THE UNIVERSITY OF WARWICK

University of Warwick institutional repository: http://go.warwick.ac.uk/wrap

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

http://go.warwick.ac.uk/wrap/74306

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

Please scroll down to view the document itself.

Please refer to the repository record for this item for information to help you to cite it. Our policy information is available from the repository home page.

RADICALS OF GROUP ALGEBRAS

AND

PERMUTATION REPRESENTATIONS OF SYMPLECTIC GROUPS

by

ROBERT JOHN CLARKE

submitted in partial fulfilment of the requirements for the degree of Ph.D. at the University of Warwick.

July, 1969.

ABSTRACT

In part A we consider three separate problems concerned with the radical of the group algebra of a finite group over a field of characteristic p dividing the order of the group. In Section I we characterise group-theoretically those soluble groups for which the radical of the centre of the group algebra is an ideal of the group algebra. In Section II we find a canonical basis for the radical of the centre of the group algebra of a finite group. In Section III we give an algorithm for determining the radical of the group algebra of a p-soluble group. We evaluate the result for groups of p-length one and prove that the exponent of the radical in this case is the same as for a Sylow p-subgroup. We show by examples that no similar result holds in the general case.

In part B we quote a conjecture of J. A. Green's on characters of Chevalley groups and prove

Theorem A (i) If the conjecture holds then, excepting for each r at most a finite number of values of q, the group $PSp(2^{r+1},q)$ has no multiply transitive permutation representations for $r > 1$.

(ii) $PSp(4,q)$ has no multiply transitive permutation representations for $q > 2$, regardless of the conjecture.

PREFACE

This thesis is in two disjoint parts, part A and part B. Therefore they are treated as two separate theses, each having a separate introduction and a separate body of references. Any resemblence between the two parts is purely coincidental.

The work contained here was done during the years 1966 to 1969, under the supervision of Professor J. A. Green. I should like to express my gratitude to Professor Green for his help and advice, without which this thesis, far from being completed, could not even have been begun. I should also like to thank Mr. S. W. Dagger for several helpful conversations.

While preparing this thesis I was supported by a Commonwealth Scholarship. I should like to thank the British Council for their generosity in providing this scholarship.

All results here not attributed to anyone else are original, with the exceptions of Lemmas 1 and 11 of Part B, whose origins are lost in the mists of antiquity. §2 and §3 of B are wholly derivative.

CONTENTS

PART A

RADICALS OF GROUP ALGEBRAS

PART A

RADICALS OF GROUP ALGEBRAS

Introduction.

In this part we consider three fairly separate problems concerned with the radical of the group algebra of a finite group over a field of non zero characteristic p dividing the order of the group. In Section I. we characterise group-theoretically those soluble groups for which the radical of the centre of the group algebra is an ideal of the group algebra. So we are characterising a certain class of groups, albeit a very restricted class, by a purely algebra-theoretic property of their group algebras. This is an extension of the work of D. A. R. Wallace in the same direction, in particular of his papers [11] and [12]. The results of this section are to appear in the Journal of the London Mathematical Society.

In Section II. we consider the radical of the centre of the group algebra of any finite group and find a basis for it consisting of elements of special type. We relate the radical of the centre to that of certain ideals of the centre, associated with p-subgroups of the group, which appear in the work of J. A. Green and A. Rosenberg. Unfortunately we have been unable to use this canonical basis to say much about the stucture of the radical of the centre.

In Section III. we give an "algorithm" for determining the radical of the group algebra of a p-soluble group in terms of the radical for groups of smaller p-length. We evaluate the result in the case of p-length one and prove a result on the exponent of the radical in this case. The corresponding result is not true for groups of p-length more than one, and indeed it is difficult to conjecture what the correct result might be. For the case of a non soluble group, of course, the situation seems impossible. There is almost no information as to what the radical might be in such a case. The methods of Section III, depending as they do on series of normal subgroups, are of little use.

Theorem 1. of Section III. has appeared in similar form in my dissertation for the degree of M.Sc. at this University.

Notation.

Through this part p denotes a fixed prime, k an algebraically closed field of characteristic p, C the complex field and G a finite group. kG and CG are the group algebras of G over k and C respectively and $\Lambda = \Lambda(G)$ is the centre of kG.

The standard notation of group and representation theory is used. For example G' denotes the derived group of G and Z(G) the centre of G. All kG modules are left kG modules. In accordance with this convention, maps are written on the left,

all transversals are left transversals and the symbol x^y means yxy^{-1}, for x and y in a group G.

If $H < G$ and L is a kH module, L^G is the induced module $kG \otimes_{kH} L$. If K is a kG module, $K|_{kH}$ is the restriction of K to kH.

Definition. The radical of a finite dimensional k-algebra A, radA, is defined to be the maximal nilpotent ideal of A.

Since A is finite dimensional, radA is also the intersection of the kernels of the irreducible representations of A. We put for brevity

$N = N(G) = \text{rad}(kG)$ and

$M = M(G) = \text{rad}\Lambda(G)$.

Any more specialised notation used will be defined as it occurs.

Section I.

On the Radical of the Centre of a Group Algebra

In this section we consider the radical of the centre of the group algebra of a finite group over a field of non zero characteristic, and characterise those soluble groups for which this radical is an ideal of the group algebra. We shall use R. Brauer's theory of blocks of modular characters, for which we refer the reader to [3] Chapter XII.

As always, p is a fixed prime, k an algebraically closed field of characteristic p and G a finite group. We shall assume throughout this section that $p||G|$. N is the radical of kG, Λ the centre of kG and M its radical.

Definition. Let J be the class of finite groups G for which $p||G|$ and $kG.M = M = M.kG$.

Our aim is to classify group-theoretically the p-soluble groups contained in J.

1. Subsidiary Lemmas

The following result is basic:

Lemma 1. Let $H \Delta G$, $p\nmid|H|$ and $e = \sum_{h\in H} h/|H| \in kG$. Then

$kGe \cong k(G/H)$ under the isomorphism

$$\theta: (\sum_{g\in G} \lambda_g g)e \longrightarrow \sum_{g\in G} \lambda_g (gH).$$ Moreover,

$\theta(Ne) = N(G/H)$.

Proof. θ is well defined and is easily seen to be an

isomorphism of algebras. Hence $\theta(\mathrm{rad}(kGe)) = N(G/H)$. We therefore have to prove that $Ne = \mathrm{rad}(kGe)$. Now e is clearly a central kG idempotent. Hence $kG \cong kGe \oplus kG(1-e)$ as algebras. Thus

$$kG.\mathrm{rad}(kGe) = kGe.\mathrm{rad}(kGe) \oplus kG(1-e).\mathrm{rad}(kGe)$$
$$= \mathrm{rad}(kGe) = \mathrm{rad}(kGe).kG.$$

Therefore rad(kGe) is a nilpotent ideal of kG, and so $\mathrm{rad}(kGe) \subset N \cap kGe = Ne$. But Ne is a nilpotent ideal of kGe. Hence $Ne \subset \mathrm{rad}(kGe)$. This proves the result.

Lemma 2. Let e be a primitive central idempotent of kG. If the block kGe contains n ordinary irreducible characters then

$$\dim_k Me = n - 1.$$

If G has r ordinary irreducible characters and t blocks then

$$\dim_k M = r - t.$$

Proof. Let E be the central idempotent of CG corresponding to e in the sense of [3] page 615. Decompose E into primitive central idempotents: $E = E_1 + \ldots + E_n$. The number of summands equals the number of ordinary irreducible characters belonging to kGe.

Now $Z(CG)E = Z(CG)E_1 \oplus \ldots \oplus Z(CG)E_n$ and each $Z(CG)E_i$ is a simple abelian algebra over C and therefore has C-dimension 1. Thus $\dim_k \Lambda e = \dim_C Z(CG)E = n$. Now, by [3] page 607, $\Lambda e/Me \cong k$. Thus $\dim_k Me = \dim_k \Lambda e - 1 = n - 1$.

The second part follows immediately from the remark that each

ordinary irreducible character belongs to exactly one block of kG.

Lemma 3. Let e be a central idempotent of kG and suppose $M = Me$. Then $N = Ne$.

Proof. Decompose $1-e$ into primitive central idempotents: $1-e = e_1 + \ldots + e_n$. Then

$0 = M(1-e) = Me_1 \oplus \ldots \oplus Me_n$. Hence $Me_i = 0$ for all i. Now by Lemma2. this means that each block kGe_i contains exactly one ordinary irreducible character, and is therefore a block of defect zero (see [3] page 611). Hence $Ne_i = 0$ for all i. Thus $N(1-e) = Ne_1 \oplus \ldots \oplus Ne_n = 0$. This proves the lemma.

Lemma 4. Let $G \in J$ and write $\sigma = \sum_{g \in G'} g \in kG$. Then for all $a \in M$, $g \in G'$ we have $ag = a$ and $M \subset kG\sigma$.

If $p \mid |G'|$ then $M = kG\sigma$.

If $p \nmid |G'|$ then $e = \sigma/|G'|$ is an idempotent and $M = \mathrm{rad}(kGe) = Ne$.

Proof. Let $x,y \in G$, $a \in M$.

$$ax^{-1}y^{-1}xy = y^{-1}ax^{-1}xy, \text{ as } ax^{-1} \in M.kG = M \subset \Lambda,$$
$$= y^{-1}ay$$
$$= a, \text{ as } a \in M \subset \Lambda.$$

Therefore $ag = a$ for all $g \in G'$. Hence $a \in kG\sigma$.

If $p \mid |G'|$, $\sigma^2 = 0$. Hence $\sigma \in N \cap \Lambda = M$. Therefore $M = kG\sigma$.

If $p \nmid |G'|$ we have $M \subset kGe$. Now clearly kGe is central in kG and so $M = \mathrm{rad}(kGe) = Ne$.

Corollary. If $G \in J$ and $p \nmid |G'|$ then $N = M$.

Proof. By the Lemma $M = Ne$ and hence $Me = Ne^2 = Ne$. Hence, by Lemma 3, $M = Ne = N$.

Lemma 5. If $G \in J$ and $H \Delta G$ then either $G/H \in J$ or $p \nmid (G:H)$. Moreover if $p \mid |H|$ then $G' \subset H$.

Proof. (1). Suppose $p \nmid |H|$ and write e as in Lemma 1. We have an isomorphism θ between kGe and $k(G/H)$.

$$\begin{aligned} \mathrm{rad}(Z(kGe)) &= \mathrm{rad}(Z(kG)e) \\ &= \mathrm{rad}(\Lambda e) = Me. \end{aligned}$$

Hence $kGe.\mathrm{rad}(Z(kGe)) = kGe.Me$

$= Me$. Using θ we obtain

$k(G/H).M(G/H) = M(G/H)$. Thus $G/H \in J$.

(2). Suppose $p \mid |H|$. Then $\tau = \sum_{h \in H} h$ is central in kG and $\tau^2 = 0$. Thus $\tau \in M$. Therefore $\tau = \tau g = \sum_{h \in H} hg$ for all $g \in G'$. Thus $g \in H$ and $G' \subset H$. But then G/H is abelian, so the result follows.

The following results of D. A. R. Wallace are important for our classification:

Theorem 1. ([11] page 128). If G is a finite group, P a Sylow p-subgroup of G and $|P| = p^a$ then $\dim_k N(G) \geq p^a - 1$, equality holding if and only if P has a normal complement H and G is a Frobenius group with kernel H.

Theorem 2. ([12] page 103). Let G be a finite group with

order divisible by p. Then N = M if and only if either

(1) G is abelian or

(2) if G has Sylow p-subgroup P then G'P is a Frobenius group with kernel G'.

Lemma 6. If G is a finite group such that $\dim_k M = 1$ then $\dim_k N = 1$ and G is 2-nilpotent. Also $|G| = 2n$ with n odd.

Proof. Let $\chi_1, \ldots, \chi_r$ be the ordinary irreducible characters and $\varphi_1, \ldots, \varphi_s$ be the modular irreducible characters of G and suppose G has t blocks. Then $t \leq s \leq r$ and by Lemma 2., $1 = \dim_k M = r - t$. Now if $s = r$, every block of G has defect zero and so $p \nmid |G|$. But then $M = 0$, contradiction. Hence $s = t = r - 1$.

Thus one block, say B_1, contains one modular character φ_1 and two ordinary characters χ_1 and χ_2, while B_i for $i > 1$ contains one modular character φ_i and one ordinary character χ_{i+1}. These latter blocks have defect zero and therefore cannot contain the trivial character. Hence φ_1 is the trivial modular character and χ_1 is the trivial ordinary character.

Now for all p-regular elements g of G,

$$\begin{aligned} \chi_2(g) &= z\varphi_1(g) \\ &= z\varphi_1(1) \\ &= \chi_2(1), \end{aligned}$$

where z denotes the degree of χ_2. Thus if Z is the CG module with character χ_2, L = kerZ contains all of the p-regular

elements of G. So G/L is a p-group, which implies that $G' \neq G$. Hence G has a non trivial ordinary one dimensional character. Such a character cannot be in a block of defect zero and so must be χ_2. Hence $z = 1$.

Now $\dim_k N = (1+z^2) - 1 = 1$. The remainder of the Lemma now follows from Theorem 1.

2. The Discussion of J

Lemma 7. If $G \in J$ then $G' \neq G$.

Proof. Suppose $G = G'$. Then by Lemma 4, $\dim_k M = 1$. But then by Lemma 6, G is 2-nilpotent and so $G' \neq G$, contradiction.

Lemma 8. A group G with a non trivial normal p-subgroup is in J if and only if one of the following conditions is satisfied:

(1) G is abelian or

(2) G is an extension of an elementary abelian p-group P by an abelian p'-group H acting transitively on $P-\{1\}$, every element of H either acting fixed point free on $P-\{1\}$ or centralising P, or

(3) G is an extension of a 2-group P by an abelian group H of odd order such that $G' = Z(P)$ has order 2.

Proof. (a). The necessity of the conditions:

Let $G \in J$ have a normal p-subgroup Q. If $G' = \{1\}$ we have case (1). Suppose $G' \neq \{1\}$. By Lemma 5, $G' \subset Q$ Hence G has a normal Sylow p-subgroup P.

Let $x \in Z(P)-\{1\}$ and write $n = (G:C_G(x))$. Let α be the

conjugacy class sum of x in G. Now Z(P) is characteristic in P and hence normal in G, so $N(Z(P)) \subset N(G)$. Thus $1-z \in N$ for all $z \in Z(P)$. Hence $n.1 - \alpha = \Sigma(1-z) \in N$, sum taken over all conjugates z of x in G. Also $n.1 - \alpha$ is in Λ. Hence $n.1 - \alpha$ is in M. By Lemma 4. we have that for all $g \in G'$, $ng - \alpha g = n.1 - \alpha$. Now as $P \subset C_G(x)$, $p \nmid n$. Comparing coefficients, it follows that for all $g \in G' - \{1\}$, g is conjugate in G to x. Thus $g \in Z(P)$, so that $G' \subset Z(P)$. But x is conjugate to an element of G', so $x \in G'$. This is true for every non identity element of Z(P), so $G' = Z(P)$.

We also know that $Z(P)-\{1\}$ consists of one conjugacy class in G. Hence Z(P) is elementary abelian.

Write $|Z(P)| = p^r$. We have three cases:

I. Suppose $p^r = 2$. As $P \Delta G$, P has a complement H. H is abelian, for $H \cong G/P$ is a homomorphic image of G/G'. Case (3) holds.

II. Suppose $p^r > 2$ and $Z(P) = P$. Then P is elementary abelian. Let H be a complement to P in G and suppose there is a y in H such that y does not centralise P. Write $n = (P:C_P(y))$. Since $G' \subset P$ we have that the conjugacy class sum of y in G is of form $\beta = y(1+x_2+ \ldots +x_n)$; $x_i \in P$.

Since $P \Delta G$, $1-x_i \in N(G)$ for all i. Thus $y(1-x_i) \in N$ and so $ny - \beta \in N$. Since $p|n$ this means that $\beta \in N$. As $\beta \in \Lambda$, $\beta \in M$. Then for all z in P, Lemma 4 shows that $\beta = \beta z$. Comparing

coefficients of z on each side gives that $z = x_i$ for some i. Thus $\beta = \sum_{z \in P} yz$. Therefore $n = p^r$ and y centralises no element of P except 1. This is case (2).

III. Suppose $p^r > 2$ and $Z(P) \neq P$. Consider $X = \bigcup_{x \in Z(P)-\{1\}} C_G(x)$. If $x \in Z(P)-\{1\}$ the conjugates of x are just the elements of $Z(P)-\{1\}$ and so $(G:C_G(x)) = p^r-1$. Thus

$$|X| < \sum_{x \in Z(P)-\{1\}} |C_G(x)|$$

$$= (p^r-1)|G|/(p^r-1)$$

$$= |G|.$$

Therefore $X \neq G$ and there is a y in G centralising no element of $Z(P)-\{1\}$.

Put $n = (G:C_G(y))$. As $G/Z(P)$ is abelian, the conjugacy class sum of y is of form $\beta = y(1+x_2+ \ldots +x_n)$; $x_i \in Z(P)$ for all i. Thus $n \leq p^r$. Now we already have that $C_P(y) \cap Z(P) = \{1\}$. Hence

$$|C_P(y).Z(P)| = |C_P(y)|.|Z(P)|$$

$$\geq |P|/p^r.p^r$$

$$= |P|.$$

Therefore $C_P(y).Z(P) = P$. However

$$C_P(y) = C_P(y)/C_P(y) \cap Z(P)$$

$$\cong C_P(y).Z(P)/Z(P) \text{ is abelian, for } P' \subset G' = Z(P).$$

Thus P is abelian, contradiction.

