CLASS TWO p GROUPS AS FIXED POINT FREE AUTOMORPHISM GROUPS

BY

T. R. BERGER[1]

1. Introduction

This paper concerns itself with bounds on the Fitting length of solvable groups G admitting class two odd p groups A as fixed point free automorphism groups. Previous results are listed in the papers of E. Shult [9], [10]. The cases where $A = S_3$ and A is abelian are discussed there.

The main result of this paper is the following theorem.

THEOREM. *Suppose AG is a solvable group with normal subgroup G. Assume A is an odd p group of class ≤ 2; $(|A|, |G|) = 1$; and $C_G(A) = 1$.*

Assume r is a prime and $p^c \neq r^d + 1$ for any $p^c \leq \exp A$ and $r^{2d+1} \mid |G|$. Then the Fitting length of G is bounded above by the power of p dividing $|A|$.

This result is proved by means of a representation theorem (VI. 1). The representation theorem is proved by reduction of a minimal counterexample.

The results of this work are partially contained in the author's doctoral dissertation, written under Professor's M. Hall, Jr and E. C. Dade, at the Californa Institute of Technology.

The main work is done in Section VI. Section II is a statement of results used; Section III an examination of class two groups; Section IV and V examinations of characters of particular groups; and finally, Section VII gives a proof of the main theorem using the lemma of Section VI.

II. Preliminary results

Assume that G is a group, $\mathbf{Q}$ is the rational field, δ is a primitive $|G|^{\text{th}}$ root of unity, and $\mathbf{k} = \mathbf{Q}(\delta)$. Every irreducible representation T of G by linear transformations may be written in $\mathbf{k}$. Suppose χ is the character of G associated with T. Since $\chi = \operatorname{tr} T$ and $\det T$ are invariants the function

$$\phi(\chi) = \det T$$

is well defined. By linearity we may extend ϕ from a function on irreducible characters to a linear function on all characters of G. Then ϕ maps characters of G onto sums of linear characters of G.

(II.1) *Assume that H is a normal subgroup of G and let λ be an irreducible character of H such that*

(1) *λ is G invariant,*

Received February 5, 1968.

[1] This research was partially supported by a National Science Foundation grant.

(2) *$\phi(\lambda)$ extends to a linear character α of G,*
(3) *$\lambda(1)$ and $[G:H]$ are relatively prime.*
Then there exists a unique character χ of G such that
(a) $\chi|_H = \lambda$
(b) $\phi(\chi) = \alpha$

This theorem is proved in [5]. It may also be proved using Schur's lemma and factor sets. The author has given a shorter and more elementary proof than either of these [1].

(II.2) *Suppose G is a group with normal subgroup H. Assume that λ is an irreducible character of H and χ is an irreducible character of G such that $\chi|_H = \lambda$. Then if ψ is any irreducible character of G such that $\psi|_H$ contains λ then*

$$\psi = \mu\chi$$

for an appropriate irreducible character μ on G/H. Further, for any irreducible μ on G/H, $\mu\chi$ is an irreducible character of G.

The proof of this is elementary and may be found in [2, (51.7)].

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

The proof of this is well known. The method is given in [2, (10.8)]. As an immediate corollary we obtain

(II.4) *Suppose that H is a group with normal subgroup N of index n. Assume that U is a completely reducible N module over a field $\mathbf{K}$ of characteristic zero or prime to n. Then $U|^H|_N$ is completely reducible so $U|^H$ is completely reducible.*

(II.5) *Suppose $Y \triangle X \leq G$ are A invariant subgroups of AG where $(|A|, |G|) = 1$. If A fixes the coset xY for $x \in X$ then A fixes an element $xy \in xY$. So $C_{X/Y}(A) = C_X(A)Y/Y$.*

A proof is given in [6].

(II.6) *Suppose $p \mid |G|$, and $G \triangle AG$ where $(|A|, |G|) = 1$. Then A fixes P some p Sylow subgroup of G.*

This result is clear from the Sylow theorems.

(II.7) *If $G \triangle AG$ where $(|A|, |G|) = 1$ and $H \leq C_G(A)$ and $N = N_G(H)$ then*

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

The Three Subgroup lemma applies here. See [4, (3.1)].

We now apply these to obtain some specialized lemmas. In what follows assume we have a group AG with normal subgroup G where $(|A|, |G|) = 1$.

(II.8) *Suppose $M \leq G$ is normal in AG. Assume $\pi \in G$. Then we may choose $\pi' \in \pi M$ so that*

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

Let $A_0 = A \cap (AM)^{\pi}$. Now $\pi M \in C_{G/M}(A_0)$. So we may choose $\pi' \in \pi M$ so that $\pi' \in C_G(A_0)$ by (II.5). Then $C_A(\pi') = A \cap (AM)^{\pi'} = A \cap (AM)^{\pi} = A_0$.

For the remainder of this section suppose $\mathbf{K}$ is a field of characteristic zero or prime to $|A|$. Assume $\mathbf{K}$ is a splitting field for all subgroups of AG.

(II.9) *Suppose that V is a completely reducible $\mathbf{K}[AG]$ module. Assume $M < G$ is normal in AG. Suppose $A_1 \leq A$. Then $V|_{A_1M}$ is completely reducible.*

This is an application of Clifford's theorems and (II.3).

(II.10) *Suppose V is an irreducible $\mathbf{K}[AG]$ module and $V|_{A_0G}$ is not homogeneous for $A_0G \triangle AG$. Assume that A is nilpotent. Then there is subgroup A^* such that $A_0 \leq A^* \triangle A$, $[A : A^*] = n$ is a prime, and*

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

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

We know that A_0G is normal in AG. So by Clifford's theorems $V|_{A_0G}$ is completely reducible. So

$$V|_{A_0G} = V_1 \dotplus \cdots \dotplus V_e$$

where the V_i are homogeneous components. Let $A_1 = \mathrm{Stab}\,(A, V_1)$ the stabilizer in A of V_1. Since $A_0G \triangle AG$, $A_1G = \mathrm{Stab}\,(AG, V_1)$. So V_1 (written $V_1(A_1G)$ when considered as an A_1G module) is an irreducible A_1G module and $V_1(A_1G)|^{AG} \simeq_{AG} V$. But A is nilpotent so there is $A_1 \leq A^* \triangle A$ maximal of prime index n so that $V|_{A^*G} = U_i \dotplus \cdots \dotplus U_n$ where the U_i are irreducible A^*G modules with $U_1 \simeq_{A^*G} V_1(A_1G)|^{A^*G}$ and so $U_1|^{AG} \simeq_A{}^G V$.

Next we prove a result about $\mathbf{K}[A]$ modules.

(II.11) *Suppose $A' \leq A^* \leq A$ and $A_1 \leq A$. Also J is an irreducible $\mathbf{K}[A_1]$ module. Assume*

$$L = \ker\,[A_1 \to \mathrm{Aut}\,J] \geq A_1 \cap A^*.$$

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

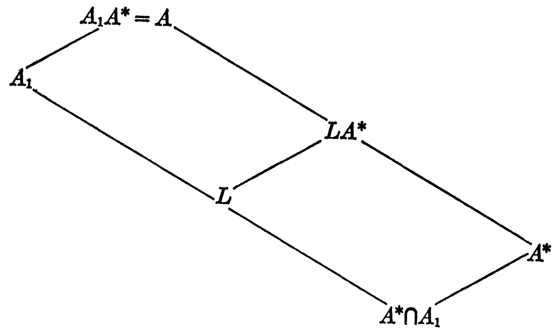
$$\ker\,[A \to \mathrm{Aut}\,I] = LA^*.$$

First suppose $C_{J|^{A_1A^*}}(A^*) = J_0$ has kernel LA^*. Set $J_1 = [A^*, J|^{A_1A^*}]$. Then $J|^{A_1A^*} = J_0 \dotplus J_1$ as a $\mathbf{K}[A_1A^*]$ 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 $J_0|^A$. But

$$J_0|^A|_{LA^*} = \sum_{\pi A_1A^*} \dotplus\, \pi \otimes J_0|_{IA^*}$$

where summation is over cosets in A. Now A^*, $LA^* \triangle A$ so $\pi \otimes J_0 |_{LA^*}$ is both a trivial LA^* and A^* module. Hence $J_0 |^A = I$.

So we may assume that $A_1 A^* = A$ and prove the lemma in that case



Now

$$J |^A |_{LA^*} \simeq_{LA^*} \textstyle\sum_{A_1 \pi LA^*} \dot{+}\ \pi \otimes J |_{A_1^{\pi^{-1}} \cap LA^*} |^{LA^*} \simeq_{LA^*} J |_{A_1 \cap LA^*} |^{LA^*} = J |_L |^{LA^*}$$

since $A_1 LA^* = A$ and $L \leq A_1 \cap LA^* \leq L(A_1 \cap A^*) = L$. But L is trivial on $J |_L$ so

$$J |^A |_{LA^*} \simeq_{LA^*} (\dim J) 1_L |^{LA^*}$$

where 1_L is the trivial L module of dimension 1. Next

$$\dim \mathrm{Hom}_{\mathbf{K}[LA^*]} (1_{LA^*}, 1_L |^{LA^*}) = \dim \mathrm{Hom}_{\mathbf{K}[L]} (1_{LA^*} |_L, 1_L) = 1.$$

So $\dim C_{J|A}(LA^*) = \dim J$. Clearly $C_{J|A}(LA^*)$ is contained in I. But also

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

And

$$J |^A |_{LA^*} |_{A^*} \simeq_{A^*} (\dim J) 1_L |^{LA^*} |_{A^*}.$$

Therefore $\dim I = \dim J = \dim C_{J|A}(LA^*)$. Hence $C_{J|A}(LA^*) = I$. So LA^* is in the kernel of I. Since $A_1/A^* \cap A_1$ is abelian, A_1/L is cyclic and $J |_{A_1}$ is a sum of cyclic faithful A_1/L modules. So the kernel of I is LA^*.

