 \pmod 5$ so that $x-33 \equiv 5 \pmod 8$ and $a = 2$. Thus $x \equiv 1 \pmod{11}$, since -1 is not a quadratic residue (mod 11). Hence also $x - 33 \equiv 1 \pmod{11}$, a contradiction, as $x - 33 = 3.7^d$ and d is odd.

Subcase 1 c) : $x = 2^a .7^b$

In this case, x-33 is prime to 2,3,5 7 and 11 , contrary to the fact that x-33 divides $|G|$.

Subcase 1 d) : $x = 2^a .3^b .7^c$

In this case, $x - 33 = 3^d$, and d is even, as $x - 33 \equiv 1 \pmod 5$. Thus $b = 1$. Now $x - 33 \equiv 1 \pmod{11}$, since 3 is a quadratic residue (mod 11). Consequently 5 divides d , so that 20 divides d (as $3^d \equiv 1 \pmod 5$) , contrary to Lemma 2.1.8.

Subcase 1 e) : $x = 3^a$

In this case, $a \equiv 2 \pmod 4$, since $x \equiv -1 \pmod 5$. Thus 9 cannot divide $x - 33$. Since $a \equiv 2 \pmod 4$, we see that $x \equiv 9 \pmod{16}$, so that 8 divides $x-33$, but 16 does not . We now know that $x-33 = 24.7^b$ for some integer b ,

and $b \neq 0$, since $x-33 \equiv 1 \pmod 5$.

Thus $x \equiv 5 \pmod 7$,a contradiction, as $x = 3^a$,where a is even, but 5 is not a quadratic residue (mod 7).

Subcase 1 f) : $x = 3^a.7^b$

In this case, $x-33 = 2^c.3^d$. If a= 1,then b is odd,as $x \equiv -1 \pmod 5$ Thus $x \equiv -1 \pmod{11}$, as 7 and -1 are not quadratic residues (mod 11) , but 3 is . Then $b \equiv 1 \pmod{10}$,so that b = 1, contrary to the fact that $x > 33$. Thus d = 1.

Now $x-33 \equiv 2 \pmod 7$, so that d is even,since 3 is a quadratic non-residue (mod 7) , but 2 is a residue (mod 7). This contradiction eliminates case 1f).

Subcase 1 g) : $x = 7^a$

As $x \equiv -1 \pmod 5$, a is even .Thus $x \equiv 1 \pmod{11}$,so that $a \equiv 0 \pmod{10}$, contrary to the fact that $x \neq 1$ and 7^{10} does not divide $|G|$.

The elimination of subcase 1g) completes the elimination of case 1.

Case 2 : 11 divides x

Let $x = 11y$. We seek integers y which satisfy :

i) $y \equiv -1 \pmod 5$.

ii) Neither y nor y-3 is divisible by a prime other than 2, 3 or 7.

Subcase 2 a) : $y = 2^a$

In this case , a is even. Also we have : $y-3 = 7^b$ .Now b is also even, as $y-3 \equiv 1 \pmod 5$ .Thus $y \equiv 4 \pmod 8$, so that y = 4 and x = 44 .

However,we proved in the previous Lemma that B contains precisely three characters of degree 11 , so that the solution x = 44 does not lead to a set of valid degrees for b.

Subcase 2 b) : $y = 2^a.7^b$

In this case , y - 3 is prime to 2,3, 5 , 7 and 11, a contradiction ,as y divides |G| and $y \neq 1$ (for we know that $y \equiv -1 \pmod 5$).

Subcase 2 c) : $y = 7^a$

In this case,a is even, since

$y \equiv -1 \pmod 5$. Thus $y \equiv 1 \pmod 8$, so that $y - 3 = 2$ (for 3 does not divide $y - 3$) , a contradiction .

Subcase 2 d) : $y = 2^a.3^b$

If 7 does not divide y-3 in this case, then $2^a.3^b - 3 = 3^c$. Then c is even as $3^c \equiv 1 \pmod 5$,so that b = 1 and $2^a - 1$ is a power of 3 . However, as $3.2^a \equiv -1 \pmod 5$, $a \equiv 3 \pmod 4$, so that $2^a \equiv 2 \pmod 3$, a contradiction.

If 7 divides y-3 in this case,then b is odd , as $y \equiv 3 \pmod 7$ and 3 is not a quadratic residue (mod 7), but 2 is. Thus a is also odd , as $y \equiv -1 \pmod 5$. Since a is odd , 9 cannot divide y-3. Then $y-3 = 3.7^a$. Since $y-3 \equiv 1 \pmod 5$, $a \equiv 1 \pmod 4$. Thus $y \equiv 8 \pmod{16}$,so that a = 3.

We now have :

$$8.3^b = 3(7^a + 1)$$,so that

$$8.3^{b-1} = (7^a + 1).$$

Since 3 does not divide $7^a + 1$, we deduce that b = 1 , so that y = 24.

This value of y leads to the solution x = 264 , x-33 = 231 .