We have now shown that case III does not occur and that the conditions of the Lemma are necessary. We now show their sufficiency.

(b). If (1) holds, clearly $G \in J$.

Suppose (2) holds. $G = PH$, where P is a Sylow p-subgroup of G and H is an abelian p'-group, every element of which acts either trivially or fixed point free on $P-\{1\}$. We may assume G is non abelian, and then $G' = P$.

If $x \in (P-\{1\})^{Z(G)}$, the conjugacy class sum of x is

$$ma = m\sum_{z\in P-\{1\}} z, \quad m \in Z(G).$$

If $x \in G-(P \cup Z(G))$, $(G:C_G(x)) = |P|$ and the conjugacy class sum of x is $\sum_{z\in P} xz = x(1+a)$.

If $x \in Z(G)$ then x is a p-regular element of G. A basis for Λ therefore consists of the elements

(i) m; $m \in Z(G)$,

(ii) $ma = m\sum_{z\in P-\{1\}} z$, $m \in Z(G)$,

(iii) $m(1+a)$; $m \in H-Z(G)$.

A basis for $N(G)$ consists of elements $m(1-z)$, $m \in H$, $z \in P-\{1\}$. One easily calculates that a basis for $M = N \cap \Lambda$ consists of elements $m(1+a)$; $m \in H$. Hence clearly $M = kG.M$ and $G \in J$.

Suppose (3) holds. $G = PH$, where $P \triangle G$ is a 2-group and H an abelian group of odd order such that $G' = Z(P)$ has order 2. Put $Z(P) = \{1,z\}$. If $x \notin Z(G)$, $(G:C_G(x)) = 2$ and the conjugacy class sum of x is $x(1+z)$. Λ is therefore spanned by elements x; $x \in Z(G)$ and $x(1+z)$; $x \notin Z(G)$.

A basis for $N(G)$ consists of elements $m(1-x)$; $m \in H$,

$x \in P-\{1\}$. Hence $M = N \cap \Lambda$ is spanned by elements $g(1+z)$; $g \in G$. Thus clearly $M = kG.M$ and $G \in J$. This completes the proof.

Corollary. A p-group P is in J if and only if either P is abelian or $P' = Z(P)$ has order 2.

Lemma 9. If $G \in J$ is p-soluble then G has p-length one.

Proof. By definition, $p||G|$. If G is simple, $p = |G|$ and the result is clear. Suppose G is not simple and induce on the order of G. Let H be a minimal normal subgroup of G. As G is p-soluble, H is either a p-group or a p'-group. If H is a p-group, Lemma 8. applies and G is easily seen to have p-length one. If H is a p'-group, Lemma 5. shows that $G/H \in J$ and by induction G/H has p-length one. Hence so has G.

Theorem. G is p-soluble and $G \in J$ if and only if one of the following conditions holds:

(1) G is p-nilpotent with abelian Sylow p-subgroup P and G'P is a Frobenius group with kernel G', or

(2) G is p-nilpotent with Sylow p-subgroup P and p-complement H, $P' = Z(P)$ has order 2 and G'P is a Frobenius group with kernel $G' \cap H$, or

(3) G is abelian, or

(4) G has normal subgroups H, K such that H and G/K are p'-groups, $G \supset K \supset H$, $K/H \cong P$, a Sylow p-subgroup of G, and $G' = H.Z(P)$. $G/H \in J$ and K is a Frobenius group with kernel H.

Proof. (a). Assume G is p-soluble and $G \in J$. If G is abelian there is nothing to prove, so suppose not.

Suppose G is p-nilpotent. Let P be a Sylow p-subgroup of G and H its normal complement. $G/H \cong P$ and so by Lemma 5, $P \in J$. By the corollary to Lemma 8. we have two cases:

(1). Let P be abelian. Then $G' \subset H$ and $p \nmid |G'|$. By the corollary to Lemma 4, $N = M$. Now by Theorem 2, $G'P$ is a Frobenius group with kernel G'.

(2). Let $P' = Z(P)$ have order 2. Consider $G' \cap H$. This is a p'-group. Further, defining $f = \sum_{h \in G' \cap H} h/|G' \cap H|$ and

$\sigma = \sum_{h \in G'} h$, we have $\sigma \in kGf$, since $G' \cap H \subset G'$. By Lemma 4, $M = kG\sigma \subset kGf$. Hence $M = Mf$ and by Lemma 3, $N = Nf$.

Now as $G'P \Delta G$, $N(G'P) \subset kG.N(G'P) \subset N(G)$. Thus

$$N(G'P) = N(G'P)f$$
$$= \text{rad}(k(G'P)f)$$
$$\cong N(G'P/G' \cap H) \text{ by Lemma 1.}$$
$$\cong N(P), \text{ for } G' = (G' \cap H)P'. \text{ Thus}$$
$$\dim_k N(G'P) = \dim_k N(P)$$
$$= |P| - 1.$$

Now by Theorem 1, $G'P$ is a Frobenius group with kernel $G' \cap H$.

Suppose now that G is not p-nilpotent. By Lemma9, G has p-length one and so has a normal series $G \supset K \supset H \supset \{1\}$ such

that G/K and H are p'-groups and K/H ≅ P, a Sylow p-subgroup of G. Choose the series such that (G:K) is maximal.

By Lemma 5, G/H ∈ J. Now G/H is not abelian, for if it were G would be p-nilpotent. Hence by Lemma 8,

$(G/H)' = Z(K/H) \cong Z(P)$. So $G'H = H.Z(P)$. Now $G' \subset K$ and (G:K) is maximal prime to p. Hence (K:G') is a power of p. We therefore have $G' \supset H$ and then $G' = H.Z(P)$.

Define $f = \sum_{h \in H} h/|H|$, $\sigma = \sum_{h \in G'} h$. By Lemma 4,

$M = kG\sigma \subset kGf$. Therefore $M = Mf$. By Lemma 3, $N = Nf$. Now as $K \Delta G$, $N(K) \subset N(G)$ and so

$$\begin{aligned} N(K) &= N(K)f \\ &= \text{rad}(kKf) \\ &\cong \text{rad}(k(K/H)) \text{ by Lemma 1.} \\ &\cong N(P). \end{aligned}$$

Thus $\dim_k N(K) = |P| - 1$. By Theorem 1, K is a Frobenius group with kernel H. This is case (4).

(b). Suppose (1) holds. By Theorem 2. we have that N = M. Hence $G \in J$. If (3) holds we come to the same conclusion.

Suppose (2) or (4) hold. In the former case put K = G. Write $f = \sum_{h \in G' \cap H} h/|G' \cap H|$.

$$\begin{aligned} \dim_k N(G'P)f &= \dim_k N(G'P/G' \cap H) \\ &= \dim_k N(P) \\ &= |P| - 1 \\ &= \dim_k N(G'P) \text{ by Theorem 1.} \end{aligned}$$

Thus $N(G'P) = N(G'P)f$.

By [12] Lemma 6, $N(G) = kG.N(G'P)$

$= kG.N(G'P)f$

$= N(G)f$.

Hence $M = Mf \cong M(G/G' \cap H)$, by Lemma 1. Now in case (2), $G/G' \cap H \cong (H/G' \cap H) \times P \in J$, while in case (4), $G/G' \cap H = G/H \in J$. In each case write

$\tau = \sum_{a \in (G/G' \cap H)'} a$ and $\sigma = \sum_{h \in G'} h$. ~~Then by Lemma 4, $M(G/G' \cap H) \subset k(G/G' \cap H)\tau$. If θ is the canonical map from kG to $k(G/G' \cap H)$, $\theta(\sigma) = \tau$. Thus $M(G) \subset \theta^{-1}(M(G/G' \cap H)) \subset kG\sigma$. In fact $M(G) = kG\sigma$, for $p \| |G'|$.~~ Hence

$kG.M = kG.kG\sigma = kG\sigma = M$ and $G \in J$. This proves the theorem.

By Lemma 4, $M(G/G' \cap H) = k(G/G' \cap H)\tau$, which has dimension $(G : G')$. Consider $kG\sigma$. $kG\sigma \subseteq M(G)$. Also $kG\sigma$ has dimension $(G : G')$. But $M(G) \cong M(G/G' \cap H)$. Hence $M(G) = kG\sigma$.

R J Clarke

Section II.

A Basis for the Radical of the Centre

The purpose of this section is to use some concepts of J. A. Green [6] and A. Rosenberg [8] to exhibit a canonical k-basis for the radical of the centre of a group algebra. We use the notation of the preceding section. As an example we will take the general linear group.

Let $H \leqslant K \leqslant G$ and $\{t_i\}$ be a transversal for H in K.

Definition. $(kG)_H = \{\alpha \in kG;\ \alpha^h = \alpha \text{ for all } h \in H\}$.

$(kG)_H$ is a subalgebra of kG. We have

$(kG)_H \supset (kG)_K \supset (kG)_G = \Lambda$.

Definition. $T_{H,K}$ is the map from $(kG)_H$ to $(kG)_K$ given by $T_{H,K}(\alpha) = \sum_i \alpha^{t_i}$. $T_{H,K}$ is clearly independent of the choice of the transversal.

Definition. $(kG)_{H,K} = \mathrm{Im}T_{H,K} = T_{H,K}((kG)_H)$ and

$$\Lambda_H = (kG)_{H,G}.$$

The various properties posessed by these entities are indicated in [6]. In particular we have:

Lemma 1.([6] Lemma 4h) If D, $H \leqslant K \leqslant G$ then

(i) $(kG)_{D,G} \subset (kG)_{K,G}$

(ii) $(kG)_{H,K} \subset \sum_{k\in K} (kG)_{H^k \cap D, D}$

(iii) $(kG)_{H,K}.(kG)_{D,K} \subset \sum_{k\in K} (kG)_{H^k \cap D, K}$.

Definition. Let $D \leq G$ and let Γ be any collection of subgroups of G all contained in K. Then D' denotes the set of proper subgroups of D,

$$(kG)_\Gamma = \sum_{H \in \Gamma} (kG)_H \text{ and}$$

$$(kG)_{\Gamma,K} = \sum_{H \in \Gamma} (kG)_{H,K}.$$

From Lemma 1. we see that $(kG)_{D',G}$ is an ideal of $(kG)_{D,G}$. The factor algebra $(kG)_{D,G}/(kG)_{D',G}$ is denoted by $W(D,G)$.

For the remainder of this section D will be a p-subgroup of G and H its normaliser in G. Let R be any conjugacy class of G and S the corresponding class sum in Λ. Define $\sigma(S)$ to be the sum of all the elements in $R \cap C_G(D)$, if such elements exist, zero otherwise. Since the class sums form a basis for Λ, σ can be extended linearly to Λ.

Lemma 2.([8] Lemma 3.3) σ is a homomorphism from $\Lambda(G)$ to $\Lambda(H)$. $\mathrm{Ker}\sigma$ is spanned by the class sums S with $R \cap C_G(D) = \phi$.

We use Rosenberg's definitions of the defect group of a class and of a block:

Definition. Let R be the conjugacy class of G containing the element x. A Sylow p-subgroup of $C_G(x)$ is called a defect group of R.

Definition. Let e be a primitive central kG idempotent. A

defect group of the block kGe is a p-subgroup D of G such that $e \in \Lambda_D$, $e \notin \Lambda_{D'}$.

By [8] 5.2, the defect group of a block is determined up to conjugacy. The defect group of a class is obviously determined up to conjugacy. We shall also speak of the defect group of a class sum in the natural way.

By [6] page 142 we see that $(kG)_{D,G}$ is spanned by the class sums with defect groups contained in D.

Lemma 3. σ gives rise to an isomorphism

$$\tau : W(D,G) \longrightarrow W(D,H).$$

Proof. σ may be restricted to $(kG)_{D,G}$. From Lemma 2. we see that $\ker\sigma \cap (kG)_{D,G}$ is spanned by those class sums S whose defect groups are in D'. So we have a monomorphism

$W(D,G) \longrightarrow \Lambda(H)$. Now [8] Lemma 3.4 tells us that the image of this map is spanned by the class sums of $\Lambda(H)$ with defect group D. Now by [8] Lemma 4.1 these classes form an algebra which must be isomorphic to the algebra $(kH)_{D,H}/(kH)_{D',H} = W(D,H)$. Hence the result follows.

Lemma 4. $\mathrm{rad}W(D,G) = (\Lambda_D \cap M + \Lambda_{D'})/\Lambda_{D'}$.

Proof. $(\Lambda_D \cap M + \Lambda_{D'})/\Lambda_{D'}$ is a nilpotent ideal of W(D,G) and is therefore contained in rad W(D,G).

Let $x \in \Lambda_D$ such that $x + \Lambda_{D'} \in \mathrm{rad}W(D,G)$. For every one dimensional representation φ of Λ_D over k such that

$\varphi(\Lambda_{D'}) = 0$ we have $\varphi(x) = 0$.

Let $e_1, \ldots, e_r$ be the primitive central kG idempotents corresponding to those blocks with defect groups not containing any conjugate of D. Put

$y = \sum_{i=1}^{r} xe_i$. Let e_i correspond to a block with defect group C. $xe_i \in \Lambda_D.\Lambda_C \subset \Lambda_{D'}$ by Lemma 1(iii). Hence $y \in \Lambda_{D'}$.

Let φ be a one dimensional representation of Λ over k. If $\varphi(\Lambda_{D'}) = 0$ then $\varphi(y) = 0 = \varphi(x)$. Hence $\varphi(x-y) = 0$. Suppose $\varphi(\Lambda_{D'}) \neq 0$. Then by [8] Lemma 3.2, φ belongs to exactly one of the blocks kGe_i, that is for exactly one i we have $\varphi(e_i) = 1$, while for all other j we have $\varphi(e_j) = 0$. Thus $\varphi(y) = \varphi(x)\varphi(e_i) = \varphi(x)$ and $\varphi(x-y) = 0$. x-y is therefore in the kernel of every irreducible k-representation of Λ and so $x-y \in M$. So we have

$$x + \Lambda_{D'} = x-y + \Lambda_{D'} \in (\Lambda_D \cap M + \Lambda_{D'})/\Lambda_{D'}.$$

Let Ω be a complete set of pairwise non conjugate p-subgroups of G. For each D in Ω let n_D be the number of conjugacy classes of G with defect group D, and m_D the number of blocks of G with defect group D.

Lemma 5. (i) For each D, $\dim_k \mathrm{rad}W(D,G) = n_D - m_D$.

(ii) $M = \sum_{D \in \Omega} (\Lambda_D \cap M - \Lambda_{D'} \cap M)$ as a disjoint sum of

vector spaces.

Proof. (i). Since n_D, m_D and $W(D,G)$ are unchanged when passing to $H = N_G(D)$, we may assume $D \Delta G$.

$Dim_k W(D,G) = n_D$. Let $W(D,G)$ contain s_D primitive central idempotents. As $W(D,G)$ is an abelian algebra it is easy to see that $dim_k radW(D,G) = n_D - s_D$. Now by [8] 4.4 a primitive central idempotent of kG lies in the algebra $\Lambda_D - \Lambda_{D'} \cong W(D,G)$ if and only if it corresponds to a block of kG with defect group D. Moreover an idempotent is primitive in Λ if and only if it is primitive in $\Lambda_D - \Lambda_{D'}$. Hence $s_D = m_D$ and the result follows.

(ii). $$Dim_k M = \sum_{D\in\Omega} n_D - \sum_{D\in\Omega} m_D$$

$$= \sum_{D\in\Omega} dim_k radW(D,G)$$

$$= \sum_{D\in\Omega} dim_k(\Lambda_D \cap M) - dim_k(\Lambda_{D'} \cap M).$$

Since $(\Lambda_{D_1} \cap M - \Lambda_{D_1'} \cap M) \cap (\Lambda_{D_2} \cap M - \Lambda_{D_2'} \cap M) = \phi$ for $D_1 \neq D_2 \in \Omega$, the result follows.

On account of this result we may choose a basis for M consisting of elements of form

$x = \Sigma\lambda_\alpha S_\alpha + \Sigma\mu_\beta S_\beta$, where the S_α are class sums having a common defect group D, say, the S_β all have defect groups

properly contained in D and some $\lambda_\alpha \neq 0$. x has a well defined defect group D. We call such a basis a canonical basis for M.

To apply Lemma 5. to find M, one need only consider those D which are defect groups of a block. For if $D \in \Omega$ is not the defect group of a block, W(D,G) is nilpotent. Let $e_1, \ldots, e_r$ be the primitive central idempotents of $k\mathcal{G}$ corresponding to blocks of defect group containing D. Then from the proof of Lemma 4. we see that the elements

$\{ S\Sigma e_i$; S a class sum with defect group D $\}$ form a basis for $\Lambda_D \cap M - \Lambda_{D'} \cap M$.

One might hypothesize that $\Lambda(G) \cong \bigoplus_{D \in \Omega} W(D,G)$, since the corresponding identity is true for representation algebras. This hypothesis is false, however, because W(D,G) can be a nilpotent algebra, whereas $\Lambda(G)$ cannot have a nilpotent direct summand.

Example.

We illustrate these results for the case $G = GL_n(q)$, $q = p^r$, k of characteristic p.

Let m be the p' part of the exponent of G, ζ a primitive m'th root of 1 in the complex field C and $\varkappa$ a primitive m'th root of 1 in k. Extend the map $\theta: \zeta \to \varkappa$ to an isomorphism between the groups of m'th roots of 1 in C and in k. For any

matrix A in G write $d(A) = \theta^{-1}(\det A)$. It is known that G has exactly q-1 ordinary irreducible characters of defect zero, $\varphi_0, \ldots, \varphi_{q-2}$, related by $\varphi_i(A) = \varphi_0(A)(d(A))^i$. See for example [4] page 49 . Here φ_0 is the Steinberg character of G (see [10]).