(II.12) *Suppose $A' \leq A^* \leq A$ and $A_1 \leq A$. Assume U is a $\mathbf{K}[A_1 G]$ module and $V \simeq_{AG} U |^{AG}$. Then*

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

If $C_V(A^*) \neq (0)$ then

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

Remark. With $A^* = A$, (i) says $C_U(A_1) = (0)$ if and only if $C_V(A) = (0)$.

For (i) we know that

$$V |_{A^*} \simeq_{A^*} U |^{AG} |_{A^*} \simeq_{A^*} \textstyle\sum_{A^* \pi A_1 G} \dot{+}\ \pi \otimes U |_{(A_1 G^{\pi^{-1}} \cap A^*} |^{A^*}.$$

The π's may be chosen in A. Because $A^* \triangle A$ and $\pi \in A$ we have the modules in the sum conjugate to $U |_{A_1 G \cap A^*} |^{A^*}$. So the centralizer of A^* is the same dimension in each summand. But $A_1 G \cap A^* = A_1 \cap A^*$ so (i) follows immediately.

For (ii) we apply (i) and (II.11).

Remark. (II.12) and the remark following it will be used heavily in section VI, often without mention.

(I.13) *Suppose A is a p group in which every characteristic abelian subgroup is cyclic. Then A is the central product of a cyclic with an extra special group.*

A proof is given in [7].

III. 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, $\mathbf{Q}$ is the rational field, δ is a primitive $|P|^{\text{th}}$ root of unity, and $\mathbf{k} = \mathbf{Q}(\delta)$.

(III.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 $\beta(x) = 0$.

(III.2) THEOREM. *Suppose β is a faithful irreducible character of P. Then*

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

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

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

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

This completes the proof.

(III.3) *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*

$$s(P) \leq (p^{2d} - 1)p/(p - 1).$$

Consider $P/Z(P)$. By (II.2) this group has order p^{2d}. The largest possible number of subgroups of order p in $P/Z(P)$ is then $(p^{2d}-1)/(p-1)$. Let $B/Z(P)$ be cyclic of order p. Then B is abelian of rank two or one. In any case, it contains no more than $(p^2-1)/(p-1) = p+1$ subgroups of order p. One of these must be the subgroup of order p in $Z(P)$. Hence

$$s(P) \leq (p^{2d}-1)p/(p-1).$$

(III.4) THEOREM. *Suppose that p is an odd prime and $r\,(\neq p)$ is a prime. Assume that V is an irreducible $GF(q)[P]$, $q = r^m$, faithful on P. Then there exists a vector $v \in V^{\#}$ which is fixed by no element of $P^{\#}$.*

We proceed by contradiction.

Since $r \neq p$, ordinary character theory holds. So we apply (III.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 $q^{tp^d}-1$ 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.

Suppose A is cyclic of order p and $A \cap Z(P) = 1$. Then by (III.2) we have $\dim C_V(A) = tp^{d-1}$. So the prescribed product is $s(P)[q^{tp^{d-1}}-1]$. In order to have every $v \in V^{\#}$ fixed by some $A \leq P$ we must have

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

Using (III.3) we obtain

$$p(p^{2d}-1)/(p-1) \geq (q^{tp^d}-1)/(q^{tp^{d-1}}-1).$$

A simple computation shows that with p odd we must have $p = 3$, $q = 2$, $d = 1, 2$, and $t = 1$ for the inequality to hold. In particular V is absolutely irreducible. But then $V|_{Z(P)}$ is a multiple of a single one dimensional $Z(P)$ module. Or equivalently, $GF(2)$ contains a primitive $|Z(P)|^{\text{th}}$ root of one. This contradiction proves the theorem.

IV. Extensions of extra special groups

In this section we compute characters of groups which are extensions of normal extra special subgroups. Preliminary results in this direction are in [3, 4 (13.6)].

We reintroduce the field of Section II. Suppose that $\mathbf{Q}$ is the rational field and δ is a primitive $|AR|^{\text{th}}$ root of unity over $\mathbf{Q}$. We let $\mathbf{k} = \mathbf{Q}(\delta)$. In what follows we will be discussing $\mathbf{k}$ characters.

Suppose AR is a group with normal extra special r subgroup R of order r^{2m+1}. Assume that A centralizes $D(R)$ and $(|A|, r) = 1$. Let $\mathbf{K} = GF(r)$ ($\mathbf{K}$ and $\mathbf{k}$ are different fields). Consider the $\mathbf{K}$ 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 $(v_1, v_2) = [x, y] \in D(R)$. We may identify $D(R) = GF(r)^+ = \mathbf{K}^+$. Using this identification $(\cdot, \cdot)$ becomes a nonsingular symplectic pairing on $V = R/D(R)$ into $\mathbf{K}^+$. For $v = xD(R) \in V$, $y \in A$ we set

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

With this conjugation as action V becomes a left $\mathbf{K}[A]$ module. Further, A centralizes $D(R)$ so A fixes the pairing $(\cdot, \cdot)$.

Fix $\alpha : A \to A$ as that unique antiautomorphism of A which sends $x \to x^{-1}$ for all $x \in A$. Then α extends linearly to an antiautomorphism of $\mathbf{K}[A]$.

(IV.1) *Suppose that* $1 = e_1 + \cdots + e_t$ *is a decomposition of* 1 *into primitive central orthogonal idempotents of* $\mathbf{K}[A]$. *Then, except possibly when* $e_i^\alpha = e_j$, *we have*

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

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

$$(e_i v_i, e_j v_2) = (v_1, e_i^\alpha e_j v_2) = 0.$$

The symplectic space V is nonsingular. So if $e_i V \neq (0)$ then $e_i^\alpha V \neq (0)$. By choosing complementary bases we see that $\dim_{\mathbf{K}} e_i V = \dim_{\mathbf{K}} e_i^\alpha V$. Further $e_i V + e_i^\alpha V$ is a nonsingular subspace of V if it is not (0). Let

$$N_{e_i} = \ker [A \to \operatorname{Aut} e_i V].$$

Since $x \in N_{e_i}$ implies $x^{-1} \in N_{e_i}$, we also have $N_{e_i} = N_{e_i}\alpha$. So (IV.1) has the following corollary.

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

(a) $N_{e_i} = N_{e_i}\alpha$,

(b) $\dim_{\mathbf{K}} e_i V = \dim_{\mathbf{K}} e_i^\alpha V$, *and*

(c) $e_i V + e_i^\alpha V$ *is nonsingular or* (0).

Now we decompose the space V. Since $(|A|, r) = 1$, as a $\mathbf{K}[A]$ module, V is completely reducible. That is,

$$V = V_0 \dotplus V'$$

as a $\mathbf{K}[A]$ module where V_0 is irreducible.

(IV.3) *As a* $\mathbf{K}[A]$ *module*

$$V = V_1 \dotplus \cdots \dotplus V_s$$

where

(a) V_i *is nonsingular*

(b) $(V_i, V_j) = (0)\ i \neq j$

(c) (i) *V_i is irreducible or* (ii) $V_i = W_i \dotplus W_i^*$ *as a* $\mathbf{K}[A]$ *module with* W_i, W_i^* *irreducible isotropic subspaces of* V_i.

We prove this by induction on dim V. We examine the decomposition $V = V_0 \dotplus V'$. First, suppose that V_0 is nonsingular. Then set $V_0 = V_1$ and consider $V^* = V_1^{\perp}$. Since V_1 and (,) are A invariant and V_1 is nonsingular we get

$$V = V_1 \dotplus V^*$$

as a $\mathbf{K}[A]$ module and V^* is nonsingular. Second, suppose V_0 is singular. Since (,) and V_0 are A invariant, $V_0^{\perp}$ is $\mathbf{K}[A]$ invariant. So by complete reducibility

$$V = V_0^{\perp} \dotplus W_1$$

as a $\mathbf{K}[A]$ module. Now rad $V_0 \neq (0)$ and is A invariant. Further, V_0 is irreducible so rad $V_0 = V_0$; that is, $V_0 = W_1^*$ is isotropic. In particular, $V_0 \subseteq V_0^{\perp}$.
We see then that

$$V_1 = W_1 \dotplus W_1^*$$

is a $\mathbf{K}[A]$ decomposition. Further, by choosing complementary bases we see that V_1 is nonsingular and W_1, W_1^* are irreducible isotropic subspaces. Setting $V_1^{\perp} = V^*$, as before we get, the $\mathbf{K}[A]$ decomposition

$$V = V_1 \dotplus V^*.$$

Now dim $V^* <$ dim V so induction completes the proof.

