CLASS TWO p GROUPS AS FIXED POINT FREE AUTOMORPHISM GROUPS

Thesis by

Thomas Robert Berger

In Partial Fulfillment of the Requirements

For the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California
1967

(Submitted April 28, 1967)

ACKNOWLEDGMENTS

This research was carried out while on grants from the National Science Foundation, 1964 to 1967, and the Woodrow Wilson Foundation, 1963-64. The author was also assisted by the California Institute of Technology.

Acknowledgment is due to Professor Marshall Hall, Jr. who, during the last year, advised the author on the many problems of just remaining a graduate student. Grateful thanks are due to Professor H. Nagao and Mr. Edward Cline who read completely the initial drafts and offered many simplifying and helpful suggestions. An unwitting assistant has been E. Shult in his paper (8).

The author is indebted to Professor E. C. Dade for being his adviser. It was his initial prompting that kept the author on this problem. He read through the many drafts of this thesis and provided major simplifications, especially in sections I and II. The method of approach in section III is largely due to his seminar notes on a theorem of Thompson. It was largely through his courses, seminars, articles, notes and discussions that the author learned about group theory.

The author is also grateful to those who assisted him along the way, especially those who helped ease the last minute rush.

Errors in this thesis are the sole responsibility of the author. Time limitations did not allow complete consideration of all suggestions. And unfortunately, as always, unfound misprints live eternally under the eyes of the author.

ABSTRACT

Suppose that AG is a solvable group with normal subgroup G where $(|A|, |G|) = 1$. Assume that A is a class two odd p group all of whose irreducible representations are isomorphic to subgroups of extra special p groups. If $p^c \neq r^d + 1$ for any $c = 1,2$ and any prime r where r^{2d+1} divides $|G|$ and if $C_G(A) = 1$ then the Fitting length of G is bounded by the power of p dividing $|A|$.

The theorem is proved by applying a fixed point theorem to a reduction of the Fitting series of G. The fixed point theorem is proved by reducing a minimal counter example. If R is an extra special r subgroup of G fixed by A_1, a subgroup of A, where A_1 centralizes D(R), then all irreducible characters of A_1R which are nontrivial on Z(R) are computed. All nonlinear characters of a class two p group are computed.

TABLE OF CONTENTS

	Acknowledgments	ii
	Abstract	iv
	Introduction	1
I	Extensions of Group Characters	4
II	Class Two p Groups	9
III	Extensions of Extra Special Groups	15
IV	Extra Special Extensions	32
V	Reduction Lemmas	43
VI	The Main Lemma	51
VII	The Fitting Structure	67
VIII	The Main Theorem	75
	Bibliography	77

INTRODUCTION

Suppose that AG is a group with normal subgroup G where $(|A|, |G|) = 1$. Assume that A is fixed point free on G, that is, $C_G(A) = 1$. Suppose that $|A|$ is divisible by d primes, counting multiplicities. There is a conjecture that, not only is G solvable, but the Fitting length of G is bounded by d. The solvability half of the conjecture seems difficult and Thompson (10) made the first step by showing that for A of prime order G is nilpotent. Under the assumption that G is solvable more progress has been made. Without the requirement that $C_G(A) = 1$ Thompson has given a large bound depending upon the Fitting length of $C_G(A)$ (9). The cases where A is of order 4 have been handled (1, 4). The case where $A = S_3$ has also been treated (7). A large class of abelian groups for A have been handled by E. Shult in his thesis (8). The exceptions to his result relate to numbers like Fermat and Mersenne primes, but his exceptions add in certain composite numbers. These exceptions arise because of certain "bad" representations on extra special groups. As we allow A to become a nonabelian p group these same exceptions arise. However, in the cases treated here, except for one, these "bad" cases only arise from abelian representations of A.

(See (V. 8)). Thus it appears that, as far as exceptions to the conjecture go, if they exist at all, they probably exist for abelian groups.

The main result of this thesis is contained in section VI. The proof proceeds by reducing a minimal counterexample. Several comments should be made here. The method of proof seems to be very general. Many of the reduction steps can be made without any hypothesis upon A. Others require the relative primeness and solvability of A. The real restrictions start at (VI. 10). Here a devious route is taken which depends upon I) a remarkable property of class two group characters (II. 2), and II) an even more fortunate coincidence of inequalities (II. 7). Section II then gets us past (VI. 10). All is fairly well until the very end. In (VI. 15) we are forced to invoke the property (*). It is at this point that the exceptions enter. And it is (*) which requires the development of sections I, III, IV. (The results of section I are known. This is a simplification of the proof.)

It is highly possible that the results of these sections hold for almost all choices of nonabelian A. It is this route which will be followed in further investigations. In fact, the case when A is an odd class two p group seems to be well within reach and requires only an extension of the argument in section IV. This is now under investigation.

The theorem proven here then is,

Theorem: If A is a class ≤ 2 odd p group all of whose representations occur as subgroups of extra special p groups and $p^c \neq r^d + 1$ for $c = 1, 2$ and, for prime r, r^{2d+1} dividing $|G|$ then the number of primes dividing $|A|$ bounds the Fitting length of G provided G is solvable.

This includes all class two groups of exponent p (with exceptions on primes, of course). Originally, the result was attempted for A extra special. This choice was made first, because it seemed the next natural step above the abelian case and second, because of the important role played by these groups. Now, all special groups are included.

As a sidelight, section VII contains a reduction of the Fitting series of a solvable group. A sequence of useful prime power factor groups is found on which the Fitting length depends. The complexity of the definition prompts the word edifice. But the situation is much less intricate than the words. This reduction in conjunction with the fixed point theorem of section VI is used to prove the theorem.

I. EXTENSIONS OF GROUP CHARACTERS

Suppose that AG is a group with normal subgroup G and solvable subgroup A where $(|A|, |G|) = 1$. Let Q be the field of rational numbers and δ a primitive $|AG|^{th}$ root of unity over Q. Let $k = Q(\delta)$ be the field over Q generated by δ. In this section all characters will be k characters. For the remainder of this section we assume λ is a fixed irreducible character of G which is stabilized by A, that is,

$$\lambda(x) = \lambda(x^y) \qquad \text{for all } x \in G,\ y \in A.$$

We start by defining a function which maps characters into characters. Suppose that N is any group for which k is a splitting field, and α any character of N. Then there is a representation by linear transformations $A(x)$ over the field k such that

$$\text{tr } A(x) = \alpha(x) \qquad \text{for all } x \in N$$

where tr $A(x)$ denotes the trace of $A(x)$. The representation A by linear transformations is uniquely determined up to similarity by α. In fact, if $\alpha' \neq \alpha$ is another character of N then an associated representation A' is not similar to A. Thus we may set

$$\phi_N(\alpha) = \det A.$$

This function is well defined since A is uniquely determined up to similarity. It is clear that $\phi_N(\alpha)$ is a linear character on N. Hence ϕ_N is a function mapping characters of N onto linear characters of N.

The object of this section is to determine, by use of ϕ, all possible characters on AG which contain λ when restricted to G.

(I. 1) <u>There exists a unique character</u> θ <u>of</u> AG <u>satisfying</u>:

$$\text{i)}\quad \theta|_G = \lambda \qquad \underline{\text{and}}$$

$$\text{ii)}\quad \phi_A(\theta|_A) = 1_A.$$

We proceed by induction on $|A|$. Choose $A_o \Delta A$ of prime index p, and let α be a faithful linear character on AG/A_oG. By induction there is a unique character θ^* of A_oG such that

$$\text{i)}\quad \theta^*|_G = \lambda \qquad \text{and}$$

$$\text{ii)}\quad \phi_{A_o}(\theta^*|_{A_o}) = 1_{A_o}.$$

The character θ^* is fixed by A. For let $y \in A$. Then $\phi_{A_o}(\theta^{*y}|_{A_o}) = \phi_{A_o}(\theta^*|_{A_o})^y = 1_{A_o}{}^y = 1_{A_o}$. Also, $\theta^{*y}|_G = (\theta^*|_G)^y = \lambda^y = \lambda$ so by the uniqueness of θ^* we find that $\theta^{*y} = \theta^*$.

Hence, $\theta^*|^{AG} = \sum \theta_i$ is a sum of p irreducible characters and $\theta_i|_{A_oG} = \theta_1|_{A_oG} = \theta^*$ for $i = 1, \ldots, p$. Now $\phi_A(\theta_1|_A)$ is a linear character of A with A_o in its kernel since $\phi_{A_o}(\theta_1|_{A_o}) = \phi_{A_o}(\theta^*|_{A_o}) = 1_{A_o}$. And then $\phi_A(\theta_1|_A) = \alpha^j$ for some j. There is a unique character α^f such that $\alpha^{f\theta_1(1)+j} = 1_A$. We set $\theta = \alpha^f\theta_1$. Clearly then

$\theta|_G = \lambda$, and $\phi_A(\theta|_A) = \phi_A([\alpha^f\theta_1]|_A) = \alpha^{f\theta_1(1)}\phi_A(\theta_1|_A) = \alpha^{f\theta_1(1)}\alpha^j = 1_A$. Since $\theta_i = \alpha^{j(i)}\theta_1$ for some $j(i)$, θ is unique.

(I. 2) Theorem: <u>Suppose β is any irreducible character of AG such that $\beta|_G$ contains λ. Suppose θ is the unique character of AG given in (I. 1). Then there is a unique character γ of AG/G such that</u>

$$\beta = \gamma\theta$$

<u>Further, if γ is any irreducible character of AG/G then $\gamma\theta$ is a uniquely determined irreducible character of AG.</u>

First, let β_o be any irreducible character of AG which is nontrivial on G. Then by the Clifford Theorems $\beta_o|_G = n(\lambda_1+\ldots+\lambda_t)$ where $\lambda_1, \ldots, \lambda_t$ are all distinct nontrivial conjugate irreducible characters of G. So we have $(1_G, \beta_o|_G)_G = 0$.

Second, let γ be any irreducible character of AG/G. We want to compute $(\gamma, \gamma\beta_o)_{AG}$. If it is greater than zero then $\gamma\beta_o = a\gamma + \ldots$ or $(\gamma\beta_o)|_G = \gamma(1)\beta_o|_G = a\gamma(1)1_G + \ldots$ and $(1_G, \beta_o|_G)_G > 0$. But, as above, all $\lambda_i \neq 1_G$ so $(\gamma, \gamma\beta_o)_{AG} = 0$.

Third, consider θ. Now $1 = (\theta,\theta)_{AG} = (1_{AG},\theta\bar{\theta})_{AG}$ so $\theta\bar{\theta} = 1_{AG} + \Delta$ where $(1_{AG}, \Delta)_{AG} = 0$. So Δ is a sum of characters like β_o above. Hence, $(\gamma, \gamma\Delta)_{AG} = 0$. And we get $1 = (\gamma,\gamma)_{AG} = (\gamma,\gamma(1_{AG} + \Delta))_{AG} = (\gamma,\gamma\theta\bar{\theta})_{AG} =$

$(\gamma\theta, \gamma\theta)_{AG}$. So $\gamma\theta$ is irreducible.

Fourth, $\gamma\theta$ is uniquely determined. For suppose γ' is an irreducible character of AG/G such that $\gamma'\theta = \gamma\theta$. If $\gamma \neq \gamma'$ then $(\gamma\theta, \gamma'\theta)_{AG} = (\gamma, \gamma'\theta\bar{\theta})_{AG} = (\gamma, \gamma' + \gamma'\Delta)_{AG} = (\gamma, \gamma'\Delta)_{AG} = 0$. This last is zero since, by the second part, to be nonzero, $(1_G, (\gamma'\Delta)|_G)_G > 0$; but it isn't. Therefore, $\gamma = \gamma'$ and $\gamma\theta$ is uniquely determined.

Finally, $\gamma(1) = (\gamma(1)\lambda, \lambda)_G = ((\gamma\theta)|_G, \lambda)_G = (\gamma\theta, \lambda|^{AG})_{AG}$. Further, $\sum_\gamma \gamma(1)(\gamma\theta)(1) = (\sum \gamma(1)^2)\lambda(1) = |A|\lambda(1) = \lambda|^{AG}(1)$. So we get

$$\lambda|^{AG} = \sum_\gamma \gamma(1)\gamma\theta$$

where γ ranges over irreducible characters of AG/G. Since $(\beta, \lambda|^{AG})_{AG} = (\beta|_G, \lambda)_G \neq 0$ we get the result that there is a unique γ such that

$$\beta = \gamma\theta$$

(I. 3) <u>Suppose that</u> $M \leq \text{Stab}\,(\text{Aut}(AG), \lambda)$, <u>the stabilizer in</u> Aut(AG) <u>of</u> λ, <u>or</u> $M \leq \text{Stab}\,(G(k/Q), \lambda)$, <u>the stabilizer of</u> λ <u>in the Galois group of</u> k/Q. <u>Then</u> θ <u>of</u> (I. 1) is <u>stabilized by</u> M.

Suppose $x \in M$. Then $\theta^x|_G = \lambda^x = \lambda$. And $\phi_A(\theta^x|_A) = \phi(\theta|_A)^x = 1_A{}^x$, $1_A = \phi_A(\theta|_A)$. So by (I.1) the result follows, since A^x is conjugate to A in AG.

(I. 4) <u>Suppose that</u> β <u>is any irreducible character of</u> AG <u>and</u> $\beta|_G$ <u>contains the irreducible character</u> π <u>of</u> G. <u>Suppose that</u> $A_o = \text{Stab}\,(A, \pi) = \{x \in A | \pi^x = \pi\}$ <u>is the</u>

stabilizer of π in A. Then there is an irreducible character γ on A_oG/G such that $\beta = (\gamma\theta)|^{AG}$ where θ is given in (I. 1).

First we show that Stab $(AG, \pi) = A_oG$. Clearly A_oG stabilizes π. Suppose $x \in AG$ stabilizes π. Then $x = zy$ where $y \in A$, $z \in G$. And $\pi = \pi^x = \pi^{zy} = \pi^y$. Hence $y \in A$ stabilizes π. So $y \in A_o$. Therefore, $z \cdot y \in A_oG$.

Next by (I. 2) we find γ on A_oG/G so that $\gamma\theta$ is irreducible on A_oG. Consider $(\gamma\theta)|^{AG}$. This character is irreducible. Further $\sum_\gamma \gamma(1)\, (\gamma\theta)|^{AG} = \pi|^{AG}$ where γ runs over the irreducible characters of A_oG/G. So for some choice of γ, $(\gamma\theta)|^{AG} = \beta$.

II. CLASS TWO p GROUPS

In this section we compute the nonlinear irreducible characters of a class two p group. We then use this result to prove a fixed point theorem for a class two odd p group irreducible on a module over a prime Galois field. For the remainder of this section suppose that P is a class two p group, Q is the rational field, δ is a primitive $|P|^{th}$ root of unity, and $k = Q(\delta)$.

(II. 1) Suppose that P has a faithful irreducible character β. Then $\beta(x) = 0$ for all $x \in P - Z(P)$.

Let $x \in P - Z(P)$. By the Clifford theorems $\beta|_{Z(P)} = m\alpha$, a multiple of a single linear faithful character of Z(P). Choose y so that $[x,y] = x^{-1}x^{y} \neq 1$. Then $\beta(x) = \beta(x^{y}) = \beta(x[x,y]) = \beta(x)\alpha([x,y])$ since $[x, y] \in Z(P)$. But α is faithful on Z(P) so $\alpha([x, y]) \neq 1$. Hence $\beta(x) = 0$.

(II. 2) Theorem: Suppose β is a faithful irreducible character of P. Then

$$\beta = \begin{cases} p^{d}\alpha; & \alpha \text{ faithful linear on } Z(P) \\ 0; & \text{outside } Z(P) \end{cases}$$

and $|P| = p^{2d}|Z(P)|$.

Clearly $\beta|_{Z(P)} = p^{d}\alpha$ for some linear α faithful on Z(P) and p^{d} dividing $|P|$. Now

$$1 = (\beta, \beta)_P = \frac{1}{|P|} \sum_{x \in P} \beta(x)\beta(x^{-1}) =$$

$$\frac{1}{|P|} p^{2d} \sum_{x \in Z(P)} \alpha(x)\alpha(x^{-1}) = \frac{1}{|P|} p^{2d} |Z(P)|.$$

This completes the proof.