A complete set of representatives for conjugacy classes of defect zero in G consists of matrices

$$A = \begin{bmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_r \end{bmatrix}, \quad C_i \text{ all different,}$$

where C_i is the companion matrix of an irreducible polynomial of degree m_i over GF(q). An elementary calculation shows that

$$|C_G(A)| = (q^{m_1}-1)\ldots(q^{m_r}-1).$$

As before we write Λ for the centre of kG and M for the radical of Λ. We find $\Lambda_D \cap M = \Lambda_{D'} \cap M$ for each element D of a complete set Ω of non conjugate p-subgroups of P, the Sylow p-subgroup of G.

(1). $D = \{1\}$. Let $\omega_0, \ldots, \omega_{q-2}$ be the linear characters of $Z(CG)$ corresponding to $\varphi_0, \ldots, \varphi_{q-2}$. By definition

$$\omega_i(A) = \frac{|G|}{|C_G(A)|} \times \frac{\varphi_i(A)}{\varphi_i(1)}$$

$$= \frac{q^{\frac{1}{2}n(n-1)}(q-1)\ldots(q^n-1)(-1)^{n-r}(d(A))^i}{(q^{m_1}-1)\ldots(q^{m_r}-1)q^{\frac{1}{2}n(n-1)}}$$

Hence the linear characters ψ_i of Λ obtained by taking the above expression modulo p are given by

$$\psi_i(A) = (-1)^n(-1)^{n-r}(\det A)^i/(-1)^r$$
$$= (\det A)^i.$$

Now $\Lambda_D \cap M$ consists of those elements of Λ_D in the kernels of every ψ_i, as one sees from [8] 4.4. For each $\rho \in GF(q)^*$, the multiplicative group of GF(q), let $R_{\rho_1} \ldots R_{\rho_{n_\rho}}$ be the conjugacy classes of elements of G with defect zero and determinant ρ, and $S_{\rho_1}, \ldots, S_{\rho_{n_\rho}}$ the corresponding class sums in Λ. Consider the elements $S_{\rho_1} - S_{\rho_j}$; $j \neq 1$, $\rho \in GF(q)^*$. These are all in the kernel of every ψ_i and are therefore in $\Lambda_D \cap M$. Since they are linearly independent, they span a subspace of Λ_D of co-dimension q-1. However the ψ_i are all linearly independent and therefore span a subspace of Λ_D of the same dimension. Hence we have a basis for $\Lambda_D \cap M$.

(2). Let $\{1\} < D < P$ and let e be the sum of the central kG idempotents for blocks of defect zero. G has no blocks of defect group D ([4] page 19). Hence for any class sum S with defect group D, $S(1-e)$ is a basis element for $\Lambda_D \cap M - \Lambda_{D'} \cap M$.

(3). Let $D = P$. Let P be the set of upper unitriangular

matrices. $H = N_G(P)$ consists of upper triangular matrices and $C_G(P)$ of matrices of form $\alpha \begin{bmatrix} 1 & & \beta \\ & 1 & 0 \\ & & \ddots \\ 0 & & 1 \end{bmatrix}$, $\alpha \neq 0$. Call this matrix $\alpha I.z_\beta$.

The H-conjugacy classes in $C_G(P)$ are of two types:

(i) $R_\alpha = \{\alpha I\}$, $\alpha \in GF(q)^*$,

(ii) $R'_\alpha = \{\alpha I.z_\beta;\ \beta \in GF(q)^*\}$, $\alpha \in GF(q)^*$. Call the corresponding class sums S_α and S'_α. Now $N(H)$ has basis $\{\alpha I - \alpha I.z_\beta;\ \alpha,\beta \neq 0\}$. Hence the algebra $\Lambda(H)_P - \Lambda(H)_{P'}$ spanned by these class sums has radical with basis the elements $T_\alpha = S_\alpha + S'_\alpha$; $\alpha \neq 0$. The elements $T_\alpha + \Lambda(H)_{P'}$ thus give a basis for $\mathrm{rad}W(P,H)$.

Let U_α, U'_α be the conjugacy class sums in kG "containing" the elements αI, $\alpha I.z_\beta$ respectively. Let e be as in (2). From Lemmas 3. and 4. we see that the elements $S_\alpha + S'_\alpha + \Lambda_{P'}$ form a basis for $\mathrm{rad}W(P,G)$ and the elements $(S_\alpha + S'_\alpha)(1-e)$, $\alpha \neq 0$ form a basis for $\Lambda_P \cap M - \Lambda_{P'} \cap M$. This completes the canonical basis for M.

Section III.

Radicals of Group Algebras of p-soluble Groups

As before, p denotes a fixed prime, G a finite group and k an algebraically closed field of characteristic p. In this section we give an algorithim for determining N(G) in the case when G is p-soluble. We calculate the radical explicitly for the case of p-length one and make some remarks on the exponent of the radical.

If M is a left kG module, $\Phi(M)$ denotes the Frattini submodule of M. $\Phi(M) = N(G).M$ is the smallest submodule L of M such that M/L is completely reducible. See [1].

1. Useful Lemmas

Lemma 1. Let H be a normal p'-subgroup of G and L an irreducible kH module. Write $E = \mathrm{End}_{kG}(L^G)$, $F = \mathrm{rad}\, E$ and $N = N(G)$. Then, using the natural action of F on L^G, $\Phi(L^G) = N.L^G = F.L^G$ and for all i, $N^i.L^G = F^i.L^G$.

Proof. We may take $L = kHe$ for some primitive kH idempotent e, and $L^G = kGe$. Write $1 = e + e_2 + \ldots + e_n$, a sum of primitive kH idempotents.

$kG = kGe \oplus kGe_2 \oplus \ldots \oplus kGe_n$ as left kG modules. Hence

$$\Phi(L^G) = N.L^G = Ne = kG.Ne$$
$$= kGeNe + kGe_2Ne + \ldots + kGe_nNe \text{ as left kG modules, where the sum is not necessarily direct.}$$

Now $e_ikGe \cong \mathrm{Hom}_{kG}(kGe_i, kGe)$ under the map

$a \to \varphi \in \mathrm{Hom}_{kG}(kGe_i, kGe)$ such that $\varphi(b) = ba$ for all b in kGe_i. We use this fact to show that $Ne = kGeNe$.

Let f and f_i be the primitive central kH idempotents corresponding to e and e_i respectively. Denote by $N_G(f)$ the group of elements of G commuting with f and by T, T_i left transversals for $N_G(f)$ and $N_G(f_i)$ respectively in G. Then $F = \sum_{g \in T} f^g$ and $F_i = \sum_{g \in T_i} f_i^g$ are central kG idempotents. Also $Ff = f$ and $F_i f_i = f_i$. Now if f and f_i are not conjugate in G, $F_i F = 0$. Hence $e_i kGe = e_i f_i F_i kGFfe = 0$.

Suppose f and f_i are conjugate in G, say $f = f_i^g$. Now $e_i^g f = (e_i f_i)^g = e_i^g$. Hence e_i^g and e are in the same kH block kHf. Since k has characteristic p and $p \nmid |H|$ we may use ordinary representation theory to deduce that $kHe \cong kHe_i^g$. Thus $kGe \cong kGe_i^g \cong kGe_i$. We claim that in this case, $e_i Ne = e_i kGeNe$. For there is an a in $e_i kGe$ such that the map $\varphi: kGe_i \longrightarrow kGe$ given by $\varphi(x) = xa$ is an isomorphism. Hence there is a b in $ekGe_i$ such that $\varphi^{-1}(y) = yb$ for y in kGe. Now $\varphi^{-1}\varphi$ is the identity map on kGe_i, and $\varphi^{-1}\varphi(x) = xab$. Hence $e_i = e_i ab = ab$, as $a \in e_i kGe$. Now let $c \in e_i Ne$. Then $bc \in eNe$ and $c = e_i c = abc = a(bc) \in e_i kGeNe$. Thus $e_i Ne \subset e_i kGeNe$. Since the reverse inclusion is obvious, we have equality.

Hence $kGe_iNe = kGe_ikGeNe \subset kGeNe$.

Therefore $Ne = kGeNe = (kGe)(eNe)$. Now by [3] 54.6 we know that eNe and F are anti-isomorphic as rings. Hence $N.L^G = F.L^G$. Thus our result holds for $i = 1$.

Suppose $N^j.L^G = F^j.L^G$ for all $j \leq i$, that is

$$N^je = kGe(eNe)^j \tag{1}$$

Multiplying (1) on the left by N gives

$$N^{j+1}e = (Ne)^{j+1} \tag{2}$$

Multiplying (1) on the right by Ne gives

$$(N^je)(Ne) = kGe(eNe)^{j+1}. \tag{3}$$

Hence $N^{i+1}e = (Ne)^{i+1}$, taking (2) with $j = i$,

$= (Ne)^i(Ne)$

$= (N^ie)(Ne)$, taking (2) with $j = i-1$,

$= kGe(eNe)^{i+1}$, taking (3) with $j = i$.

Therefore $N^{i+1}.L^G = F^{i+1}.L^G$. Hence the result follows by induction.

<u>Definition.</u> If $H \Delta G$ and L is a kH module, the stabiliser $S = S(L)$ of L in G is defined by $S = \{g \in G;\ L^g \cong L\}$.

S is a subgroup of G containing H.

<u>Lemma 2.</u> In the situation of Lemma 1, if S is the stabiliser of L in G, $N^i.L^G = kGN(S)^i.L^S$ for all $i \geq 0$.

<u>Proof.</u> First we prove the well known result that $End_{kG}(L^G) \cong End_{kS}(L^S)$ as rings.

Let $g_1, \ldots, g_s$ be a left transversal for H in S and

$g_1, \ldots g_n$ a left transversal for H in G.

$L^S = \overset{s}{\underset{1}{\oplus}} g_i \otimes L$ may be embedded naturally as a kS submodule of $L^G = \overset{n}{\underset{1}{\oplus}} g_i \otimes L$ and L may be embedded naturally as a kH submodule of L^S.

Let $\theta \in \mathrm{End}_{kS}(L^S)$ and define φ: $\mathrm{End}_{kS}(L^S) \longrightarrow \mathrm{End}_{kG}(L^G)$ by putting $\varphi(\theta) = \theta'$ such that $\theta'(g_i \otimes 1) = g_i\theta(1)$, $1 \in L$, $i = 1, \ldots, n$ and extending linearly to L^G.

Let $g \in G$. There is a j such that $gg_i = g_jh$, $h \in H$.

$$\begin{aligned} \text{Hence } \theta'(g(g_i \otimes 1)) &= \theta'(g_j \otimes hl) \\ &= g_j\theta(hl) \\ &= g_jh\theta(1) \\ &= gg_i\theta(1) \\ &= g\theta'(g_i \otimes 1). \text{ So } \theta' \in \mathrm{End}_{kG}(L^G). \end{aligned}$$

Let $\psi \in \mathrm{End}_{kS}(L^S)$. Clearly $\theta' + \psi' = (\theta + \psi)'$.

$$\begin{aligned} \theta'\psi'(g_i \otimes 1) &= \theta'(g_i\psi(1)) \\ &= g_i\theta'\psi(1) \\ &= g_i\theta\psi(1), \text{ as } \theta'|_{L^S} = \theta, \\ &= (\theta\psi)'(g_i \otimes 1). \text{ So } \theta'\psi' = (\theta\psi)' \text{ and } \varphi \text{ is a} \end{aligned}$$

homomorphism.

Let $\theta \in \ker\varphi$. As $\theta' = 0$, $\theta'|_{L^S} = \theta = 0$. Hence $\ker\varphi = 0$.

Finally, let $\psi \in \mathrm{End}_{kG}(L^G)$. Denote by π_i the projection from L^G onto $g_i \otimes L$, $i = 1, \ldots, n$. If $j \leq s$, $\pi_i\psi|_{g_j \otimes L} \in \mathrm{Hom}_{kH}(g_j \otimes L, g_i \otimes L)$. Now as $g_i \otimes L$ is for all i an irreducible kH module, $\mathrm{Hom}_{kH}(g_j \otimes L, g_i \otimes L) = k$ if $g_j \otimes L \cong g_i \otimes L$, $= 0$ otherwise. Now $g_j \otimes L \cong g_i \otimes L$ if and only if $i \leq s$, so if $i > s$ we have $\pi_i\psi|_{g_j \otimes L} = 0$. Thus $\psi|_{L^S} \in \mathrm{End}_{kS}(L^S)$, say $\psi|_{L^S} = \theta$. Then

$$\begin{aligned}\theta'(g_i \otimes 1) &= g_i\theta(1)\\ &= g_i\psi(1)\\ &= \psi(g_i \otimes 1) \text{ for all } i \text{ and } 1.\end{aligned}$$

Hence $\theta' = \psi \in \mathrm{Im}\varphi$. φ is therefore the required isomorphism.

Under this isomorphism, θ and $\varphi(\theta)$ have the same action on L. Thus $N^i.L^G = (\mathrm{radEnd}_{kG}(L^G))^i \sum_1^n g_j \otimes L$, by Lemma 1,

$$\begin{aligned}&= \sum_1^n g_j(\mathrm{radEnd}_{kG}(L^G))^iL\\ &= \sum_1^n g_j(\mathrm{radEnd}_{kS}(L^S))^iL\\ &\subset kGN(S)^i.L^S \text{ by Lemma 1.}\end{aligned}$$

The reverse inclusion is proven similarly. Hence the result follows.

Lemma 3. Let Q be a normal p-subgroup of the finite group G and let $\theta: kG \longrightarrow k(G/Q)$ be the natural homomorphism. Then

$$N(G) = \theta^{-1}(N(G/Q)).$$

Proof. As Q is a p-group, $N(Q) = \{ \sum_{h\in Q} \alpha_h h;\ \Sigma\alpha_h = 0\}$, so $\ker\theta = kG.N(Q) \subset N(G)$. Now N(G) is the intersection of the kernels of all the irreducible representations of kG. Since $\ker\theta \subset N(G)$, every such representation may be regarded as a representation of k(G/Q). The result therefore follows.

2. p-Soluble Groups

We use these results to give an "algorithm" for determining the radical of the group algebra of a p-soluble group G with p-length n. We assume the radical is known for all groups with p-length less than n.

G has p-series $\{1\} \trianglelefteq N_0 < P_1 \quad \ldots < P_n \trianglelefteq N_n = G$. N_i/P_i is the maximal normal p'-subgroup of G/P_i and P_i/N_{i-1} the maximal normal p-subgroup of G/N_{i-1}.

Let $1 = e_1 + \ldots + e_r$ be a decomposition of 1 into a sum of primitive kN_0 idempotents. Let the irreducible kN_0 module $L_i = kN_0e_i$ have stabiliser S_i in G. $L_i{}^G = kGe_i$.

$kG = \oplus_i kGe_i = \oplus_i L_i{}^G$ as left kG modules. Therefore

$$N = \oplus_i N.L_i{}^G = \oplus_i kG.N(S_i)L_i{}^{S_i}.$$

So we must determine $\Phi(L_i^{S_i})$ for every i.

Consider the series $\{1\} \leqslant M_0 \leqslant \ldots \leqslant Q_n \leqslant M_n = S_i$ obtained from the p-series of G by intersecting each term with S_i. $M_0 = N_0 \cap S_i = N_0$. Now if some p-factor Q_i/M_{i-1} is trivial, S_i has p-length less than n and its radical is known. So suppose no p-factor is trivial, in particular $Q_1 > M_0$.

Now $E = End_{kS_i}(L_i^{S_i}) \cong B$, a twisted group algebra over $(S_i/N_0)^*$, the opposite group to Si/N_0. For see [2] page 162 for a more general version of the same result. Moreover we see from Remark 5. on page 155 of the same paper that there is a group T with a cyclic central p'-subgroup K and a kK idempotent f such that

(i) $B \cong kTf$ as algebras and

(ii) $(T/K)^* \cong S/N_0$.

T has a p-series $\{1\} \leqslant K < R_1 \leqslant K_1 < \ldots < R_n \leqslant K_n = T$, where $(K_i/K)^* \cong M_i/M_0$, $(R_i/K)^* \cong Q_i/M_0$. Now let U be a Sylow p-subgroup of R_1. As K is central in R_1, U is unique and therefore characteristic in R_1. Hence $U \Delta T$.

T/U has p-length less than n, for a p-series for T/U is obtainable by factoring the p-series for T by U. Hence we can find N(T/U). By Lemma 3. we can find N(T) and therefore $radB \cong N(T)f$ and radE. However by Lemma 1. $\Phi(L_i^{S_i}) = radE.L_i^{S_i}$. Hence we can find N(G).

In fact, by a well known result which we will now indicate, we only need to find $N(P_n)$:

Definition. Let R be a ring and P a subring of R. $d(R,P) = 0$ means that every exact sequence of R modules splitting as P modules splits over R.

Theorem. ([13] page 28.) In the above notation, suppose that $d(R,P) = 0$ and that R is a free P module with basis $\{u_i\}$ such that $u_iP = Pu_i$ for every i and the map $\sigma: p \to p'$ given by $u_ip = p'u_i$ is an automorphism of P for every i. Then $RadR = R.radP$.

Lemma 4. Let H be a normal subgroup of the finite group G of index prime to p. Then $N(G) = kG.N(H)$.

Proof. From page 373 of [7] we have that $d(kG, kH) = 0$. For a basis of kG over kH we just take a transversal for H in G. The hypotheses of Villamayor's theorem are now clearly satisfied.