Case 2e) : $y = 3^a$

In this case , a is even , since $y \equiv -1 \pmod 5$. Thus $y-3 \equiv 2 \pmod 4$, and 9 does not divide y-3, so y-3 has the form 6.7^b . Since a is even , 7 cannot divide $3^a - 3$, so that b = 0 and y-3 = 6 . Thus y = 9 , and we have the solution : x = 99 , x-33 = 66.

Subcase 2f) : $y = 3^a.7^b$

In this case , $y-3 = 3^c.2^d$ .Now $3^c.2^d \equiv -3 \pmod 7$, so that c is even. Since $y-3 \equiv 1 \pmod 5$, d is also even . As $y \equiv -1 \pmod 5$, $a \equiv b \pmod 2$. Then $y \equiv 1 \pmod 4$,so that 4 does not divide y-3 ,contrary to the fact that d is even and $d \neq 0$.

Subcase 2 g) : $y = 2^a.3^b.7^c$

In this case, $y-3 = 3^d$. Since $y-3 \equiv 1 \pmod 5$, $d \equiv 0 \pmod 4$. Thus $y \equiv 4 \pmod{16}$, so that a = 2 . Now y has the form 12.7^c ,and we know that $4.7^c - 1 = 3^{d-1}$. Thus $d \equiv 4 \pmod 6$,so that $d \equiv 4 \pmod{12}$ and d = 4 ,as 3^{12} does not divide |G| .

Hence y = 84, and we have the solution x = 924 , x-33 = 891.

In case 2, we have considered every possible prime factorization for y, so that the proof of the Lemma is complete.

Lemma 4.7.7

The character degrees 11,11,11,264,231 cannot occur .

Proof

Suppose that these degrees do occur. We first claim that $|T| \geq 7^3$. Suppose that $|T| = 49$. Then the character of degree 231 lies in a 7-block of defect 1 and is the only character of B that lies in that 7-block of defect 1 , contrary to Lemma 1.2.14, as G contains no element of order 35. Thus $|T| \geq 7^3$. This argument also shows that all of the irreducible characters in B lie in the same 7-block.

We may choose an element ,u say, of T , such that X(u) is not rational. Let X_1 and X_2 be the other characters of B which are 7-conjugate to X . Then we may suppose that $X_1(u) = X(u^2)$, and $X_2(u) = X(u^4)$.

Let $z = X(u) + X_1(u) + X_2(u)$.

We note that, as $X|_T$ is real valued, $(X|_{\langle u \rangle}, 1_{\langle u \rangle}) = (11 + 2z)/7$. Now the character table of G has a fragment of the form :

	1	u	s
X	11	$X(u)$	1
X_1	11	$X(u^2)$	1
X_2	11	$X(u^4)$	1
θ_1	231	y	1
θ_2	264	$(y + z)$	-1

where s is an element of order 5 in G. We note that θ_1 and θ_2 are 7-rational, as B is invariant under 7-conjugation. Thus y is an integer (and is divisible by 7).

Let $r = |X(u)|^2 + |X(u^2)|^2 + |X(u^4)|^2$.

We note that $121 + 2r = 7(X|_{\langle u \rangle}, X|_{\langle u \rangle})$.

Also, by Lemma 4.2.4, we see that :

$$\frac{6|G|}{|C(u)|^2}\left(\frac{r}{11} + \frac{y^2}{231} - \frac{(y+z)^2}{264}\right)$$

is an integer.

Then we see that , as [G:C(u)] is not divisible by 7 ,

$$r + \frac{y^2}{21} - \frac{(y+z)^2}{24} \equiv 0 \pmod{|T|}$$

(We are working here in the 7-adic integers. Since 7 divides y , this is permissible.) . Let y = 7t.

$$\text{Then } r + \frac{7t^2}{3} - \frac{(7t+z)^2}{24} \equiv 0 \pmod{7^3}$$

In particular, we have:

$$r + \frac{7t^2}{3} - \frac{(7t+z)^2}{24} \equiv 0 \pmod{49}.$$

Thus

$$24r + 7t^2 - 14tz - z^2 \equiv 0 \pmod{49}$$

Now 0_1 lies in a 7-block of full-defect , so that we have:

$$[G:C(u)] \frac{0_1(u)}{0_1(1)} \equiv [G:C(u)] \pmod{7}.$$

Since 7 does not divide [G:C(u)] ,we see that $7t/231 \equiv 1 \pmod{7}$, so that $t \equiv 5 \pmod{7}$.

Since 7 divides 11+2z ,we also note that $z \equiv 5 \pmod{7}$.Consequently,

$$7t^2 - 14tz \equiv 21 \pmod{49}$$

Thus $z^2 - 24r \equiv 21 \pmod{49}$.

Now we know that

$$X(u) = a + b(w+\bar{w}) + c(w^2+\bar{w}^2) + d(w^4+\bar{w}^4)$$

where w is some primitive 7th-root of unity and a,b,c and d are non-negative integers such that $a + 2(b+c+d) = 11$.