Using (IV.3) we set R_i equal to the inverse image in R of V_i. Because V_i is nonsingular we know that R_i is extra special with $D(R_i) = D(R)$.

(IV.4) *R is the central product of the R_i, $i = 1, \cdots, s$.*

Since each $R_i \geq D(R)$, $\prod_i R_i = M \geq D(R)$. Further,

$$M/D(R) = \sum \dotplus V_i = V = R/D(R).$$

Hence $M = R$. Also $Z(R_i) = Z(R) = D(R)$.

Next, if $i \neq j$ then $[R_i, R_j] = 1$. This is immediate since $(V_i, V_j) = (0)$ or equivalently $[R_i, R_j] = 1$.

Therefore, R is the central product of the R_i.

For the following lemma, the construction of the central product is important. Let $R_0 = \prod_i \odot R_i$ be the direct product of the R_i. Also set M equal to the subgroup of all $\prod \odot y_i \in R_0$ such that the product in $R \prod y_i = 1$. This subgroup is normal in R_0 and is in $\prod \odot D(R_i)$. Further, $R \simeq R_0/M$ in a natural way. Since $V = \sum \dotplus V_i$ for $y \in R$, $yD(R) = \sum v_i$ uniquely. Choose $z_i \in v_i$ so that the product in $R \prod z_i = y$. Then setting $\Phi(y) = \prod \odot z_i M$ gives the desired isomorphism. In fact, this is an A isomorphism as is easily verified.

(IV.5) *Suppose that θ_i is an irreducible character of R_i (given in (IV.3)) which is nontrivial on $D(R) = D(R_i)$. Suppose that for every i, $\theta_i|_{D(R)}$ contains the fixed linear character λ of $D(R) = D(R_i)$. Assume that X_i is an irreducible character of AR_i and $X_i|_{R_i} = \theta_i$. Then the direct product character.*

$$\beta = \prod X_i$$

is irreducible on $AR \simeq A^{\Delta}R_0/M$ where A^{Δ} is the diagonal subgroup of $\prod_{i=1}^{s} \odot A$.

It is sufficient to note that $\beta|_{R_0} = \prod \theta_i$ is an irreducible character of R_0 with M in its kernel. Hence, β, considered as a character on AR, is irreducible.

(IV.6) *Suppose that $A_0 = C_A(R)$. Assume also that $C_A(R_i) = H_i$. Further, let β be an irreducible character of AR constructed as in* (IV.5). *Suppose that $(X_i|_A, \gamma)_A > 0$ for every irreducible character γ of A/H_i. Then*

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

for every irreducible character σ of A/A_0.

Since $A_0 = \bigcap H_i$ it is not difficult to see that A/A_0 is isomorphic to a subgroup of $\prod \odot A/H_i$.

Next, let Y_i be the sum of every irreducible character of A/H_i. We prove that if the direct product character $\prod Y_i$ is considered as a character of A^{Δ} then Y_i contains every character of A/A_0.

Now Y_i is a character of A/H_i. Further, A/A_0 is a "subgroup" of $\prod \odot A/H_i$. Suppose μ is any irreducible character of $B = \prod \odot A/H_i$. Then

$$\mu = \prod \mu_i$$

where μ_i is an irreducible character of A/H_i. But $Y_i = \mu_i + \mu_i'$. Hence

$$\prod Y_i = \prod (\mu_i + \mu_i') = (\prod \mu_i) + \mu' = \mu + \mu'.$$

Therefore, $\prod Y_i$ contains every character of B.

Finally, if σ is any irreducible character of A/A_0, a subgroup of B, then there is a character μ on B such that $\mu|_{A/A_0}$ contains σ. But $\prod Y_i$ contains μ so $(\prod Y_i)|_{A/A_0}$ contains σ.

The result is immediate since Y_i is contained in $X_i|_A$ by hypothesis.

Character Values. From (IV.3), (IV.5), and (IV.6) it is evident that, in order to compute the character values on AR, we need only consider the spaces V_i. In other words, we need only consider submodules of V which are faithful on A/H_i.

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

(IV.7) *Suppose A is cyclic and $H_i = C_A(R_i)$. Now $\dim_{\mathbf{K}} V_i = n_i d_i$ where n_i $(=1, 2)$ is the number of $\mathbf{K}[A]$ irreducible submodules of V_i and d_i is the dimension of one of these. Then $r^{n_i d_i/2} \equiv (-1)^{n_i} \pmod{[A:H_i]}$.*

If $[A:H_i] = 1$ the result is trivial. If $[A:H_i] = 2$ then $([A:H_i], r) = 1$ by hypothesis so r is odd and again we are done. So we may assume $[A:H_i] > 2$.

Let $e \in \mathbf{K}[A]$ be a primitive central idempotent such that $eV_i \neq (0)$. For the antiautomorphism α, $e^\alpha V_i \neq (0)$. In particular, (IV.2) says that $\dim eV_i = \dim e^\alpha V_i$. That is, every $\mathbf{K}[A]$ irreducible submodule of V_i has the same dimension since there are at most two. Hence $\dim V_i = n_i d_i$.

Let t be the smallest positive integer such that $r^t \equiv 1 \pmod{[A:H_i]}$. Now $e\mathbf{K}[A]$ is an extension of $\mathbf{K} = GF(r)$ by a primitive $[A:H_i]$ root of unity. Therefore $e\mathbf{K}[A] \simeq GF(r^t)$. In particular,

$$\dim_{\mathbf{K}} e\mathbf{K}[A] = \dim_{\mathbf{K}} GF(r^t) = t = d_i$$

the dimension of an irreducible submodule of V_i.

Suppose $V_i = W_i \dotplus W_i^*$. Then $n_i = 2$ and we get

$$r^{n_i d_i/2} = r^{2t/2} = r^t \equiv 1 = (-1)^2 = (-1)^{n_i} \pmod{[A:H_i]}.$$

So we assume V_i is irreducible. Since V_i is nonsingular, its dimension is even. So $n_i = 1$ and $d_i = t$ is even. By the choice of t we get

$$r^{n_i d_i/2} = r^{t/2} \equiv -1 = (-1)^{n_i} \pmod{[A:H_i]}.$$

This completes the proof.

We now build a character. Fix i. Consider R_i, the inverse image in R of V_i. Suppose $\dim V_i = n_i d_i$ where n_i is the number of irreducible $\mathbf{K}[A]$ submodules in a reduction of V_i and d_i is the dimension of one of these. Assume $H_i = C_A(R_i)$

(IV.8) *Suppose A is cyclic and λ is a nontrivial linear character of $D(R_i)$. Then*

$$\begin{aligned} X_{\lambda i}(x) &= r^{n_i d_i/2}\lambda(z); \qquad x = yz, \quad y \in H_i, \quad z \in D(R_i) \\ &= (-1)^{n_i}\lambda(z); \qquad x \sim yz, \quad yA - H_i, \quad z \in D(R_i) \\ &= 0 \quad \textit{elsewhere} \end{aligned}$$

is an irreducible character of AR_i.

This result is well known [3, 4 (13.6)]. A remark on its proof: Let $n_i = n$, $d_i = d$, $R_i = R$, $H_i = H$, $X_{\lambda i} = X_\lambda$.

$$\begin{aligned} \beta_\lambda(x) &= r^{nd/2}\lambda(x); \qquad x \in D(R) \\ &= 0 \quad \text{elsewhere} \end{aligned}$$

is an irreducible character of R. The character β_λ extends to the direct product $H \odot R$ so that the extended character β_λ^e is trivial on H. Set

$$\begin{aligned} N_\lambda(x) = \beta_\lambda^e|^{AR}(x) &= [A:H]r^{nd/2}\lambda(z); \qquad x = yz, \quad y \in H, \quad z \in D(R) \\ &= 0 \quad \text{elsewhere.} \end{aligned}$$

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

$$\begin{aligned} M_\lambda(x) = \lambda^e|^{AR}(x) &= r^{nd}\lambda(z); \quad x = yz, \quad y \in H, \quad z \in D(R) \\ &= \lambda(z); \quad x \sim yz, \quad y \in A - H, \quad z \in D(R) \\ &= 0 \quad \text{elsewhere.} \end{aligned}$$

By (IV.7), $(1 - (-1)^n r^{nd/2})/[A:H]$ is an integer.
Further

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

From this remark, the proof is straightforward. Further, this way of writing X_λ gives:

(IV.9) *Assume the conditions of* (IV.8). *Suppose* $r^{d_i} + 1 \neq [A:H_i]$. *Then* $X_{\lambda i}|_A$ *contains every character of* A/H_i.

For we get

$$X_\lambda|_A = \left[\frac{r^{n_i d_i/2} - (-1)^{n_i}}{[A:H_i]}\right] \rho_{A/H_i} + (-1)^{n_i} 1_A$$

where ρ_{A/H_i} is the regular character of A/H_i.

We still consider A to be cyclic, but now we want to find a character on all of R rather than just R_i. First we define some numbers.