3. Groups with p-Length One

The above method does not appear to enable us to find the radical of kG explicit ly. However we can do this if G has p-length one.

Let G have p-length one and p-series $\{1\} \leq N_0 < P_1 \leq N_1 = G$. $N(G) = kG.N(P_1)$, and P_1 is p-nilpotent. We may therefore assume that G is p-nilpotent. Changing the notation somewhat, let $G = HP$ be a p-nilpotent group with Sylow p-subgroup P and normal p-complement H. Let

$1 = e_1 + \ldots + e_r$ be a decomposition of 1 as a sum of primitive kH idempotents. Put $L_i = kHe_i$ and let L_i have stabiliser $S_i = HQ_i$ in G. Here Q_i is a Sylow p-subgroup of S_i and we may as well take $P \supset Q_i$.

Now $E = \mathrm{End}_{kS_i}(L_i{}^{S_i}) \cong \mathrm{Hom}_{kH}(L_i, L_i{}^{S_i}|_H)$ as k-spaces, via the map $\theta \in E \to \theta|_{L_i} \in \mathrm{Hom}_{kH}(L_i, L_i{}^{S_i}|_H)$, for θ is completely determined by its action on L_i. Since $L_i{}^{S_i}|_H = \bigoplus_{q \in Q_i} q \otimes L_i$,

we have $E \cong \bigoplus_{q \in Q_i} \mathrm{Hom}_{kH}(L_i, q \otimes L_i)$. (1)

Now we know from [9] that there is a unique kS_i module X such that $X|_{kH} = L_i$. Let X afford the representation ρ on S_i. For each $q \in Q_i$, the map T_q: L_i ---> $q \otimes L_i$ given by

$T_q(l) = q \otimes \rho(q^{-1})l$, $l \in L_i$, is a kH *homo*morphism. For if $h \in H$, $T_q(hl) = q \otimes \rho(q^{-1})(hl)$

$= q \otimes \rho(q^{-1}h)l$ by definition of ρ,

$= q \otimes \rho(q^{-1}hq)\rho(q^{-1})l$

$= q.q^{-1}hq \otimes \rho(q^{-1})l$ as $q^{-1}hq \in H$,

$= h.T_q(l)$. Thus as $\mathrm{Hom}_{kH}(L_i, q \otimes L_i) \cong k$, T_q gives a k-basis for it. $\{T_q;\ q \in Q_i\}$ is therefore a k-basis for the right hand side of (1). E therefore has k-basis $\{\eta_q;\ q \in Q_i\}$, where η_q is defined by

$\eta_q(q' \otimes 1) = q'\eta_q(1 \otimes 1)$

$= q'q \otimes \rho(q^{-1})1.$

Now $\eta_q\eta_{q'} = \eta_{q'q}$. Hence $E \cong kQ^*$, Q^* being the opposite group to Q, and radE has basis $\{\eta_1 - \eta_q;\ q \in Q - \{1\}\}$.

Define $\eta(q,l) = 1 \otimes 1 - q \otimes \rho(q^{-1})l$, $l \in L_i$. Let W be a set of basis elements for L_i.

Theorem 1. A basis for $\Phi(L_i{}^{S_i})$ consists of the elements $\eta(q,l)$; $q \in Q - \{1\}$, $l \in W$.

Proof. These elements are clearly linearly independent. Now as $\Phi(L_i{}^{S_i}) = \text{radE}.L_i{}^{S_i}$, $\Phi(L_i{}^{S_i})$ is spanned by the elements $(\eta_1 - \eta_q)(q' \otimes 1)$; $q \in Q - \{1\}$, $q' \in Q$, $l \in W$. But

$(\eta_1 - \eta_q)(q' \otimes 1) = q' \otimes 1 - q'q \otimes \rho(q^{-1})1$

$= -\eta(q',\ \rho(q')1) + \eta(q'q,\ \rho(q')1)$. Thus

$(\eta_1 - \eta_q)(1 \otimes 1) = \eta(q,1)$. Since $\eta(q,l)$ is linear in l, the result follows.

Now $N(G) = \sum_i N(G).L_i{}^G$

$= \sum_i kG.\Phi(L_i{}^{S_i})$, which can be calculated.

Definition. The exponent of $N(G)$ is the least integer n such that $N(G)^n = 0$.

We are now in a position to deduce the exponent of $\mathcal{A}^{N(G)}$ for the case of p-length one.

Theorem 2. If G has p-length one and P is a Sylow p-subgroup of G then N(G) and N(P) have the same exponent.

Proof. We may assume G to be p-nilpotent and use the previous notation.

Let θ be the canonical homomorphism $kG \longrightarrow kP$ and consider the idempotent $e = \sum_{h \in H} h/|H|$ of kG. The elements $(1 - x)e$; $x \in P$ span a two sided ideal I of kG, and clearly $\theta(I) = N(P)$. Since I and N(P) have the same dimension, they are isomorphic as algebras and so I is nilpotent. Thus $I \subset N(G)$.

Let $N(G)^n = 0$. Then $I^n \subset N(G)^n = 0$ and $N(P)^n = \theta(I^n) = 0$.

Suppose conversely that $N(P)^n = 0$. We have that

$$N(G)^n = \sum_i N(G)^n L_i{}^G$$

$$= \sum_i kG.N(S_i)^n L_i{}^{S_i} \text{ by Lemma 2,}$$

$$= \sum_i kG.\{\text{radEnd}_{kS_i}(L_i{}^{S_i})\}^n L_i{}^{S_i} \text{ by Lemma 1.}$$

Now as $N(Q_i) \subset N(P)$, $N(Q_i)^n = 0$ for all i. Hence $N(Q_i^*)^n = 0$, applying an anti-isomorphism. Since $\text{End}_{kS_i}(L_i{}^{S_i}) \cong kQ_i^*$ we have $\{\text{radEnd}_{kS_i}(L_i{}^{S_i})\}^n = 0$ for all i and therefore $N(G)^n = 0$.

We now give two examples to show that nothing can be

salvaged from Theorem 2, even in the case of p-length 2.

Example 1. Take p = 2 and G the symmetric group on four symbols. G is generated by elements a = (1234), b = (12)(34) and c = (123). A Sylow 2-subgroup of G is P = <a, b>, which is dihedral of order 8. We show that $N(P)^4 = 0$ but $N(G)^4 \neq 0$.

Jennings in [5] has investigated the exponent of the radical for a p-group, and shown that it is the same as the length of the R-series of the group. The R-series is a series of subgroups defined by

$R_1 = P$

$R_i = \langle [R_{i-1}, P], R_{[i/p]}^{(p)} \rangle$, where [i/p] denotes the ~~least~~ greatest integer not ~~less~~ greater than i/p and $R_{[i/p]}^{(p)}$ denoted the group generated by the p'th powers of the elements of $R_{[i/p]}$. It is easily seen that for $P = \langle a, b; a^4 = b^2 = 1, baba = 1 \rangle$ we have $R_1 = P$, $R_2 = R_3 = \langle a^2 \rangle$ and $R_4 = 1$. Hence $N(P)^4 = 0$.

Consider the idempotent $e = 1 + c + c^2$ of kG and write $U = kGe$. Since $kG = kGe \oplus kG(1-e)$, U is a direct summand of kG. Define the descending Loewy series of U,

$U = U_0 > U_1 > \ldots > U_r = 0$, by $U_i = N^i.U$. U_i/U_{i+1} is the greatest completely reducible factor of U_i (see [1]). Let n be the exponent of N(G). $N(G)^n = 0$, so $n \geq r$. We show that

$r > 4$.

U, being a direct summand of kG, is a direct sum of principal indecomposable kG modules. Now U has dimension 8, and each principal indecomposable kG module has dimension divisible by 8 ([3] 84.15). Hence U is indecomposable. But then U has a unique maximal submodule $U_1 = N.U$ ([3] 54.11). One easily sees that $N(P)e$ is a submodule of U, and as $N(P)e$ has dimension 7 it is maximal in U. Hence $U_1 = N(P)e$.

Write $Q = \langle a^2, b \rangle \Delta G$.

$N(P) = k\{1+x;\ x \in P - \{1\}\}$

$= kP.N(Q) + k\{1+a\}$.

Hence $U_1 = kP.N(Q)e + k\{1+a\}e$. Now as $Q \Delta G$, $N(Q) \subset N(G)$. Therefore $U_2 = N(G).U_1 \supset N(Q).U_1$

$= kP.N(Q)^2e + N(Q)(1+a)e$.

$N(Q)^2$ has basis $1+a^2+b+ba^2$. So $N(Q).U_1$ has basis $\{(1+a^2+b+ba^2)e,\ (1+a^2+b+ba^2)ae,\ (1+a^2)(1+a)e,\ (1+b)(1+a)e\}$. Thus $U_1/N(Q).U_1$ has basis $\{x_1 = \overline{(1+a)e},\ x_2 = \overline{(1+a^2)e},$

$x_3 = \overline{(1+b)e}\ \}$. Here the bar refers to the coset of the element with respect to $N(Q).U_1$.

By using the relations $ca = a^3bc^2$, $cb = a^2bc$ and $ca^2 = bc$ it can easily be calculated that in the representation ρ afforded by the module $U_1/N(Q).U_1$,

$$\rho(a) = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad \rho(c) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Now as U_1/U_2 is the greatest completely reducible factor of U_1, it is the greatest completely reducible factor of $U_1/N(Q).U_1$. An easy calculation shows that $U_1/N(Q).U_1$ has no one dimensional submodules. As it has a one dimensional factor module, it is not completely reducible. Now the submodule $k\{x_2, x_3\}$ has no one dimensional submodules and so is irreducible. Therefore the only possibility is that $U_2/N(Q).U_1 = k\{x_2, x_3\}$.

$$U_2 = N(Q).U_1 + k(1+a^2)e + k(1+b)e$$

$$= kP.N(Q)^2e + N(Q)(1+a)e + k(1+a^2)e + k(1+b)e.$$

$$U_3 = N(G).U_2 \supset N(Q).U_2$$

$$= kP.N(Q)^3e + N(Q)^2(1+a)e + N(Q)(1+a^2)e +$$

$N(Q)(1+b)e$. $N(Q)^3 = 0$. Hence $N(Q).U_2$ is two dimensional, being equal to $kP.N(Q)^2$.

Suppose $U_4 = 0$. We know from Exercise 1. on page 598 of [3] that U has a unique minimal submodule of dimension 1. Hence U_3 has dimension 1. This contradicts the fact that $U_3 \supset N(Q).U_2$. Hence $U_4 \neq 0$ and so $N(G)^4 \neq 0$.

Example 2. Let Q be the quaternion group:

$Q = \langle i, j, k, d; ij = k, i^2 = j^2 = k^2 = d, d^2 = 1 \rangle$. Consider

the group $G = \langle Q, b, c, c^{-1}ic = j, c^{-1}jc = k, b^{-1}ib = i^{-1}, b^{-1}jb = k^{-1}, b^{-1}cb = c^{-1}, b^2 = c^3 = 1\rangle$. G is an extension of Q by S_3, the symmetric group on 3 letters. We take p = 2.

G has Sylow 2-subgroup $P = \langle Q, b\rangle$. The R-series of P is $R_1 = P$, $R_2 = R_3 = \langle i\rangle$, $R_4 = R_5 = R_6 = R_7 = \langle d\rangle$, $R_8 = 1$. Hence $N(P)^8 = 0$, $N(P)^7 \neq 0$. We show that $N(G)^7 = 0$.

First we compute the powers of N(Q).

N(Q) has basis $\{1+x;\ x \in Q - \{1\}\}$.

$N(Q)^2$ has basis $\{1+d,\ i+i^{-1},\ j+j^{-1},\ k+k^{-1},\ 1+i+j+k\}$.

$N(Q)^3$ has basis $\{1+d+i+i^{-1},\ 1+d+j+j^{-1},\ 1+d+k+k^{-1}\}$.

$N(Q)^4$ has basis $\{\sigma = 1+d+i+i^{-1}+j+j^{-1}+k+k^{-1}\}$.

$N(Q)^5 = 0$.

These are easily checked.

Let θ be the canonical map $kG \longrightarrow k(G/Q)$. By Lemma 3, $N(G) = \theta^{-1}(N(G/Q))$. We must therefore find the radical for $G/Q \cong S_3$.

S_3 has character table

	1	(12)	(123)
ζ_1	1	1	1
ζ_2	1	−1	1
ζ_3	2	0	−1

Now for p = 2, S_3 has two p-regular conjugacy classes and therefore two distinct modular irreducible characters ([3] 83.5). ζ_1 is irreducible mod 2, being a linear character, and ζ_3 is irreducible mod 2 by [3] 86.3. Hence the irreducible

representations of kS_3 have dimensions 1 and 2 and $N(S_3)$, the intersection of their kernels, has dimension $6 - 1^2 - 2^2 = 1$, and basis element $e = (1+(12))(1+(123)+(132))$

Write $E = (1+b)(1+c+c^2)$. Then $\theta(E) = e$ and

$$N(G) = kE + \ker\theta$$
$$= kE + kG.N(Q).$$

Now $N(G)^7$ is a sum of "words" of form $kE^{m_1}(\ker\theta)^{n_1} \ldots E^{m_r}(\ker\theta)^{n_r}$, where $\sum_i m_i+n_i = 7$. We show that every such word is zero.

Since $Q \Delta G$, $kG.N(Q) = N(Q).kG$ and therefore the above word is contained in $\ker\theta^l$, where $l = \sum_i n_i$. Hence for this word to be non zero we must have $l < 5$. Moreover $E^2 = 0$, hence we must have $m_1 = 0$ or 1 and $m_i = 1$ for $i \neq 0$.

Now $EiE = Ei(1+b)(1+c+c^2)$
$= E(i+bi^{-1}+cj+bcj^{-1}+c^2k+bc^2k^{-1})$
$= E(\sigma+1+d)$. Therefore $E(\ker\theta)E$ has basis $E(\sigma+1+d)$.

However $E(1+i+j+k)E = 3EiE = EiE \bmod 2$. Therefore $E(\ker\theta)^2E = E(\ker\theta)E$. This means that any word containing a section $E(\ker\theta)E$ can be replaced by a longer word. From these remarks we see that the only possible non zero word is $E(\ker\theta)^2E(\ker\theta)^2E$. But

$E(\ker\theta)^2E(\ker\theta)^2E = E(\sigma+1+d)(\ker\theta)^2E$

$\subset E(\ker\theta)^4E$

$= E\sigma E$

$= E^2\sigma = 0$, for σ is central in kG. Hence $N(G)^7 = 0$.

In conclusion we note that more complicated examples exist for $p \neq 2$. There seems to be no obvious way of generalizing Theorem 2.

References

[1] E. Artin, C. J. Nesbitt and R. M. Thrall. "Rings with Minimal Condition". University of Michigan, Ann Arbor 1944.

[2] S. B. Conlon. "Twisted Group Algebras and their Representations". Aust. Math. Soc. J. 4 (1964), 152-173.

[3] C. W. Curtis and I. Reiner. "Representation Theory of Finite Groups and Associative Algebras". New York 1962.

[4] S. W. Dagger. "On the Representation Theory of the Chevalley Groups". Ph.D. thesis, University of Warwick, 1969.

[5] S. A. Jennings. "The Structure of the Group Ring of a p-Group over a Modular Field". Trans. Amer. Math. Soc. 50 (1941), 175-185.

[6] J. A. Green. "Some Remarks on Defect Groups". Math. Zeitschr. 107 (1968), 133-150.

[7] D. G. Higman. "On Modules with a Group of Operators". Duke Math. J. 21 (1954), ~~509-515.~~ 369-376.

[8] A. Rosenberg. "Blocks and Centres of Group Algebras". Math. Zeitschr. 76 (1961), 209-216.

[9] B. Srinavasan. "On the Indecomposable Representations of a Certain Class of Groups". Proc. London Math. Soc. 10 (1960), 497-513.

[10] R. Steinberg. "A Geometric Approach to the Representations of the Full Linear Group over a Galois Field". Trns. Amer. Math. Soc. 71 (1951), 274-282.

[11] D. A. R. Wallace. "Note on the Radical of a Group Algebra". Proc. Cambridge Philos. Soc. 54 (1958), 128-130.

[12] D. A. R. Wallace. "Group Algebras with Central Radicals". Proc. Glasgow Math. Soc. 5 (1962), 103-108.

[13] C. E. Villamayor. "On the Semisimplicity of Group Algebras II". Proc. Amer. Math. Soc. 10 (1959), 27-31.

PART B

PERMUTATION REPRESENTATIONS OF SYMPLECTIC GROUPS

PART B

PERMUTATION REPRESENTATIONS OF SYMPLECTIC GROUPS

Introduction.

In this part we consider multiply transitive permutation representations of some projective symplectic groups.

Many non abelian simple groups have multiply transitive permutation representations, and it was at one time thought that this was true for all non abelian simple groups. The first counter example, PSU(4,4), was pointed out by Parker in [10]. A proof of this result for the same group in its guise of PSp(4,3) was given by Huppert in [6]. Here we generalise the result considerably and give an infinite class of simple groups with no multiply transitive permutation representations, namely the groups PSp(4,q), q a prime power greater than 2. In fact we show that, modulo an almost proven conjecture of J. A. Green quoted in §4, the groups $PSp(2^{r+1},q)$, $r > 1$, have no multiply transitive representations, excepting for each r at most a finite number of prime powers q.

There seems no reason why the methods used should not apply to a much wider class of Chevalley groups, except that the complexity of the calculations would increase prohibitively.