(II. 3) Suppose β is a faithful irreducible character of P. Assume that A is a subgroup with $A \cap Z(P) = 1$. Then $\beta|_A = p^m \rho_A$ where $p^m = p^d/|A|$ and ρ_A is the regular character of A.

This is immediate from (II. 2).

$$\beta|_A = \begin{cases} p^d & \text{on } 1 \\ 0 & \text{on } A^{\#} \end{cases}$$

Hence $\beta|_A = n\rho_A$. But $\beta(1) = p^d = n\rho_A(1) = n|A|$.

(II. 4) Suppose P has a faithful irreducible character of degree p^d. Let s(P) be the number of subgroups $A \leq P$ of order p such that $A \cap Z(P) = 1$. Then

$$s(P) \leq \left(\frac{p^{2d}-1}{p-1}\right) p$$

Consider P/Z(P). By (II. 2) this group has order p^{2d}. The largest number of subgroups of order p that P/Z(P) can contain is $\frac{p^{2d}-1}{p-1}$. This occurs precisely when P/Z(P) is of exponent p. Let B/Z(P) be a subgroup cyclic of order p. Then B is an abelian group of rank two or one. If it is of rank one then $B \geq Z(P)$ and B is cyclic. If it is of rank two then $B = A \times Z(P)$ where A has order p. Further, B contains $\frac{p^2-1}{p-1} = p + 1$ subgroups of order p. One of these is $\langle x \mid x \in Z(P),\ x^p = 1 \rangle$. Hence B contains at most p cyclic subgroups A of order p such that $A \cap Z(P) = 1$. Hence the largest s(P) can be is $(\frac{p^{2d}-1}{p-1})\,p$.

Remark: The only time $s(P) = (\frac{p^{2d}-1}{p-1})\,p$ occurs when P/Z(P) is of exponent p and B = AXZ(P), where A is of order p. This case is of special importance because P is the central product of cyclic group Z(P) and an extra special group of order p^{2d+1}.

(II. 5) Suppose that p is an odd prime and r is a prime not p. Suppose $d \geq 2$. Then

$$p^{2d+1} < r^{p^{d-1}(p-1)}$$

unless p = 3, r = 2 and d = 2. In the latter case

$$p^{2d+1} < r^{2p^{d-1}(p-1)}.$$

Clearly $r^{p^{d-1}(p-1)}$ increases more rapidly in d than p^{2d+1}. The extreme case of the inequality for d > 2 occurs at d = 3, r = 2 and p = 3. But here

$$\log_{10} 3^7 < 7 \times .48 = 3.36 \leq 5.4 = 18 \times .30 < \log_{10} 2^{3^2 \times 2}.$$

Hence we may assume d = 2. Then we have the table below. It is clear that for fixed p extremal cases occur for small r. If the inequality holds for fixed p and r then it still holds if we enlarge p. Hence the inequality holds as the table shows.

$d = 2$

p	3	3	5
$\log p^{2d+1}$ <	2.40	2.40	3.50
r	2	5	2
$\log r^{p^{d-1}(p-1)}$ >	1.80	3.00	6.00
$\log r^{2p^{d-1}(p-1)}$ >	3.60		

(II. 6) <u>Suppose</u> p <u>is an odd prime and</u> r <u>is a prime not</u> p. <u>Assume</u> $d \geq 1$. <u>Then</u>

$$\left(\frac{p^{2d}-1}{p-1}\right)p < \frac{r^{tp^d}-1}{r^{tp^{d-1}}-1}$$

<u>for all</u> $t \geq 1$, <u>except when</u> $p = 3$, $r = 2$ <u>and</u> $d = 1,2$. <u>In the latter case the inequality holds for</u> $t \geq 2$.

We have $\left(\frac{p^{2d}-1}{p-1}\right)p < p^{2d+1}$ and $r^{tp^{d-1}(p-1)} < \frac{r^{tp^d}-1}{r^{tp^{d-1}}-1}$.
So for $d \geq 2$ the result follows from (II. 5). Hence, we may assume $d = 1$. That is, we want to prove

$$\left(\frac{p^2-1}{p-1}\right)p = p(p+1) < \frac{r^{tp}-1}{r^t-1}.$$

The right hand side is obviously increasing in t.

Again we can note that for fixed p the extremal cases occur for small r. Further, if the inequality holds for fixed p and r, it remains valid if we increase p. Hence the table shows that (II. 6) holds if $d = 1$.

p	3	3	5
$p(p+1)$	12	12	30
r	2	5	2
$r^p-1/r-1$	7	31	31
$r^{2p}-1/r^2-1$	21		

(II. 7) Theorem: <u>Suppose that</u> p <u>is an odd prime and</u> $r \neq p$, r <u>a prime</u>. <u>Assume that</u> V <u>is an irreducible</u> $GF(r)[P]$ <u>module faithful on</u> P. <u>Then there exists a vector</u> $v \in V^{\#}$ <u>which is fixed by no element of</u> $P^{\#}$.

We proceed by contradiction.

Since $r \neq p$, ordinary character theory holds. Hence, we apply (II. 2) several times. Now $|P| = p^{2d}|Z(P)|$ so the Brauer character of V is a sum of t algebraic conjugates of the character of (II. 2). The number $t = 1$ if and only if V is absolutely irreducible. Hence

$$\dim V = tp^d.$$

So there are $r^{tp^d} - 1$ vectors in $V^{\#}$. We know that $Z(P)$ is elementwise fixed point free on V. Hence, if $v \in V^{\#}$ and $C_P(v) \neq 1$ then $C_P(v) \cap Z(P) = 1$. Further, $C_P(v)$ contains a cyclic subgroup of order p. So the largest number of vectors in $V^{\#}$ which can be fixed by subgroups of order p will be $s(P)$ times the maximum number of vectors in $V^{\#}$ which can be fixed by a single subgroup of order p.

Now by (II. 2) and (II. 3) we have $\dim C_V(A) = tp^{d-1}$ where A is cyclic of order p and $A \cap Z(P) = 1$. So the latter number is $r^{tp^{d-1}} - 1$. Hence, we must have

$$s(P)\left[r^{tp^{d-1}} - 1\right] \geq r^{tp^{d}} - 1.$$

Using (II. 4) and (II. 6) we see we must have $p = 3$, $r = 2$ and $d = 1,2$ and $t = 1$. But now $V|_{Z(P)}$ is a multiple of a single linear $Z(P)$ module since $t = 1$ implies V is absolutely irreducible. But this means $2 \equiv 1 \pmod{|Z(P)|}$ which is ridiculous for $p = 3$. Hence, (II. 7) holds.

Remarks: (II. 7) holds for $p = 2$ except possibly when P is the central product of d dihedral groups of order 8 when

d	1	2	3
r	3	3	3

. When $d = 1$, $p = 2$, $r = 3$ and P is dihedral then this is a real exception to (II. 7). However, all this requires proof.

III. EXTENSIONS OF EXTRA SPECIAL GROUPS

In this section we investigate representations on symplectic spaces. We then combine this with results from section I to obtain all characters which are extensions over an extra special group.

We assume that V is a nonsingular symplectic space over a field K = GF(r), r a prime, with pairing (,): $V \times V \longrightarrow K^+$. Suppose that A is a group represented upon V fixing the form (,). That is,

$$(v_1, v_2)^x = (xv_1, xv_2) = (v_1, v_2) \quad \text{or}$$

$$(xv_1, v_2) = (v_1, x^{-1}v_2) \quad \text{for all } x \in G;\ v_1, v_2 \in V.$$

Further, we assume that $(|A|, r) = 1$.

This done, we fix $\alpha: A \longrightarrow A$ as that unique antiautomorphism of A which sends $x \longrightarrow x^{-1}$ for all $x \in A$. Then α extends linearly to an antiautomorphism of $K[A]$. Assume that $e \in K[A]$ is an idempotent. Then e^α is also an idempotent. Further, e is primitive if and only if e^α is primitive. And e is central if and only if e^α is central. If e is central then eV is a left $K[A]$ module. Let

$$K_e = \ker [A \longrightarrow \mathrm{Aut}\ eV].$$

(III. 1) <u>Suppose that</u> $1 = e_1 + \ldots + e_t$ <u>is a decomposition of</u> 1 <u>into primitive central orthogonal idempotents of</u> $K[A]$. <u>Then</u>, <u>except possibly when</u> $e_i^\alpha = e_j$, <u>we have</u>

$$(e_i V, e_j V) = 0.$$

Choose any $v_1, v_2 \in V$. Suppose $e_i^{\alpha} \neq e_j$. Then $e_i^{\alpha} e_j = 0$. So, $(e_i v_1, e_j v_2) = (v_1, e_i^{\alpha} e_j v_2) = 0$.

The symplectic space V is nonsingular. So if $e_i V \neq (0)$ then $e_i^{\alpha} V \neq (0)$. Further, $e_i V = (0)$ implies $e_i^{\alpha} V = (0)$. By choosing complementary bases we see that $\dim_K e_i V = \dim_K e_i^{\alpha} V$. Further, $e_i V + e_i^{\alpha} V$ is a nonsingular subspace of V. Since $x \in K_{e_i}$ implies $x^{-1} \in K_{e_i}$ we also have $K_{e_i} = K_{e_i^{\alpha}}$. So, (III. 1) has the following corollary:

(III. 2) In the notation of (III. 1) we have, for all i,

a) $K_{e_i} = K_{e_i^{\alpha}}$

b) $\dim_K e_i V = \dim_K e_i^{\alpha} V$, and

c) $e_i V + e_i^{\alpha} V$ is a nonsingular subspace of V if $e_i V \neq (0)$.

For each primitive central idempotent e, eK[A] is a left K[A] module. Let S_A be the collection of all subgroups H of A such that:

There exists a primitive central idempotent $e \in K[A]$ with $eV \neq (0)$ and $H = \ker [A \longrightarrow \text{Aut } e\,K[A]]$.

For $H \in S_A$ let E_H be the set of all primitive central idempotents $e \in K[A]$ such that

i) $H = \ker [A \longrightarrow \text{Aut } e\,K[A]]$ and

ii) $eV \neq (0)$.

So, S_A is the collection of kernels of irreducible $K[A]$ submodules of V. And $E_H \neq \emptyset$ is the collection of idempotents associated with irreducible $K[A]$ submodules of V having kernel H. We then set

$$e_H = \sum_{e \in E_H} e.$$

From (III. 2) c) we conclude that $V_H = e_H V$ is a nonsingular subspace of V and $E_H{}^{\alpha} = E_H$.

And so we have $V = \sum_{H \in S_A} \dot{+} V_H$.

Next we define some numbers.

(III. 3) $2m(x) = \dim_K C_V(x)$, $x \in A$

$n(x)$ = the number of nontrivial irreducible $K[\langle x \rangle]$ modules in a complete decomposition of V.

Note that if $B \leq A$ is a subgroup of A then all the preceding discussion holds for B also. Further, the numbers in (III. 3) may also be defined for spaces other than V. In particular, we may consider nonsingular subspaces of V. In these situations notation gets a bit messy. Distinguishing notation is added in these cases.

We have set up the apparatus needed from symplectic spaces. We proceed now to develop apparatus for extra special groups expressed as central products.

Suppose AR is a group with normal extra special r subgroup R of order r^{2m+1}. Assume that A centralizes D(R).

Consider the K vector space $R/D(R) = V$. If $v_1, v_2 \in V = R/D(R)$ choose $x \in v_1 = xD(R)$ and $y \in v_2 = yD(R)$. Then set $(v_1, v_2) = [x,y] \in D(R) = GF(r)^+ = K^+$. Using the identification of $D(R)$ with $GF(r)^+ = K^+$, (,) becomes a nonsingular symplectic pairing on $V = R/D(R)$ into K^+. For $x \in R$, $y \in A$ we set

$$y(xD(R)) = (yxy^{-1})D(R) = x^{y^{-1}}D(R).$$

With this conjugation as action V becomes a left $K[A]$ module. Further, A centralizes $D(R)$ so A fixes the pairing (,). We now may apply all the notation and machinery developed in the first part of this section.

We define R_H for $H \in S_A$ to be the inverse image in R of V_H. That is, R_H is "the part of R" with kernel H. If $C_R(A) = D(R)$ then $C_R(H) \geqq R_H$ precisely. Because V_H is nonsingular, R_H is an extra special group.

(III. 4) R _is_ _the_ _central_ _product_ _of_ _the_ R_H, $H \in S_A$.

Since each $R_H \geq D(R)$, $\prod_{H \in S_A} R_H = M \geq D(R)$.

Further, $M/D(R) = \sum_{H \in S_A} \dot{+} V_H = V = R/D(R)$. Hence $M = R$.

Next, if $H, H^* \in S_A$ then $[R_H, R_{H^*}] = 1$.

This is immediate since (III. 1) applies to show that V_H is orthogonal and disjoint to V_{H^*}. That is, $(V_H, V_{H^*}) = 0$ or equivalently $[R_H, R_{H^*}] = 1$.

Therefore, R is the central product of the R_H.

We now reintroduce the field of section I. Suppose that Q is the rational field and δ is a primitive $|AR|^{th}$ root of unity over Q. We let $k = Q(\delta)$. This field is distinct from $K = GF(r)$. In what follows we will be discussing k characters.

For the following lemma, the construction of the central product is important. Let $R_o = \prod_{H \in S_A} X R_H$. Also, set M equal to the subgroup of all $\pi^x y_H \in R_o$ such that the product in R $\pi y_H = 1$. This subgroup is normal in R_o and is in $\prod_{H \in S_A} X\, D(R_H)$. Further, $R \simeq R_o/M$ in a natural way. Since $V = \sum \dotplus V_H$ for $y \in R$, $yD(R) = \sum v_H$ uniquely. Choose $z_H \in v_H$ so that the product in R $\pi z_H = y$. Then setting $\phi(y) = \pi^x z_H M$ gives the desired isomorphism. In fact, this is an A isomorphism as is easily verified.

(III. 5) Suppose that θ_H is an irreducible character of R_H which is nontrivial on $D(R) = D(R_H)$. Suppose that for every $H \in S_A$, $\theta_H|_{D(R_H)}$ contains the fixed linear character λ of $D(R) = D(R_H)$. Assume that X_H is an irreducible character of AR_H and $X_H|_{R_H} = \theta_H$. Then the direct product character

$$\beta = \prod_{H \in S_A} X_H$$

is irreducible on $AR \simeq A^{\Delta} R_o/M$ where A^{Δ} is the diagonal subgroup of $\prod_{H \in S_A} X\, A$.

It is sufficient to note that $\beta|_{R_o} = \prod_{H \in S_A} \theta_H$ is an irreducible character of R_o with M in its kernel. Hence, β, considered as a character on AR, is irreducible.

(III. 6) <u>Suppose that</u> $A_o = C_A(R)$. <u>We know that</u> $C_A(R_H) = H$. <u>Further, assume that</u> β <u>is a character of</u> AR <u>constructed as in</u> (III. 5). <u>Suppose that</u> $(X_H|_A, \gamma) > 0$ <u>for every irreducible character</u> γ <u>of</u> A/H. <u>Then</u>

$$(\beta|_A, \sigma)_A > 0$$

<u>for every irreducible character</u> σ <u>of</u> A/A_o.

First let us prove the following statement: A/A_o is isomorphic to a subgroup of $B = \prod_{H \in S_A} X\ A/H$.

We know that $A_o = \bigcap H$. So consider the following map of A into B. For $y \in A$ let

$$\phi(y) = \prod^{x}(yH) \in B.$$

Clearly ϕ is a homomorphism of A. Assume then that $\phi(y) = 1$. Since $y \in H$ for every $H \in S_A$, $y \in A_o = \bigcap H$. Conversely, $x \in \ker \phi$ if $x \in A_o$. Therefore, $\phi(A) \simeq A/A_o$.

Second, we prove that if Y_H is the character of A which is the sum of every character of A/H, and $\prod Y_H$ is considered as a character of A^Δ then $\prod Y_H$ contains every character of A/A_o.

Now Y_H is a character of A/H. Further, A/A_o is a "subgroup" of $\prod X\ A/H$. Suppose γ is any irreducible character of $B = \prod X\ A/H$. Then

$$\gamma = \prod \gamma_H$$

where γ_H is an irreducible character of A/H. But $Y_H = \gamma_H + \gamma_H'$. Hence, $\prod Y_H = \prod(\gamma_H + \gamma'_H) = (\prod \gamma_H) + \gamma' = \gamma + \gamma'$. Therefore, $\prod Y_H$ contains every character of B.