Definition. Let $x \in A$. By (IV.2) $C_V(x) = C_R(x)/D(R)$ is of even dimension since it is non-singular. Let

$$2m(x) = \dim_{\mathbf{K}} C_V(x).$$

Also let

$$n(x) = \text{number of nontrivial } \mathbf{K}[\langle x\rangle] \text{ irreducible submodules}$$

in a direct decomposition of V.

It is not difficult to see that

$$m(x) = \sum n_i d_i/2$$

where summation is over all i such that x centralizes V_i. And in the same fashion

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

where summation is over all i such that x is nontrivial on V_i. So that (IV.5) applied to AR using the character of (IV.8) gives

(IV.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 above. Then*

$$Y_\lambda(y) = r^{m(x)}(-1)^{n(x)}\lambda(z); \qquad y \sim xz, \qquad x \in A, \qquad z \in D(R)$$
$$= 0 \quad \textit{elsewhere}$$

is an irreducible character of AR.

We may also apply (IV.5), (IV.6), and (IV.9) to prove

(IV.11) *Assume the conditions of* (IV.10). *If $A_0 = C_A(R)$ then $Y_\lambda|_A$ contains every character of A/A_0 provided that $r^{d_i} + 1 \neq [A:H_i]$ for every i.*

The inequality here may be restricted under certain conditions.

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

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

The proof of this is a direct computation.

(IV.13) *Suppose A is a cyclic odd p group. Assume the hypothesis of* (IV.10). *Also assume $A_0 = C_A(R)$. Then $Y_\lambda|_A$ contains every character of A/A_0 except when*

$$[A:A_0] = \sqrt{[R:C_R(A)]} + 1$$

and $R/C_R(A)$ is a faithful irreducible A/A_0 module. In this exceptional case

$$Y_\lambda|_A = \sqrt{[C_R(A):D(R)]}\ (\rho_{A/A_0} - 1_A)$$

Consider the decomposition of (IV.3). Suppose e is that primitive central idempotent of $\mathbf{K}[A]$ yielding $e\mathbf{K}[A]$, the trivial A module. Then for the anti-automorphism α, $e^\alpha = e$. Hence $C_R(A)/D(R) = eV$ is nonsingular. So also is $(1 - e)V = R/C_R(A)$. The decomposition into V_i then splits into V_i nontrivial on A and V_i trivial on A. Let $X_{\lambda i}$ be the character of AR_i given in (IV.8). If $R_i \leq C_R(A)$ then $X_{\lambda i}|_A = h_i 1_A$ is a multiple of 1_A. If $R_i \leq [R, A]$ then $X_{\lambda i}|_A = g_i \rho_{A/A_i} \pm 1_A$ for some g_i by the proof of (IV.9).

Now by the construction in (IV.5) we get

$$Y_\lambda|_A = \prod{}' (g_i \rho_{A/A_i} \pm 1_A)\cdot h1_A$$

where the product is over some i's. But by (IV.12) we see that only one i can appear in the product since p is odd. And for that i,

$$Y_\lambda|_A = (\rho_{A/A_0} - 1_A)h1_A.$$

Hence $[A:A_0] = \sqrt{[R:C_R(A)] + 1}$. For this i we also have

$$r^{n_i d_i/2} + (-1)^{n_i}1_A = [A:A_0].$$

So $n_i = 1$. Finally it is not difficult to see that $h = \sqrt{[C_R(A):D(R)]}$.

This method of proof also gives another conclusion. Recall the map ϕ of section II.

(IV.14) *For ϕ of section*II *and A cyclic we get*

$$\phi(Y_\lambda|_A) = \pm 1_A.$$

If $|A|$ is odd then it is $+1_A$.

In the proof of (IV.13) we did not use the fact that A was an odd p group until we applied (IV.12). So as before we have

$$Y_\lambda|_A = \textstyle\prod'(g_i\rho_{A/A_i} \pm 1_A)\cdot h1_A.$$

This character corresponds to a tensor product of representations. Each representation Λ_i in the product which is not trivial has a character $g_i\rho_{A/A_i} \pm 1_A$. Clearly $\phi(g_i\rho_{A/A_i} \pm 1_A) = \pm 1_A$ where the sign is + if $|A|$ is odd. Since $\det(\Lambda_i \otimes \Lambda_j) = [\det \Lambda_i]^{\deg \Lambda_j}[\det \Lambda_j]^{\deg \Lambda_i}$ we easily see that (IV.14) is true.

(IV.15) THEOREM. *Assume that AR is a group with normal extra special subgroup R of order r^{2m+1} and $(|A|, r) = 1$. Suppose A centralizes $D(R)$. Assume that λ is a nontrivial linear character on $D(R)$. Then there exists a class function*
$\gamma : A \to \{1, -1\}$ *such that*

$$\mathfrak{X}_\lambda(y) = r^{m(x)}(-1)^{n(x)}\gamma(x)\lambda(z); \qquad y \sim xz, x \in A, z \in D(R)$$

$$= 0 \text{ elsewhere}$$

is an irreducible character of AR. Further $\gamma(x) = 1$ whenever $|\langle x\rangle|$ is odd.

Let λ_0 be the irreducible character of R lying over λ. Then λ_0 is fixed by A. By (II.1) we may choose an extension χ of λ_0 on AR such that

(i) $\chi|_R = \lambda_0$
(ii) $\phi(\chi|_A) = 1_A$.

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

Let $x \in A$. By (II.2) and (IV.10)

$$\chi|_{\langle x\rangle R} = Y_\lambda\beta_x$$

for some linear character β_x of $\langle x\rangle R/R$. But $\phi(\chi|_{\langle x\rangle}) = 1 = \phi(Y_\lambda)\phi(\beta_x) = \pm\beta_x$. Hence $\beta_x = \pm 1_{\langle x\rangle}$ and is a character of $\langle x\rangle R/\langle x^2\rangle R$. That is, β_x maps x into $\{1, -1\}$. Further $\beta_x(x) = 1$ if $|\langle x\rangle|$ is odd. Therefore $\chi = \mathfrak{X}_\lambda$ has the values of (IV.15) where $\gamma(x) = \beta_x(x)$.

Remark: 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 $\mathfrak{X}_\lambda|_{\langle x\rangle R}$.

V. Class two extensions

Following (IV.10) we proved (IV.11) and finally (IV.13) which concerned themselves with which characters appear in $Y_\lambda\,|_A$. We now derive an analogous result to follow (IV.15) when A is an odd class two p 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 $\mathbf{K} = GF(r)$ and $\mathbf{k} = \mathbf{Q}(\delta)$ as before. All characters are $\mathbf{k}$ 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 (III.2). Hence, $\dim_{\mathbf{K}} V = tp^d$. 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 $b = 1$,

$$r^{m_1} \equiv 1 \pmod{p}.$$

As an obvious result we have

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

Further, we have

(V.2) *$GF(r^{m_a})$ is the splitting field for P on V where $|\,Z(P)\,| = p^a$.*

The Brauer character of an absolutely irreducible P module over an extension of $GF(r)$ is given by (II.2) and "lifts" values from $GF(r^{m_a})$ 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.

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

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

(V.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 $n(x) \equiv n \pmod 2$ and $m(x) = 0$.*

(c) *If $x \in P$, $\langle x\rangle \cap Z(P) = 1$ and $|\,\langle x\rangle\,| = p^f$ then $n(x) \equiv 0 \pmod 2$ and $m(x) = m/p^f$.*

The $\mathbf{K}$ 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 $\mathbf{K}[\langle x\rangle]$ submodule is faithful of dimension m_f. Hence

$$n(x) = 2m/m_f \equiv t/m_f = m_1 np^{a-c}/m_1 p^{f-c} \equiv n \pmod 2$$

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 (III.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 $\rho - 1$. Let n_0 be the number of irreducible $\mathbf{K}[\langle x\rangle]$ representations in $\rho - 1$. Then $n(x) = (2m/p^f)n_0$. But p is odd so $2m/p^f$ is even and hence

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

This completes the proof of (V.5).

(V.6) (a) $r^{m/p^i} \equiv (-1)^n \pmod{p^{d-i+a}}$, $0 \le i \le d$.

(b) $[r^{m/p^{i-1}} - (-1)^n] - p[r^{m/p^i} - (-1)^n] = s_i\, p^{2(d-i)+2+1} > 0$

for $1 \le i \le d$ *unless* $d = i$, $a = n = 1$, $p = 3$, $m = p^d$ *and* $r = t = 2$.

(c)

$$\begin{aligned} 0 = w_0 < w_1 < \cdots < w_e \\ &= 2d + ar^m + \textstyle\sum_{i=1}^{e} r^{m/p^i}(p^{w_i} - p^{w_{i-1}+1}) + \sum_{i=1}^{e} (-1)^n(p^{w_{i-1}+1} - p^{w_{i-1}}) \\ &\quad - p^{w_e} r^{m/p^e} > 0 \end{aligned}$$

for $e \ge 1$ *unless* $e = 1$, $d = a = n = 1$, $m = p = 3$, *and* $r = t = 2$.