We begin with introductory sections on groups with B-N pairs, Chevalley groups and symplectic groups. The results quoted here can be found in [1], [2] and [11]. Section 4 lists a few isolated results we need and in section 5 we prove the main theorem.

1. Groups with BN-pairs.

Let G be a finite group with subgroups B and N.

Definition. (B,N) is a BN-pair for G if the following 3 conditions hold:

(i) $G = \langle B, N \rangle$

(ii) $H = B \cap N \triangleleft N$.

Write $W = N/H$, the Weyl group of the BN-pair. If $w \in W$, $w = n_w H$ for some $n_w \in N$. For convenience we write Bw for the coset Bn_w.

(iii) There is a set R of involutory generators of W such that (a) if $r \in R$ and $w \in W$ then

$rBwB \subset BwB \cup BrwB$ and $BwBr \subset BwB \cup BwrB$,

(b) if $r \in R$, $rBr \neq B$.

For any subset J of R, define W_J as $\langle J \rangle$ and G_J as $BW_JB \subset G$.

Theorem 1.([11] Prop. 2.2)

(a) G_J is a subgroup of G and in particular $G = G_R = BWB$.

(b) If $w, w' \in W$ such that $BwB = Bw'B$ then $w = w'$.

(c) If $J, J' \subset R$ such that $G_J = G_{J'}$ then $J = J'$.

(d) Every subgroup of G containing B is of form G_J for some $J \subset R$.

(e) Each subgroup G_J is self normalising.

The G_J are called parabolic subgroups of G. The map $J \to G_J$ gives a lattice isomorphism between the subsets of R and the parabolic subgroups of G.

Theorem 2.([11] Prop. 2.5) Let $G_1 < G$ and write $B_1 = B \cap G_1$, $N_1 = N \cap G_1$. Suppose that $HB_1 = B$. Then there is a subset J of R such that $HG_1 = G_1H = G_J$.

As examples of groups with BN-pairs we have the Chevalley groups. We now give a very brief discussion of them.

2. Chevalley Groups.

For a fuller explanation of the results indicated here we refer the reader to [2] and the bibliography of that article.

Let L be a simple Lie algebra of rank l over the complex field, having root system Π, ordered as usual. Let Π^+ be the set of positive roots and Σ the set of fundamental roots of L. L has a C-basis $\{b_i\}$ with the property that $[b_i, b_j] = \sum_k a_{ijk} b_k$, a_{ijk} integers. Let K be a finite field of characteristic p and size q. Then we can define a Lie algebra L_K over K by taking as a K-basis for L_K elements c_i with multiplication $[c_i, c_j] = \sum_k a_{ijk} c_k$. Here we take the a_{ijk} modulo p. The Chevalley group L(q) is a certain finite subgroup of the automorphism group of L_K.

For each $r \in \Pi$, $t \in K$, $L(q)$ contains an element $x_r(t)$. The $x_r(t)$ generate $L(q)$. $X_r = \{x_r(t);\ t \in K\}$ is a subgroup of $L(q)$ naturally isomorphic to K^+, the additive group of K, and known as a root subgroup of $L(q)$. Writing $[a,b]$ for the commutator $a^{-1}b^{-1}ab$, we have the Chevalley Commutator Formula

$[x_s(u),x_r(t)] = \prod_{\substack{i,j>0 \\ ir+js\in\Pi}} x_{ir+js}(C_{ijrs}(-t)^i u^j)$. Here r and s are independent roots and C_{ijrs} is ± 1, 2, or 3, depending on the root system of the Lie algebra L. The product is taken in increasing order of roots.

$U = \prod_{r\in\Pi^+} X_r$, product taken over roots in increasing order, is a Sylow p-subgroup of G. If $m = |\Pi^+|$, $|U| = q^m$.

Write $B = N_{L(q)}(U)$. U has an abelian complement H in B such that $|H| = (q-1)^l/d$ for a certain integer d depending on L and q. H normalises each root subgroup.

For each $r \in \Pi$, write $n_r = x_r(1)x_{-r}(-1)x_r(1)$. Then if $N = \langle H, n_r;\ r \in \Pi\rangle$, $H = B \cap N \Delta N$ and $N/H \cong W$, the Weyl group of the Lie algebra L. For each w in W choose n_w in N such that $n_w \in w$.

$L(q)$ has BN-pair (B,N) with Weyl group which we may take to be W. The involutory generators are the fundamental

reflections w_r, $r \in \Sigma$.

Theorem 3.(Chevalley) $L(q)$ is simple except for $A_1(2)$, $A_1(3)$, $B_2(2)$ and $G_2(2)$.

3. Symplectic Groups.

Throughout this part we write G^* for the symplectic group $Sp(2^{r+1},q)$ and G for the projective symplectic group $PSp(2^{r+1},q)$, $r \geq 1$, $q = p^t$, p prime. We may look on G in any of three ways, as convenient.

(1) G^* is the subgroup of $GL(2^{r+1},q)$ consisting of all matrices A satisfying $A'JA = J$, where

$$J = \begin{bmatrix} 0 & 1 & & & 0 & 0 \\ -1 & 0 & 0 & \cdots & 0 & \\ & 0 & & & & \\ & & \ddots & & & \\ & & & & 0 & 1 \\ 0 & & & & -1 & 0 \end{bmatrix}$$

Factoring this group by its centre, the group of scalar matrices in G^*, gives G.

$|G| = q^{2^{2r}} \prod_{k \leq 2^r} (q^{2k}-1)/d$, $d = (2,q-1)$. "Uncapped" matrices will denote elements of G.

(2) Let V be a 2^{r+1} dimensional vector space over $GF(q)$ with basis $\{x_i\}$ and symplectic form δ:

$\delta(x_i,x_j) = 1$ if $j = i+1$, i odd

-1 if $i = j+1$, j odd

0 otherwise.

G^* is the group of linear transformations of V commuting with δ.

From V we derive a $2^{r+1}-1$ dimensional projective space $\underline{P}$ as usual. G^* has a natural action on the points of $\underline{P}$, and the permutation group on $\underline{P}$ so produced is the projective symplectic group G.

The equivalence of (1) and (2) is fairly obvious. The following equivalence is not obvious, but we have not the space to prove it here.

(3) G is isomorphic to the Chevalley group $C_{2^r}(q)$. So G has a BN-pair with $|B| = q^{2^{2r}}(q-1)^{2^r}$.

We can be more explicit for $r = 1$: C_2 has fundamental roots p_1, p_2 and positive roots p_1, p_2, p_1+p_2 and $2p_1+p_2$. For the corresponding elements $x_r(t)$ of $C_2(q)$ we may write

$$x_{p_1}(t) = \begin{vmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -t & 0 & 1 \end{vmatrix}, \quad x_{p_2}(t) = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{vmatrix},$$

$$x_{p_1+p_2}(t) = \begin{vmatrix} 1 & 0 & 0 & t \\ 0 & 1 & 0 & 0 \\ 0 & t & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}, \quad x_{2p_1+p_2}(t) = \begin{vmatrix} 1 & t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

and $x_{-r}(t) = (x_r(t))'$. We also have H as the set of "matrices"

$$\begin{vmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda^{-1} & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu^{-1} \end{vmatrix}, \quad \lambda, \mu \in GF(q)^*.$$

The Weyl group W of C_2 is $\langle w_1, w_2; w_1^2 = w_2^2 = (w_1 w_2)^4 = 1 \rangle$. Here $w_1(p_1) = -p_1$, $w_1(p_2) = 2p_1 + p_2$,

$w_2(p_1) = p_1 + p_2$, $w_2(p_2) = -p_2$.

4. Little Lemmas.

For convenience we collect in this section various unconnected results and definitions which we require.

Lemma 1. Let $A \in K = GL(m,q)$ have the following form:

$A = \begin{bmatrix} C_1 & & \\ & \ddots & \\ & & C_r \end{bmatrix}$, each $C_i \in GL(m_i,q)$, C_i, C_j for $i \neq j$ are not conjugate in any linear group and C_i has order r_i dividing $q^{m_i}-1$ but not dividing q^l-1 for any $l < m_i$. Then

$$|C_K(A)| = \prod_i (q^{m_i}-1).$$

This well known lemma may be obtained using Schur's lemma and Theorem 7.3 on page 187 of [6].

Lemma 2.([9]) Let K be an algebraic group over the finite field k. If $x \in K$ denote by $x^{(q)}$ the element obtained by raising all the coordinates of x to the q'th power. Then the

map $f: x \to x^{-1}x^{(q)}$ is a surjective map of K into itself.

Lemma 3.([13]) Let a group K have a k-ply transitive permutation representation on a set Ω, L the subgroup of K fixing some k points and U a subgroup of L such that for every G-conjugate V of U contained in L, V is conjugate to U in L. Then $N_K(U)$ acts k-ply transitively on the points of Ω fixed by U.

Definition. If U is a subgroup of a group K, U is called pronormal in K if for all $g \in K$, U and U^g are conjugate in $\langle U, U^g \rangle$.

Evidently, if U is pronormal in K, Lemma 3. shows that $N_K(U)$ acts k-ply transitively on the points fixed by U.

Lemma 4. Let a group K have a k-ply transitive permutation representation of degree n on a set Ω. Let L be the subgroup of K fixing some k points and U a subgroup of L fixing exactly m points. Then

* $|N_K(U)| \leq |N_L(U)|m(m-1)\ldots(m-k+1)$. Equality holds if and only if every subgroup V of L conjugate to U in G is conjugate to U in L. In this case

** $(K:N_K(U)) = (L:N_L(U)) \frac{n(n-1)\ldots(n-k+1)}{m(m-1)\ldots(m-k+1)}$.

Proof. * simply results from the fact that $N_K(U)$ acts as a permutation group on the points of Ω fixed by U, and $N_L(U)$ is

the subgroup of $N_K(U)$ fixing some k points.

** is a restatement of * in the case when equality holds, and is seen to be a formula for the number of subgroups of K conjugate to U. Each such subgroup is contained in exactly C_k^m subgroups of K fixing k points. There are C_k^n subgroups of K fixing k points, each one of which contains at least $(L:N_L(U))$ K-conjugates of U, and exactly that many K-conjugates of U if the condition stated in the Lemma holds. Hence the result follows.

Lemma 4. is equivalent to Lemma 3. The fact that the right hand side of ** is an integer is often a useful restriction on m.

Lemma 5. Let K have a doubly transitive permutation representation of degree n on a set Ω, let $\alpha, \beta \in \Omega$, let $K_{\alpha\beta}$ be the subgroup of K fixing α and β and let p be a prime dividing both n-1 and $|K_{\alpha\beta}|$. If Q is a Sylow p-subgroup of $K_{\alpha\beta}$ then $Q = O_p(N_K(Q))$, that is Q is the maximal normal p-subgroup of its normaliser.

Proof. Let $P = O_p(N_K(Q))$ and suppose Q fixes exactly m points of Ω. $N = N_K(Q)$ is doubly transitive on these m points and as $P \Delta N$, P acts either trivially or transitively on them ([12] 9.9). Now $m \equiv n \equiv 1 \pmod{p}$. So P, being a p-group,

cannot act transitively on m points. Hence P acts trivially on them, which means $P \subset K_{\alpha\beta}$. But $K_{\alpha\beta} \cap O_p(N) = Q$. Hence $P = Q$.

Lemma 6. Let $K = K_1 \times K_2$ have a doubly transitive permutation representation ρ of degree n on a set Ω. Then either $\ker\rho \supset K_1$, $\ker\rho \supset K_2$ or $n = 2$.

Proof. Suppose not. K_1 and K_2, being normal in K, act transitively on Ω. Let $\alpha, \beta \in \Omega$. Take $g \in K_1$ with $g\alpha = \beta$. Consider $K_\alpha \cap K_2$. If $h \in K_\alpha \cap K_2$,

$h\beta = hg\alpha = gh\alpha$ as $h \in K_2$,

$= g\alpha = \beta$. Hence $h \in \ker\rho$. Therefore

$K_\alpha \cap K_2 \subset \ker\rho$ and similarly $K_\alpha \cap K_1 \subset \ker\rho$. We may therefore assume $K_\alpha \cap K_2 = K_\alpha \cap K_1 = \{1\}$. But then $|K_1| = (K_1 : K_\alpha \cap K_1) = n = |K_2|$. Hence $|K| = n^2$. However $n-1 \mid |K|$. Therefore $n = 2$.

We now look at the doubly transitive permutation representations of metacyclic groups.

Lemma 7. Let $N = \langle y, a;\ y^b = a^c = 1,\ aya^{-1} = y^q \rangle$ have a doubly transitive permutation representation of degree m on a set Γ. Then either (i) $m = 2$ and the kernel of the representation is $\langle y, a^2 \rangle$ or

(ii) $m \mid b$, $m-1 \mid c$, m is a prime power, y^m is in the kernel and y is transitive on Γ.

Proof. Let ρ be the representation. $\rho(\langle y\rangle) \Delta \rho(N)$ is a normal subgroup of a multiply transitive group so acts either trivially or transitively on Γ. If $\rho(y) = \{1\}$, the abelian group $N/\langle y\rangle$ acts doubly transitively on Γ. Hence $m = 2$ and we have case (i).

Suppose $\rho(\langle y\rangle)$ is transitive on Γ. As $\langle y\rangle$ is abelian, it acts regularly on Γ. Hence $m|b$ and $y^m \in \ker\rho$. Now $|\rho(N)|$ divides mc and $m(m-1)||\rho(N)|$. Hence $m-1|c$. m is a prime power by [12] 11.3.

Lemma 8. Let a group K have a permutation representation on a set Ω and let Γ be an orbit of some $y \in K$. Let s be a power of a prime s_0 such that s divides the order of y and let y^u have order s. Then if y^u fixes any point of Γ it fixes all points of Γ, while otherwise $s_0||\Gamma|$.

Proof. Let y^u fix $\alpha \in \Gamma$ and let $\beta \in \Gamma$. For some i, $y^i\alpha = \beta$. Hence
$$\begin{aligned} y^u\beta &= y^u y^i \alpha \\ &= y^i y^u \alpha \\ &= y^i\alpha = \beta. \end{aligned}$$

Suppose y^u fixes no points of Γ. y^u permutes the points of Γ, so Γ is a union of y^u orbits, each of which has length divisible by s_0. Hence $s_0||\Gamma|$.

Lemma 9. If $K = SL(2,q)$ has a doubly transitive representation

of degree m on a set Γ then either

(i) $m = q+1$ or

(ii) $q = 2$ and $m = 2$, $q = 3$ and $m = 2$ or 3, $q = 4$ and $m = 6$ or $q = 9$ and $m = 6$.

Proof. Let $\alpha \in \Gamma$. K has an irreducible character ζ of degree $m-1$ such that $1_{K_\alpha}{}^K = 1_K + \zeta$ as complex characters. For each g in K, $\zeta(g)$ is a rational integer not less than -1. Examination of the character table of $SL(2,q)$, for which we refer the reader to [8], yields the result.

We note that this result could have been proven by the methods we use in section 5.

Theorem 4. ([3]) In the notation of §2, let Σ be the set of fundamental roots of L and $J,K \subset \Sigma$. Define the subgroup W_J of W to be the group generated by the fundamental reflections for the roots in J and define $G_J = BW_JB$. Write $\psi_J = 1_{W_J}{}^W$ and $\chi_J = 1_{G_J}{}^G$. Then the mapping

$\theta: \psi = \sum_J a_J\psi_J \to \chi = \sum_J a_J\chi_J$ is an isometry between the complex vector spaces generated by the ψ_J and the χ_J. In fact the scalar product (χ_J,χ_K) = number of (G_J,G_K) double cosets in G = number of (W_J,W_K) double cosets in W = (ψ_J,ψ_K).

We finish with some arithmetical lemmas.

Lemma 10. For all integers $u \geq 1$, $(q-1)^u \leq q^{u+1}-2q^{u-1}$, equality holding if and only if $u = 1$ or 2 or $q = 2$.

Proof. $q-1 = q+1-2$, so the result holds for $u = 1$. Suppose it holds for u. $(q-1)^u \leq q^{u+1}-2q^{u-1}$.

$$(q-1)^{u+1} \leq q^{u+1}+q-2q^u-q^u-1+2q^{u-1}$$
$$= q^{u+1}+1-2q^u-(q^u-2q^{u-1}-q+2)$$
$$= q^{u+1}+1-2q^u-(q-2)(q^{u-1}-1).$$ Hence the result follows.

Lemma 11. For all integers i and j, $(q^i-1, q^j-1) = q^{(i,j)}-1$ and $(2q^i-1, q^j-1) \mid 2^{j/(i,j)}-1$.

Proof. If $i \mid j$, $q^i-1 \mid q^j-1$. Hence $q^{(i,j)}-1 \mid (q^i-1, q^j-1)$. Choose a and $b > 0$ such that $ai-bj = (i,j)$, b minimal. Since $(q^{ai}-1)-q^{(i,j)}(q^{bj}-1) = q^{(i,j)}-1$ we have $(q^i-1, q^j-1) \mid q^{(i,j)}-1$. This proves the first part.

Write $a' = j/(i,j)-a$, $b' = i/(i,j)-b$. Then $-a'i+b'j = ai-bj = (i,j)$. Since b was minimal we have $b' > 0$ and $a' > 0$. Now

$(2^a q^{ai}-1)-2^a q^{(i,j)}(q^{bj}-1) = 2^a q^{(i,j)}-1$ and

$q^{(i,j)}(2^{a'} q^{a'i}-1)-2^{a'}(q^{b'j}-1) = 2^{a'}-q^{(i,j)}$. Hence

$(2q^i-1, q^j-1) \mid (2^a q^{(i,j)}-1, 2^{a'}-q^{(i,j)})$

$\mid 2^{a+a'}-1 = 2^{j/(i,j)}-1$ as required.