Finally, assume that σ is an arbitrary irreducible character of A/A_o. Then $\sigma|^B = \gamma_1 + \ldots + \gamma_t$ where γ_i is irreducible. Also, $\gamma_1|_{A/A_o} = \sigma + \ldots$. But γ_1 appears in $\prod Y_H$ on B so σ appears in $\prod Y_H$ restricted to A/A_o.

The result is immediate since Y_H is contained in $X_H|_A$ by hypothesis.

Character Values

From (III. 5) and (III. 6) it is evident that, in order to compute the character values on AR, we need only consider the spaces V_H. In other words, we need only consider submodules of V which are faithful on A/H.

The next few lemmas are technical in nature and are used to compute actual character values.

Look again at A represented on the nonsingular symplectic space V fixing the form (,). Let W be an irreducible K[A] submodule of V. Let W_o be the sum of all irreducible K[A] submodules of V which are isomorphic to W. That is, for some $H \in S_A$ and some $e \in E_H$, $W_o = eV$. By (III. 2) we know that $W_o^{\alpha} = e^{\alpha}V$ is complementary to W_o and $W_o + W_o^{\alpha}$ is a nonsingular symplectic space.

First consider the case that $e^{\alpha} \neq e$. Then $(W_o, W_o) = 0$. Since rad W in $W_o \dotplus W_o^{\alpha}$ is K[A] invariant, we may, by choosing appropriate complementary bases, split $W_o \dotplus W_o^{\alpha}$ as

$$(W \dotplus W^*) \dotplus W' = W_o \dotplus W_o^{\alpha} \qquad \text{where}$$

$W \dotplus W^*$ and W' are nonsingular symplectic spaces and also K[A] modules. In particular, if $W_o = W_1 \dotplus \ldots \dotplus W_t$ is a sum of t copies of W then $W_o^{\alpha} = W_1^* \dotplus \ldots \dotplus W_t^*$ may be written as the sum of t copies of W^* satisfying: $W_i \dotplus W_i^*$ is a nonsingular symplectic space.

Second, we consider the case that $e^{\alpha} = e$. This case is a bit more complex. Here $W_o^{\alpha} = W_o$, so W_o is a nonsingular symplectic space. Two cases can arise for W. It may be nonsingular. In which case $W_o = W \dotplus W'$ where W, W' are nonsingular and K[A] invariant. In the other case W is isotropic since $W \cap \text{rad } W \neq (0)$ is a K[A] submodule of W. As above then we may choose K[A] invariant submodules so that $W_o = (W \dotplus W^*) \dotplus W'$ where $W \dotplus W^*$ and W' are nonsingular. In any case

$$W_o = \sum \dotplus (W_i \dotplus W_i^*) \dotplus \sum \dotplus W_j \qquad \text{where all}$$

W_f, W_i^* are irreducible K[A] modules isomorphic to W, the W_i have symplectic complement W_i^*, and the W_j are nonsingular.

Notice then what the situation is. If W is an irreducible K[A] module of dimension g then V contains an irreducible K[A] module isomorphic to W which is nonsingular, or $W_o + W_o^{\alpha}$ is a sum of complementary paired

$K[A]$ modules isomorphic to W or W^{α}. If V contains nonsingular W of dimension g then we say situation (i) arises. If W_o is a sum of paired modules as described we say situation (ii) arises.

(III. 7) Suppose A is cyclic. Assume that $H \in S_A$ and consider V_H. Suppose that W is an irreducible $K[A]$ submodule of V_H of dimension g. In situation

(i) $r^{g/2} \equiv -1 \pmod{[A:H]}$ where g is even,

(ii) $r^g \equiv 1 \pmod{[A:H]}$

Further, every irreducible $K[A]$ submodule of V_H has dimension g. So if $\dim V_H = hg$ then

(iii) $r^{hg/2} \equiv (-1)^h \pmod{[A:H]}$.

If $[A:H] = 1$ the result is trivial. If $[A:H] = 2$ then $([A:H], r) = 1$ by hypothesis so r is odd and $r^j \equiv 1 \equiv (-1)^i \pmod 2$ for all i,j. So we may assume $[A:H] > 2$.

Let t be the smallest positive integer such that $r^t \equiv 1 \pmod{[A:H]}$. Consider the collection E_H of all primitive idempotents of $K[A]$ such that $eV_H \neq (0)$. If we take $e \in E_H$ then $eK[A]$ is an extension field of $K = GF(r)$ since A is cyclic. As a left $K[A]$ module, $eK[A]$ is faithful on A/H, so $eK[A] \simeq GF(r^t)$. In particular, $\dim_K eK[A] = \dim_K GF(r^t) = t$. This holds for every $e \in E_H$. Therefore, $t = g$ is the dimension of every irreducible $K[A]$ submodule of V_H.

In situation (i), there is an irreducible submodule W of V_H which is nonsingular and hence of even dimension g. Now $r^g \equiv 1 \pmod{[A:H]}$ and $[A:H] > 2$ so $r^{g/2} \equiv -1 \pmod{[A:H]}$. In situation (ii) we obviously have $r^g \equiv 1 \pmod{[A:H]}$.

For (iii) we consider situation (i) first. Here we just raise the congruence of (i) to the h power. Second we consider situation (ii). Here V_H is a sum of pairs of modules so h is even. That is, $(-1)^h = 1$ or

$$r^{hg/2} \equiv 1 = (-1)^h \pmod{[A:H]}.$$

This completes the proof of (III. 7).

We now build a character. Assume that $H \in S_A$ and consider R_H, the inverse image in the extra special group R of V_H. Suppose that dim V_H = hg where g is the dimension of an irreducible K[A] submodule and A is cyclic.

(III. 8) <u>Suppose that</u> A <u>is cyclic and</u> λ <u>is a nontrivial linear character of</u> $D(R_H)$. <u>Then</u>

$$X_\lambda(x) = \begin{cases} r^{hg/2}\lambda(z); & x = yz,\ y \in H,\ z \in D(R_H) \\ (-1)^h\lambda(z); & x \sim yz,\ y \in A-H,\ z \in D(R_H) \\ 0 & \underline{\text{elsewhere}} \end{cases}$$

<u>is an irreducible character of</u> AR_H.

By (II. 2)

$$\beta_\lambda(x) = \begin{cases} r^{hg/2}\lambda(x) & x \in D(R_H) \\ 0 & \text{elsewhere} \end{cases}$$

is an irreducible character of R_H. The character β_λ

extends to $H \times R_H$ so that $\beta_\lambda{}^e$ is trivial on H. Set

$$N_\lambda(x) = \beta_\lambda{}^e|^{AR_H}(x) = \begin{cases} [A:H]r^{hg/2}\lambda(z); \; x = yz, \\ y \in H, \; z \in D(R_H) \\ 0 \qquad \text{elsewhere} \end{cases}$$

The character λ extends to a linear character λ^e of $A \times D(R_H)$ which is trivial on A. Set

$$M_\lambda(x) = \lambda^e|^{AR_H}(x) = \begin{cases} r^{hg}\lambda(z); \; x=yz, \; y \in H, \; z \in D(R_H) \\ \lambda(z); \; x \sim yz, \; y \in A-H, \; z \in D(R_H) \\ 0 \qquad \text{elsewhere} \end{cases}$$

By (III. 7) $\dfrac{1-(-1)^h r^{hg/2}}{[A:H]}$ is an integer. Hence,

$$X_\lambda = \left[\frac{1-(-1)^h r^{hg/2}}{[A:H]}\right] N_\lambda - (-1)^h M_\lambda$$

is a generalized character of AR_H.

$$X_\lambda(1) = r^{hg/2} > 0.$$

$$|AR_H| \; (X_\lambda, X_\lambda)_{AR_H} = r^{hg} \sum_{y \in H \times D(R_H)} \lambda^e(y)\lambda^e(y^{-1}) + \sum_{y \sim z \in [A-H] \times D(R_H)} \lambda^e(z)\lambda^e(z^{-1})$$

$$= r^{hg+1}|H| + r \; |A - H| \; (|R_H|/|C_{R_H}(A)|).$$

But $C_{R_H}(A) = D(R_H)$ so

$$= r^{hg+1} \; |H| + r^{hg+1} \; |A - H|$$

$$= |AR_H|.$$

Therefore (III. 8) holds.

(III. 9) Assume the conditions of (III. 8). If $[A:H] \neq r^{hg/2} - (-1)^h$ or $(-1)^h = 1$ then $X_\lambda|_A$ contains every character of A/H.

$$X_\lambda|_A(x) = \begin{cases} r^{hg/2} & x \in H \\ (-1)^h & x \in A-H \end{cases}$$

$$= \left[\frac{r^{hg/2} - (-1)^h}{[A:H]}\right] \rho_{A/H} + (-1)^h 1_A$$

where $\rho_{A/H}$ is the regular character of A/H.

We still consider A to be cyclic, but now we want to find a character on all of R rather than just R_H.

(III. 10) Assume that A is cyclic. Suppose that λ is a nontrivial linear character of D(R). For $x \in A$ we consider m(x) and n(x) as defined in (III. 3). Then

$$Y_\lambda(y) = \begin{cases} r^{m(x)}(-1)^{n(x)}\lambda(z); & y \sim xz,\ x \in A, \\ & z \in D(R) \\ 0 & \text{elsewhere} \end{cases}$$

is an irreducible character of AR.

We apply (III. 5) and (III. 8). From (III. 8) for each $H \in S_A$ we get h_H and g_H dependent upon H. From (III. 5) we form the product character. It is not difficult to see that

$$r^{m(x)} = \prod_{x \in H \in S_A} r^{h_H g_H/2}.$$

And in the same fashion

$$n(x) \equiv \sum_{x \notin H \in S_A} h_H \pmod 2.$$

So that (III. 5) yields, using the character of (III. 8), the values given for Y_λ.

(III. 11) <u>Assume the conditions of</u> (III. 10). <u>If</u> $A_o = \ker [A \longrightarrow \mathrm{Aut}\ R/D(R)]$ <u>then</u> $Y_\lambda|_A$ <u>contains every character of</u> A/A_o <u>provided that</u>

$$[A:H] \neq r^{h_H g_H/2} - (-1)^{h_H} \quad \underline{\text{or}} \quad (-1)^{h_H} = 1$$

<u>for every</u> $H \in S_A$.

Here we apply (III. 9) and (III. 6) in much the same manner as in (III. 10) above.

The inequality hypothesis of this lemma may be improved under certain restricted hypotheses.

(III. 12) <u>Assume that</u> A <u>is cyclic and</u> A* <u>is a subgroup</u>. <u>Suppose that</u> ρ_A <u>is the regular character of</u> A <u>and</u> $\rho_A^{\#} = \rho_A - 1_A$ <u>and</u> $\rho_{A/A*}^{\#} = \rho_{A/A*} - 1_A$. <u>If</u> β <u>is any linear character of</u> A <u>and</u> $\gamma = \rho_A^{\#}\rho_{A/A*}^{\#}$ <u>then</u>

$$(\gamma, \beta)_A = \begin{cases} [A:A*] - 1 & \beta = 1_A \\ [A:A*] - 2 & \beta \neq 1_A,\ \beta|_{A*} = 1_{A*} \\ [A:A*] - 1 & \beta|_{A*} \neq 1_{A*}. \end{cases}$$

We treat the three cases separately.

$$\gamma(x) = \begin{cases} (|A| - 1)([A:A^*] - 1) & x = 1 \\ 1 - [A:A^*] & x \in A^{*\#} \\ 1 & \text{elsewhere.} \end{cases}$$

We treat $\gamma^{o} = \gamma - 1_A$. Then $|A|(\gamma^{o}, 1_A)_A$
$= \left[(|A| - 1)([A:A^*]-1)-1\right] + (-[A:A^*])(|A^*| - 1)$
$= |A|([A:A^*] - 2)$. Suppose $\beta \neq 1_A$, $\beta|_{A^*} = 1_{A^*}$. Then
$|A|(\gamma^{o}, \beta)_A = [(|A| - 1)([A:A^*] - 1) - 1] +$
$(-[A:A^*])(|A^*| - 1) = |A|([A:A^*] - 2)$. Finally take
$\beta|_{A^*} \neq 1_{A^*}$. Then $|A|(\gamma^{o},\beta)_A = [(|A| - 1)([A:A^*] - 1) - 1]$
$+ (-[A:A^*])(|\ker \beta|_{A^*}| - 1) + |\ker \beta|_{A^*}|\,[A:A^*]$
$= |A|([A:A^*] - 1)$. If in each case we note the value of
$(1_A, \gamma^{o})_A$ then the proof is complete.

(III. 13) Suppose that A is a cyclic p group for odd p. Assume the hypotheses of (III. 10). Let $A_o = C_A(R)$. Then $Y_\lambda|_A$ contains every character of A/A_o except when $[A:A_o] = \sqrt{[R:C_R(A)]} + 1$ and $R/C_R(A)$ is an irreducible $K[A]$ module.

Note that $A_o \in S_A$ since A is a cyclic p group. The subgroups of A form a chain. So suppose there is an $A^* \in S_A$ such that $A_o < A^* < A$. The character Y_λ is constructed from (III. 6) and (III. 9). But since both $A^*, A_o \in S_A$ from (III. 12) we get $Y_\lambda|_A$ containing every character of A/A_o. Therefore, only A and A_o can be in S_A. Since $R/C_R(A) \simeq_A V_{A_o}$ the result follows directly from (III. 11). For if $A_o = A$ the result is trivial. If

$A_o \neq A$ then an exception can only occur if $[A:A_o] = r^f + 1$ where $[R:C_R(A)] = r^{2f}$ and $R/C_R(A)$ is an irreducible A module.

We are now in a position to prove the main theorem of this section. The previous results apply for cyclic A. We remove this restriction now. We apply the previous results to cyclic subgroups of A.

Before the main theorem we prove a simple lemma concerning the Galois group of k/Q.

(III. 14) <u>Assume that</u> a,b <u>are positive integers and</u> $(a,b) = 1$. <u>Suppose that</u> δ <u>is a primitive</u> ab <u>root of unity over</u> Q, <u>the rational field. Then there is</u> $x \in G^*$, <u>the Galois group of</u> $Q(\delta)/Q$ <u>which fixes</u> δ^b <u>and takes</u> δ^a <u>into</u> δ^{-a}.

The automorphisms of k/Q are given by $\delta \longrightarrow \delta^n$ where $(n,ab) = 1$. So we need only find n so that $n \equiv 1 \pmod a$ and $n \equiv -1 \pmod b$. But $a'b \equiv 1 \pmod a$ and $b'a \equiv 1 \pmod b$ are solvable for a' and b' so $n = a'b - b'a$ works since $(n,ab) = 1$.

(III. 15) Theorem: <u>Assume that</u> AR <u>is a solvable group with normal extra special subgroup</u> R <u>of order</u> r^{2m+1} <u>and</u> $(|A|,r) =1$. <u>Suppose that</u> A <u>centralizes</u> D(R). <u>Assume that</u> λ <u>is a nontrivial linear character on</u> D(R). <u>Then</u>

$$\divideontimes_\lambda(y) = \begin{cases} r^{m(x)} \ (-1)^{n(x)} \gamma(x)\lambda(z); \ y \sim xz, \ x \in A, \\ \qquad\qquad\qquad\qquad\qquad z \in D(R) \\ 0 \qquad\qquad\qquad \underline{\text{elsewhere}}, \end{cases}$$

<u>where</u> $\gamma : A \longrightarrow \{1,-1\}$ <u>is</u> <u>a</u> <u>class</u> <u>function</u>, <u>is</u> <u>an</u> <u>irreducible</u> <u>character</u> <u>of</u> AR. <u>Further</u> $\gamma(x) = 1$ <u>whenever</u> $|\langle x\rangle|$ <u>is</u> <u>odd</u>.