To do this we require (IV.7). We examine the representation of $Z(P)$ on V. Since an irreducible faithful $\mathbf{K}[Z(P)]$ module 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

$$(-1)^n = 1 \equiv (r^{m_a})^{np^d/2p^i} = r^{m/p^i} \pmod{p^{d+a-i}}.$$

Now suppose n is odd. We look at V as a $Z(P)$ module. Here (IV.3) tells us that there must be some V_j irreducible. So for that j, (IV.7) tells us, $n_j = 1$ and $r^{d_j/2} \equiv -1 \pmod{p^a}$. But then $d_j = m_a$ by (V.1). Hence

$$(r^{m_a/2})^{np^d/2p^i} = r^{m/p^i} \equiv (-1)^n = -1 \pmod{p^{d+a-i}}.$$

For (b) we rewrite

$$\begin{aligned} [r^{m/p^{i-1}} - (-1)^n] - p[r^{m/p^i} - (-1)^n] \\ &= r^{m/p^i}(r^{[m(p-1)]/p^i} - p) + (p-1)(-1)^n. \end{aligned}$$

Using (a) we have $r^{m(p-1)/p^i} = hp^{d-i+a} + 1$ for some $h > 0$. Hence our expression becomes

$$r^{m/p^i}(1 + hp^{d-i+a} - p) + (p - 1)(-1)^n.$$

We assume this number is less than or equal to zero. So

$$r^{m/p^i}(1 + hp^{d-i+a} - p) \leq (p - 1)(-1)^{n+1}.$$

But $i \leq d$ so the left hand side is positive and hence $n + 1$ is even. Further, the left hand side is greater than $p - 1$ unless $h = 1$ and $d + a - i = 1$.

Now

$$m(p - 1)/p^i = tp^d(p - 1)/2p^i = t(p - 1)/2p^{a-1}.$$

So $r^{t(p-1)/2p^{a-1}} = 1 + p$. Therefore $r = 2$. But $t = m_1 p^g n$ for some $g \geq 0$ by (V.1). And $r^{m_1} = 1 + fp$ for some $f \geq 0$. But

$$m_1 \leq t(p - 1)/2p^{a-1}$$

so $f = 1$ and

$$m_1 = m_1 p^g n(p - 1)/2p^{a-1}.$$

Therefore $p^g n = p^{a-1}$, and $p = 3$. Hence $m_1 = 2$ and $m_a = 2p^{a-1}$ again by (V.1). So $g = a - 1$ and $n = 1$. Therefore, we have $r = m_1 = m_1 n = t = 2$, $p = 3$. Now $m(p - 1)/p^i = m_1 = 2$ so $m = p^i = tp^d/2 = p^d$. And $d = i$, $a = n = 1$. And we have the exceptional case.

We argue on congruences for the rest of (b). By (a) we have

$$r^{m/p^i} \equiv (-1)^n \pmod{p^{d-i+a}}.$$

Therefore $r^{m/p^i} = (-1)^n + fp^{d+a-i}$. Next

$$\begin{aligned} r^{m/p^{i-1}} &= [(-1)^n + fp^{d+a-i}]^p \\ &= (-1)^n + fp^{d+a-i+1} + \textstyle\sum_{j=2}^{p} \binom{p}{j} (fp^{d+a-i})^j (-1)^{n(p-j)}. \end{aligned}$$

And finally

$$\begin{aligned} &[r^{m/p^{i-1}} - (-1)^n] - p[r^{m/p^i} - (-1)^n] \\ &\qquad = \textstyle\sum_{j=2}^{p} \binom{p}{j} (fp^{d+a-i})^j (-1)^{n(p-j)} \equiv 0 \pmod{p^{2(d-i)+2a+1}}. \end{aligned}$$

From this and the above, (b) follows.

Now consider (c). We rearrange terms.

$$\begin{aligned} &r^m + \textstyle\sum_{i=1}^{e} r^{m/p^i} (p^{w_i} - p^{w_{i-1}+1}) + \sum_{i=1}^{e} (-1)^n (p^{w_{i-1}+1} - p^{w_{i-1}}) - p^{w_e} r^{m/p^e} \\ &\qquad = \textstyle\sum_{i=1}^{e} p^{w_{i-1}}[(r^{m/p^{i-1}} - (-1)^n) - p(r^{m/p^i} - (-1)^n)] \\ &\qquad = \textstyle\sum_{i=1}^{e} p^{w_{i-1}} s_i\, p^{2(d-i)+2a+1}. \end{aligned}$$

Now $s_i = 0$ by (b) only if $d = i$. Hence (c) holds unless $e = 1$ and the exceptions of (b) hold. This completes the proof.

The preceding will help us evaluate inner products of characters. To take the inner products we must know more about the elements of P. Suppose $x \in P$. If $\langle x\rangle \cap Z(P) \neq 1$ then we say x has *central intersection*, otherwise we say x has *noncentral intersection.* Now p is odd and P is class two; so P is a regular p group. Suppose P has exponent p^e. For $i \leq e$, setting $\Omega_i = \langle x \mid x^{p^i} = 1, x \in P\rangle$, we have Ω_i of exponent p^i and; the elements of P of order p^i are exactly the elements in the set $\Omega_i - \Omega_{i-1}$. Suppose $|\Omega_i| = p^{w_i}$ and set $\Omega_0 = 1$, $w_0 = 0$. Then P contains $|\Omega_i - \Omega_{i-1}| = p^{w_i} - p^{w_{i-1}}$ elements of order p^i.

(V.7) *Suppose that P has exponent e. Then for $1 \leq i \leq e$ P contains*
(a) $p^{w_i} - p^{w_{i-1}+1}$ *elements of order p^i with noncentral intersection, and*
(b) $p^{w_{i-1}+1} - p^{w_{i-1}}$ *elements of order p^i with central intersection.*

We have the subgroups Ω_i of P. We want to define a new collection of subgroups Θ_i with

$$\Omega_i \geq \Theta_i \geq \Omega_{i-1}.$$

Further, the elements in $\Omega_i - \Theta_i$ are precisely those of order p^i with noncentral intersection and $\Theta_i - \Omega_{i-1}$ those with central intersection. The order of Θ_i is $p^{w_{i-1}+1}$. Hence (a) follows from $|\Omega_i - \Theta_i| = p^{w_i} - p^{w_{i-1}+1}$ and (b) follows from $|\Theta_i - \Omega_{i-1}| = p^{w_{i-1}+1} - p^{w_{i-1}}$.

Let $Z = \Omega_1 \cap Z(P)$. Then define the map $\theta_i(x) = (xZ)^{p^{i-1}} = \bar{x}^{p^{i-1}}$ for $x \in \Omega_i$. Now θ_i is a homomorphism of Ω_i. For suppose $x, y \in \Omega_i$. Then $[x, y] \in Z(P) \cap \Omega_i$ so $[x, y]^{p^{i-1}} \in Z$. In other words,

$$\theta_i(x)\theta_i(y) = \bar{x}^{p^{i-1}}\bar{y}^{p^{i-1}} = \bar{x}^{p^{i-1}}\bar{y}^{p^{i-1}}[\bar{y}, \bar{x}]^{C(p^{i-1},2)} = (xy)^{p^{i-1}}Z = \theta_i(xy),$$

since p^{i-1} divides the binomial coefficient $C(p^{i-1}, 2)$.

Let $\Theta_i = \ker \theta_i$. Now clearly

$$\Omega_{i-1} \leq \Theta_i \leq \Omega_i.$$

Suppose $x \in \Omega_i - \Omega_{i-1}$. Suppose x has noncentral intersection. Then $x^{p^{i-1}} \notin Z(P)$ hence $\theta_i(x) \neq 1$. Suppose x has central intersection. Then $x^{p^{i-1}} \in Z(P) \cap \Omega_1 = Z$ so $\theta_i(x) = 1$. Hence Θ_i partitions $\Omega_i - \Omega_{i-1}$ as required.

Now we need only compute the order of Θ_i. Consider the map $\psi_i(x) = x^{p^{i-1}}$ of Θ_i. So for $x, y \in \Theta_i$,

$$\psi_i(xy) = xy)^{p^{i-1}} = x^{p^{i-1}}y^{p^{i-1}}[y, x]^{C(p^{i-1},2)} = x^{p^{i-1}}y^{p^{i-1}} = \psi_i(x)\psi_i(y)$$

since $[y, x]^{C(p^{i-1},2)} = [y, x]^{p^{i-1}b} = [y, x^{p^{i-1}}]^b = 1$. Next choose $x \in P$ of order p^e. We may choose x so that $x^{p^{e-1}} \in Z$. For suppose not. Then there is $y \in P$ so that $[x^{p^{e-1}}, y] \neq 1$. So $[x, y] \in Z(P)$ and $[x, y]$ has order p^e. Substituting $[x, y]$ for x we get the desired result, $x^{p^{e-1}} \in Z$. But then $x^{p^{e-i}} \in \Theta_i - \Omega_{i-1}$. So $\psi_i(x^{p^{e-i}}) \neq 1$. And ψ_i is a nontrivial homomorphism of Θ_i with kernel Ω_{i-1} onto Z. Hence $[\Theta_i{:}\Omega_{i-1}] = p$ or $|\Theta_i| = p^{w_{i-1}+1}$. This completes the proof.

In what follows, we retain the notation for Ω_i and Θ_i.