Consider the ring $Z[x]$. This is a unique factorisation domain, so the statement "$f, g \in Z[x]$ are coprime" may be defined to mean "f and g have no irreducible factors in common". Write $\langle f,g \rangle$ for the ideal generated by f and g.

Definition. If f and g in $Z[x]$ are coprime, (f,g) is the unique positive integer generating the Z-ideal $Z \cap \langle f,g \rangle$.

The above ideal is clearly non zero. (f,g) is the least positive integer which can be written in the form $uf+vg$, $u,v \in Z[x]$.

If k is an odd integer write $\varphi = \varphi(x)$ for the cyclotomic polynomial for $2k$, the monic polynomial in $Z[x]$ whose complex roots are the primitive $2k$'th roots of 1. Evidently $\varphi | x^k+1$. Write $x^k+1 = \varphi\psi$.

Lemma 12. φ and ψ are coprime and (φ,ψ) divides 1, the product of the distinct primes dividing k. If $q \in Z^+$, the set of positive integers, $(\varphi(q),\psi(q))$ and $(\varphi(q),2k)$ divide 1.

Proof. If φ and ψ were not coprime they would have a common factor f in $Z[x]$, $f \neq \pm 1$. If f had degree zero it would be an integer dividing x^k+1, contradiction. If f had positive degree it would have a root in C, the complex field. Then φ and ψ would have a common root in C which they do not.

Let $\{p_i\}$ be the distinct primes dividing k and write $k_i = k/p_i$. For each i, $\varphi | (x^k+1)/(x^{k_i}+1)$

Hence $\varphi \mid x^{k_i(p_i-1)} - \ldots - x^{k_i}+1$. By substituting $x^{k_i} = -1$ in this polynomial we see that $((x^k+1)/(x^{k_i}+1), x^{k_i}+1) \mid p_i$. Hence $(\varphi, x^{k_i}+1) \mid p_i$.

Now $\psi \mid \prod_i (x^{k_i}+1)$ and one easily proves that $(f,gh) \mid (f,g)(f,h)$ for any f, g and h $\in Z[x]$. Hence $(\varphi,\psi) \mid \prod_i (\varphi, x^{k_i}+1) \mid \prod_i p_i$ as required.

This clearly implies that $(\varphi(q),\psi(q)) \mid 1$.

Now let s be a prime dividing $(\varphi(q),2k)$. We must show $s^2 \nmid \varphi(q)$. Let s' be a prime dividing k and write $k' = k/s'$.

$\varphi \mid (x^k+1)/(x^{k'}+1)$. Now if q is even, $\varphi(q)$ is odd, so $s \neq 2$. If q is odd, ~~$q^k \equiv q^{k'} \equiv 1 \pmod 4$. Hence~~ $2 \nmid (q^k+1)/(q^{k'}+1)$ and we again have $s \neq 2$. Therefore $s \mid k$. Write $k' = k/s$.

$q^{k'} \equiv q^k \equiv -1 \pmod s$, ~~and k' is odd, so $q^{k'} \equiv -1 \pmod s$~~. Write $q^{k'} = us-1$.

$$\varphi(q) \mid (q^k+1)/(q^{k'}+1) = \sum_i q^{k'i}(-1)^i$$

Now $q^{k'i} = (us-1)^i$

$$\equiv (-1)^{i-1} ius + (-1)^i \pmod{s^2}.$$ Hence

$$\sum_{i=0}^{s-1} q^{k'i}(-1)^i \equiv \sum_{i=0}^{s-1} (-ius+1) \pmod{s^2}$$

$$\equiv -us.\tfrac{1}{2}s(s-1)+s \pmod{s^2}$$

$$\equiv s \pmod{s^2}.$$ Therefore $s^2 \nmid \varphi(q)$.

Finally we have the following conjecture of J. A. Green:

Conjecture I. Let $L(q)$ be a Chevalley group with BN-pair (B,N) and let the complex character 1_B^G have irreducible constituents $1_G, \chi_1, \ldots, \chi_r$. Then r is independent of q and there exist fixed polynomials $f_1, \ldots, f_r$ independent of q, with rational coefficients and constant coefficient zero, such that $\deg\chi_i = f_i(q)$ for each i.

This conjecture is true for many groups of low rank and has been proven in part for the general case. The proof proceeds by exploiting the isomorphism between the group algebra of the Weyl group and the CG-endomorphism algebra of the module corresponding to 1_B^G.

Corollary. Let L be a fixed Lie algebra. In the above notation, except for a finite number of values of q the degrees of the characters χ_i, $i \geq 1$, are not coprime to q.

Proof. Write $f_i(x) = g_i(x)/D$, D an integer and $g_i \in Z[x]$. If q does not divide D, $f_i(q)$ and q will not be coprime, for f_i has constant coefficient zero.

5. The Main Theorem.

Our object is to prove the following theorem:

Theorem A. (i) If Conjecture I holds then, excepting for each r at most a finite number of values of q, $PSp(2^{r+1},q)$ has no multiply transitive permutation representations for $r > 1$.

(ii) $PSp(4,q)$ has no multiply transitive permutation representations for $q > 2$, regardless of I.

We prove these results in a number of stages. Write $G^* = Sp(2^{r+1},q)$ and $G = PSp(2^{r+1},q)$ as before, $r \geq 1$, and suppose G has a multiply transitive permutation representation ρ on a set Ω with $|\Omega| = n$. G^* has an action on Ω via the map $G^* \to G$, which it will at times be convenient to consider. Let $\alpha \in \Omega$ and let G_α be the subgroup of G fixing α.

(A) If $q = p^t$ and $p \nmid n$ then G_α is a maximal parabolic subgroup of G.

Proof. Consider G as a Chevalley group. G has a BN-pair and as $p \nmid n$ we may take the Sylow p-subgroup U of G to be contained in G_α. Writing $B_\alpha = B \cap G_\alpha$ we have $B \supset HB_\alpha \supset HU = B$. Hence, by Theorem 2. of §1, HG_α is a parabolic subgroup of G. Now G_α, being the stabiliser of a point in a multiply transitive G-set, is maximal in G. Thus either $HG_\alpha = G_\alpha$ or $HG_\alpha = G$. In the first case we have the required result. In the second case, H acts transitively on Ω. Now H normalises each root subgroup X_r and if $r > 0$, $X_r \subset U \subset G_\alpha$. For each $\beta \in \Omega$ there is an $h \in H$ such that $h\alpha = \beta$. Then

$X_r = X_r{}^h \subset G_\alpha{}^h = G_\beta$. X_r therefore acts trivially on Ω. But in the cases we are considering G is simple. Hence ρ is faithful, contradiction.

Note that this result holds for arbitrary L(q).

(B) p|n.

Proof. If p∤n, $G_\alpha = G_J$ for some maximal $J \subset R$, the set of involutory generators of the Weyl group W. Now the number of (G_α, G_α) double cosets is 2, so by Theorem 4, the number of (W_J, W_J) double cosets is 2. We show this is false. The structure of the Weyl group of $C_{2^{r+1}}$ is given in [7].

For C_l, the Weyl group W may be considered as a permutation group on the 2l points 1, ... ,l,-1, ... ,-l. The fundamental reflections $w_1, \ldots, w_l$ are given by

$w_i = (i\ i+1)(-i\ -i-1)$, $1 \leq i < l$,

$w_l = (l\ -l)$.

Thus $|W| = 2^l l!$

Write $J_i = \langle w_j;\ j \neq i \rangle$ and $W_i = W_{J_i}$. We must prove that the number of (W_i, W_i) double cosets is more than 2.

Now W_l is the symmetric group on {1, ... ,l} and $|W_l| = l!$. $(1\ -1) \notin W_l$ and $(1\ -1)W_l(1\ -1)$ is symmetric on {-1,2, ... ,l}. Hence $W_l \cap W_l^{(1\ -1)}$ is symmetric on {2, ... ,l} and has order (l-1)!.

Thus $|W_l(1\ -1)W_l| = |W_l|^2/|W_l \cap W_l^{(1\ -1)}|$

$= (l!)^2/(l-1)!$

$= l.l!$

So $W = W_1 \cup W_1(1\ -1)W_1$ if and only if $2^l l! = l!+l.l!$. Hence $2^l = 1+l$, which is $l = 1$. But this is not one of our cases. Hence there are more than 2 (W_1,W_1) double cosets.

Now let $i< l$. $W_i = \langle w_1, \ldots, w_{i-1}\rangle \times \langle w_{i+1}, \ldots, w_l\rangle$ has order $i!2^{l-i}(l-i)!$. $(1\ -1) \notin W_i$ and clearly $|W_i \cap W_i^{(1\ -1)}| = (i-1)!2^{l-i}(l-i)!$. Hence

$$|W_i(1\ -1)W_i| = [i!2^{l-i}(l-i)!]^2/[(i-1)!2^{l-i}(l-i)!]$$
$$= i.i!2^{l-i}(l-i)!.$$

Hence $W = W_i \cup W_i(1\ -1)W_i$ if and only if $2^l l! = (i+1)!2^{l-i}(l-i)!$. It may easily be shown that if $l > 1$ this does not happen. Thus (B) is proven.

(C) $n||B| = q^{2^{2r}}(q-1)^{2^r}$, except for each r at most a finite number of prime powers q, if Conjecture I holds.

<u>Proof.</u> In the notation of Conjecture I we have $1_B{}^G = 1_G+\chi_1+ \ldots +\chi_r$, χ_i irreducible. We can also write $1_{G_\alpha}{}^G = 1_G+\zeta$, where ζ is an irreducible character. ζ has degree $n-1 \not\equiv 0 \pmod p$. If every χ_i has degree divisible by the prime p, ζ is not among the χ_i, so the scalar product $(1_B{}^G, 1_{G_\alpha}{}^G) = 1$. This means that $BG_\alpha = G_\alpha B = G$. Hence $n = (G:G_\alpha)||B|$. By the corollary to I this situation occurs

almost always if I holds, so we have the result.

Later we shall show that I holds for $r = 1$.

(D) For some $c = 1$ or 2, $n \equiv c \pmod{(q^{2^r}+1)/d}$.

Proof. Write GL for $GL(2^{r+1},q)$, $\overline{GL}$ for $GL(2^{r+1},q^{2^{r+1}})$ and $\overline{G}$ for $Sp(2^{r+1},q^{2^{r+1}})$. Let x be a primitive $q^{2^{r+1}}-1$'th root of 1 in $GF(q^{2^{r+1}})$ and $\zeta = x^{q^{2^r}-1}$. Write X for the diagonal matrix in $\overline{GL}$ such that $X = (X_{ij})$ with $X_{ij} = 0$ if $i \neq j$, $X_{2i+1,2i+1} = x^{q^i}$, $X_{2i,2i} = x^{q^{2^r+i-1}}$. Put $X^{q^{2^r}-1} = Y$. Then $Y = (Y_{ij})$ with $Y_{2i+1,2i+1} = \zeta^{q^i}$, $Y_{2i,2i} = \zeta^{-q^{i-1}}$. Thus $Y \in \overline{G}$ and $Y^{q^{2^r}+1} = 1$. Now if A is the element of $\overline{GL}$ defined by $A_{i,i+2} = 1$, $1 \leq i \leq 2^{r+1}-2$,

$A_{2^{r+1}-1,2} = 1$, $A_{2^{r+1},1} = -1$,

$A_{ij} = 0$ otherwise, we see that $A \in \overline{G}$ and $AXA^{-1} = X^q$.

From Lemma 2, there is a B in $\overline{G}$ such that $A^{-1} = B^{-1}B^{(q)}$. Put $x = BXB^{-1}$, $y = BYB^{-1}$ and $a = BAB^{-1}$. Then

$$x^{(q)} = B^{(q)}X^{(q)}B^{-(q)}$$
$$= B^{(q)}AXA^{-1}B^{-(q)}, \text{ as } X^{(q)} = X^q,$$
$$= BXB^{-1} = x. \text{ Hence } x \in GL. \text{ Similarly } y \text{ and } a \text{ are in } GL.$$

Therefore y and a are in $GL \cap \overline{G} = G^*$.

Write $N = \langle y, a \rangle$. We have $y^{q^{2^r}+1} = a^{2^{r+1}} = 1$, $aya^{-1} = y^q$.

Let b be any integer not divisible by $(q^{2^r}+1)/d$. Then

$C_{G^*}(y^b) = G^* \cap C_{GL}(y^b)$

$= G^* \cap \langle x \rangle$, by Lemma 1,

$= \langle y \rangle$. For if s is an integer, $x^s \in G^*$ if and only if $X^s \in \bar{G}$, which happens if and only if s is divisible by $q^{2^r}-1$, if and only if $X^s \in \langle Y \rangle$.

From Theorem 7.3 on page 187 of [6] we see that $N = N_{G^*}(\langle y^b \rangle)$.

In this section we consider the action of G^* on Ω.

Let s be a prime power dividing $(q^{2^r}+1)/d$ and write $s = s_0^e$, s_0 prime. Now s_0 is prime to $(G^* : \langle y \rangle)$, so the Sylow s_0-subgroup of $\langle y \rangle$, which is cyclic, is a Sylow s_0-subgroup of G^*. If $S = \langle y^b \rangle$, the unique subgroup of $\langle y \rangle$ of order s, then S is the unique subgroup of order s in any Sylow s_0-subgroup of G^* which contains S. Hence S is pronormal in G^*.

Let Γ_s be the set of points fixed by S. If $|\Gamma_s| = m_s$, either $m_s = 0$, $m_s = 1$ or $m_s \geq 2$. In the last case we know from Lemma 3. that $N_{G^*}(S)$ acts doubly transitively on Γ_s, which means that N acts doubly transitively on Γ_s.

Consider the following four possibilities:

(1) $m_s = 0$.

(2) $m_s = 1$. By Lemma 8, y fixes exactly one point of Ω.

(3) $m_s = 2$ and y fixes Γ_s. y fixes no other points of Ω.

(4) $m_s = 1+2^i$, $i \leq r$;[1] and y acts transitively on Γ_s. y fixes no point of Ω.

We see from Lemma 7. that these are the only possibilities.

If (1) holds we have from Lemma 8. that $s_0|n$. But $|B|$ and $(q^{2^r}+1)/d$ are coprime, $s_0|(q^{2^r}+1)/d$ and $n||B|$ almost always, contradiction (for the remainder of the proof we are assuming that $n||B|$).

If (2) holds it is clear that $m_{s'} = 1$ for every prime power s'. Now let Δ be an S orbit of Ω of length greater than one. Suppose $s\not||\Delta|$. Then $|\Delta| = s_0^f$ for some $f < e$. Now $y^{bs_0^f}$ has order s_0^{e-f} and fixes all points of the orbit Δ, a contradiction, since an element of order a power of s_0 fixes only one point of Ω. Hence $s||\Delta|$.

We therefore have $s|n-1$ for all prime powers s dividing $(q^{2^r}+1)/d$, so $(q^{2^r}+1)/d|n-1$.

If (3) holds, it holds for every s and similar reasoning shows that $(q^{2^r}+1)/d|n-2$.

Suppose (4) holds, and suppose first that $m_s = 2$ for all s.

We see that y^2 fixes exactly 2 points of Ω. Therefore for every prime power s dividing $(q^{2^r}+1)/d$, the corresponding subgroup S fixes the same 2 points. Similar reasoning to case (1) gives that $(q^{2^r}+1)/d \mid n-2$.

Now suppose that for some s, $m_s = 1+2^i > 2$. Take a prime power s' dividing m_s. Then $s' \mid (q^{2^r}+1)/d$ and $m_{s'} = 1+2^j$ for some j. Γ_s and $\Gamma_{s'}$ are each y-orbits of Ω. We have two cases:

(i) $\Gamma_s = \Gamma_{s'}$. Then $s_0 \mid m_s$ and as $s_0 \mid n-m_s$ by Lemma 8, $s_0 \mid n$, contradiction.

(ii) $\Gamma_s \cap \Gamma_{s'} = \varphi$. Write $\{a,b\}$ for the least common multiple of a and b. Now y^{m_s} fixes the points of Γ_s and $y^{m_{s'}}$ fixes the points of $\Gamma_{s'}$, so $y^{\{m_s,m_{s'}\}}$ fixes the points of $\Gamma_s \cup \Gamma_{s'}$. It follows that no odd prime divides the order of $y^{\{m_s,m_{s'}\}}$, for otherwise $y^{\{m_s,m_{s'}\}}$ would have to fix only the points in one y-orbit, which it does not. We must have $y^{2\{m_s,m_{s'}\}} = 1$, since $4 \nmid q^{2^r}+1$.

Thus $q^{2^r}+1 \mid 2\{1+2^i,1+2^j\}$. As $q \geqslant 2$ we have $2^{2^r} < 2.2^{i+1}2^{j+1} = 2^{i+j+3} \leqslant 2^{2r+5}$. Hence $2^r < 2r+5$ and $r \leqslant 3$.

<u>r = 3</u>: $q^8+1 \mid 2\{1+2^i,1+2^j\}$, $i,j \leqslant 4$,

$\leqslant 2.9.17$. Thus $q = 2$, $q^8+1 = 257$, which gives no

solutions.

$\underline{r = 2}$: $q^4+1 \mid 2\{1+2^i, 1+2^j\}$, $i,j \leq 3$

$\leq 2.5.9$. Hence $q = 2$ or 3, $q^4+1 = 17$ or 82,

giving no solutions.