Also, we have :

$$(a^2 + 2(b^2 + c^2 + d^2)) = (X|_{\langle u \rangle}, X|_{\langle u \rangle})$$

and $a = (X|_{\langle u \rangle}, 1_{\langle u \rangle})$.

Since $121 + 2r = 7(X|_{\langle u \rangle}, X|_{\langle u \rangle})$

and $11 + 2z = 7(X|_{\langle u \rangle}, 1_{\langle u \rangle})$, we see that

$$11 + 2z = 7a$$

and $$121 + 2r = 7(a^2 + 2(b^2 + c^2 + d^2))$$

Thus: $z^2 \equiv (28a+19)^2 \equiv (35a+18) \pmod{49}$

$$24r \equiv 35(a^2 + 2(b^2 + c^2 + d^2)) + 18 \pmod{49}$$

so we have :

$$z^2 - 24r \equiv 35(a - a^2 - 2(b^2 + c^2 + d^2)) \pmod{49}$$

and :

$$2(a^2 + 2(b^2 + c^2 + d^2) - a) \equiv 3 \pmod{7}.$$

Thus we have :

$$(a^2 + 2(b^2 + c^2 + d^2) - a) \equiv 5 \pmod{7}.$$

This equation is symmetric in b, c and d. We handle several cases separately.

Case i) : a = 7 , b = 2.

This case cannot occur, since u acts with minimum polynomial of degree 4 or more in any reduction (mod 7) of G by Lemma 2.1.5, so must have at least four eigenvalues.

Case ii) : a = 7 , b = 1, c = 1

In this case , we have:

$$a^2 + 2(b^2 + c^2 + d^2) - a \equiv 4 \pmod 7 ,$$

so this case cannot occur.

Case iii) : a = 5 , b = 3

Again this case cannot occur, as u must have at least 4 eigenvalues

Case iv) : a = 5, b = 2, c = 1

In this case, we have :

$$a^2 + 2(b^2 + c^2 + d^2) - a \equiv 2 \pmod 7,$$ so this case does not occur.

Case v) : a = 5, b = c = d = 1

In this case, X(u) = 4, which contradicts the assumption that X (u) is not rational.

Case vi) : a = 3 , b = 4

Again this case cannot occur, as u must have at least 4 eigenvalues.

Case vii): a = 3, b = 2, c = 2

In this case,we have :

$a^2 + 2(b^2 + c^2 + d^2) - a \equiv 1 \pmod 7$, so this case does not occur.

Case viii): a = 3, b = 3, c = 1

In this case,we have :

$a^2 + 2(b^2 + c^2 + d^2) - a \equiv 5 \pmod 7$, so that this case might occur.

Case ix): a = 1, b = 5

Again this case cannot occur,as u must have at least 4 eigenvalues.

Case x): a = 1, b = 4, c = 1

In this case,we have :

$a^2 + 2(b^2 + c^2 + d^2) - a \equiv 6 \pmod 7$, so this case does not occur.

Case xi) : a = 1, b = 3, c = 2

In this case,we have :

$a^2 + 2(b^2 + c^2 + d^2) - a \equiv 5 \pmod 7$, so this case might occur.

Case xii) : a = d = 1, b = c = 2

In this case, we have :

$a^2 + 2(b^2 + c^2 + d^2) - a \equiv 4 \pmod 7$, so this case does not occur.

Case xiii) : a = 1, b = 3, c = d = 1

In this case,we have :

$a^2 + 2(b^2+c^2+d^2) - a \equiv 1 \pmod 7$, so that this case does not occur.

This deals (up to symmetry in b , c and d), with every possibility, since a + 2(b+c+d) = 11. We now show that , in fact , neither case viii) nor case xi) can occur.

Case viii): a = 3, b = 3, c = 1

In this case, we have :

z = 5 and r = 41 since

$$11 + 2z = 7a \quad \text{and}$$

$$121 + 2r = 7(a^2 + 2(b^2+c^2+d^2)).$$

The equation we set out to solve was

$$r + \frac{7t^2}{3} - \frac{(7t+z)^2}{24} \equiv 0 \pmod{7^3}$$

We have only shown so far that the values of a,b,c and d in case viii) lead to solutions of :

$$r + \frac{7t^2}{3} - \frac{(7t+z)^2}{24} \equiv 0 \pmod{49}$$

Suppose that t satisfies:

$$41 + \frac{7t^2}{3} - \frac{(7t+5)^2}{24} \equiv 0 \pmod{7^3}.$$

Then :

$$7t^2 - 70t + 959 \equiv 0 \pmod{7^3}.$$

so that : $t^2 - 10t + 137 \equiv 0 \pmod{49}$.

and $(t-5)^2 + 112 \equiv 0 \pmod{49}$,

a contradiction, as $t \equiv 5 \pmod{7}$.

Thus case viii) does not occur .

Case xi) : a = 1, b = 3, c = 2

In this case, z = -2 and r = 34.