Let λ_o be the irreducible character of R lying over λ. Then λ_o is fixed by A. By (I.1), (I. 3) we may choose an extension of λ_o on AR, Θ, such that

i) $\Theta|_R = \lambda_o$ and

ii) G_o^*, the subgroup of G^* fixing all r^{th} roots of unity of the field $k = Q(\delta)$ where δ is a primitive $|AR|$ root of unity over Q, fixes Θ. Θ of (I.1) is a good choice.

This choice of Θ is unique. Further, if $A^* \leq A$ is a subgroup then $\Theta|_{A^*R}$ is the corresponding unique character of (I. 1) on A^*R also satisfying i) and ii).

Let $x \in A$. By (III. 10) and (I. 2)

$$\Theta|_{\langle x\rangle R} = Y_\lambda \beta$$

for some linear character β of $\langle x\rangle R/R$. But β is an r' character. By (III. 14) G_o^* contains an element taking $\beta \longrightarrow \beta^{-1}$. But both Θ and Y_λ are fixed by G_o^*. So β is a character of $\langle x\rangle R/\langle x^2\rangle R$. That is, β maps x into $\{1,-1\}$. Therefore, $\gamma\Theta = \divideontimes_\lambda$ has the values of (III. 15).

<u>Remark</u>: If $x \in A$ and $x^2 = y$ and $[\langle x\rangle : \langle y\rangle] = 2$ then $\gamma(y) = 1$. This follows by looking at $\chi_\lambda|_{\langle x\rangle R}$.

IV. EXTRA SPECIAL EXTENSIONS

Following (III. 10) we proved (III. 11) which concerns itself with which characters appear in $Y_\lambda|_A$. Ideally, we would like an analogous result to follow (III.15). For purposes of the main theorem it would be sufficient to have such a result for A a class two odd p group. For such a case, the computations here are incomplete. So we settle for the case where A is the central product of a cyclic group of order p or p^2 and an extra special group. We carry the argument as far as possible for the class two group.

Assume that p, r are distinct primes and p is odd. Suppose that P is a class two p group of order $p^{2d}|Z(P)|$ where $|Z(P)| = p^a$. Assume that PR is a group with normal extra special r subgroup R of order r^{2m+1}. Suppose that every irreducible P submodule of $R/D(R) = V$ is faithful, and P centralizes D(R). Let $K = GF(r)$ and $k = Q(\delta)$ where Q is the rational field and δ is a primitive $|PR|^{th}$ root of unity. All characters are k characters unless otherwise specified.

Recall that V is a symplectic space. The Brauer character of P on V ($p \neq r$) is a sum of t characters as in (II. 2). Hence, $\dim_K V = tp^d$. We must find out what t is. Let m_b be the smallest positive integer such that

$$r^{m_b} \equiv 1 \pmod{p^b}.$$

Then for b = 1, $r^{m_1} \equiv 1 \pmod{p}$.

(IV. 1) <u>Suppose</u> c <u>is the largest positive integer such that</u> $r^{m_1} \equiv 1 \pmod{p^c}$. <u>Then</u> $m_b = m_1$ <u>if</u> $b \leq c$ <u>and</u> $m_b = m_1 p^{b-c}$ <u>if</u> $b > c$.

If $b \leq c$ the result is obvious. Suppose $b \geq c$, and $n = m_1 p^{b-c}$, and $r^n \equiv 1 \pmod{p^b}$ but $r^n \not\equiv 1 \pmod{p^{b+1}}$. Clearly $m_{b+1} = np$. The question then is, what about $r^{np} \equiv 1 \pmod{p^{b+2}}$? That is, what about

$$\frac{r^{np} - 1}{r^n - 1} \equiv 1 \pmod{p^2}?$$

Now $(r^{np} - 1) = (r^n - 1)(r^{n(p-1)} + r^{n(p-2)} + \ldots + r^n + 1)$ and $r^{n(p-j)} \equiv 1 \pmod{p^b}$ exactly. Therefore,

$$(r^{n(p-1)} + \ldots + 1) \equiv p \pmod{p^b}.$$

If $b > 1$ then we are done. So we may assume that $b = c = 1$. Hence, $n = m_1$. Now $r^{nj} \equiv 1 \pmod{p}$ exactly for $j = 0, 1, \ldots, p-1$. So $r^n = 1 + fp$ and $r^{nj} = 1 + jfp + f_j p^2$. Therefore

$$\sum_{j=0}^{p-1} r^{nj} \equiv p + fp \sum_{j=0}^{p-1} j = p\left(1 + f\frac{p(p-1)}{2}\right) \equiv$$

$p \pmod{p^2}$ since p is odd. Hence the result.

(IV. 2) $GF(r^{m_a})$ <u>is the splitting field for</u> P <u>on</u> V <u>where</u> $|Z(P)| = p^a$.

The character of an absolutely irreducible P module over an extension of GF(r) is given by (II. 2) and takes its values in $GF(r^{m_a})$ exactly. If $|P| = p^{2d}\,|Z(P)|$ then an irreducible $GF(r^{m_a})[P]$ module has dimension p^d over some finite division algebra by the Wedderburn Structure Theorems. So by the Wedderburn theorem on finite division algebras, $GF(r^{m_a})$ is the splitting field for P.

(IV. 3) _If_ $|Z(P)| = p^a$ _then_ $t = m_a n$ _where_ n _is the number of irreducible_ GF(r)[P] _modules in a decomposition of_ V.

The dimension over GF(r) of V is tp^d. By (IV. 1) and (IV. 2) every irreducible GF(r)[P] submodule must have dimension $m_a p^d$. There are n of them so $tp^d = m_a n p^d$. Hence the result.

Next we compute information concerning $m(x)$ and $n(x)$.

(IV. 5) a) $n(1) \equiv 0 \pmod 2$

$m(1) = m$

b) _If_ $x \in P$ _and_ $\langle x\rangle \cap Z(P) \neq 1$ _then_

$n(x) \equiv n \pmod 2$

$m(x) = 0$

c) _If_ $x \in P$, $\langle x\rangle \cap Z(P) = 1$, _and_ $|\langle x\rangle| = p^f$ _then_

$n(x) \equiv 0 \pmod 2$

$m(x) = m/p^f$.

The K dimension of V is 2m. Hence (III.3) shows immediately that $m(1) = m$. Further, $n(1) = 2m$ so $n(1) \equiv 0 \pmod 2$. Next, Z(P) is fixed point free elementwise on V. So if $x \in P$ and $\langle x\rangle \cap Z(P) \neq 1$ then $\langle x\rangle$ is fixed point free elementwise on V. Therefore, $m(x) = 0$. If $|\langle x\rangle| = p^f$ then an irreducible $K[\langle x\rangle]$ submodule is faithful of dimension m_f. Hence $n(x) = 2\, m/m_f \equiv t/m_f = m_1 p^{a-c} n/m_1 p^{f-c} \equiv n \pmod 2$ since p is odd. Finally, for $x \in P$, $\langle x\rangle \cap Z(P) = 1$, and $|\langle x\rangle| = p^f$ we find from (II. 3) that $\langle x\rangle$ acts as tp^{d-f} regular representations on V. Therefore, $m(x) = tp^{d-f}/2 = m/p^f$. Now $[V,\langle x\rangle]$ has dimension $2m - (2m/p^f) = (2m/p^f)(p^f - 1)$. In other words, if ρ is the regular representation of $\langle x\rangle$ then $\langle x\rangle$ is represented upon $[V,\langle x\rangle]$ as $2m/p^f$ times $\rho - 1$. We notice that for an appropriate extension field ρ contains $p^g - p^{g-1}$ absolutely irreducible representations with kernel precisely of order p^{f-g}. Hence $[V,\langle x\rangle]$ contains $(2m/p^f m_g)(p^g - p^{g-1})$ irreducible submodules with kernel precisely of order p^{f-g}. But $n(x)$ is the sum of these numbers as g runs from 1 to $f - 1$. Fix g. Then $g<f \leq d \leq a$ since $|\langle x\rangle| \leq p^d$ and $|[\langle x\rangle,P]| = p^a$. Therefore, $(2m/p^f m_g)p^{g-1} = (m_a/m_g)np^{d+g-f-1}$ isan integer; so $n(x)$ is even since $p - 1$ is even. This completes (IV. 5).

(IV. 6) a) $r^{[m(p-1)]/p} \equiv 1 \pmod{p^{d+a-1}}$

b) $r^m - (-1)^n - p[r^{m/p} - (-1)^n] = sp^{2d+2a-1} > 0$ <u>for</u> $s > 0$ <u>unless</u> $d = a = n = 1$, $m = p = 3$, <u>and</u> $r = t = 2$.

To do this we require (III. 7). We examine the representation of Z(P) on V. Since an irreducible faithful Z(P) module over K always has dimension m_a and since $V|_{Z(P)}$ is a sum of such modules, $V|_{Z(P)}$ must contain $tp^d/m_a = np^d$ irreducible Z(P) modules. In our case p is odd. If n is even then a) follows by a simple computation. If n is odd we are in situation i) of (III. 7) and $r^{m_a/2} \equiv -1 \pmod{p^a}$. We raise this expression to the $np^{d-1}(p-1)$ power to get a) since $[m(p-1)]/p = (m_a/2)(np^{d-1}(p-1))$.

For b) we rewrite $r^m - (-1)^n - p[r^{m/p} - (-1)^n]$ $= r^{m/p}(r^{[m(p-1)]/p} - p) + (p-1)(-1)^n$. Using a), for some q this becomes $r^{m/p}(1 + qp^{d+a-1} - p) + (p-1)(-1)^n$. We assume this number is less than or equal to zero. Hence, $r^{m/p}(1 + qp^{d+a-1} - p) \leq (p-1)(-1)^{n+1}$. But the left hand side is positive so $n + 1$ is even. Further, the left hand side is greater than $p-1$ unless $q = 1$ and $d + a - 1 = 1$. This forces $d = a = 1$. And $[m(p-1)]/p$ becomes $t(p-1)/2$. So $r^{t(p-1)/2} = 1 + p$. So $r = 2$. Now $t = m_1 n$ and $r^{m_1} = 1 + fp$ for some f. But $m_1 \leq t(p-1)/2$ so $f = 1$ and $m_1 = m_1 n(p-1)/2 = t(p-1)/2$. Therefore, $n = 1$ and

$p = 3$. From here we get $d = a = n = 1$, $r = m_1 = m_1 n = t = 2$, and $p = tp^d/2 = m = 3$.

We argue on congruences for the rest. As above, when n is even, $r^{m_a n/2} \equiv (-1)^n \pmod{p^a}$. And when n is odd $r^{m_a n/2} \equiv (-1)^n \pmod{p^a}$. In particular, $r^{m/p} \equiv (-1)^n \pmod{p^{d+a-1}}$. Therefore, $r^{m/p} = (-1)^n + fp^{d+a-1}$.
$r^m = [(-1)^n + fp^{d+a-1}]^p = (-1)^n + fp^{d+a} + \sum_{j=2}^{p} \binom{p}{j} (fp^{d+a-1})^j (-1)^{n(p-j)}$. And finally
$r^m - (-1)^n - p\,[r^{m/p} - (-1)^n] = \sum_{j=2}^{p} \binom{p}{j} (fp^{d+a-1})^j (-1)^{n(p-j)} \equiv 0 \pmod{p^{2d+2a-1}}$.
From this, and the above argument, b) follows.

We now put strong hypotheses upon P. We assume that P is the central product of an extra special group of order p^{2d+1} and a cyclic group of order p^a where $a = 1,2$.

(IV. 7) <u>If</u> $|Z(P)| = p$ <u>then</u> P <u>contains</u>

a) $p^{2d+1} - 1$ <u>elements of order</u> p <u>or</u>

b) $p^{2d} - 1$ <u>elements of order</u> p <u>and</u> $p^{2d}(p-1)$ <u>elements of order</u> p^2.

<u>If</u> $|Z(P)| = p^2$ <u>then</u> P <u>contains</u> $p^{2d+1} - 1$ <u>elements of order</u> p <u>and</u> $p^{2d+1}(p-1)$ <u>elements of order</u> p^2.

Here P' is of order p so $x \longrightarrow x^p$ is a homomorphism of P whose kernel contains all elements of order p plus 1, the identity. In case a) P is of exponent p and in the remaining cases P is of exponent p^2. Using the order of

P equal to $p^{2d}|Z(P)|$, the result follows easily.

(IV. 8) <u>Assume that</u> P <u>is the central product of</u> Z(P) <u>with an extra special</u> p <u>group. The character</u> χ_λ <u>of</u> (III. 15) <u>on</u> PR <u>has the property that</u> $(\chi_\lambda|_P,\mu)_P > 0$ <u>for all</u> μ <u>irreducible on</u> P <u>except when</u> $|P| = 27$ <u>and</u> $|R| = 2^7$ <u>and</u> R/D(R) <u>is a faithful irreducible</u> K[P] <u>module</u>.

We compute the inner product directly.

First suppose that $\mu|_{P'} \neq 1_{P'}$. Then $\mu|_{Z(P)} = p^d\mu_o$ for a faithful linear character μ_o of Z(P). $|P|(\chi_\lambda|_P,\mu)$ $= r^m p^d + p^d \sum_{x\in Z(P)^\#} (-1)^{n(x)}\mu_o(x^{-1})$. By (IV. 5) b) $n(x) \equiv n \pmod 2$ so

$$= r^m p^d - (-1)^n p^d \neq 0$$

Therefore $\qquad (\chi_\lambda|_P,\mu)_P > 0.$

Second, suppose that $\mu|_{P'} = 1_{P'}$.

$$|P|(\chi_\lambda|_P,\mu) = r^m + \sum_{x\in P^\#} (-1)^{n(x)} r^{m(x)}\mu(x^{-1}).$$

For our group P, $x^p \in Z(P)$ for every $x \in P$. So for every element x of order p^2, $\langle x\rangle \cap Z(P) \neq 1$ and so $m(x) = 0$ and $n(x) \equiv n \pmod 2$. For the elements of order p, $\langle x\rangle \cap Z(P) = 1$ unless $x \in Z(P)$. If $x^p = 1$ and $x \notin Z(P)$ then $n(x) \equiv 0 \pmod 2$ and $m(x) = m/p$.

A) Suppose that P is of exponent p. Here a = 1.

i) Assume that $\mu = 1_P$.

$$= r^m - (-1)^n + p(-1)^n + r^{m/p}(p^{2d+1} - p) > 0.$$

ii) Assume that $\mu \neq 1_P$. In this case $\ker\mu$ is of order p^{2d}. So $P^{\#} \cap \ker\mu$ contains $p^{2d} - p$ elements not in $Z(P)$ and $p - 1$ elements in $Z(P)^{\#}$. There are then $p^{2d+1} - p^{2d}$ elements on which μ is nontrivial. Thus

$$= r^m - (-1)^n + p(-1)^n + pr^{m/p}(p^{2d-1} - 1)$$
$$- pr^{m/p}\left(\frac{p^{2d} - p^{2d-1}}{p - 1}\right)$$
$$= r^m - (-1)^n - p\left[r^{m/p} - (-1)^n\right] > 0$$

except when $r = 2$, $m = p = 3$, and $n = 1$.

B) Suppose P is of exponent p^2. Here $a = 1, 2$. Also, P contains $p^{2d+a} - p^{2d+a-1}$ elements of order p^2 and $p^{2d+a-1} - 1$ elements of order p.

i) Assume that $\mu = 1_P$.

$$= r^m - (-1)^n + p(-1)^n + r^{m/p}(p^{2d+a-1} - p)$$
$$+ (-1)^n(p^{2d+a} - p^{2d+a-1})$$
$$= r^m - (-1)^n - p[r^{m/p} - (-1)^n]$$
$$+ p^{2d+a-1}(r^{m/p} - (-1)^n) + (-1)^n p^{2d+a}$$
$$= sp^{2d+2a-1} + p^{2d+a-1}(r^{m/p} - (-1)^n) + (-1)^n p^{2d+a} > 0$$

since $2a - 1 \geq a$.

ii) Suppose that $\mu \neq 1_P$.

a) Assume $\ker\mu$ has exponent p. Then $(\ker\mu)^{\#}$ is precisely the set of all elements of order p.

$$= r^m - (-1)^n + p(-1)^n + r^{m/p}(p^{2d+a-1} - p)$$
$$- (-1)^n\left(\frac{p^{2d+a} - p^{2d+a-1}}{p - 1}\right)$$

$$= r^m - (-1)^n - p[r^{m/p} - (-1)^n] + p^{2d+a-1}[r^{m/p} - (-1)^n] > 0.$$

b) Assume that $\ker\mu$ contains an element of order p^2. Then it contains $p^{2d+a-2}(p-1)$ elements of order p^2 and $p^{2d+a-2} - p$ noncentral elements of order p. Outside of $\ker\mu$ there are $(p^{2d+a-1} - p^{2d+a-2})(p-1)$ elements of order p^2 and $p^{2d+a-2}(p-1)$ of order p.

$$\begin{aligned} &= r^m - (-1)^n + p(-1)^n - r^{m/p}p^{2d+a-2} \\ &\qquad - (-1)^n(p^{2d+a-1} - p^{2d+a-2}) \\ &\qquad + r^{m/p}(p^{2d+a-2} - p) \\ &\qquad + (-1)^n(p^{2d+a-1} - p^{2d+a-2}) \\ &= r^m - (-1)^n - p[r^{m/p} - (-1)^n] > 0 \end{aligned}$$

except for the noted cases.