$\underline{r = 1}$: $q^2+1 \mid 2\{1+2^i, 1+2^j\}$, $i,j \leq 2$,

$\leq 2.3.5$. Thus $q = 2$ or 3. But in each of these cases, q^2+1 is not divisible by two odd primes, contradiction. We have therefore proven (D).

(E) We may reduce to the following possibilities:

(a) $r = 1$, (i) $q = 3$, $n = 6$

(ii) $q = 4$, $n = 18$

(iii) $q = 5$, $n = 40$

(iv) $q = 8$, $n = 196$

(v) $q = 11$, $n = 550$

(b) $n = q^{2^{r+1}}$, $r \geq 1$, any q.

(c) $n = 2q^{2^{r+1}a}$, some $a \geq 1$, $r \geq 1$, any q.

$\underline{\text{Proof.}}$ $n \equiv c \pmod{(q^{2^r}+1)/d}$, $c = 1$ or 2, $q = p^t$, p prime. Write $n = q^i p^{-b} m$, $1 \leq i \leq 2^{2r}$, $0 \leq b < t$, $p \nmid m$ and $i = l2^r - j$, $1 \leq l \leq 2^r$, $0 \leq j < 2^r$. Now

$1/q^{2^r} \equiv -1 \pmod{(q^{2^r}+1)/d}$. Hence

$m = nq^{-l2^r} q^j p^b \equiv c(-1)^l q^j p^b$. Write

* $m = k(q^{2^r}+1)/d + (-1)^l c q^j p^b \mid (q-1)^{2^r}/d$.

We have to consider various separate cases.

(1) l even. Then $k \leq 0$.

(i) $k = 0$. As $p \nmid q-1$, $b = j = 0$. $m = (-1)^l c = c$,

$n = cq^{l2^r} = cq^{\frac{1}{2}l2^{r+1}}$. If $c = 2$ this is case (c).

Suppose $c = 1$, $a = \frac{1}{2}l > 1$. We show we have a contradiction.

$n-1 = q^{a2^{r+1}}-1 \mid \prod_{k=1}^{2^r}(q^{2k}-1)$. Now by Lemma 11,

$(q^{a2^{r+1}}-1, q^{2k}-1) = q^{2(a2^r,k)}-1$,

$(q^{a2^r}-1, q^{2k}-1) = q^{2(a2^{r-1},k)}-1$ and $(q^{a2^r}-1, q^{a2^r}+1) = d$. It follows that unless $k = 2^r$, $(q^{a2^r}+1, q^{2k}-1) = d$. Also

$q^{2^{r+1}}-1 = (q^{2^r}+1)(q^{2^r}-1)$ and $(q^{a2^r}+1, q^{2^r}-1) = d$,

$(q^{a2^r}+1, q^{2^r}+1) = d$. Hence

$q^{a2^r}+1 \mid d^{2^r}$, contradiction. So we in fact have $a = 1$ and case (b).

(ii) $k < 0$. Since $m > 0$ we have

$q^{2^r}+1 < cdq^j p^b \leq cdq^{j+1}/p$. Thus $p < cd/q^{2^r-j-1}$. This gives $p = 3$, $j = 2^r-1$, $c = d = 2$ and $b = t-1$.

$2m = -(q^{2^r}+1)+4q^{2^r}/3$

$= (q^{2^r}-3)/3 \mid (q-1)^{2^r}$. Now $(q-1, q^{2^r}-3) = (q-1,2) = 2$. Thus $(q^{2^r}-3)/3 \mid 2^{2^r}$. $3^{2^r} \leq q^{2^r} \leq 3.2^{2^r}+3$. The only solution is

$r = 1$, $q = 3$. Then $m = 1$ and $n = 3^3$. But $n-1 = 26 \nmid |PSp(4,3)|$, contradiction.

(2) Suppose l is odd. Then as $m > 0$, $k > 0$.

(i) $k = 1$.

$q^{2^r}+1-cdq^j p^b \leq (q-1)^{2^r} \leq q^{2^r}+1-2q^{2^r-1}$, by Lemma 10.

Hence $2q^{2^r-1} \leq cdq^j p^b \leq cdq^{j+1}/p$. Thus $p \leq cd/(2q^{2^r-2-j})$.

Hence $j = 2^r-1$ and $dm = q^{2^r}+1-cdq^{2^r-1}p^b \mid (q-1)^{2^r}$. Now $(q-1, dm) = (q-1, 2-cdp^b)$. Hence we have

$dm \mid (cdp^b-2)^{2^r}$.

Now $cdp^b \geq 2$, else $dm > (q-1)^{2^r}$. We have two cases.

(a) $cdp^b = 2$.

$dm = q^{2^r}+1-2q^{2^r-1} \mid (q-1)^{2^r}$. From Lemma 10. we have $r = 1$ or $q = 2$.

<u>$r = 1$</u>: $dm = q^2+1-2q = (q-1)^2$. $i = 2l-j = 1$. $n = q(q-1)^2/dp^b$.

If $dp^b = 1$, $n-1 = q(q-1)^2-1 \,||\, |G|$, and $|G| = q^4(q-1)^2(q+1)^2(q^2+1)$. Now $q^2+1 \mid n-2$, so $(q^2+1, n-1) = 1$. Also $(n-1, q) = (n-1, q-1) = 1$. Hence $n-1 \mid (q+1)^2$. But $(n-1, q+1) = (5, q+1) \mid 5$, so $q(q-1)^2 \mid 25$. This is false for any prime power greater than 2, so this case does not occur.

It follows that $dp^b = 2$, $n = \frac{1}{2}q(q-1)^2$.

$n-1 = \frac{1}{2}q(q-1)^2-1 \mid q^4(q-1)^2(q+1)^2(q^2+1)/d$. Therefore, as

$n-1 = \frac{1}{2}(q^2+1)(q-2)$, we obtain

$q-2 \mid 2q^4(q-1)^2(q+1)^2/d$. Now $(q-2,q-1) = 1$ and $(q-2,q+1) \mid 3$.

Hence $q-2 \mid 2.3^2$. $q = 3,4,5,8$ or 11. These are case (a).

<u>$q = 2$</u>: $m = 1$ and $i = 12^r - j = u2^r+1$, u even.

$n = 2^{u2^r+1}/p^b$, $p^b = 1$ or 2. This gives cases (b) and (c) again.

(b) $cdp^b > 2$. $dm = q^{2^r+1} - cdq^{2^r-1}p^b < (cdp^b)^{2^r}$. Hence $q^{2^r-1}(q-cdp^b) < (cdp^b)^{2^r}$. If $q = cdp^b$ we have $p = c = 2$, $b = t-1$, $d = 1$. Then $n = 2q^{u2^r+1}q^{-1}$, u even,

$$= 2q^{a2^{r+1}} \text{ as before.}$$

If $q > cdp^b$ it is easy to see that $q \geq 5cdp^b/4$. Hence $q^{2^r}/5 \leq (cdp^b)^{2^r}$ and $q \leq cdp^b.5^{1/2^r}$. Hence $5/4 \leq 5^{1/2^r}$.

We have $r = 1$ or 2.

<u>$r = 1$</u>: $dm = q^2+1-cdqp^b \mid (q-1)^2$. Now

$(q^2+1-cdqp^b,(q-1)^2) = (2q-cdqp^b,(q-1)^2) = (2-cdp^b,(q-1)^2)$.

Hence $q^2+1-cdqp^b \mid cdp^b-2$. $q^2+3 \leq cdp^b(q+1)$,

$cdp^b \geq q-1+4/(q+1)$. Thus either $p = c = 2$, $p^b = \frac{1}{2}q$, $m = 1$ and $n = 2$ or $p = 3$, $c = d = 2$, $p^b = q/3$ and $m = \frac{1}{2}-q^2/6$. Each of these cases is clearly impossible.

<u>$r = 2$:</u> $dm = q^4+1-cdq^3p^b \mid (q-1)^4$. Now

$(q^4+1-cdq^3p^b,(q-1)^4) = (4q^3-6q^2+4q-cdq^3p^b,(q-1)^4)$

$\mid 4q^2-6q+4-cdq^2p^b$. Therefore

$q^4+1-cdq^3p^b \leqslant cdq^2p^b-4q^2+6q-4$ and
$q^4+4q^2-6q+5 \leqslant cdq^2p^b(q+1)$. Hence $cdp^b \geqslant q$. As $dm > 0$ we have equality, with $p = c = 2$, $d = 1$, $p^b = \frac{1}{2}q$. Then $m = 1$, $l = 1$ or 3, $i = 1$ or 9 and $n = 2$ or $2q^8$. The first is plainly impossible, the second is covered by (c).

(ii) $k > 1$. Then $dm = k(q^{2^r}+1)-cdq^jp^b \mid (q-1)^{2^r}$. As in (i) we have $j = 2^r-1$. Now $dm = (k-1)(q^{2^r}+1)+q^{2^r-1}(q-cdp^b)+1$. Hence $q < cdp^b$. We must have $p = 3$, $c = d = 2$, $p^b = q/3$. Then
$2m = 2(q^{2^r}+1)-4q^{2^r-1}.q/3 = 2(q^{2^r}+3)/3 \mid (q-1)^{2^r}$.
$(q^{2^r}+3, q-1) \mid 4$. Hence $2(q^{2^r}+3) \mid 3.4^{2^r}$. Thus $r = 1$, $q = 3$.
$m = (3^2+3)/3 = 4$ and $m \mid 2^2/2$, contradiction.

This completes the proof of (E). We now consider separately the cases $r = 1$ and $r > 1$.

<u>Proof of Theorem A(ii).</u> We have to show first that the above values of n give contradictions for $r = 1$ and secondly that $n \mid\mid |B|$ for $r = 1$.

(F) All the cases of (E) give contradictions for $r = 1$.

<u>Proof.</u> (a) (i) $q = 3$, $n = 6$. $|PSp(4,3)| = 2^6 3^4 5$. But $|S_6| = 6! = 2^4 3^2 5$. Hence we have a contradiction.

(iii) and (v) we do together.

$|G| = 2^6 3^2 5^4 13$, $q = 5$

$2^6 3^2 5^2 11^4 61$, $q = 11$. Let $\alpha, \beta \in \Omega$, $\alpha \neq \beta$.

$|G_\alpha| = 2^3 3^2 5^3 13$, $q = 5$

$2^5 3^2 11^3 61$, $q = 11$.

$|G_{\alpha\beta}| = 2^3 3.5^3$, $q = 5$

$2^5 11^3$, $q = 11$.

Let Q be a Sylow q-subgroup of $G_{\alpha\beta}$ and let Q fix exactly m points of Ω. $(G_\alpha : N_{G_\alpha}(Q)) = (G_{\alpha\beta} : N_{G_{\alpha\beta}}(Q))(n-1)(m-1)^{-1}$ is integral, so, by Sylow's Theorem,

$(G_{\alpha\beta} : N_{G_{\alpha\beta}}(Q)) = 1$ or 6, $q = 5$

1, $q = 11$.

Consider $q = 11$. $m = 11k$, $k < 50$, and by integrality $11k-1 \mid 550-1$. There is no such k. Hence $q = 11$ may be ignored.

Consider $q = 5$. $m = 5k$, $k < 8$, and by integrality $5k-1 \mid 40-1$ or $6(40-1)$. Hence $k = 2$ and $(G_{\alpha\beta} : N_{G_{\alpha\beta}}(Q)) = 6$.

$|N_G(Q)| = |N_{G_{\alpha\beta}}(Q)|m(m-1)$ by Lemma 4.

$= 2^3 5^3 .10.9 = 2^4 3^2 5^4$. We show this is not the case.

$|Q| = 5^3$, $|U| = 5^4$. Hence we may take Q as a normal subgroup of U with cyclic factor group. $U' < Q$.

From the Chevalley Commutator Formula, or by matrix calculations, $[X_{p_1}, X_{p_2}] < X_{p_1+p_2} X_{2p_1+p_2}$,

$[X_{p_1}, X_{p_1+p_2}] = X_{2p_1+p_2}$. Commutators of other root subgroups of U are trivial. Hence $U' = X_{p_1+p_2} X_{2p_1+p_2}$.

$Q = \langle x_{p_1}(t_1)x_{p_2}(t_2), U' \rangle$, $t_1, t_2 \in GF(q)$, not both zero.

(1) Suppose $t_1 \neq 0$. Then $Q' = X_{2p_1+p_2}$ and $C_Q(Q') = X_{p_1+p_2}X_{2p_1+p_2}$. Both these groups are characteristic in Q. Hence $N_G(Q) < N_G(X_{2p_1+p_2}) \cap N_G(X_{p_1+p_2}X_{2p_1+p_2}) = \overline{N}$, say.

By the Commutator Formula, $B < \overline{N}$. Thus if $w \in W$, $Bn_wB \subset \overline{N}$ if and only if $n_w \in \overline{N}$.

$$n_w X_{2p_1+p_2} n_w^{-1} = X_{w(2p_1+p_2)} \text{ by [2] page 214}$$

$$= X_{2p_1+p_2} \text{ if and only if } w(2p_1+p_2) = 2p_1+p_2,$$

if and only if $w = w_2$ (in the notation of §3). But

$n_{w_2} X_{p_1+p_2} n_{w_2}^{-1} = X_{w_2(p_1+p_2)} = X_{p_1}$. Thus $\overline{N} = B$. But $|B| = 2^3 5^4$, so $|N_G(Q)| \mid 2^3 5^4$, contradiction.

(2) Suppose $t_1 = 0$. Then $Q = X_{p_2}X_{p_1+p_2}X_{2p_1+p_2}$. As before $N_G(Q) \supset B$. Routine calculation shows that $N_G(Q) = B \cup Bn_{w_1}B$. Thus $|N_G(Q)| = |B|(1+q^{N_w})$, where N_w is the number of positive roots of C_2 transformed by w_1 into negative roots ([2] page 220). In this case $N_w = 1$. Thus $|N_G(Q)| = \frac{1}{2}.5^4(5-1)^4(5+1) = 2^6 3.5^4$, contradiction.

(ii) $q = 4$, $n = 18$. $|G| = 2^8 3^2 5^2 17$, $|G_\alpha| = 2^7 5^2 17$ and $|G_{\alpha\beta}| = 2^7 5^2$.

Let P be a Sylow 5-subgroup of $G_{\alpha\beta}$ and suppose P fixes m

points of Ω. $m = 3$ or 8. By Sylow's Theorem, $(G_{\alpha\beta}:N_{G_{\alpha\beta}}(P)) = 1$ or 2^4. Now $(G_\alpha:N_{G_\alpha}(P)) = (G_{\alpha\beta}:N_{G_{\alpha\beta}}(P))(n-1)/(m-1)$ is integral. Hence $m = 3$ and $(G_{\alpha\beta}:N_{G_{\alpha\beta}}(P)) = 2^4$.

$|N_G(P)| = |N_{G_{\alpha\beta}}(P)|m(m-1) = 2^4 3.5^2$. We show this is false.

Since $G = G^* = SP(4,4)$ we may work with matrices in G^*.

A Sylow 5-subgroup of G^* is generated by elements

$$a = \begin{bmatrix} A & 0 \\ 0 & I_2 \end{bmatrix}, \quad b = \begin{bmatrix} I_2 & 0 \\ 0 & A \end{bmatrix},$$

where $A \in SL(2,4)$ has order 5. Using Lemma 1 we see that $|C_{GL(4,4)}(ab^2)| = (4^2-1)^2$. In fact the centraliser consists of elements $\begin{bmatrix} C & 0 \\ 0 & D \end{bmatrix}$, such that $C,D \in C_{GL(2,4)}(A)$, which is generated by an element of order 15 with determinant a primitive cube root of 1. Such an element is in G^* if and only if $C,D \in SL(2,4)$. Hence $|C_{G^*}(ab^2)| = 5^2$. Thus $|C_G(P)| = 5^2$ and $C_G(P) = P$.

The only elements of P with the same eigenvalues as a are a, b, a^{-1} and b^{-1}. Thus if $g \in N_G(P)$, $gag^{-1} = a, b, a^{-1}$ or b^{-1} and there are the same choices for gbg^{-1}. Using the fact that gag^{-1} and gbg^{-1} generate P we see that $(N_G(P):P) \leq 8$. This

is a contradiction.

(iv) $q = 8$, $n = 196$.

$|G| = 2^{12}3^4 5.7^2 13$, $|G_\alpha| = 2^{10}3^4 5.13$ and $|G_{\alpha\beta}| = 2^{10}3^3$. We work in $Sp(4,8)$ and apply Lemma 5, taking $p = 3$. Let Q be a Sylow 3-subgroup of $G_{\alpha\beta}$ and P a Sylow 3-subgroup of G. P is generated by elements $a = \begin{bmatrix} A & 0 \\ 0 & I_2 \end{bmatrix}$, $b = \begin{bmatrix} I_2 & 0 \\ 0 & A \end{bmatrix}$, where $A \in SL(2,8)$ has order 9. The argument used in the preceeding case shows that $C_G(P) = P$. Now $C_G(a^i b^j) = P$ unless $i = 0$, $j = 0$ or $i = j$. Clearly Q, being a subgroup of P of order 27, must contain elements other than the elements a^i, b^i and $(ab)^i$. Hence $C_G(Q) = Q$.

If $g \in N_G(Q)$, $g \in N_G(C_G(Q)) = N_G(P)$. Hence $P \Delta N_G(Q)$. This contradicts Lemma 5.

(b) $n = q^4$, any q.

Let $\alpha \in \Omega$. If U is a Sylow p-subgroup of G, $G = UG_\alpha$. We may take the elements of U as left coset representatives for G_α in G.