Suppose that

$$34 + \frac{7t^2}{3} - \frac{(7t-2)^2}{24} \equiv 0 \pmod{7^3}.$$

Then :

$$7t^2 + 28t + 812 \equiv 0 \pmod{7^3}.$$

Thus $t^2 + 4t + 116 \equiv 0 \pmod{49}$,

so that $(t+2)^2 + 112 \equiv 0 \pmod{49}$,

a contradiction, as $t \equiv 5 \pmod{7}$.

Thus case xi) does not occur, and the proof of this Lemma is complete.

Lemma 4.7.8

The character degrees 11,11,11,891,924 cannot occur .

Proof

Suppose that these degrees do occur. We again claim that $|T| \geq 7^3$. Suppose that $|T| = 49$. Then the character of

degree 924 lies in a 7-block of defect 1 and is the only character of B that lies in that 7-block of defect 1, contrary to Lemma 1.2.14 as G contains no element of order 35. Thus $|T| \geq 7^3$. This argument also shows that all of the irreducible characters in B lie in the same 7-block.

We may choose an element, u say, of T, such that X(u) is not rational. Let X_1 and X_2 be the other characters of B which are 7-conjugate to X. Then we may suppose that $X_1(u) = X(u^2)$, and $X_2(u) = X(u^4)$.

Let $z = X(u) + X_1(u) + X_2(u)$.

We note that, as $X|_T$ is real valued, $(X|_{\langle u \rangle}, 1_{\langle u \rangle}) = (11 + 2z)/7$. Now the character table of G has a fragment of the form:

	1	u	s
X	11	X(u)	1
X_1	11	$X(u^2)$	1
X_2	11	$X(u^4)$	1
θ_1	891	y	1
θ_2	924	(y + z)	-1

where s is an element of order 5 in G .

We note that θ_1 and θ_2 are 7-rational, as B is invariant under 7-conjugation .

Thus y+z is an integer divisible by 7.

Let $r = |X(u)|^2 + |X(u^2)|^2 + |X(u^4)|^2$.

We note that $121 + 2r = 7(X|_{\langle u \rangle}, X|_{\langle u \rangle})$.

Also, by Lemma 4.2.4, we see that :

$$\frac{6|G|}{|C(u)|^2}\left(\frac{r}{11} + \frac{y^2}{891} - \frac{(y+z)^2}{924}\right)$$

is an integer.

Then we see that , as [G:C(u)] is not divisible by 7 ,

$$r + \frac{y^2}{81} - \frac{(y+z)^2}{84} \equiv 0 \pmod{|T|}$$

(We are working here in the 7-adic integers.Since 7 divides y+z , this is permissible.) . Let y+z = 7t.

Then $r + \frac{(7t-z)^2}{81} - \frac{7t^2}{12} \equiv 0 \pmod{7^3}$

In particular, we have:

$$r + \frac{(7t-z)^2}{32} - \frac{7t^2}{12} \equiv 0 \pmod{49}$$

Thus

$$-7t^2 + 7tz + 3z^2 - 2r \equiv 0 \pmod{49}.$$

Now 0_2 lies in a 7-block of full-defect, so that we have:

$$[G:C(u)]\,\frac{0_2(u)}{0_2(1)} \equiv [G:C(u)] \pmod 7.$$

Since 7 does not divide $[G:C(u)]$, we see that $7t/924 \equiv 1 \pmod 7$, so that $t \equiv 6 \pmod 7$.

Since 7 divides $11+2z$, we also note that $z \equiv 5 \pmod 7$. Consequently,

$$7tz - 7t^2 \equiv 7 \pmod{49}$$

Thus $3z^2 - 2r \equiv 42 \pmod{49}$.

Now we know that

$$X(u) = a + b(w+\bar{w}) + c(w^2+\bar{w}^2) + d(w^4+\bar{w}^4),$$

where w is some primitive 7th-root of unity and a, b, c and d are non-negative integers such that $a + 2(b+c+d) = 11$.

Also, we have :

$$(a^2 + 2(b^2 + c^2 + d^2)) = (X|_{\langle u\rangle}, X|_{\langle u\rangle})$$

and $a = (X|_{\langle u\rangle}, 1_{\langle u\rangle})$.

Since $121 + 2r = 7(X|_{\langle u\rangle}, X|_{\langle u\rangle})$

and $11 + 2z = 7\,(X|_{\langle u\rangle}, 1_{\langle u\rangle})$, we see that

$$11 + 2z = 7a$$

and $$121 + 2r = 7\,(a^2 + 2(b^2+c^2+d^2))$$

$$\text{so, } 3z^2 \equiv 3(28a+19)^2 \equiv (7a+5) \pmod{49}$$

$$2r \equiv 7(a^2 + 2(b^2+c^2+d^2)) - 23 \pmod{49}$$

so we have :

$$3z^2 - 2r \equiv -7(a^2 - a - 2(b^2+c^2+d^2)) + 28 \pmod{49}$$

and :

$$-7(a^2 + 2(b^2 + c^2 + d^2) - a) \equiv 14 \pmod{49}.$$

Thus we have :

$$(a^2 + 2(b^2+c^2+d^2) - a) \equiv 5 \pmod{7}.$$

This equation is the same one that occurred in the previous Lemma . As in that case, the only possibilities that might occur are :

Case i): a = 3, b = 3, c = 1 .