(V.8) *Assume that P is a class ≤ 2 odd p group. Suppose PR is a group with normal extra special r subgroup $R\,(r \neq p)$. Assume that P centralizes $D(R)$. Suppose $P_0 = C_P(R)$. Also $p^c \neq r^d + 1$ for any $r^d \mid r^m$ where $|R| = r^{2m+1}$ and $p^c \leq \exp P = p^e$. Then*

$$(\mathfrak{X}_\lambda |_P, \mu)_P > 0$$

for every character μ of P/P_0 and $(\mathfrak{X}_\lambda |_P, \mu)_P = 0$ for all $\mu \neq 1$ of P such that $\mu |_{P_0} \neq 1$, if $\mathfrak{X}_\lambda$ is the character of PR given in (IV.15).

We proceed by induction on $|P| + |R|$. First, we use (IV.3) to decompose $V = R/D(R)$ into V_i. Then we define R_i as the inverse image in R of V_i. We consider the character $\mathfrak{X}_{\lambda i}$ of PR_i given by (IV.15). Since $|P| + |R_i| < |P| + |R|$ if V decomposes we may apply (IV.5), (IV.6) and induction to obtain the result.

Therefore, V is irreducible or the sum of two irreducible isotropic subspaces, W, W^*. Further $P_0 = C_P(V) = C_P(W) = C_P(W^*)$. From (IV.15) we see that $\mathfrak{X}_\lambda |_{P_0}$ is trivial. So $\mathfrak{X}_\lambda$ is a character of PR/P_0. So applying induction to $|P/P_0| + |R|$ we may assume that $P_0 = 1$.

If P is abelian then P must be cyclic. So (IV.13) gives the conclusion.

So we are reduced to the group described in the second paragraph of this section.

Now we start computing inner products. Consider an irreducible character μ of P. Suppose $\mu(1) > 1$. Then applying (III.2) which gives the values of μ we see that if $P_1 = \ker \mu$ then

$$\begin{aligned} \mu(x) &= p^d \nu(x);\ xP_1 \in Z(P/P_1) \\ &= 0 \text{ otherwise.} \end{aligned}$$

Letting $P_2/P_1 = Z(P/P_1)$ we then get $|P_2| + |R| < |P| + |R|$. So by induction,

$$0 < (p^d/[P : P_2])(\mathfrak{X}_\lambda |_{P_2}, \nu)_{P_2} = (\mathfrak{X}_\lambda |_P, \mu)_P.$$

Therefore we may assume that $\mu(1) = 1$. Next suppose that $\mu^{p^s} \neq 1$, $\mu^{p^{s+1}} = 1$ for $s \geq 0$. Let $P_2 = \ker \mu^{p^s}$. We want to prove that for $s \geq 1$,

$$\textstyle\sum_{x \in P - P_2} \mathfrak{X}_\lambda(x) \mu(x^{-1}) = 0.$$

In that case, $|P_2| + |R| < |P| + |R|$ so

$$0 < (1/p)(\mathfrak{X}_\lambda |_{P_2}, \mu |_{P_2})_{P_2} = (\mathfrak{X}_\lambda |_P, \mu)_P.$$

So if we prove this, we may assume that $\mu^p = 1$.

Let $P_1 = \ker \mu$. Let $x \in P$ so that $\langle x, P_1 \rangle = P$. For any $y \in P_1$, $\langle xy, P_1 \rangle = P$. Hence $|\langle xy \rangle| \geq p^{s+1}$. From (IV.15) it is clear that $\mathfrak{X}_\lambda(xy) = \mathfrak{X}_\lambda([xy]^i)$ for any $(i, p) = 1$.

We now define a map η_i of P_1 onto P_1 which is one-one and given by

$\eta_i(y) = y^*$ where $x^i y^* = (xy)^i$. Suppose $(xy)^i = (xy')^i$. Fix m so that $im \equiv 1 \pmod{p^e}$. Then $xy = (xy)^{im} = (xy')^{im} = xy'$. Therefore $y = y'$. In other words, η_i, $(i, p) = 1$, is one-one onto.

Hence

$$(\alpha) \qquad \sum_{x \in P - P_2} \mathfrak{X}_\lambda(x)\mu(x^{-1}) = \sum_{1 \leq i \leq p^{s+1}, (i,p)=1} \sum_{y \in P_2} \mathfrak{X}_\lambda(x^i y)\mu(x^{-i})$$
$$= \sum_{y \in P_2} \mathfrak{X}_\lambda(xy) \sum_{1 \leq i \leq p^{s+1}, (i,p)=1} \mu(x^{-i}).$$

So if $s \geq 1$ then $\sum_{1 \leq i \leq p^{s+1}, (i,p)=1} \mu(x^{-i}) = 0$.

So finally we assume that $\mu^p = 1$. Suppose $\mu \neq 1$. Then $\sum_{1 \leq i < p} \mu(x^{-i}) = -1$ and (α) gives (since $P_2 = P_1$ here)

$$\sum_{x \in P - P_1} \mathfrak{X}_\lambda(x)\mu(x^{-1}) = -\sum_{y \in P_2} \mathfrak{X}_\lambda(zy) = (-1/(p-1)) \sum_{x \in P - P_1} \mathfrak{X}_\lambda(x)$$

for $z \in P - P_1$. Therefore, with

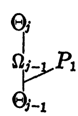
$$A = |P_1|(\mathfrak{X}_\lambda|_{P_1}, 1_{P_1})_{P_1} = \sum_{x \in P_1} \mathfrak{X}_\lambda(x), \quad B = \sum_{x \in P - P_1} \mathfrak{X}_\lambda(x)$$

we get

$$|P|(\mathfrak{X}_\lambda|_P, \mu)_P = A - (1/(p-1))B \quad \text{and} \quad |P|(\mathfrak{X}_\lambda|_P, 1_P)_P = A + B.$$

These are the only two inner products which remain to be shown unequal to zero.

Suppose $P_1 \geq \Theta_{j-1}$ but P_1 is not $\geq \Theta_j$. Then $[\Omega_{j-1}:\Omega_{j-1} \cap P_1] = 1$ or p. First we compute $B = \sum_{x \in P - P_1} \mathfrak{X}_\lambda(x)$. We sum up $\mathfrak{X}_\lambda(x)$ on the sets, $i \geq j$,



$$(\Omega_i - \Theta_i) - (\Omega_i \cap P_1 - \Theta_i \cap P_1) \quad \text{and} \quad (\Theta_i - \Omega_{i-1}) - (\Theta_i \cap P_1 - \Omega_{i-1} \cap P_1)$$

including finally the elements of

$$\Omega_{j-1} - P_1 \cap \Omega_{j-1}.$$

If $|\Omega_i - \Theta_i| = p^{w_i} - p^{w_{i-1}+1}$ then

$$|\Omega_i \cap P_1 - \Theta_i \cap P_1| = p^{w_i - 1} - p^{w_{i-1}}$$

and similarly for the second set since $[P:P_1] = p$. We set $\xi = 0$ if $[\Omega_{j-1}:\Omega_{j-1} \cap P_1] = 1$ and $\xi = 1$ otherwise. So that

$$|\Omega_{j-1} - \Omega_{j-1} \cap P_1| = \xi(p^{w_{j-1}} - p^{w_{j-1}-1}).$$

Now

$$|(\Omega_i - \Theta_i) - (\Omega_i \cap P_1 - \Theta_i \cap P_1)| = ((p-1)/p)(p^{w_i} - p^{w_{i-1}+1})$$

and

$$|(\Theta_i - \Omega_{i-1}) - (\Theta_i \cap P_1 - \Omega_{i-1} \cap P_1)| = ((p-1)/p)(p^{w_{i-1}+1} - p^{w_{i-1}}).$$

And so,

$$\begin{aligned}
B &= \sum_{x\in P-P_1} \mathfrak{X}(x) \\
&= \sum_{i=j}^{e} r^{m/p^i}(p^{w_i} - p^{w_{i-1}+1})((p-1)/p) \\
&\quad + \sum_{i=j}^{e}(-1)^n(p^{w_{i-1}+1} - p^{w_{i-1}})((p-1)/p) + \xi r^{m/p^{j-1}}(p^{w_{j-1}} - p^{w_{j-1}-1}).
\end{aligned}$$

Next we compute $A = \sum_{x\in P_1} \mathfrak{X}_\lambda(x)$. Here the computations are similar.

$$\begin{aligned}
A &= r^m + \sum_{i=1}^{j-2} r^{m/p^i}(p^{w_i} - p^{w_{i-1}+1}) + \sum_{i=1}^{j-1}(-1)^n(p^{w_{i-1}+1} - p^{w_{i-1}}) \\
&\quad + \sum_{i=j}^{e} r^{m/p^i}(p^{w_i} - p^{w_{i-1}+1})(1/p) + \sum_{i=j}^{e}(-1)^n(p^{w_{i-1}+1} - p^{w_{i-1}})(1/p) \\
&\quad + r^{m/p^{j-1}}(p^{w_{j-1}-1} - p^{w_{j-2}+1}) + (1-\xi)r^{m/p^{j-1}}(p^{w_{j-1}} - p^{w_{j-1}-1})
\end{aligned}$$

So we have

$$\begin{aligned}
|P|(\mathfrak{X}_\lambda|_P, \mu)_P &= A - (1/(p-1))B \\
&= r^m + \sum_{i=1}^{j-1} r^{m/p^i}(p^{w_{i-1}+1}) \\
&\quad + \sum_{i=1}^{j-1}(-1)^n(p^{w_{i-1}+1} - p^{w_{i-1}}) - \xi p^{w_{j-1}} r^{m/p^{j-1}}.
\end{aligned}$$

But this is greater than zero by (V.6) c). Finally

$$\begin{aligned}
&|P|(\mathfrak{X}_\lambda|_P\, 1_P)_P \\
&= A + B = r^m + \sum_{i=1}^{e} r^{m/p^i}(p^{w_i} - p^{w_{i-1}}) + \sum_{i=1}^{e}(-1)^n(p^{w_{i-1}+1} - p^{w_{i-1}})
\end{aligned}$$

which again is greater than zero by (V.6) c). This completes the induction.