Choose $\theta \in GF(q)^*$, the multiplicative group of $GF(q)$, of maximal order such that $h = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \theta & \\ & & & \theta^{-1} \end{bmatrix}$ is in some G_α^*. Such a θ exists because $(q-1)^2/d \,|\, |G_\alpha|$. Now $h \in H$ normalises U, so if

$u \in U$, $h(uG_\alpha) = (huh^{-1})hG_\alpha = (huh^{-1})G_\alpha$. Thus the number of points of Ω fixed by h is $|C_U(h)|$.

A general element of U is

$u = x_{p_1}(t_1)x_{p_2}(t_2)x_{p_1+p_2}(t_3)x_{2p_1+p_2}(t_4)$ and one checks that

$huh^{-1} = x_{p_1}(\theta^{-1}t_1)x_{p_2}(\theta^2 t_2)x_{p_1+p_2}(\theta t_3)x_{2p_1+p_2}(t_4)$. Here

$t_1, \ldots, t_4 \in GF(q)$.

Now either $\theta^2 \neq 1$ and h fixes exactly q points or $\theta^2 = 1$ and h fixes q^2 points. If $\theta^2 = 1$ it is clear that $q = 3$. We do this case later.

Suppose $\theta^2 \neq 1$ and write $S = \langle h \rangle$. By Lemma 4,

$|N_G(S)| \leq |N_L(S)|q(q-1)$, $L = G_{\alpha\beta}$, $\beta \neq \alpha \in \Omega$.

$\leq |L|q(q-1) = q(q-1)^2(q+1)/d$. But h is centralised by the elements $\begin{vmatrix} A & 0 & 0 \\ & 0 & 0 \\ 0\ 0 & a & 0 \\ 0\ 0 & 0 & a^{-1} \end{vmatrix}$ of G, $A \in SL(2,q)$, $a \neq 0$. Thus

$|C_G(S)| \geq (q-1)|PSL(2,q)| = q(q-1)^2(q+1)/d$. Also

$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{vmatrix}$ normalises S. Thus

$|N_G(S)| > q(q-1)^2(q+1)/d$, contradiction.

We now dispose of $q = 3$. h fixes 9 points. Hence

$|N_G(S)| \leq |L|.9(9-1) = 2^2 3^2 2^3 = 2^5 3^2$.

Now h is centralised by elements $\begin{vmatrix} A & 0 \\ 0 & B \end{vmatrix}$ of G,

$A,B \in SL(2,3)$. Thus $|C_G(S)| \geq \frac{1}{2}|SL(2,3)|^2$

$= \frac{1}{2}(3.2.4)^2$

$= 2^5 3^2$. As before

$|N_G(S)| > 2^5 3^2$, contradiction.

The case PSp(4,3) was first studied by Parker in [10].

(c) $n = 2q^{4a}$, any q. As $n||G|$ we have $a = 1$.

$n-1 = 2q^4-1 \,|\, (q-1)^2(q+1)^2(q^2+1)/d$. But as

$n-2 = 2(q^4-1) = 2(q-1)(q+1)(q^2+1)$ we have

$(q-1,n-1) = (q+1,n-1) = (q^2+1,n-1) = 1$. Hence $n-1\,|\,1/d$, contradiction.

We have now proven (F). We now have to show that $n||B|$ for $r = 1$. This involves proving that if $1_B{}^G = 1_G + \chi_1 + \ldots + \chi_r$, χ_i irreducible, then $p|\deg\chi_i$, $i \geq 1$.

For the Weyl group W of C_2 we have subgroups $W_{\{p_1\}} = \langle w_1 \rangle$, $W_{\{p_2\}} = \langle w_2 \rangle$, $W_\Sigma = W = \langle w_1, w_2 \rangle$, $W_\varphi = \{1\}$. Using the notation of Theorem 4. of §4, write ψ_1 for $\psi_{\{p_1\}}$, etc.

W has conjugacy classes $C_0 = \{1\}$, $C_1 = \{(w_1w_2)^2\}$, $C_2 = \{w_1w_2, w_2w_1\}$, $C_3 = \{w_1, w_2w_1w_2\}$ and $C_4 = \{w_2, w_1w_2w_1\}$. We have for the characters ψ_J:

	C_0	C_1	C_2	C_3	C_4
ψ_Σ	1	1	1	1	1
ψ_1	4	0	0	2	0
ψ_2	4	0	2	0	0
ψ_ϕ	8	0	0	0	0

The entries in the following table are the scalar products of these characters:

	ψ_Σ	ψ_1	ψ_2	ψ_ϕ
ψ_Σ	1	1	1	1
ψ_1	1	3	2	4
ψ_2	1	2	3	4
ψ_ϕ	1	4	4	8

A similar table is valid for χ_Σ, χ_1, χ_2 and χ_ϕ, by Theorem 4. Using it, we see that

$\chi_\Sigma = 1_G$, $\chi_1 = 1_G+\varphi+\psi$, $\chi_2 = 1_G+\varphi+\psi'$ and

$\chi_\phi = 1_B^G = 1_G+2\varphi+\psi+\psi'+\chi$, where φ,ψ,ψ' and χ are irreducible characters. Now $\chi = \chi_\phi-\chi_1-\chi_2+\chi_\Sigma$. Hence

$\deg \chi = (G:B)-(G:G_{\{p_1\}})-(G:G_{\{p_2\}})+(G:G)$. Now

$G_{\{p_1\}} = B \cup Bn_{w_1}B$. As before, $|Bn_{w_1}B| = q|B|$. Also

$|B| = q^4(q-1)^4/d$. Hence

$\deg \chi = (q+1)^2(q^2+1)-2(q+1)(q^2+1)+1 = q^4$.

Consider $G_{\{p_2\}}$. Using (3) of §3 we may write

$n_{w_2} = x_{p_2}(1)x_{-p_2}(-1)x_{p_2}(1)$, by page 214 of [2],

$$= \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{vmatrix}.$$

Moreover we see from §3 that B is contained in the subgroup of "matrices" in G with first column $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. Hence $G_{\{p_2\}} = B \cup Bn_{w_2}B$ is contained in this subgroup, fixing the point $P = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ of projective 3-space $\underline{P}$. Since $G_{\{p_2\}}$ is maximal, $G_{\{p_2\}}$ is the whole subgroup. As $1_{G_{\{p_2\}}}{}^G = 1_G+\varphi+\psi'$, G has rank 3 action on the points of $\underline{P}$. The orbits of $G_{\{p_2\}}$ on $\underline{P}$ consist of the point P, the $q+q^2$ points $\neq P$ on the orthogonal hyperplane to P and the q^3 points outside this hyperplane. We shall use the results of Higman in [5] to obtain the degrees of the characters φ and ψ'.

In Higman's notation, $k = q+q^2$, $l = q^3$, $k < l$. We wish to calculate the Higman parameters λ and μ.

Lemma ([5] Lemma 5.) $\mu l = k(k-\lambda-1)$.

In our case $\mu q^3 = (q+q^2)(q+q^2-\lambda-1)$. Hence $q^2 | q-\lambda-1$. Since $\lambda < k = q+q^2$, $\lambda = q^2+q-1$ or $\lambda = q-1$. In the former case $\mu = 0$. But as $G_{\{p_2\}}$ is maximal in G, the rank 3 representation of G is primitive. By [5] page 149, $\mu \neq 0$. Therefore $\lambda = q-1$ and $\mu = q+1$.

Write $D = (\lambda-\mu)^2+4(k-\mu) = 2^2+4(q^2-1) = 4q^2$. For the degrees f_2 and f_3 of φ and ψ' we have in some order

$$f_2, f_3 = [2k+(\lambda-\mu)(k+1) \mp D(k+1)]/(\mp 2\sqrt{D})$$

$$= \pm\tfrac{1}{2}q^2+\tfrac{1}{2}q(1+q+q^2).$$

Thus as $q > 2$, $p | f_2, f_3$. We therefore have that p divides the degrees of the irreducible non trivial constituents of $1_B{}^G$. This completes the proof of Theorem A (ii).

Proof of Theorem A (i). If $G = PSp(2^{r+1}, q)$, $r > 1$, has a multiply transitive permutation representation of degree n on a set Ω, then excepting for each r at most a finite number of prime powers q, $n = q^{2^{r+1}}$ or $2q^{2^{r+1}}a$, a integral. We eliminate these cases, discarding as we go a finite number of prime powers.

Write $k = 2^r-1 \cdot q^{2k}-1 \,||G|$. Similar reasoning to that on page 63 shows that G* contains an element

$$x = \begin{bmatrix} y & 0 \\ 0 & I_2 \end{bmatrix}, \quad y \in Sp(2k,q) \text{ of order } q^k+1.$$ If b is an integer

such that x^b has order not dividing $q^{2k'}-1$ for any $k' < k$ then $C_{G*}(x^b)$ consists of elements $\begin{vmatrix} y^t & 0 \\ 0 & z \end{vmatrix}$, t integral, $z \in SL(2,q)$. Write $C = C_{G*}(x)$.

$N = N_{G*}(\langle x \rangle) = \langle C, a \rangle$, where $a = \begin{vmatrix} A & 0 \\ 0 & I_2 \end{vmatrix}$ satisfies the relations $a^{2k} = 1$, $axa^{-1} = x^q$.

Write $N = H \times K$, where $H = \langle x, a \rangle$ and $K \cong SL(2,q)$. We consider the action of G^* on Ω with regard to the orbits of N.

In the notation of §4 let φ be the cyclotomic polynomial for 2k and write $x^k+1 = \varphi\psi$. Let l be the product of the distinct prime divisors of k. Put $l_q = (\varphi(q), \psi(q))$. By Lemma 12, $l_q | l$ and $(\varphi(q), 2k) | l$.

Write $z = x^{\psi(q)}$. z has order $\varphi(q)$. Let Π be the set of prime powers dividing $\varphi(q)$ and coprime to 2k. If u is the product of the maximal prime powers in Π, we have that $(q)/l | u$. Let $s = s_0^{\,e} \in \Pi$, s_0 prime and let $S = \langle z^b \rangle$ be the unique subgroup of $\langle x \rangle$ of order s.

If $k' < k$, $(s, q^{2k'}-1) | (q^k+1, q^{2k'}-1)$. Now $(q^{2k}-1, q^{2k'}-1) = q^{2(k,k')}-1$ and $(q^k-1, q^{2k'}-1) = q^{(k,2k')}-1 = q^{(k,k')}-1$. Hence $(q^k+1, q^{2k'}-1) = q^{(k,k')}+1 | \psi(q)$. Thus $(s, q^{2k'}-1) | (\varphi(q), \psi(q)) = l_q$. Since $s \nmid l_q$ we have $s \nmid q^{2k'}-1$.

Therefore $C_{G*}(S) = C$, $N_{G*}(S) = N$.

s_0 is coprime to l_q, as $l_q | k$, so s_0 is coprime to $(G*:\langle z\rangle)$. A Sylow s_0-subgroup of $\langle z\rangle$ is therefore a Sylow s_0-subgroup of $G*$. As on page 64 we deduce that S is pronormal in $G*$.

Let Γ_s be the set of points of Ω fixed by S. If $|\Gamma_s| = m_s$ then either $m_s = 0$, $m_s = 1$ or $m_s \geq 2$. In the last case $N = N_{G*}(S)$ is doubly transitive on Γ_s.

Consider the following four possibilities:

(1) $m_s = 0$

(2) $m_s = 1$. By Lemma 8, x fixes exactly one point of Ω.

(3) x fixes the points of Γ_s. x fixes no other points of Ω.

$m_s = 2$ or $q+1$, any q,

2 and $q = 2$,

3 and $q = 3$,

6 and $q = 4$, or

6 and $q = 9$.

(4) m_s is a prime power, $m_s - 1 | 2k$, x^{m_s} fixes the points of Γ_s and x acts transitively on Γ_s. x fixes no point of Ω.

We see from Lemmas 6,7,8 and 9 that these are the only possibilities.

If (1) holds, we have from Lemma 8 that the S-orbits of Ω each have length divisible by s_0, so $s_0 | n$. As s_0 is coprime to

$|B|$ and $n||B|$ we have a contradiction.

If (2) holds then for all $s' \in \Pi$ $m_{s'} = 1$. By the argument of page 65 we have that $s'|n-1$ for all such s'. Hence $u|n-1$ and $\varphi(q)/l|n-1$.

If (3) holds, it holds for every $s' \in \Pi$ and $m_s = m_{s'} = m$ for all $s,s' \in \Pi$. By the same sort of reasoning we have $\varphi(q)/l|n-m$ with m taking one of the values mentioned in (3).

If (4) holds then it holds for all $s' \in \Pi$. Suppose first that every $m_s = 2$. x^2 must fix exactly 2 points of Ω, so for each s, the corresponding subgroup S fixes the same 2 points. Hence we get $\varphi(q)/l|n-2$.

Suppose now some $m_s > 2$. If $m_s = m_{s'} = m$ for all $s \in \Pi$ we get $\varphi(q)/l|n-m$ as before. If in this case m is a prime power coprime to $2k$ then $m \in \Pi$ and so $m|n-m$. Therefore $m|n$, contradiction. Hence $m|2k$. Since m divides the order of y, $\varphi(q)$, as well we get $m|(\varphi(q),2k)|l$. Hence m is a prime dividing k.

Finally, suppose that for some $s,s' \in \Pi$, $m_s \neq m_{s'}$. The x-orbits Γ_s and $\Gamma_{s'}$ are disjoint. Now we know that x^{m_s} fixes the points of Γ_s and $x^{m_{s'}}$ fixes the points of $\Gamma_{s'}$. Hence $x^{\{m_s,m_{s'}\}}$ fixes the points of $\Gamma_s \cup \Gamma_{s'}$. The order of

$x^{\{m_s,m_{s'}\}}$ is therefore divisible by no prime powers $s \in \Pi$, and therefore divides $(q^k+1)/u$. Thus $u|\{m_s,m_{s'}\}$. Since $\varphi(q)/l|u$ we have $\varphi(q)/l|\{m_s,m_{s'}\}$. Now m_s and $m_{s'}$ are bounded in terms of r, for $m_s-1|2k = 2^{r+1}-2$. Therefore only a finite number of prime powers q can satisfy the relation $\varphi(q)/l|\{m_s,m_{s'}\}$ for each r. We ignore these primes. In fact it is easily shown that the only case we are dismissing is PSp(8,2).

We have deduced that $\varphi(q)/l|n-m$, where m may take one of the following values:

(i) m = 1,2 or q+1,

(ii) m is a prime dividing k,

(iii) m = 2 and q = 2, m = 3 and q = 3, m = 6 and q = 4 or m = 6 and q = 9.

Now $n = q^{2^{r+1}}$ or $2q^{2^{r+1}a}$. But $q^{2^{r+1}} \equiv q^2 \pmod{\varphi(q)/l}$. Also if r > 2 it is easily seen that the degree of the polynomial $\varphi(x)$, the number of coprime residues mod 2k, is greater than 2. Hence the relation $q^2 \equiv m \pmod{\varphi(q)/l}$, where m is one of the above numbers, is satisfied for at most a finite number of primes q for each r. This disposes of the case $n = q^{2^{r+1}}$ except for the case r = 2.

If r = 2, $\varphi(x) = x^2-x+1$ and l = 3. So

$q^2 \equiv q-1 \pmod{\varphi(q)/l}$. Clearly only a finite number of prime powers satisfy the relation $q-1 \equiv m \pmod{\varphi(q)/l}$. This case is therefore disposed of as well. In fact we can again show that we are only dismissing PSp(8,2).

Finally, let $n = 2q^{2^{r+1}a}$. $n-1 \mid\mid |G|$, so $n-1 \mid \prod_{k=1}^{2^r} (q^{2k}-1)$. But by Lemma 11, $(2q^{2^{r+1}a}{}_{-1}, q^{2k}{}_{-1}) \mid 2^{2k/(2k,2^{r+1}a)}{}_{-1}$. Hence $2q^{2^{r+1}a}{}_{-1} \mid \prod_{k=1}^{2^r} (2^{2k/(2k,2^{r+1}a)}{}_{-1})$. Clearly only a finite number of prime powers q can satisfy this equation.

The proof of Theorem A is now complete.

References

[1] E. Artin. "Geometric Algebra". New York 1957.

[2] R. W. Carter. "Simple Groups and Simple Lie Algebras". London Math. Soc. J. 40 (1965), 193-240.

[3] C. W. Curtis. "The Steinberg Character of a Finite Group with a BN-pair". J. of Algebra 4 (1966), 433-441.

[4] L. E. Dickson. "Linear Groups with an Exposition of the Galois Field Theory". Leipzig 1901.

[5] D. G. Higman. "Finite Permutation Groups of Rank 3". Math. Zeitschr. 86 (1964), 145-156.

[6] B. Huppert. "Endliche Gruppen I". Berlin 1967.

[7] N. Jacobson. "Lie Algebras". New York 1962.

[8] H. E. Jordan. "Group Characters of Various Types of Linear Groups". Amer. Math. J. 29 (1907), 387-405.

[9] S. Lang. "Algebraic Groups over Finite Fields". Amer. Math. J. 78 (1956), 555-563.

[10] E. T. Parker. "A Simple Group having no Multiply Transitive Representation". Proc. Amer. Math. Soc. 5 (1954), 606-611.

[11] J. Tits. "Algebraic and Abstract Simple Groups". Annals of Math. 80 (1964), 313-329.

[12] H. Wielandt. "Finite Permutation Groups". New York 1964.

[13] E. Witt. "Die 5-fach Transitiven Gruppen von Mathieu". Abhandl. Math. Sem. Univ. Hamburg 12 (1937), 256-264.