Case ii) : a = 1, b = 3, c = 2 .

We again show that neither case can occur.

Case i): a = 3, b = 3, c = 1

In this case, we have :

z = 5 and r = 41 since

$$11 + 2z = 7a \quad \text{and}$$

$$121 + 2r = 7(a^2 + 2(b^2+c^2+d^2)).$$

The equation we set out to solve was

$$r + \frac{(7t-z)^2}{81} - \frac{7t^2}{12} \equiv 0 \pmod{7^3}$$

We have only shown so far that the values of a,b,c and d in case viii) lead to solutions of :

$$r + \frac{(7t-z)^2}{81} - \frac{7t^2}{12} \equiv 0 \pmod{49}$$

Suppose that t satisfies:

$$41 + \frac{(7t-5)^2}{81} - \frac{7t^2}{12} \equiv 0 \pmod{7^3}$$

Then :

$$100 + 41.324 + 7t^2 - 280t \equiv 0 \pmod{7^3}$$

so that :

$$t^2 - 40t + 1912 \equiv 0 \pmod{49},$$

and

$$t^2 - 40t + 1 \equiv 0 \pmod{49}.$$

However, since $t \equiv 6 \pmod 7$, we know that $(t-20)^2 \equiv 0 \pmod{49}$, so that

$t^2 - 40t + 1 = -399 \equiv -7 \pmod{49}$, a contradiction.

Thus case i) does not occur.

Case ii) : a = 1, b = 3, c = 2

In this case, z = -2 and r = 34.

Suppose that

$$34 + \frac{(7t+2)^2}{81} - \frac{7t^2}{12} \equiv 0 \pmod{7^3}.$$

Then :

$$16+136.81 + 7t^2 + 112t \equiv 0 \pmod{7^3},$$ so

that :

$$t^2 + 16t + 1576 \equiv 0 \pmod{49}, \text{ so}$$

that $t^2 + 16t + 8 \equiv 0 \pmod{49}$.

However, since $t \equiv 6 \pmod 7$, we know that $(t+8)^2 \equiv 0 \pmod{49}$, so that

$t^2 + 16t + 8 \equiv -7 \pmod{49}$, a contradiction.

The proof of this Lemma is complete.

Lemma 4.7.9

$|T| = 49$.

Proof

We know that the character degrees for B are 11,11,11,66,99. By Lemma 1.2.14 it is not difficult to see that all characters in B lie in the same 7-block.

Let u be any element of T such that X(u) is not rational.

Let X_1 and X_2 be the other characters of B which are 7-conjugate to X . Then we may suppose that $X_1(u) = X(u^2)$, and $X_2(u) = X(u^4)$.

Let $z = X(u) + X_1(u) + X_2(u)$.

We note that , as $X|_T$ is real valued , $(X|_{\langle u \rangle}, 1_{\langle u \rangle}) = (11 + 2z) / 7$. Now the character table of G has a fragment of the form :

	1	u	s
X	11	X(u)	1
X_1	11	$X(u^2)$	1
X_2	11	$X(u^4)$	1
0_1	66	y	1
0_2	99	(y + z)	-1

where s is an element of order 5 in G .

We note that 0_1 and 0_2 are 7-rational, as B is invariant under 7-conjugation .

Let $r = |X(u)|^2 + |X(u^2)|^2 + |X(u^4)|^2$.

We note that $121 + 2r = 7(X|_{\langle u \rangle}, X|_{\langle u \rangle})$.

Also, by Lemma 4.2.4, we see that :

$$\frac{6|G|}{|C(u)|^2}\left(\frac{r}{11}+\frac{y^2}{66}-\frac{(y+z)^2}{99}\right)$$

is an integer.

Then we see that, as [G:C(u)] is not divisible by 7,

$$r+\frac{y^2}{6}-\frac{(y+z)^2}{9}\equiv 0 \pmod{49}$$

Thus $18r + y^2 - 4yz - 2z^2 \equiv 0 \pmod{49}$

Now $y \equiv 3 \pmod 7$ and $y+z \equiv 1 \pmod 7$, since $\theta_1(u) = y$ and $\theta_2(u) = y+z$.

Then $(y-2z)^2 \equiv 0 \pmod{49}$, so that

$18r - 6z^2 \equiv 0 \pmod{49}$ and :

$$z^2 \equiv 3r \pmod{49}.$$

Now we know that

$$X(u) = a + b(w+\bar{w}) + c(w^2+\bar{w}^2) + d(w^3+\bar{w}^3)$$

where w is some primitive 7th-root of unity and a, b, c and d are non-negative integers such that $a + 2(b+c+d) = 11$.

Also, we have :

$$(a^2 + 2(b^2 + c^2 + d^2)) = (X|_{\langle u\rangle}, X|_{\langle u\rangle})$$

and $a = (X|_{\langle u \rangle}, 1_{\langle u \rangle})$.