It is always true that $P - \ker\mu$ contains an element of order p^2. Suppose $x \in \ker\mu$ and $|\langle x\rangle| = p^2$. Suppose $y \in P - \ker\mu$ and $y^p = 1$. Then

$$(xy)^p = x^p y^p [x,y]^{\binom{p}{2}} = x^p \neq 1.$$

But $\mu(xy) = \mu(y) \neq 1$. Hence $xy \in P - \ker\mu$. So we have treated all possible cases and

$$(\chi_\lambda|_P, \mu)_P > 0.$$

(IV. 9) <u>Suppose that</u> P <u>is an extra special odd</u> p <u>group</u>. <u>Assume also that</u> $P_1 \leq P$, <u>and</u> $P_o \,\Delta\, P_1$, <u>and</u> P_1/P_o <u>has a faithful irreducible</u> $k[P_1/P_o]$ <u>module</u>. <u>Then</u> P_1/P_o <u>is cyclic of exponent</u> p <u>or</u> p^2, <u>or</u> P_1/P_o <u>is the central</u>

product of an extra special group with $Z(P_1/P_o)$ *and is of exponent* p *or* p^2.

If $x \in P$ then $x^p \in D(P) = Z(P)$ and $|Z(P)| = p$; so the exponent is p or p^2. Set $\underline{P} = P_1/P_o$. Suppose $\underline{P}$ is nonabelian. Then $D(\underline{P}) = D(P)P_o/P_o$. Hence, $Z(\underline{P}) \geq D(\underline{P})$. But $Z(\underline{P})$ is cyclic. The result follows easily since $\underline{P}/Z(\underline{P})$ must be of exponent p and be a nonsingular symplectic space.

(IV. 10) *Suppose* P *is a subgroup of an extra special odd* p *group. Assume that* PR *is a group with normal extra special* r *subgroup* R $(r \neq p)$. *Suppose that* P *centralizes* $D(R)$. *Suppose* $P_o = C_p(R)$. *Assume that* $p^c \neq r^d + 1$ *for any* $r^d | r^m$ *where* $|R| = r^{2m+1}$ *and* $c = 1,2$. *Then*

$$(\chi_\lambda|_P, \mu)_P > 0$$

for every character μ *of* P/P_o *and* $(\chi_\lambda|_P, \mu)_P = 0$ *for all* $\mu \neq 1$ *of* P *such that* $\mu|_{P_o} \neq 1$, *if* χ_λ *is the character of* PR *given in* (III. 15).

As in section III, let S_P be the collection of all subgroups of P which appear as kernels of irreducible $K[P]$ submodules of $V = R/D(R)$. For $H \in S_P$ let E_H be the collection of all primitive central idempotents of $K[P]$ where $eV \neq (0)$ and $\ker[P \longrightarrow \text{Aut } eK[P]] = H$. Let V_H be the corresponding subspace of V and R_H the inverse image in R of V_H. Note that $(P/H)R_H$ is a group just as was considered in this section. That is, V_H is a sum of faithful irreducible $K[P/H]$ modules. By (IV. 9) the character $\divideontimes_\lambda$ of (III. 15) on PR_H is either that considered in (IV. 8) or that in (III. 13). Applying these two results with (III. 6) gives the conclusion.

(IV. 11) <u>Assume that</u> P <u>is a subgroup of an extra special odd</u> p <u>group</u>. <u>Assume that</u> PR <u>is a group with normal extra special</u> r <u>subgroup</u> R $(r \neq p)$ <u>of order</u> r^{2m+1}. <u>Suppose</u> $C_P(R) = 1$. <u>Assume that</u> P <u>centralizes</u> D(R). <u>Assume that</u> $p^c \neq r^d + 1$ <u>for</u> $c = 1,2$ <u>or</u> $d \leq m$. <u>Suppose</u> X <u>is an irreducible character of</u> PR <u>nontrivial on</u> D(R). <u>Then</u>

$$(X|_P, 1_P)_P > 0.$$

For γ irreducible on P, $(\gamma\bar{\gamma}, 1_P)_P > 0$. By (I. 2) and (III. 15) $X = \gamma\divideontimes_\lambda$. But by (IV. 10) $\gamma\bar{\gamma}$ is in $\divideontimes_\lambda$. Hence the result.

V. REDUCTION LEMMAS

Suppose that AG is a solvable group with normal subgroup G where $(|A|, |G|) = 1$. Suppose that $|G| = q^m q_o$ where $(q, q_o) = 1$, $m \geq 0$, and q is a prime. Suppose that $Q = GF(q)$ or the rational field and δ is a primitive $q_o|A|$, $(q, |A|) = 1$, root of unity and $k = Q(\delta)$. Suppose that V is a $k[AG]$ module.

(V. 1) <u>Suppose</u> $A' \leq A^* \leq A$ <u>and</u> $A_1 \leq A$. <u>Suppose that</u> J <u>is an irreducible</u> $k[A_1]$ <u>module</u>. <u>Suppose that</u>

$$L = \ker [A_1 \longrightarrow \operatorname{Aut} J] \geq A_1 \cap A^*.$$

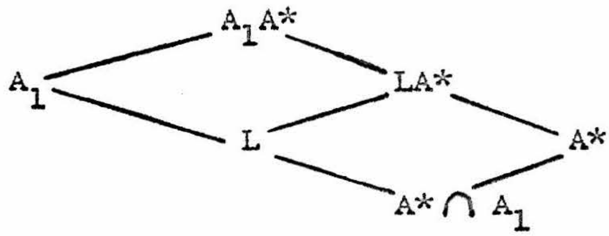
<u>Let</u> $I = C_{J|^A}(A^*)$. <u>Then</u>

$$\ker [A \longrightarrow \operatorname{Aut} I] = LA^*.$$

First suppose $C_{J|^{A_1A^*}}(A^*) = J_o$ has kernel LA^*. Set

$J_1 = [A^*, J|^{A_1A^*}]$. Then $J|^{A_1A^*} = J_o \dotplus J_1$ as a $k[A_1A^*]$ module. Let J' be an irreducible component of J_1. Then $[A^*, J'] = J'$. Hence, $[A^*, J'|^A] = J'|^A$. So I must be contained wholly in $J_o|^A$. But $J_o|^A|_{LA^*}$ $= \sum_{\pi A_1A^*} \oplus \; \pi \otimes J_o|_{LA^*}$. Now $A^*, LA^* \Delta A$ so $\pi \otimes J_o|_{LA^*}$ is both a trivial LA^* and A^* module. Hence, $J_o|^A = I$.

So we may assume that $A_1A^* = A$ and prove the lemma in that case.



Now $J|^{A_1A^*}|_{LA^*} \simeq_{LA^*} \sum_{A_1 \pi LA^*}^{\oplus} \pi\otimes J|_{A_1^{\pi^{-1}} \cap LA^*}|^{LA^*}$

$\simeq_{LA^*} J|_{A_1\cap LA^*}|^{LA^*} = J|_L|^{LA^*}$ since $A_1LA^* = A_1A^*$ and $L \le A_1\cap LA^* \le L(A_1\cap A^*) = L$. But L is trivial on $J|_L$ so $J|^{A_1A^*}|_{LA^*} \simeq_{LA^*} (\dim J)\ 1_L|^{LA^*}$ where 1_L is the trivial L module of dimension 1. Next $\dim \mathrm{Hom}_{k[LA^*]}(1_{LA^*}, 1_L|^{LA^*}) = \dim \mathrm{Hom}_{k[L]}(1_{LA^*}|_L, 1_L) = 1$. So $\dim C_{J|^{A_1A^*}}(LA^*) = \dim J$. Clearly $C_{J|^{A_1A^*}}(LA^*)$ is contained in I. But

$\dim \mathrm{Hom}_{k[A^*]}(1_{A^*}, 1_L|^{LA^*}|_{A^*}) = \dim \mathrm{Hom}_{k[LA^*]}(1_{A^*}|^{LA^*}, 1_L|^{LA^*})$

$= \dim \mathrm{Hom}_{k[L]}(1_{A^*}|^{LA^*}|_L, 1_L) = 1$. And, in addition, $J|^{A_1A^*}|_{LA^*}|_{A^*} \simeq_{A^*} (\dim J)\ 1_L|^{LA^*}|_{A^*}$. Therefore $\dim I = \dim J = \dim C_{J|^{A_1A^*}}(LA^*)$. Hence $C_{J|^{A_1A^*}}(LA^*) = I$. So LA^* is in the kernel of I.

Suppose $B > LA^*$. Then since $A_1B = A_1A^*$, $[A_1B : B] = [A_1 : A_1\cap B]$ and $A_1\cap B \ge L$ we must have $A_1\cap B > L$. Now

$$J|^{A_1A^*}|_B \simeq_B J|_{B\cap A_1}|^B. \quad \text{But}$$

$\dim \mathrm{Hom}_{k[B]}(1_B, J|_{B\cap A_1}|^B) = \dim \mathrm{Hom}_{k[B\cap A_1]}(1_B, J|_{B\cap A_1})$ $= 0$ since $A_1/A^*\cap A_1$ is abelian so A_1/L is cyclic and $J|_{B\cap A_1}$ is a sum of faithful irreducible submodules. So the kernel of I is LA^*.

(V. 2) <u>Suppose</u> $A' \leq A^* \leq A$ <u>and</u> $A_1 \leq A$. <u>Suppose</u> U <u>is a</u> $k[A_1G]$ <u>module and</u> $V \simeq_{AG} U|^{AG}$. <u>Then</u>

i) $C_V(A^*) = (0)$ <u>if and only if</u> $C_U(A_1\cap A^*) = (0)$.

<u>If</u> $C_V(A^*) \neq (0)$ <u>then</u>

ii) $C_A C_V(A^*) = A^*C_{A_1} C_U(A_1\cap A^*)$.

We know that $V|_{A^*} \simeq_{A^*} U|^{AG}|_{A^*} \simeq_{A^*}$

$$\sum_{A^*\pi A_1 G} \oplus\ \pi\otimes U|_{(A_1G)^{\pi^{-1}}\cap A^*}|^{A^*}.$$

The π's may be chosen in A. Hence $\pi\otimes U|_{(A_1G)^{\pi^{-1}}\cap A^*}|^{A^*}$ is conjugate by π^{-1} to $U|_{A_1G\cap A^*}|^{A^*}$ since $A^* \Delta A$ and $\pi \in A$.

But then $C_{U|_{A_1G\cap A^*}|^{A^*}}(A^*) \simeq_{A^*} C_{\pi\otimes U|_{(A_1G)^{\pi^{-1}}\cap A^*}|^{A^*}}(A^*)$.

Now $\dim \mathrm{Hom}_{k[A^*]}(1_{A^*}, U|_{A_1\cap A^*}|^{A^*}) =$

$$\dim \mathrm{Hom}_{k[A_1\cap A^*]}(1_{A^*}|_{A_1\cap A^*}, U|_{A_1\cap A^*}).$$

Hence $C_U(A_1\cap A^*) = (0)$ if and only if $C_V(A^*) = (0)$.

<u>Remark</u>: With $A^* = A$ this says, $C_U(A_1) = (0)$ if and only if

$C_V(A) = (0)$.

To get ii) we apply i) and (V. 1).

(V. 3) Suppose that H is a group with normal subgroup N of index n. Suppose that U is an H module over a field K of characteristic zero or prime to n. Assume that $U|_N$ is completely reducible. Then U is completely reducible.

Let $1 = \pi_1, \ldots, \pi_n$ be coset representatives of N in G. Then $\pi_i \pi_j = \pi_{(i,j)} n_{ij}$ where $n_{ij} \in N$. Let J be an irreducible submodule of U. Then $U|_N = J|_N \dotplus I$ where I is an N module. We may find I since $U|_N$ is completely reducible. Let $w \in U$. Then $w = y + z$ uniquely where $y \in J$ and $z \in I$. Let $\phi : w \longrightarrow y$ be the usual projective $K[N]$ homomorphism of U onto J. Set

$$\Phi = n^{-1} \sum_i \pi_i \phi \pi_i^{-1}.$$

Note that n^{-1} exists in K. This is clearly a $K[H]$ homomorphism of U into U since ϕ is a $K[N]$ homomorphism.

For $w \in U$ we have uniquely $\pi_i^{-1} w = \pi_i^{-1} y_i' + \pi_i^{-1} z_i'$ where $\pi_i^{-1} y_i' \in J$ and $\pi_i^{-1} z_i' \in I$. Now J is an H module so $y_i' \in J$. Hence,

$$\Phi(w) = n^{-1} \sum_i \pi_i \phi \pi_i^{-1} w = n^{-1} \sum_i \pi_i \phi(\pi_i^{-1} y_i' + \pi_i^{-1} z_i') = n^{-1} \sum_i \pi_i \pi_i^{-1} y_i' = n^{-1} \sum_i y_i' \in J.$$

In other words, if $w \in J$ then $\Phi(w) = w$. Hence, Φ is idempotent. So the kernel of Φ is a $K[H]$ module complementary to J in U. Therefore, U is completely reducible.

(V. 4) <u>Suppose that</u> V <u>is a completely reducible</u> k[AG] <u>module</u>. <u>Assume</u> $M \leq G$ <u>is normal in</u> AG. <u>Suppose</u> $A_1 \leq A$. <u>Then</u> $V|_{A_1M}$ <u>is completely reducible</u>.

By Clifford's Theorems $V|_M$ is completely reducible. Hence (V. 3) applies to $V|_{A_1M}$.

(V. 5) <u>Suppose that</u> H <u>is a group with normal subgroup</u> N <u>of index</u> n. <u>Assume that</u> U <u>is a completely reducible</u> N <u>module over a field</u> K <u>of characteristic</u> 0 <u>or prime to</u> n. <u>Then</u> $U|^H|_N$ <u>is completely reducible so</u> $U|^H$ <u>is completely reducible</u>.

Let $\pi_1 = 1, \ldots, \pi_n$ be coset representatives of N in H. Then $U|^H|_N = \pi_1 \otimes U \oplus \pi_2 \otimes U \oplus \ldots \oplus \pi_n \otimes U$. Suppose $U = U_1 \dotplus \ldots \dotplus U_s$ where the U_i are irreducible N modules. Then

$$\pi_i \otimes U = \pi_i \otimes U_1 \dotplus \ldots \dotplus \pi_i \otimes U_s$$

where the $\pi_i \otimes U_j$ are irreducible N modules since $N \Delta G$. So $U|^H|_N$ is completely reducible. So by (V. 3) $U|^H$ is completely reducible.

(V. 6) <u>Suppose</u> V <u>is an irreducible</u> K[AG] <u>module and</u> $V|_{A_oG}$ <u>is not homogeneous for</u> $A_oG \Delta AG$. <u>Assume that</u> A <u>is nilpotent</u>. <u>Then there is a subgroup</u> $A_o \leq A^* \Delta A$ <u>of prime index</u> n <u>such that</u>

$$V|_{A^*G} = U_1 \dotplus \cdots \dotplus U_n$$

<u>where the</u> U_i <u>are irreducible</u> A^*G <u>modules and</u> $V \simeq_{AG} U_1|^{AG}$.