(V.9) *Assume that P is a class ≤ 2 odd p group. Suppose that PR is a group with normal extra special r subgroup R ($r \ne p$) of order r^{2m+1}. Assume $C_P(R) = 1$ and $C_R(P) \ge D(R)$. Suppose that $p^c \ne r^d + 1$ for $p^c \le \exp P = p^e$ of $d \le m$. Suppose X is an irreducible character of PR nontrivial on $D(R)$. Then*

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

For γ irreducible on P, $(\gamma\bar{\gamma}, 1_P)_P > 0$. By (II.2) and (IV.15) $X = \gamma\mathfrak{X}_\lambda$ for some λ. But by (V.8), $\bar{\gamma}$ is in $\mathfrak{X}_\lambda$. Hence the result.

This theorem gives us the result like (IV.13) for class two odd p groups.

VI. The main lemma

In this section we prove the major result of this paper. For an abelian group a similar result was proven by E. Shult [10, (4.1)].

(VI.1) THEOREM. *Suppose that A is a p group of class ≤ 2 for odd p. Assume that AG is a solvable group with normal subgroup G where $(|A|, |G|) = 1$. Suppose that $|G| = q^m q_0$ ($m \ge 0$) for a prime $q \ne p$ and $(q, q_0) = 1$. Assume $\mathbf{k} = \mathbf{Q}(\delta)$ where $\mathbf{Q} = GF(q)$ or the rational field and δ is a primitive $|A|q_0$ root of unity. Suppose V is a $\mathbf{k}[AG]$ module faithful on G. Assume that*

(i) *V is a sum of equivalent irreducible $\mathbf{k}[AG]$ modules*

(ii) *if $\exp A = p^e$ then $p^d \ne r^c + 1$ for $1 \le d \le e$ and any prime r such that r^{2c+1} divides $|G|$.*

Then

(1) $C_V(A) \neq (0)$ *or*
(2) $C_V(A') = (0)$ *or*
(3) $C_V(A') \neq (0)$ *and there is cyclic* $D \leq A$ *with*
(a) $C_V(A'D) = (0)$
(b) $C_G(A'D) \geq C_G(A')$.

We assume that (VI.1) is false and choose a counter example (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[1]) $C_V(A'D) \neq (0)$ or
(b[1]) $C_G(A'D)$ is not $\geq C_G(A')$.

(VI.2) *V is an irreducible* $\mathbf{k}[AG]$ *module.*

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

(VI.3) *$V|_{A_0G}$ is a multiple of a single irreducible A_0G module for every $A_0 \triangle A$. In particular, $V|_G$ is homogeneous.*

Suppose not. By (II.10) there is $A_0 \leq A_1 \triangle A$ of prime index p so that

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

where the U_i are irreducible $A_1 G$ module and $V \simeq_{AG} U_1|^{AG}$. Let

$$G_i = \ker [G \to \operatorname{Aut} U_i], \qquad \bar{G}_i = G/G_i.$$

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

Now $V|_A \simeq_A U_1|^{AG}|_A \simeq_A U_1|_{A_1}|^A$. So by (II.12),

(1) $$C_{U_1}(A_1) = (0) \quad \text{if and only if} \quad C_V(A) = (0).$$

Also by (II.12) we have, since $A_1 \geq A' \geq A_1'$,

(2) $$(0) \neq C_{U_1}(A_1 \cap A') = C_{U_1}(A') \leq C_{U_1}(A_1').$$

Hence we find

(3) there is $D \leq A_1$ cyclic so that
(a″) $C_{U_1}(A_1' D) = (0)$ and
(b″) $C_{\bar{G}_1}(A_1' D) \geq C_{\bar{G}_1}(A_1')$.

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 $C_{\bar{G}_1}(D) \geq C_{\bar{G}_1}(A_1' D) \geq C_{\bar{G}_1}(A_1') \geq C_{\bar{G}_1}(A')$

so

(b$_1$) $C_{\bar{G}_1}(A'D) \geq C_{\bar{G}_1}(A')$.

By choosing coset representatives of A_1 in A we may prove that

(a$_i$) $C_{V_i}(A'D) = (0)$ and
(b$_i$) $C_{\bar{G}_i}(A'D) \geq C_{\bar{G}_i}(A')$

So finally

(a) $C_V(A'D) = (0)$ and
(b) $C_G(A'D) \geq C_G(A')$ by (II.5).

Therefore, $V|_{A_0G}$ is homogeneous.

(VI.4) *For every* $A_0 < A$ *we have* $C_V(A_0) \neq (0)$.

Suppose $A_0 < A$ and $C_V(A_0) = (0)$. Hence we may choose $A_0 \leq A_1 \triangle A$ and $A_1 < A$ of prime index since A is nilpotent, and $C_V(A_1) = (0)$. Clearly $A_1' \leq A'$. So $C_V(A_1') \geq C_V(A') \neq (0)$. 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

$$(3)\quad \begin{array}{ll} (\text{a}') & C_V(A_1'D) = (0) \quad \text{and} \\ (\text{b}') & C_G(A_1'D) \geq C_G(A_1') \end{array}$$

for cyclic $D \leq A_1$. So

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

or

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

Hence the conclusion.

(VI.5) *A is faithful on V.*

Suppose not. Let $A_0 = \ker [A \to \mathrm{Aut}\, V]$. Since G is faithful and V is an irreducible AG module we must have $[A_0, G] = 1$. Hence (VI.1) applies to $(A/A_0, G, V)$. In the usual way we obtain a contradiction.

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 $\pi_1 M, \cdots, \pi_m M$ form a complete set of A orbit representatives. By (II.8) we may choose π_i, $i = 1, \cdots, m$ so that

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

By taking A conjugates of $\pi_1 = 1, \cdots, \pi_m$ we get a complete set of coset representatives of M in G; $\pi_1 = 1, \cdots, \pi_m, \cdots, \pi_e$ where

$$C_A(\pi_j) = A \cap A^{\pi_j^{-1}} = A \cap (AM)^{\pi_j^{-1}} = A_j, \qquad j = 1, \cdots, e.$$

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, $V|_M = V_1 \dotplus \cdots \dotplus V_f$ 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) *If $f \neq 1$ then $f = e = [G:M]$ and the V_i may be numbered so that A fixes V_1, $\pi_i V_1 = V_i$, and A permutes the V_i exactly as it permutes the 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 is M. Since G/M is abelian, $G \cap \ker \phi$ is the subgroup fixing each V_i. And now $f = e = [G:M]$.

But ϕ is a transitive representation of $A(G/M)$ given on the cosets of a 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 $V_i = \pi_i V_1$ we get the result.

(VI.7) *If $f \neq 1$ then for (A, AM) coset representatives $\pi_1 = 1, \cdots, \pi_m$ we have*

$$V|_A \simeq_A \textstyle\sum_{i=1}^m \dotplus V_1|_{A_i}|^A \quad \textit{and} \quad V \simeq_{AG} V_1(AM)|^{AG}.$$

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

By the Mackey Decomposition we get

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

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 (II.12). So $C_V(A) = (0)$ implies that $C_{V_1}(A_j) = (0)$ for each $j = 1, \cdots, m$. (Hence also for $j = 1, \cdots, e$.)

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

(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 $A_M M \triangle AG$ since $[A_M, G] \leq M$ and $A_M \triangle A$. By (VI.3) $V|_{A_M G}$ is homogeneous and isomorphic to $V_1(A_M M)|^{A_M G}$. Hence $V_1(A_M M)$ is homogeneous. Therefore (VI.1) applies to $(A_M, M/M_1, V_1)$ where

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

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 . Hence by (II.12)

$$C_{V_1|A_j|^A}(A') = (0) \quad \text{for every} \quad j.$$

Thus $C_V(A') = (0)$. So we must have $C_{V_1}(A'_M) \neq (0)$.