Since $121 + 2r = 7(X|_{\langle u \rangle}, X|_{\langle u \rangle})$

and $11 + 2z = 7(X|_{\langle u \rangle}, 1_{\langle u \rangle})$, we see

that

$$11 + 2z = 7a$$

and $$121 + 2r = 7(a^2 + 2(b^2 + c^2 + d^2))$$

so, $$z^2 = (28a + 19)^2 \equiv (35a + 18) \pmod{49}$$

$$3r \equiv 35(a^2 + 2(b^2 + c^2 + d^2)) - 10 \pmod{49},$$

so we have :

$$3r - z^2 \equiv 35(a^2 + 2(b^2 + c^2 + d^2) - a) + 21 \pmod{49}.$$

As $3r - z^2 \equiv 0 \pmod{49}$, we have:

$$(a^2 - a + 2(b^2 + c^2 + d^2)) \equiv 5 \pmod{7}.$$

This equation is the same one that occurred in the previous Lemma . As in that case, the only possibilities that might occur are :

Case i): $a = 3, b = 3, c = 1$.

Case ii) : $a = 1, b = 3, c = 2$.

In case i) , we note that

$$X(u) + X(u^2) + X(u^4) = 5 \text{ ,and :}$$

$$|X(u)|^2 + |X(u^2)|^2 + |X(u^4)|^2 = 41.$$

In case ii) , we note that

$$X(u) + X(u^2) + X(u^4) = -2 \text{ , and :}$$

$$|X(u)|^2 + |X(u^2)|^2 + |X(u^4)|^2 = 34.$$

Let A be any cyclic subgroup of T of order 7 . We will say that A is of <u>type 1</u> if a generator , a say, of A falls into case i) above , of <u>type 2</u> if a generator of A falls into case ii) above, and of <u>type 3</u> if $X|_A$ is rational valued . Any subgroup of order 7 of T has a well-defined type.

Suppose that there are m subgroups of type 1 , n subgroups of type 2 and p subgroups of type 3 . We note that if A is a subgroup of type 3 ,then X(a)= 4 for each non-identity element of A.

We have :

$$\text{i)} \quad m + n + p = \frac{|T| - 1}{6} .$$

$$\text{ii)} \quad 121 + 82m + 68n + 96p = |T|(X|_T, X|_T)$$

$$\text{iii)} \quad 11 + 10m - 4n + 24p = |T|\,(X|_T, 1_T),$$

so that :

$$6m + 6n + 6p \equiv -1 \pmod{|T|}.$$

$$121 + 82m + 68n + 96p \equiv 0 \pmod{|T|}.$$

$$121 + 110m - 44n + 264p \equiv 0 \pmod{|T|}.$$

and

$$28m - 112n + 168p \equiv 0 \pmod{|T|}.$$

Let $|T| = 7^k$. We now have :

i) $\quad 2m - 8n + 12p \equiv 0 \pmod{7^{k-1}}$

ii) $\quad 6m + 6n + 6p \equiv -1 \pmod{7^{k-1}}$

iii) $\quad 10m - 4n + 24p \equiv -11 \pmod{7^{k-1}}$

so :

i) $\quad 2m - 8n + 12p \equiv 0 \pmod{7^{k-1}}$

ii) $- 3 \times$ i) $\quad 30n - 30p \equiv -1 \pmod{7^{k-1}}$

iii) $-5 \times$ i) $\quad 36n - 36p \equiv -11 \pmod{7^{k-1}}$

From the second new equation,

$$180(n-p) \equiv -6 \pmod{7^{k-1}}.$$

From the third new equation,

$$180(n-p) \equiv -55 \pmod{7^{k-1}}.$$

Thus $k-1 \leq 2$ and $k \leq 3$.

Suppose that $k = 3$.

Case i): $n = 0$

If $n = 0$, then $m + p = 57$, and also:

$30p \equiv 1 \pmod{49}$, so that

$p \equiv 18 \pmod{49}$, and $p = 18$,

since m and p are non-negative integers. Thus $m = 39$.

Now $121 + 82m + 96p = 5047 = 49 \times 103$

whereas we know that $|T|$ divides

$121 + 82m + 96p$,

a contradiction. Thus $n \neq 0$.

Case ii): $n \neq 0$

In this case, T has a cyclic subgroup, A say, such that

$$(X|_A, 1_A) = 1.$$

Certainly, this implies that

$$(X|_T, 1_T) \leq 1.$$

On the other hand, $X|_T$ is real-valued,

so that $(X|_T, 1_T)$ is odd, as $X(1) = 11$.

Thus $(X|_T, 1_T) = 1$.

We now have:

$$11 + 10m - 4n + 24p = |T| = 343 .$$

$$m + n + p = 57.$$

Then $14n - 14p - 11 = 227$, so that

$$n - p = 17.$$

This contradicts the earlier equation

$$30n - 30p \equiv -1 \pmod{49}.$$

Thus $|T| \neq 343$, so that $|T| = 49$.