We know that A_oG is normal in AG since A is nilpotent. So by Clifford's Theorems $V|_{A_oG}$ is completely reducible. So $V|_{A_oG} = V_1 \dotplus \cdots \dotplus V_e$ where the V_i are homogeneous components. Let $A_1 = \text{Stab}\,(A,V_1)$. Since $A_oG \Delta AG$, $A_1G = \text{Stab}(AG,V_1)$. So V_1 is an irreducible A_1G module and $V_1(A_1G)|^{AG} \simeq_{AG} V$. But A is nilpotent so there is $A_1 \leq A^* \Delta A$ maximal of prime index n so that $V|_{A^*G} = U_1 \dotplus \cdots \dotplus U_n$ where the U_i are irreducible A^*G modules with $U_1 \simeq_{A^*G} V_1(A_1G)|^{A^*G}$ and so $U_1|^{AG} \simeq_{AG} V$.

(V. 7) <u>Suppose that</u> $Y \Delta X \leq G$ <u>are</u> A <u>invariant subgroups in</u> AG. <u>If</u> A <u>fixes the coset</u> xY <u>for</u> $x \in X$ <u>then</u> A <u>fixes an element</u> $xy \in xY$. <u>Further</u> $C_{X/Y}(A) = C_X(A)Y/Y$.

Suppose that A fixes the coset xY. Let AY act upon xY by ay: $h \in xY \longrightarrow ayha^{-1}$ where $a \in A$ and $y \in Y$. Since A fixes xY and $Y \Delta X$ we see that AY fixes xY permuting the elements. Further, Y acts transitively as the regular representation of Y. The subgroup of AY fixing $h \in xY$ is then of order $[AY: Y] = |A|$. Therefore, it is a Hall $|A|$ subgroup of AY and is conjugate in AY to A. Therefore A fixes an element of xY. The rest is obvious.

(V. 8) <u>Suppose</u> $M \leq G$ <u>is normal in</u> AG. <u>Assume</u> $\pi \in G$. <u>Then we may choose</u> $\pi' \in \pi M$ <u>so that</u>

$$C_A(\pi') = A \cap (AM)^{\pi'} = A \cap (AM)^{\pi}.$$

Let $A_o = A \cap (AM)^{\pi}$. Now $\pi M \in C_{G/M}(A_o)$. So we may choose $\pi' \in \pi M$ so that $\pi' \in C_G(A_o)$. Then

$$C_A(\pi') = A \cap (AM)^{\pi'} = A \cap (AM)^{\pi} = A_o.$$

(V. 9) <u>Suppose</u> $p \mid |G|$. <u>Then</u> A <u>fixes</u> P, <u>some</u> p <u>Sylow subgroup of</u> G.

Choose P_o a p Sylow subgroup of G. Let $N = N_{AG}(P_o)$. Then NG = AG. Suppose $x \in AG$. Now $P_o{}^x$ is a p Sylow subgroup of G so there is $y \in G$ with $P_o{}^{xy} = P_o$. So $xy \in N$ or $x \in Ny^{-1} \leq NG$. Hence $AG \leq NG$.

Next $(|G|,|A|) = 1$ so $|A|$ divides $|N|$. In other words, N contains a Hall $|A|$ subgroup, A_o. There then is $z \in G$ so that $A_o{}^z = A$. By putting $P = P_o{}^z$ we get $A \leq N_{AG}(P)$.

(V. 10) <u>If</u> $H \leq C_G(A)$ <u>and</u> $N = N_G(H)$ <u>then</u>

$$N = C_N(A)C_N(H).$$

We apply the Three Subgroup Lemma here which says that for subgroups H,J,L of a group $[H,J,L] = 1$ and $[J,L,H] = 1$ implies $[L,H,J] = 1$.

Clearly $[A,H] = 1$ and $[H,N] \leq H$. Therefore

$[A,H,N] = [H,N,A] = 1$. And so $[N,A,H] = 1$ or $[N,A] \leq C_G(H)$. So by (V. 7) $N = C_N(A)C_G(H)$. But obviously $C_G(H) = C_N(H)$.

VI. THE MAIN LEMMA

In this section we prove the major result of this thesis. It is the lemma which makes everything work. The familiar technique of reducing a minimal counter example is used. The pattern was set in E. Shult's work (8). The object is to reduce the minimal counterexample so that the character lemmas of sections III and IV may be applied. The result is carried out for a general class two odd p group. Only section IV prevents us from getting the strong result.

In the beginning reduction steps are fairly complete. As arguments are repeated often they become shorter with use.

Suppose that A is a group and $(|A|, r) = 1$ for a prime r. Assume that p is a prime and $(|A|, p) = 1$, $p \neq r$. Suppose that AR is a group with extra special normal r subgroup R. We assume that A is irreducible on $R/D(R)$ and trivial on $D(R)$ with $A_o = C_A(R)$. Suppose that Q is $GF(p)$ or the rational field and δ is a primitive $|AR|^{th}$ root of unity and $k = Q(\delta)$. Assume that V is an irreducible $k[AR]$ module which is nontrivial on $D(R)$ and $C_V(A_o) = V$. We also suppose that for any $n \mid \exp A$, $n \neq r^c + 1$ for any c if $r^{2c+1} \mid |R|$.

(*) A_1 is called a (*) group if $V|_A$ contains the trivial A module for any R, V, and $A \leq A_1$ satisfying the above conditions.

By (III. 11) abelian groups are (*) groups. By (IV. 11) an odd p group P is a (*) group if all of its irreducible representations are cyclic or the central product of an extra special p group with a cyclic group of exponent p or p^2. That is, all irreducible representations are subgroups of extra special groups. Note that subgroups and factor groups of (*) groups are (*) groups. In particular, all class two groups of exponent p are (*) groups. We do not know if all those of exponent p^2 are (*) groups since there is a class two group P of order p^6 of exponent p^2 where P/Z(P) is of rank two and exponent p^2 and P has a faithful irreducible character. This group is not covered in section IV.

The lemma is stated on the next page.

(VI. 1) **Theorem:** Suppose that A is a p group of class ≤ 2 for odd p. Suppose A is a (*) group. Assume that AG is a solvable group with normal subgroup G where $(|A|, |G|) = 1$. Suppose that $|G| = q^m q_o$ for a prime $q \neq p$ $(m \geq 0)$ and $(q, q_o) = 1$. Assume $k = Q(\delta)$ where $Q = GF(q)$ or the rational field and δ is a primitive $|A| q_o$ root of unity. Suppose V is a k[AG] module faithful on G. Assume that

i) V is a sum of equivalent irreducible k[AG] modules

ii) if $\exp A = p^a$ then $p^b \neq r^c + 1$ for $1 \leq b \leq a$ and any prime r such that $r^{2c+1} \mid |G|$.

Then

1) $C_V(A) \neq (0)$ or

2) $C_V(A') = (0)$ or

3) $C_V(A') \neq (0)$ implies there is cyclic $D \leq A$ with

a) $C_V(A'D) = (0)$ and

b) $C_G(A'D) \geq C_G(A')$.

The proof begins on the next page.

We assume that (VI. 1) is false and choose a counterexample (A, G, V) minimizing $|A| + |G| + \dim V$. So we have the following:

1') $C_V(A) = (0)$ and

2') $C_V(A') \neq (0)$ and

3') for any cyclic $D \leq A$

a') $C_V(A'D) \neq (0)$ or

b') $C_G(A'D) \not\geq C_G(A')$.

(VI. 2) <u>V is an irreducible $k[AG]$ module</u>.

Here $V = V_1 \dotplus \ldots \dotplus V_t$ is a sum of equivalent irreducible $k[AG]$ modules. Hence, (A,G,V_1) is a counterexample if and only if (A,G,V) is also. So $t = 1$.

(VI. 3) <u>$V|_{A_oG}$ is a multiple of a single irreducible A_oG module for every $A_o \Delta A$. In particular, $V|_G$ is homogeneous.</u>

Suppose not. By (V. 6) there is $A_o \leq A_1 \Delta A$ of prime index p so that

$$V|_{A_1G} = U_1 \dotplus \ldots \dotplus U_p$$

where the U_i are irreducible A_1G modules and $V \simeq_{AG} U_1|^{AG}$. Let $G_i = \ker[G \longrightarrow \operatorname{Aut} U_i]$, $\underline{G}_i = G/G_i$.

Clearly $(A_1, \underline{G}_1, U_1)$ satisfies the hypotheses of (VI. 1). Hence, (VI. 1) holds in this case by induction.

Now $V|_A \simeq_A U_1|^{AG}|_A \simeq_A U_1|_{A_1}|^A$.

1) So by (V. 2) $C_{U_1}(A_1) = (0)$ if and only if $C_V(A) = (0)$.

2) Also by (V. 2) we have, since $A_1 \geq A' \geq A_1'$,
$(0) \neq C_{U_1}(A_1 \cap A') = C_{U_1}(A') \leq C_{U_1}(A_1')$.

Hence we find

3) there is $D \leq A_1$ cyclic so that

a") $C_{U_1}(A_1'D) = (0)$ and

b") $C_{\underline{G}_1}(A_1'D) \geq C_{\underline{G}_1}(A_1')$.

Using the fact that $A_1 \geq A' \geq A_1'$, from a") we get

a_1) $C_{U_1}(A'D) \leq C_{U_1}(A_1'D) = (0)$.

And $C_{\underline{G}_1}(D) \geq C_{\underline{G}_1}(A_1'D) \geq C_{\underline{G}_1}(A_1') \geq C_{\underline{G}_1}(A')$ so

b_1) $C_{\underline{G}_1}(A'D) \geq C_{\underline{G}_1}(A')$.

Choose $1 = \pi_1, \ldots, \pi_p$ as coset representatives of A_1 in A. We may arrange the π_i so that $U_i = \pi_i U_1$. Further, $x \in A_1$ acts upon U_i as $x^{\pi_i} = \pi_i^{-1} x \pi_i$ acts upon U_1, and upon $\underline{G}_i$ as x^{π_i} acts upon $\underline{G}_1$ with the isomorphism $yG_1 \longrightarrow y^{\pi_i^{-1}} G_1^{\pi_i^{-1}}$ of $\underline{G}_1$ onto $\underline{G}_i$. Since $A' \leq A_1$ and $A' \Delta A$, $A'D \Delta A$ we get

a_i) $C_{U_i}(A'D) = (0)$ and

b_i) $C_{\underline{G}_i}(A'D) \geq C_{\underline{G}_i}(A')$.

So finally

a) $C_V(A'D) = (0)$ and

b) $C_G(A'D) \geq C_G(A')$ by (V. 7).

Therefore, $V|_{A_oG}$ is homogeneous.

(VI. 4) <u>For every</u> $A_o < A$ <u>we have</u> $C_V(A_o) \neq (0)$.

Suppose $A_o < A$ and $C_V(A_o) = (0)$. Hence we may choose $A_o \leq A_1 \Delta A$ and $A_1 < A$ since A is nilpotent, and $C_V(A_1) = (0)$. Clearly $A_1' \leq A'$. So $C_V(A_o') \geq C_V(A') \neq (0)$. So by (VI. 3), $V|_{A_1G}$ is homogeneous. Hence, using induction, we may apply (VI. 1) to (A_1, G, V). From the foregoing, it is clear that we have

3) a') $C_V(A_1'D) = (0)$ and

b') $C_G(A_1'D) \geq C_G(A_1')$

for a cyclic $D \leq A_1$. So

a) $C_V(A'D) \leq C_V(A_1'D) = (0)$ and

$C_G(D) \geq C_G(A_1'D) \geq C_G(A_1') \geq C_G(A')$ or

b) $C_G(A'D) \geq C_G(A')$.

Hence the conclusion.

(VI. 5) A <u>is faithful on</u> V.

Suppose not. Let $A_o = \ker[A \longrightarrow \mathrm{Aut}\ V]$. Since G is faithful and V is an irreducible AG module we must have $[A_o, G] = 1$. Hence (VI. 1) applies to $(A/A_o, G, V)$. Let $\underline{A} = A/A_o$ and $\underline{A}_1 = A'A_o/A_o$. Then $\underline{A}_1 = \underline{A}'$ so clearly $C_V(\underline{A}) = C_V(A) = (0)$ and $C_V(\underline{A}') = C_V(A') \neq (0)$. So there is $\underline{D} \leq \underline{A}$ cyclic with

a") $C_V(\underline{A}'\underline{D}) = (0)$ and

b") $C_G(\underline{A}'\underline{D}) \geq C_G(\underline{A}')$.

Let $D \leq A$ be cyclic such that $DA_o/A_o = \underline{D}$. Then since

$A'A_o/A_o = \underline{A}'$,

a) $C_V(A'D) = (0)$.

And $C_G(D) \geq C_G(A'D) \geq C_G(A')$ so

b) $C_G(A'D) \geq C_G(A')$.

Therefore A is faithful on V.

Choose $M < G$ as a maximal AG invariant subgroup of G. The group G/M is an irreducible A module, where the action, for $x \in A$ and $\pi M \in G/M$, is

$$x(\pi M) = \pi^{x^{-1}} M = (x\pi x^{-1})M.$$

From each A orbit on G/M choose a representative $\pi_i M$. So that $\pi_1 M, \ldots, \pi_m M$ form a complete set of A orbit representatives. By (V. 8) we may choose π_i, $i = 1, \ldots, m$ so that $C_A(\pi_i) = A \cap A^{\pi_i^{-1}} = A \cap (AM)^{\pi_i^{-1}} = A_i$. By choosing A conjugates of $\pi_1 = 1, \ldots, \pi_m$ we get a complete set of coset representatives of M in G; $\pi_1 = 1, \ldots, \pi_m, \ldots, \pi_e$ where $C_A(\pi_j) = A \cap A^{\pi_j^{-1}} = A \cap (AM)^{\pi_j^{-1}} = A_j$, $j = 1, \ldots, e$. Further, A permutes the π_j if we specify for $x \in A$ that,

$$x(\pi_j M) = \pi_{j(x)} M.$$

Now $V|_G$ is homogeneous. Therefore, $V|_M = V_1 \dot{+} \ldots \dot{+} V_f$ with homogeneous components V_i. Further, G is transitive on the V_i's and M fixes each one. That is, f divides $|G/M|$.

(VI. 6) <u>If</u> $f \neq 1$ <u>then</u> $f = e = |G/M|$ <u>and the</u> V_i <u>may be numbered so that</u> A <u>fixes</u> V_1, $\pi_i V_1 = V_i$, <u>and</u> A <u>permutes the</u> V_i <u>exactly as it permutes the</u> π_i.

Consider the permutation representation ϕ of AG on the V_i's. Now M is in the kernel of ϕ. Further $G \cap \ker \phi$ is a proper AG invariant subgroup of G containing M, so it must be M. Since G/M is abelian, $G \cap \ker \phi$ is the subgroup of G fixing every V_i. And now $f = e = |G/M|$.

But ϕ is a transitive representation of A(G/M) given on the cosets of some subgroup B of order $|A(G/M)|/e = |A|$. So B and A are Hall $|A|$ subgroups of A(G/M). Hence they are conjugate in A(G/M). In other words, the representation is given on the cosets of A. Therefore A fixes, say, V_1. Setting $V_i = \pi_i V_1$, for $x \in A$ we get

$$xV_i = x(\pi_i V_1) = (x\pi_i x^{-1})V_1 = \pi_i^{\,x^{-1}} V_1 = \pi_{i(x)} V_1 = V_{i(x)}.$$

So this step is complete.

(VI. 7) <u>If</u> $f \neq 1$ <u>then for the</u> (A,AM) <u>coset representatives</u> $\pi_1 = 1, \ldots, \pi_m$ <u>we have</u>

$$V|_A \simeq_A \sum_{i=1}^{m} \oplus \; V_1|_{A_i}|^A,$$

<u>and</u> $$V \simeq_{AG} V_1(AM)|^{AG}.$$

Since AM stabilizes V_1 and $|\mathrm{Stab}(AG,V_1)| = |AG|/e = |AM|$ we have $AM = \mathrm{Stab}(AG,V_1)$. Now $M \Delta AG$ so $V \simeq_{AG}$

$V_1(AM)|^{AG}$.

By the Mackey Decomposition we get

$$V|_A \simeq_A V_1(AM)|^{AG}|_A \simeq_A \sum_{i=1}^{m}\oplus\ \pi_i V_1|_{(AM)^{\pi_i^{-1}} \cap A}|^A$$

$$\simeq_A \sum_{i=1}^{m}\oplus\ V_1|_{A_i}|^A$$

since $(AM)^{\pi_i^{-1}} \cap A = C_A(\pi_i) = A_i$.