This means that when we apply induction to $(A_M, M/M_1, V_1)$ we have a cyclic $D \leq A_M$ so that

$$(3) \quad \begin{array}{ll} (\text{a}'') & C_{V_1}(A'_M D) = (0) \\ (\text{b}'') & C_{M/M_1}(A'_M D) \geq C_{M/M_1}(A'_M). \end{array}$$

Set $M_i = \ker [M \to \operatorname{Aut} V_i]$. Now $A'_M D \leq A_M$ so $A'_M D$ is centralized by each π_i. Hence conjugation of $A'_M D$ by π^{i-1} fixes $A'_M D$ elementwise. Therefore

$$C_{M/M_i}(A'_M D) \geq C_{M/M_i}(A'_M)$$

So by (II.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 each 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) *If A/A_M is abelian then $f = 1$.*

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

(VI.10) *If $A/A_M = \bar{A}$ is non abelian then $f = 1$.*

Now G/M is an r group for some r. But $\bar{A}$ is a class two p group which is faithful and irreducible on the $GF(r)$ module G/M. So we apply (III.4) to get a $\pi_i M$ which is fixed by no element of $\bar{A}^{\#}$. In other words, $C_{\bar{A}}(\pi_i) = 1$, or $C_A(\pi_i) = A_i = A_M$. So again the remark and (VI.8) show $f = 1$.

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

Now G/M is an r section for some prime r. So by (II.6) we may choose an

r Sylow subgroup R_0 of G fixed by A. Next choose R in R_0 minimal such that

(i) R is A invariant, and
(ii) $RM = G$.

We will prove that R is extra special.

Next consider $V|_{AM} = V_1 \dotplus \cdots \dotplus V_t$ where the V_i are homogeneous components. Since $V|_M$ is homogeneous, each V_i is faithful and a multiple of a single 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 $C_{V_i}(A) = (0)$, $i = t, \cdots, t$. 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) *If A is abelian then $C_A(M) = A^* \neq 1$.*

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) a cyclic $D_1 \leq A'D$ so that

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

Also since

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

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

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

Suppose $A^* \cap A_M = A_0 \neq 1$. Now $A_0 \triangle A$ so we may take

$$A_1 = Z(A) \cap A_0 \neq 1$$

since A is nilpotent. We know that A^* centralizes M and A_M centralizes G/M. Hence by (II.5), 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 $A^*A_M/A_M \triangle A/A_M$ so

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

(VI.14) *We can choose R so that $R \leq C_G(M)$, R is extra special, and $R \,\triangle\, AG$. Further, $D(R) \leq M, D(R) \leq C_G(AG)$.*

Now $G = N_G(M)$. But $M = C_G(A^*)$ so by (II.7) $G = C_G(M)C_G(A^*) = C_G(M)M$. The group $C_G(M)$ is A invariant so R may be chosen in $C_G(M)$.

Let $R_1 = Z(R)$. We know $R_1 \leq C_G(M)$ 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 $R_1 \leq C_G(AG)$. In particular, R is nonabelian.

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_0 be any characteristic abelian subgroup of R. Now $R/D(R) \simeq_A G/M$ so if $R_0 < R$ then $R_0 \leq D(R)$. But R is nonabelian so $R_0 \leq D(R)$. But then $R_0 \leq M$. We already know that $R_0 \leq C_G(M) \cap M = Z(M)$ and $V|_M$ is homogeneous. So

$$R_0 \leq Z(R) = R_1$$

and R_0 is cyclic. By (II.13) R is the central product of a cyclic and extra special group. But by 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) *$V|_R$ is homogeneous*; $C_V(A_M) = (0)$.

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 $\mathbf{k}[AR]$ submodule of V. Let $V_0 \leq C_V(A_M)$ be an irreducible $\mathbf{k}[AR]$ submodule. Since

$$Z(R) = D(R) \leq Z(AG)$$

it acts as scalar multiplication nontrivially on V hence also on V_0. Further, on V_0, A is represented as A/A_M. Now $A_M < A$ since $C_V(A) = (0)$. Therefore V_0 is a $\mathbf{k}[(A/A_M)R]$ irreducible module. Also A/A_M is faithful and irreducible on $R/D(R)$. Now $|R| = r^{2c+1}$ divides $|G|$. 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 (V.9) to the Brauer character of V_0 to find that $(0) \neq C_{V_0}(A) \leq C_V(A)$. But $C_V(A) = (0)$. Hence $C_V(A_M) = (0)$.

(VI.16) (VI.1) *holds.*

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 hypothesis on k.

(VI.17) COROLLARY. *In* (VI.1) *we may assume that* $\mathbf{k}$ *is any subfield of* $\mathbf{Q}(\delta)$. *In particular, we may take*

$$\mathbf{k} = GF(q).$$

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

$$V \simeq_{\mathbf{K}[AG]} U^* \dotplus \cdots \dotplus U^* \quad (m \quad \text{summands})$$

It is clear that

$$C_V(L) \simeq_{\mathbf{K}[AG]} C_{U^*}(L) \dotplus \cdots \dotplus C_{U^*}(L) \quad (m \quad \text{summands})$$

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) $C_G(D) = G$.

Here $V|_{A'G} = V_1 \dotplus \cdots \dotplus V_t$ where the V_i are (in the case of (VI.1)) homogeneous components. Let $G_i = \ker[G \to \operatorname{Aut} V_i]$. Then we apply (VI.1) to $(A', G/G_1, V_1)$. 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′) $C_{G/G_1}(D) = G/G_1$.

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

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

(b) $C_G(D) = G$.

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

VII. The main theorem

Let A be a class ≤ 2 odd p group. Suppose AG is a group with normal subgroup G where $(|A|, |G|) = 1$. We define a function $\psi(G)$. Now

$$[A:C_A C_G(A')][A':C_A(G) \cap A'] = p^f$$

for some f. Set

$$\psi(G) = f.$$

Notice that $C_A C_G(A') \geq A'$ so $\psi(G) = f \leq d$ where $|A| = p^d$.

(VII.1) THEOREM. *We assume that A is an odd p group of class ≤ 2. Further, AG is solvable with normal subgroup G where* $(|A|, |G|) = 1$. *Suppose G has fitting length n and A is fixed point free on G* (i.e. $C_G(A) = 1$). *Then*

$$\psi(G) \geq n$$

unless $p^b = r^c + 1$ where r^{2c+1} divides $|G|$ and $p^b \leq \exp A$.

Proof is by induction on a minimal counter example G. First, G has a unique minimal normal A invariant subgroup M. Suppose not. Assume M_1, M_2 are minimal normal A subgroups of G. Let $G_i = G/M_i$, $i = 1, 2$. Clearly $\psi(G_i) \leq \psi(G)$. Let

$$\psi_0 = \max\{\psi(G_i) | i = 1, 2\}.$$

Then by induction the Fitting lengths of G_1 and G_2 are bounded by ψ_0. So also the Fitting length of G, which is contained in $G_1 \times G_2$, is bounded by $\psi_0 \leq \psi(G)$.

Second, for some prime q, $0_q(G) = M$. Suppose not. Now M is a q group so we consider $Q = 0_q(G)$. Let $Q_0 = D(Q)$. Then G/Q_0 has the same Fitting length n as does G. But $\psi(G/Q_0) \leq \psi(G)$ and induction applies.

Finally we prove the result. Since $M = 0_q(G)$ is unique minimal normal A invariant, $C_G(M) = M$. And as an AG/M module, M is faithful on G/M and irreducible on AG/M. Applying (VI.17), (VI.18) we find that

(2) $C_M(A') = 1$ and there is cyclic $D \leq A'$ with
 (a′) $C_M(D) = 1$ and
 (b′) $C_{G/M}(D) = G/M$

or

(3) $C_M(A') \neq 1$ and there is cyclic $D \leq A$ with
 (a) $C_M(A'D) = 1$ and
 (b) $C_{G/M}(A'D) = C_{G/M}(A')$.

In either case, $\psi(G/M) \leq \psi(G) - 1$. But the Fitting subgroup of G is M so the Fitting of G/M is $n - 1$. So $n - 1 \leq \psi(G/M) \leq \psi(G) - 1$ by induction. Or $n \leq \psi(G)$.

(VII.2) *Under the hypotheses of* (VII.1), *if $|A| = p^d$ then $n \leq d$.*

Added in proof. (II.13) is stated only for odd p. The application is made for arbitrary p. The application is correct for the strong form of (II.13) given in D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968, p. 198.

REFERENCES

1. T. R. BERGER, *Class two p groups as fixed point free automorphism groups*, Ph.D. thesis, California Institute of Technology, 1967.

2. C. W. CURTIS AND I. REINER, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.
3. E. C. DADE, Group theory seminar 1964–1965, lecture notes, California Institute of Technology.
4. W. FEIT AND J. G. THOMPSON, *Solvability of groups of odd order*, Pacific J. Math., vol. 13 (1963), pp. 775–1029.
5. P. X. GALLAGHER, *Group characters and normal Hall subgroups*, Nagoya Math. J., vol. 21 (1962), pp. 223–230.
6. G. GLAUBERMAN, *Fixed points in groups with operator groups*, Math. Zeitschrift, vol. 84 (1964), pp. 120–125.
7. D. GORENSTEIN, *On a theorem of Philip Hall*, Pacific J. Math., vol. 19 (1966), pp. 77–80.
8. M. HALL, JR., *Group theory*, Macmillan, New York, 1959.
9. E. SHULT, *Nilpotence of the commutator subgroup in groups admitting fixed point free operator groups*, Pacific J. Math., vol. 17 (1966), pp. 323–347.
10. ———, *On groups admitting fixed point free abelian operator groups*, Illinois J. Math., vol. 9 (1965), pp. 701–720.

UNIVERSITY OF MINNESOTA
MINNEAPOLIS, MINNESOTA