Lemma 4.7.10

i) 27 divides $|G|$.

ii) If $C(S)$ has order 10, then 81 divides $|G|$.

Proof

Let θ denote the character of degree 99 in B .

a) If 3 divides $|C(S)|$, then for an element s of order 5 in S and an element x of order 3 in $C(S)$, $\theta(sx) \neq 0$, so that θ does not lie in a 3-block of defect 0 of B .Thus 27 divides $|G|$.

b) Suppose that $|C(S)| = 10$, but that 81 does not divide $|G|$. If 27 divides $|G|$, then θ lies in a 3-block of defect 1, and is the only character of B which

lies in such a 3-block (for the degrees in B are : 11,11,11, 66,99) , contrary to Lemma 1.2.14 (as G contains no element of order 15). Thus we may suppose that 27 does not divide $|G|$.

Let θ_1 be the character of degree 66 in B.Then θ_1 lies in a 3-block of defect 1 and is the only character of B which lies in such a 3- block , contrary to Lemma 1.2.14 ,as above (for 9 divides $\theta_1(1)$, so 9 must divide $|G|$).

Lemma 4.7.11

G does not exist.

Proof

We may suppose that 2^{11} divides $|G|$ Then $|G|$ is of the form:

$$2^a.3^b.5.7^2.11 \quad \text{,where}$$

i) $11 \leq a \leq 15$.

ii) $3 \leq b \leq 11$.

iii) If $|C(S)|$ is even, then $3 \leq a \leq 5$.

iv) If $|C(S)| = 10$, then $4 \leq a \leq 5$.

v) For a Sylow 11-subgroup, P say, of G, we know that $|N(P)| = 55$ or 110 and $[G:N(P)] \equiv 1 \pmod{11}$.

vi) For a Sylow 5-subgroup, S say, of G, we know that $|N(S)| = 40, 60$ or 120

and $[G:N(S)] \equiv 1 \pmod{11}$.

We consider several cases:

Case a) : $|C(S)| = 10$, $|N(P)| = 110$

In this case, a is odd, because

$2^{a-1} \cdot 3^{b} \cdot 7^{2} \equiv 1 \pmod{11}$.

Since $2^{a-3} \cdot 3^{b} \cdot 7^{2} \cdot 11 \equiv 1 \pmod{5}$, we see that b is even . In this case , we we know that $4 \leq b \leq 5$, so $b = 4$.

Since $2^{a-1} \cdot 3^{4} \cdot 7^{2} \equiv 1 \pmod{11}$, we conclude that $a \equiv 5 \pmod{10}$. Since $2^{a-3} \cdot 3^{4} \cdot 7^{2} \equiv 1 \pmod{5}$, we deduce that $a \equiv 1 \pmod{4}$. Thus $a \equiv 5 \pmod{20}$, a contradiction , as $11 \leq a \leq 15$.

Case b) : $|C(S)| = 10$, $|N(P)| = 55$

In this case, a is even, since we have: $2^{a} \cdot 3^{b} \cdot 7^{2} \equiv 1 \pmod{11}$. Also, b is odd, since $2^{a-3} \cdot 3^{b} \cdot 7^{2} \equiv 1 \pmod{5}$

Since $4 \leq b \leq 5$ in this case, $b = 5$.

As $2^{a} \cdot 3^{5} \cdot 7^{2} = 1 \pmod{11}$, $a \equiv 6 \pmod{10}$ a contradiction , as $11 \leq a \leq 15$.

Case c) : $|C(S)| = 30$, $|N(P)| = 55$

In this case, a is even ,since

$2^a .3^b .7^2 \equiv 1 \pmod{11}$. Thus b is even,

since $2^{a-3} .3^{b-1} \equiv 1 \pmod{5}$.

Thus b = 4 ,as $3 \leq b \leq 5$ in this case.

Then $a \equiv 4 \pmod{10}$ since we know that

$$2^a .3^4 .7^2 \equiv 1 \pmod{11}.$$

Also ,$a \equiv 0 \pmod{4}$,since we know that

$$2^{a-3} .3^3 .7^2 \equiv 1 \pmod{5}.$$

Thus $a \equiv 4 \pmod{20}$,a contradiction,

since $11 \leq a \leq 15$.

Case d) : $|C(S)| = 30$, $N(P) = 110$

In this case,a is odd ,since

$$2^{a-1} .3^b .7^2 \equiv 1 \pmod{11}.$$

Thus b must be odd,as

$$2^{a-3} .3^{b-1} . 7^2 \equiv 1 \pmod{5}.$$

If b = 3, then $a \equiv 3 \pmod{10}$

and $a \equiv 3 \pmod{4}$,which contradicts

the fact that $11 \leq a \leq 15$.

If b = 5 ,then $a \equiv 7 \pmod{10}$,

a contradiction, as $11 \leq a \leq 17$.

Case e) : $|C(S)| = 15$

In this case, $|N(P)| = 55$, since G contains no element of order 10.