Remark: If $V_1|_{A_j}$ contains the trivial A_j module then $V_1|_{A_j}|^A$ contains the trivial A module by (V. 2). So $C_V(A) = (0)$ implies that $C_{V_1}(A_j) = (0)$ for each $j = 1, \ldots, m$. (Hence also for $j = 1, \ldots, e$.)

Let $A_M = \ker[A \longrightarrow \operatorname{Aut} G/M]$.

(VI. 8) If $V_1|_{A_M}$ does not contain the trivial A_M submodule then $f = 1$. (i.e. $V|_M$ is homogeneous.)

Suppose $V_1|_{A_M}$ does not contain the trivial A_M submodule. Now $A_M M \trianglelefteq AG$ since $[A_M, G] \leq M$ and $A_M \trianglelefteq A$. So $V_1|_{A_M M}$ is a homogeneous $A_M M$ module by (VI. 3) and (VI. 1) applies to $(A_M, M/M_1, V_1)$ where

$$M_1 = \ker[M \longrightarrow \operatorname{Aut} V_1]$$

by induction.

By assumption $C_{V_1}(A_M) = (0)$.

Next $A_M \leq A_j$ for every j. So $A_M' \leq A_j \cap A'$ for every j. If $C_{V_1}(A_M') = (0)$ then $C_{V_1}(A_j \cap A') = (0)$ for every j.

Hence by (V. 2) $C_{V_1|_{A_j}|^A}(A') = (0)$ for every j. Hence $C_V(A') = (0)$. So we must have $C_{V_1}(A_M') \neq (0)$.

This means that when we apply (VI. 1) to

$$(A_M, M/M_1, V_1)$$

we have

3) a") $C_{V_1}(A_M'D) = (0)$ and

b") $C_{M/M_1}(A_M'D) \geq C_{M/M_1}(A_M')$.

Set $M_i = \ker[M \longrightarrow \text{Aut } V_i]$, $\underline{M}_i = M/M_i$. Now $A_M'D \leq A_M$ so $A_M'D$ is centralized by every π_i. Hence conjugation of $A_M'D$ by π_i^{-1} fixes $A_M'D$ elementwise. Therefore,

$$C_{\underline{M}_i}(A_M'D) \geq C_{\underline{M}_i}(A_M').$$

So by (V. 8)

$$C_G(A_M'D) \geq C_G(A_M').$$

That is,

$$C_G(D) \geq C_G(A_M'D) \geq C_G(A_M') \geq C_G(A').$$

And

b) $C_G(A'D) \geq C_G(A')$.

Again, since every π_i centralizes A_M,

$$C_V(A_M'D) = (0).$$

That is,

a) $C_V(A'D) \leq C_V(A_M'D) = (0)$.

Hence f = 1.

(VI. 9) <u>If</u> A/A_M <u>is abelian then</u> $f = 1$.

If $f \neq 1$ then A is cyclic and irreducible on G/M. If $\pi_i \neq \pi_1 = 1$ then the orbit $\{\pi_i^x \mid x \in A\}$ is faithful on A/A_M. Hence it is the regular representation of A/A_M. That is, $A_i = A_M$. By the remark preceding (VI. 8) and (VI. 8) we are done.

(VI. 10) <u>If</u> $A/A_M = \underline{A}$ <u>is nonabelian then</u> $f = 1$.

Now G/M is an r group for a prime r. But $\underline{A}$ is a class two p group which is faithful and irreducible on the GF(r) module G/M. So we apply (II. 7) to get a $\pi_i M$ which is fixed by no element of $\underline{A}^{\#}$. In other words, $C_{\underline{A}}(\pi_i) = 1$ or $C_A(\pi_i) = A_i = A_M$. So again by (VI. 8) and the remark preceding it we get $f = 1$.

Under the hypothesis of (VI. 1) this means $V|_M$ is homogeneous and $f = 1$.

Now G/M is an r section. So by (V. 9) we may choose an r Sylow subgroup R_o of G fixed by A. Next let R be chosen in R_o minimal such that

i) R is A invariant, and

ii) $RM = G$.

We eventually show that R is extra special.

Next consider $V|_{AM} = V_1 \dotplus \dots \dotplus V_t$ where the V_i are homogeneous components. Since $V|_M$ is homogeneous, each

V_i is faithful and is a multiple of a single fixed irreducible M module. Since $C_V(A') \neq (0)$ we may choose V_1 so that $C_{V_1}(A') \neq (0)$. Clearly $C_V(A) = (0)$ implies $C_{V_i}(A) = (0)$, $i = 1, \ldots, t$. So we apply (VI. 1) to (A, M, V_1) and obtain $D \leq A$ cyclic so that

a") $C_{V_1}(A'D) = (0)$ and

b") $C_M(A'D) \geq C_M(A')$.

(VI . 11) <u>If</u> A <u>is</u> <u>abelian</u> <u>then</u> $C_A(M) = A^* \neq 1$.

In this case, $A' = 1$ so $C_M(A'D) = C_M(D) \geq C_M(A') = M$. Hence $D \leq C_A(M)$. But $C_{V_1}(A'D) = C_{V_1}(D) = (0)$ so $1 \neq D \leq A^*$.

(VI . 12) $C_A(M) = A^* \neq 1$.

We may assume that A is nonabelian. Let U be a homogeneous component of $V_1|_{A'DM}$. Since $V|_M$ is homogeneous, U is faithful on M. Now $(A'D)' = 1$ since A is class two, $A' \leq Z(A)$, and D is cyclic. Since $C_{V_1}(A'D) = (0)$, $C_U(A'D) = (0)$. Further, $C_U[(A'D)'] = U$. So in applying (VI. 1) to $(A'D, M, U)$ we get 3) and $D_1 \leq A'D$ cyclic so that

b*) $C_M[(A'D)'D_1] = C_M(D_1) \geq C_M[(A'D)'] = M$.

Also since

a*) $C_U[(A'D)'D_1] = C_U(D_1) = (0)$,

we have $D_1 \neq 1$. Hence $D_1 \leq C_A(M) = A^*$.

(VI. 13) $A^* \cap A_M = 1$ <u>and</u> $C_G(A^*) = M$.

Suppose $A^* \cap A_M = A_o \neq 1$. Now $A_o \Delta A$ so we may take $A_1 = Z(A) \cap A_o \neq 1$ since A is nilpotent. We know that A^* centralizes M and A_M centralizes G/M. Hence by (V. 7) A_1 centralizes A and G. So $A_1 \leq Z(AG)$. But V is irreducible so A_1 is cyclic and acts as scalar multiplication on V by (VI. 5). Hence $C_V(A_1) = (0)$. By (VI. 4) $A_1 = A$. But then A is cyclic and

a) $C_V(A'A) = C_V(A) = (0)$ and

b) $C_G(A) = G \geq C_G(A') = G$.

Hence $A^* \cap A_M = 1$. But then $A^*A_M/A_M \Delta A/A_M$ so

$A^*A_M/A_M \cap Z(A/A_M) \neq 1$ and $C_{G/M}(A^*) = 1$.

Hence $C_G(A^*) = M$.

(VI. 14) <u>We can choose</u> R <u>so that</u> $R \leq C_G(M)$, R <u>is extra special</u>, <u>and</u> R Δ AG. <u>Further</u>, $D(R) \leq M$, $D(R) \leq C_G(AG)$.

Now $G = N_G(M)$. But $M = C_G(A^*)$ so by (V. 10) $G = C_G(M)C_G(A^*) = C_G(M)M$. Now $C_G(M)$ is A invariant so R may be chosen so that $R \leq C_G(M)$.

Let $R_1 = Z(R)$. Now $R_1 \leq C_G(M)$ so $R_1 \leq Z(G)$, since $RM = G$. Further $V|_G$ is homogeneous and faithful so R_1 is cyclic and acts as scalar multiplication on V. In particular, because AG is faithful, $R_1 \leq Z(AG)$. So $R_1 \leq M$ and $R_1 \leq C_G(AG)$.

By the minimal choice of R we must have $M \cap R = D(R)$

as the unique maximal A invariant normal subgroup of R. Let R_o be any characteristic abelian subgroup of R. Now $R/D(R) \simeq_A G/M$ so if $R_o < R$ then $R_o \leq D(R)$. But $C_R(A^*) \leq D(R)$ and so $Z(R) = R_1 < R$. Hence $R_o \leq D(R)$. But then $R_o \leq M$. We already know that $R_o \leq C_G(M) \cap M = Z(M)$ and $V|_M$ is homogeneous. So $R_o \leq Z(R) = R_1$ and R_o is cyclic. So R is the central product of a cyclic r group and an extra special r group. By the minimality of R, this means R is extra special.

Finally, $R \leq C_G(M)$ normalizes itself and is normalized by A. Hence $R \triangle AG$.

(VI. 15) $V|_R$ <u>is homogeneous</u>; $C_V(A_M) = (0)$.

Here $V|_G$ is homogeneous. So, since $R \triangle G$, $V|_R$ is completely reducible and the homogeneous components are permuted transitively by M since $MR = G$. But M centralizes R so $V|_R$ is homogeneous.

Suppose next that $C_V(A_M) \neq (0)$. Now A_M centralizes $G/M \simeq_A R/D(R)$, so it centralizes R. Further, $A_M \triangle A$. Hence $C_V(A_M)$ is a $k[AR]$ submodule of V. Let $V_o \leq C_V(A_M)$ be an irreducible $k[AR]$ submodule. Since $Z(R) = D(R) \leq Z(AG)$ it acts as scalar multiplication (nontrivially) on V hence also on V_o. Further, on V_o, A is represented as A/A_M. Now $A_M < A$ since $C_V(A) = (0)$. Therefore V_o is a $k[(A/A_M)R]$ irreducible module. Also A/A_M is faithful and irreducible on $R/D(R)$. Now $|R| = r^{2c+1} \mid |G|$. Further, by hypothesis, $p^b \neq r^e + 1$ for any $e \leq c$ and any $p^b \leq \exp A$. Hence we may apply the fact that A is a (*) group to find that $(0) \neq C_{V_o}(A) \leq C_V(A)$. But $C_V(A) = (0)$. Hence $C_V(A_M) = (0)$.

(VI. 16) (VI. 1) <u>holds</u>.

By (VI. 12) $A^* \neq 1$. And by (VI. 13) $A^* \cap A_M = 1$. Hence $A_M < A$. So by (VI. 4) $C_V(A_M) \neq (0)$. This contradicts (VI. 15). Therefore (VI. 1) holds.

We now curtail the hypotheses on k.

(VI. 17) Corollary: <u>In</u> (VI. 1) <u>we may assume that</u> k <u>is any subfield of</u> $Q(\delta)$. <u>In particular, we may take</u>

$$k = GF(q).$$

Suppose U is a homogeneous $K[AG]$ module satisfying all of (VI. 1) except that $K \leq Q(\delta)$ is a subfield of $Q(\delta)$. Let $K(\delta) = k = Q(\delta)$. Then k is a finite extension of K. Let $\underline{U} = k \otimes_K U$. Let V be any irreducible $k[AG]$ submodule of $\underline{U}$. Then V is a $K[AG]$ module isomorphic to m copies of U for some integer dividing the degree of the extension $[k: K]$. We apply the theorem to (A,G,V). Suppose

$$V \simeq_{K[AG]} \underbrace{U \oplus \dots \oplus U}_{m}.$$

It is clear that

$$C_V(L) \simeq_{K[AG]} \underbrace{C_U(L) \oplus \cdots \oplus C_U(L)}_{m}$$

for any $L \leq A$. Also G is faithful on V since it is on U. The two isomorphisms give (VI. 17).

(VI. 18) Corollary: Suppose that in (VI. 17) conclusion 2) arises. That is,

2) $C_V(A') = (0)$.

Then there is $1 \neq D \leq A'$ with

a) $C_V(D) = (0)$ and

b) $C_G(D) = G$.

Now $V|_{A'G} = V_1 \dotplus \cdots \dotplus V_t$ where the V_i are (in the case of (VI. 1)) homogeneous components. Let

$G_i = \ker[G \longrightarrow \mathrm{Aut}\, V_i]$, $\underline{G}_i = G/G_i$.

Then we apply (VI. 1) to $(A', \underline{G}_1, V_1)$. Since $A'' = 1$, and $C_{V_1}(A') = (0)$ we get by (VI. 1) a cyclic $D \leq A'$ so that

a') $C_{V_1}(D) = (0)$ and

b') $C_{\underline{G}_1}(D) = \underline{G}_1$.

Now $D \leq A' \leq Z(A)$. So

a) $C_V(D) = (0)$ and

b) $C_G(D) = G$.

Remark: Again it is no trouble to extend this by the argument of (VI. 17) to the field $K \leq k$.

VII. THE FITTING STRUCTURE

Suppose AG is a group with normal solvable subgroup G, and $(|A|, |G|) = 1$. Consider an AG invariant series

$$1 = S_0 < S_1 < \dots < S_t \leq G$$

satisfying, for $j = 1, 2, \dots, t$,

1) a) $S_1 > S_0$

   b) $S_1^* = 1$

   c) S_1/S_1^* is a nontrivial s(1) group

   d) $S_1 > S_1^{\circ} \geq S_1^*$, S_1° is AG invariant and unique maximal containing S_1^*

   e) $\underline{S}_1 = S_1/S_1^{\circ}$ is an irreducible AG module,

2) a) $S_2 > S_1$

   b) $S_2^* = \ker [S_2 \longrightarrow \text{Aut } \underline{S}_1]$

   c) S_2/S_2^* is a nontrivial s(2) group

   d) $S_2 > S_2^{\circ} \geq S_2^*$, S_2° is unique maximal AG invariant containing S_2^*

   e) $\underline{S}_2 = S_2/S_2^{\circ}$ is a irreducible AG module,

.
.
.

j) a) $S_j > S_{j-1}$

   b) $S_j^* = \ker [S_j \longrightarrow \text{Aut } \underline{S}_{j-1}]$

   c) S_j/S_j^* is a nontrivial s(j) group

   d) $S_j > S_j^{\circ} \geq S_j^*$, S_j° is unique maximal AG invariant containing S_j^*

e) $\underline{S}_j = S_j/S_j^{\circ}$ is an irreducible AG module, and s(i), i = 1, 2, ... , t are primes.

Such a series is called a t-*edifice* in G.

(VII. 1) Hypothesis. Suppose AG is a group with normal solvable subgroup G and $(|A|, |G|) = 1$. Suppose that $E = \{S_i, S_i^*, S_i^{\circ}, \underline{S}_i \mid i = 1, \ldots , t\}$ is a t-edifice for G. Suppose $1 = F_0 < F_1 < \ldots < F_n = G$ is the Fitting series of G.

(VII. 2) *Assume* (VII. 1). *Suppose that*

$$1 = G_0 \leq G_1 \leq \ldots \leq G_r = G$$

is a normal series of G *and* G_{i+1}/G_i, i = 0, ... , r-1 *is nilpotent*. *Then*

$$F_j \geq G_j;\ j = 0, 1, \ldots , n.$$

That is, $n \leq r$.

We proceed by induction on j. For j = 0 the result is trivial. Suppose $F_{j-1} \geq G_{j-1}$. Then $G_j/(F_{j-1} \cap G_j)$ is a homomorphic image of G_j/G_{j-1} since $F_{j-1} \cap G_j \geq G_{j-1}$, and hence is nilpotent. But $G_j/(F_{j-1} \cap G_j) \simeq G_jF_{j-1}/F_{j-1} \Delta G/F_{j-1}$. Therefore

$$G_jF_{j-1}/F_{j-1} \leq F_j/F_{j-1}$$

or

$$G_j \leq G_jF_{j-1} \leq F_j.$$

(VII. 3) *Suppose* $H \leq G$ *has Fitting length* m. *Suppose* G *has Fitting length* n. *Then* $m \leq n$.