Thus we have:

i) $2^{a} .3^{b} .7^{2} \equiv 1 \pmod{11}$.

ii) $2^{a-2} .3^{b-1} .7^{2} \equiv 1 \pmod{5}$.

From the first equation, we have:

i') $a \equiv 2b + 6 \pmod{10}$.

From the second equation, we have:

ii') $a \equiv b - 1 \pmod{4}$.

Hence a is even, and b is odd. We also know that $3 \leq a \leq 11$ and that $11 \leq a \leq 15$.

If $a = 12$, then $b \equiv 3 \pmod{5}$ and $b \equiv 1 \pmod{4}$, a contradiction as $3 \leq b \leq 11$.

If $a = 14$, then $b \equiv 4 \pmod{5}$ and $b \equiv 3 \pmod{4}$, a contradiction as $3 \leq b \leq 11$.

This contradiction completes the proof of Lemma 4.7.9 , and so completes the proof of the main theorem of this thesis.

REFERENCES

[1] ASCHBACHER,M. "Finite Groups With a Proper 2-generated Core"

[2] ASCHBACHER,M and HALL,M. "Groups Generated By a Class of Elements of Order 3", J.Algebra 24, 1973

[3] BLICHFELDT,H.F.,"Finite Collineation groups", University of Chicago press, 1971.

[4] BRAUER,R.,"On Groups Whose Order Contains a Prime Number to the First Power" 1,11, Am. J. Math 64, 1942.

[5] BRAUER,R., "Uber Endliche Lineare Gruppen von Primzahlgrad",Math. Annalen 169, 73.

[6] COLLINS,M.J.,"Some Problems in the Theory of Finite Insoluble Groups", D.Phil.Thesis, Oxford, 1969.

[7] DORNHOFF,L. "Group Representation Theory, Parts A and B" Marcel Dekker Inc., New York, 1972.

[8] FEIT,W.,"Groups With a Faithful Representation of Degree Less Than p-1",Trans Amer. Math. Soc., 112,1964.

[9] FEIT,W.,"On Finite Linear Groups in Dimension at Most 10", Proceedings of the Utah Conference in Group Theory.

[10] FEIT, W.," The Current Situation in Finite Simple Groups", Actes du Congres International des Mathematiciens, Nice 1970.

[11] FEIT, W.," Representations of Finite Groups", (mimeographed notes) Maths. Dept, Yale University

[12] FEIT, W. and THOMPSON, J.G.,"Groups Which Have a Faithful Representation of Degree Less Than $\frac{1}{2}(p-1)$", Pacific J.Maths. 11,1962.

[13] GLAUBERMAN, G.,"Solvable Signalizer Functors in Finite Groups".

[14] GORENSTEIN, D.," Finite Groups", Harper and Row, 1968.

[15] GORENSTEIN, D. and HARADA, K. "Finite Groups of Sectional 2-rank at Most 4", in " Finite Groups '72", Proceedings of the Gainsville Conference.

[16] HAYDEN, S.,(1963) "On Finite Linear Groups Whose Order Contains a Prime Larger Than the Degree," Ph D. dissertation, Harvard University.

[17] HUFFMAN, W.C.,"Linear Groups Containing an Element With an Eigenspace of Codimension 2".

[18] HUFFMAN, W.C. and WALES, D.B.," Linear Groups of Degree n Containing an Element With Exactly n-2 equal eigenvalues", Linear and Multilinear Algebra,3, 1975.

[19] LEON, J.S., Doctoral Thesis, California Institute of Technology.

[20] LINDSEY, J.H.," Linear Groups or Degree 6" Can. Jour. Math. ,23,1971.

[21] MITCHELL, H.H.,"Determination of all Primitive Collineation Groups in More Than Four Variables Which Contain Homologies", Am. J.Math, 36, 1914.

[22] POWELL, M.B. and HIGMAN G." Finite Simple Groups", Academic Press, 1971.

[23] RIGBY, J.F.," Primitive Linear Groups Containing a Normal Nilpotent Subgroup Larger Than the Centre". J. London Math. Soc. 35, 1960.

[24] SHULT, E., "On Groups Admitting Fixed-point Free Abelian Operator Groups ",Illinois J. of Math. 9,1965.

[25] SIBLEY, D.A.," Certain Finite Linear Groups of Prime Degree", J. of Algebra 32, 1974.

[26] SIBLEY, D.A.,"Finite Linear Groups With a Strongly Self-centralizing Sylow subgroup I ,II. "
Journal of Algebra, 36, 1975.

[27] STINGL, V. "Endliche Einfache Component-Type Gruppen, Dern Ordnung Nicht Durch 2^{11} Teilbar Ist", Doctoral Dissertation, Mainz, 1976.

[28] WALES, D.B., "Finite Linear Groups of Degree Seven II" Pacific J. of Math. 34, 1970.

[29] WALES, D.B.,"Linear Groups of Degree n Containing an Involution With Two Eigenvalues -1, II."
J. of Algebra, 53,1978.

[30] YOSHIDA, T.,Notes on transfer.