Suppose $1 = F_0 \leq F_1 \leq \ldots \leq F_n = G$ is the Fitting series of G. We apply (VII. 2) to the normal series of H given by

$$1 = F_0 \cap H = G_0 \leq F_1 \cap H = G_1 \leq \ldots \leq F_n \cap H = G_n = H.$$

(VII. 4) <u>Suppose</u> (VII. 1). <u>Then</u> $F_i \leq K_i =$ $\ker [G \longrightarrow \mathrm{Aut}\ \underline{S}_i]$, $i = 1, 2, \ldots, t$. <u>Hence</u> $t \leq n$.

We proceed by induction on i. First consider $i = 1$. Since $S_1 \Delta G$ and is an $s(1)$ group, we know that $S_1 \leq F_1$. Suppose $p = s(1)$. Now $O_{p'}(F_1)$ centralizes S_1 and hence $\underline{S}_1$. But then $O_p(F_1)K_1/K_1$ is a normal p subgroup of G/K_1. On $\underline{S}_1$, G/K_1 is completely reducible since $G \Delta AG$ and therefore $O_p(F_1) \leq K_1$. So $F_1 = O_{p'}(F_1) \times O_p(F_1) \leq K_1$.

Suppose that $F_{j-1} \leq K_{j-1}$. We notice that $F_jK_{j-1}/K_{j-1} \simeq F_j/(F_j \cap K_{j-1})$ and $F_j \cap K_{j-1} \geq F_{j-1}$ so F_jK_{j-1}/K_{j-1} is nilpotent and normal in AG/K_{j-1}. So

$$F_jK_{j-1}/K_{j-1} \leq F(AG/K_{j-1}).$$

Further $S_jK_{j-1}/K_{j-1} \simeq S_j/(S_j \cap K_{j-1})$ and $S_j \cap K_{j-1} = S_j^*$. And so S_jK_{j-1}/K_{j-1} is normal and nilpotent in AG/K_{j-1}. Therefore $\quad S_jK_{j-1}/K_{j-1} \leq F(AG/K_{j-1})$.

Finally AG is irreducible on $\underline{S}_j$, a section of S_jK_{j-1}/K_{j-1}, hence, as in $j = 1$, F_jK_{j-1}/K_{j-1} centralizes $\underline{S}_j$. And therefore, $\quad F_j \leq F_jK_{j-1} \leq K_j$.

(VII. 5) <u>Suppose that</u> HP <u>is a group with normal</u> p <u>subgroup</u> P. <u>Assume</u> P <u>has an</u> HP <u>section</u> X/Y <u>on which</u> HP <u>is</u>

irreducible and $H_1 \Delta H$ *is nontrivial. Then* P *contains an HP invariant subgroup* P_o *where* $P_o > P_1 \geq D(P_o)$; P_1 *is HP invariant and*

i) $P_o/P_1 \simeq_{HP} X/Y$ *is an irreducible HP module,*

ii) $P_o/D(P_o)$ *is an indecomposable HP module,*

iii) P_1 *is a unique maximal HP invariant subgroup of* P_o,

and P_o *is minimal satisfying* i), ii), *and* iii).

Let J be the class of all subgroups $P_2 \leq P$ satisfying 1) P_2 is HP invariant

2) P_2 contains an HP invariant subgroup $P_2{}^*$ such that $P_2/P_2{}^* \simeq_{HP} X/Y$.

Clearly $X \in J$ so $J \neq \emptyset$. We choose $P_o \in J$ of minimal order. Since $P_o \in J$ there is $P_1 \geq D(P_o)$ so that $P_o/P_1 \simeq_{HP} X/Y$. So P_o satisfies i).

Since X/Y is HP irreducible, P_1 is a maximal HP invariant subgroup of P_o. Suppose $P_1{}^* \geq D(P_o)$ is also a maximal HP invariant subgroup of P_o. Then as an HP module

$$P_o/(P_1 \cap P_1{}^*) \simeq_{HP} P_1/(P_1 \cap P_1{}^*) \dotplus P_1{}^*/(P_1 \cap P_1{}^*) ,$$

where now

$$P_1{}^*/(P_1 \cap P_1{}^*) \simeq_{HP} P_1P_1{}^*/P_1 = P_o/P_1 \simeq_{HP} X/Y.$$

So $P_1{}^* \in J$. This contradicts the minimality of $P_o \in J$. Hence iii) holds.

Suppose that as an HP module

$$P_o/D(P_o) = P_o{}^*/D(P_o) \dotplus P_o{}''/D(P_o) \quad \text{is decomposable.}$$

Choose $P_1{}^*$ maximal HP invariant in $P_o{}^*$ and $P_1{}''$ maximal HP invariant in $P_o{}''$. Then $P_1{}^*P_o{}''$ and $P_1{}''P_o{}^*$ are distinct maximal HP invariant subgroups of P_o contradicting iii). Hence ii) holds.

Clearly P_o is minimal satisfying i), ii), and iii).

(VII. 6) <u>Suppose that</u> AG <u>is a group with normal solvable subgroup</u> G <u>and</u> $(|A|, |G|) = 1$. <u>Suppose that</u> F <u>is the Fitting subgroup of</u> G. <u>Suppose that</u> $S \leq G$ <u>and</u> S/F <u>is a normal</u> p <u>subgroup of</u> AG/F. <u>Then there is a prime</u> $r \neq p$ <u>and a section of</u> $O_r(F)$ <u>on which</u> AG <u>is irreducible and</u> S <u>is nontrivial</u>.

Consider an r Sylow subgroup R of F. Suppose $r \neq p$. Let P be a p Sylow subgroup of S. Suppose that $[R, P] = 1$ for each such r. Then $S = P \times O_{p'}(F) \Delta G$ so $S \leq F$. This means there is some r for which $[R, P] \neq 1$. In particular, P is nontrivial on R/D(R). Now let

$$D(R)/D(R) = R_0/D(R) < R_1/D(R) < \dots < R_e/D(R) = R/D(R)$$

be an AG composition series of R/D(R). Then R_{i+1}/R_i is an irreducible AG module. Since $p \neq r$, P is nontrivial for some i, say i = j. Then $X = R_{j+1}$, $Y = R_j$ is the desired section.

(VII. 7) <u>Assume</u> (VII. 1). <u>Let</u> $K = \ker [G \longrightarrow \mathrm{Aut}\ \underline{S_1}]$, $\underline{G} = G/K$, $T_i = S_{i+1}K/K$, $T_i{}^* = S_{i+1}{}^*K/K$, $T_i{}^o = S_{i+1}{}^oK/K$, <u>and</u>

$\underline{T}_i = T_i/T_i^{\circ}$ *for* i = 1, 2, ... , t-1. *Then*

$\underline{E} = \{ T_i, T_i^*, T_i^{\circ}, \underline{T}_i \mid i = 1, \ldots , t-1\}$ *is a* t-1 *edifice for* G.

We just verify the definition. We do just 1). Of course, $T_0 = 1$. Then since $K \cap S_2 = S_2^* < S_2$, $T_1 > T_0$. Further $S_2^* \leq K$ so $T_1^* = 1$. Now $T_1/T_1^* \cong_{AG} S_2/S_2^*$ proving the rest.

(VII. 8) *Suppose* AG *is a group with normal solvable subgroup* G *and* $(|A|, |G|) = 1$. *Suppose that the Fitting length of* G *is* n. *Then* G *has an* n *edifice*.

Proof is by induction on n. For n = 1 we take a minimal AG invariant subgroup of G for S_1.

So suppose n > 1. Hence G/F satisfies (VII. 8) by induction. So we get an n-1 edifice for G/F.

$\underline{E} = \{T_i/F, T_i^*/F, T_i^{\circ}/F, \underline{T}_i \mid i = 1, \ldots , n-1\}$.

We apply (VII. 5) and (VII. 6) to obtain S_1. Then with $T_i = S_{i-1}$, $T_i^* = S_{i-1}^*$, $T_i^{\circ} = S_{i-1}^{\circ}$ we get the desired n edifice.

(VII. 9) *Assume* (VII. 1). *Set* $K_i = \ker [G \longrightarrow \mathrm{Aut}\ \underline{S}_i]$ *and* $\underline{G}_i = G/K_i$. *Then for all* $j > i$, $K_j \geq K_i$ *and* $\underline{S}_j$ *is* AG *isomorphic to a section of* $\underline{G}_i$.

We first prove that $K_j \geq K_i$ for $j > i$. We proceed by induction on j - i and save the "first case" of

$j - i = 1$ for last. So assume the result holds for all numbers less than $j - i$ and $j - i > 1$. Then choose $j > f > i$. By induction $K_j \geq K_f \geq K_i$. Hence we need only prove the result for $j - i = 1$.

Since $K_f \geq S_i^{\circ}$ for all $f \geq i$, we may assume $S_i^{\circ} = 1$ by considering G/S_i°, and K_f/S_i°, $f \geq i$. But in this case $i = 1$, $j = 2$, simplifying the notation. We want to prove that $K_2 \geq K_1$. Suppose $x \in K_1$ has order prime to $s(2)$ and x is nontrivial on $\underline{S}_2$. Then x is nontrivial on $S_2/ S_2^* = S_2/K_1 \cap S_2$. Therefore, since x is of order prime to $s(2)$, x is nontrivial on $S_1 = \underline{S}_1$. This contradiction forces K_1K_2/K_2 to be a normal $s(2)$ subgroup of AG/K_2 which is faithful and irreducible on the $GF(s(2))$ module $\underline{S}_2$. Therefore, $K_1 \leq K_1K_2 = K_2$ completing the proof of: $K_j \geq K_i$ for all $j > i$.

The rest is easy since $S_j \cap K_{j-1} = S_j^*$.

(VII. 10) <u>Assume</u> (VII. 1). <u>Suppose</u> $K_i = \ker[G \longrightarrow \mathrm{Aut}\,\underline{S}_i]$ <u>and</u> $\underline{G}_i = G/K_i$. <u>Assume that</u> A <u>is a class two</u> p <u>group</u>.

i) <u>If</u> $D \leq A'$ <u>and</u> $C_{\underline{G}_i}(D) = \underline{G}_i$ <u>then</u> $[D, \underline{S}_j] = (0)$ <u>for all</u> $j > i$.

ii) <u>If</u> $D \leq A$, and $C_{\underline{G}_i}(A'D) \geq C_{\underline{G}_i}(A')$ <u>then for every</u> $j > i$ <u>such that</u> $C_{\underline{S}_j}(A') = (0)$ <u>we have</u> $[D, C_{\underline{S}_j}(A')] = (0)$.

Consider i) first. By (VII. 9), $\underline{S}_j$ for $j > i$

is a section of $\underline{G}_i$. Therefore, D centralizes this section.

Next consider ii). The condition that $C_{\underline{G}_i}(A'D) \geq C_{\underline{G}_i}(A')$ says that D centralizes every section of $\underline{G}_i$ which admits A'D and is centralized by A'. But $C_{\underline{S}_j}(A')$ is just such a section, by (VII. 9) so $[D, C_{\underline{S}_j}(A')] = (0)$.

VIII. THE MAIN THEOREM

We are now in a position to prove the final theorem of the thesis.

(VIII. 1) Theorem: *We assume that A is an odd p group of class ≤ 2. Further, A must be a (*) group as defined in section VI. Assume that AG is solvable with normal subgroup G where $(|A|, |G|) = 1$. Suppose that $\exp A = p^a$ and for every prime r and every integer c such that r^{2c+1} divides $|G|$, and every $1 \leq b \leq a$ we have $p^b \neq r^c + 1$. Suppose $|A| = p^d$ and G has Fitting length n. Assume that A is fixed point free on G (by this we mean only that $C_G(A) = 1$). Then*

$$d \geq n.$$

Let $E = \{S_i, S_i^{\circ}, S_i^*, \underline{S}_i \mid i = 1, \ldots, n\}$ be an n edifice of G. Let $K_i = \ker [G \longrightarrow \operatorname{Aut} \underline{S}_i]$ and $\underline{G}_i = G/K_i$. We apply (VI. 17), (VI. 18), and (VII. 10) to obtain descending chains of subgroups in A.

Set $A_n^{\circ} = \ker [A' \longrightarrow \operatorname{Aut} \underline{S}_n]$.

If $C_{\underline{S}_n}(A') = (0)$ set $A_n^* = A$. If $C_{\underline{S}_n}(A') \neq (0)$ set $A_n^* = \ker [A \longrightarrow \operatorname{Aut} C_{\underline{S}_n}(A')]$.

Continuing inductively we set $A_j^{\circ} = \ker [A' \longrightarrow \operatorname{Aut} \underline{S}_j]$

If $C_{\underline{S}_j}(A') = (0)$ set $A_j^* = A_{j+1}^*$. If $C_{\underline{S}_j}(A') \neq (0)$

set $A_j^* = \ker\left[A_{j+1}^* \longrightarrow \operatorname{Aut} C_{\underline{S}_j}(A')\right]$.

Now either $A_{j+1}^{\circ} > A_j^{\circ}$ or $A_{j+1}^* > A_j^*$. Suppose not. Then by (VII. 10) we get $A_{j+1}^{\circ} = A_j^{\circ}$ and $A_{j+1}^* = A_j^*$. So we must investigate the representation of $A\underline{G}_j$ on $\underline{S}_j$. Suppose first that $C_{\underline{S}_j}(A') \neq (0)$. Then by (VI. 17) applied to $(A, \underline{G}_j, \underline{S}_j)$ there is a $D \leq A$ so that $C_{\underline{S}_j}(A'D) = (0)$ but $C_{\underline{G}_j}(A'D) \geq C_{\underline{G}_j}(A')$. If for some $i > j$, $C_{\underline{S}_i}(A') \neq (0)$ then we may choose $i > j$ minimal so that $C_{\underline{S}_i}(A') \neq (0)$. Fix this i. Then $A_{j+1}^* = A_i^*$ by definition. Now $D \leq A_{j+1}^* = A_i^*$ but $D \not\leq A_j^*$. Therefore, $A_{j+1}^* > A_j^*$. So we may assume that $C_{\underline{S}_i}(A') = (0)$ for all $i > j$. But then $A_{j+1}^* = A_n^* = A \geq D$ and again $A_j^* < A_{j+1}^*$.

Hence we assume that $C_{\underline{S}_j}(A') = (0)$. Now by (VI. 18) applied to $(A, \underline{G}_j, \underline{S}_j)$ we get $1 < D \leq A'$ with $C_{\underline{S}_j}(D) = (0)$ and $C_{\underline{G}_j}(D) = \underline{G}_j$. In particular, $D \not\leq A_j^{\circ}$ but $D \leq A_{j+1}^{\circ}$ so $A_{j+1}^{\circ} > A_j^{\circ}$.

Therefore we get a chain (A_i°, A_i^*) where $A_i^{\circ} < A_{i+1}^{\circ}$ or $A_i^* < A_{i+1}^*$. It is easy to see that the length of this chain is bounded by d where $|A| = p^d$. The length is obviously n. Therefore

$$d \geq n.$$

BIBLIOGRAPHY

1) Bauman, S., "The Klein Group As a Fixed Point Free Automorphism Group," Phd. thesis, University of Illinois, 1962.

2) Curtis, Charles W., and Irving Reiner, *Representation Theory of Finite Groups and Associative Algebras*, New York, c. 1962.

3) Dade, E. C., *Group Theory Seminar 1964 - 1965*, California Institute of Technology, Pasadena, 1966.

4) Gorenstein, D., and I. N. Herstein, "Finite Groups Admitting a Fixed Point Free Automorphism of Order 4," *American Journal of Mathematics*, vol. 83(1961), pp. 71-78.

5) Hall, Marshall, Jr., *The Theory of Groups*, New York, c. 1959.

6) Higman, G., "p-length Theorems," *1960 Institute on Finite Groups*, Providence, 1962, pp. 1-16.

7) Shult, Ernest E., "Nilpotence of the Commutator Subgroup in Groups Admitting Fixed Point Free Operator Groups," *Pacific Journal of Mathematics*, vol. 17(1966), pp. 323-347.

8) Shult, Ernest E., "On Groups Admitting Fixed Point Free Abelian Operator Groups," *Illinois Journal of Mathematics*, vol. 9(1965), pp. 701-720.

9) Thompson, J. G., "Automorphisms of Solvable Groups," *Journal of Algebra*, vol. 1(1964), pp. 259-267.

10) Thompson, J. G., "Finite Groups with Fixed Point Free Automorphisms of Prime Order," *Proceedings of the National Academy of Sciences U. S. A.*, vol. 45 (1959), pp. 578-581.