TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 155, Number 1, March 1971

UNDER THE DEGREE OF SOME FINITE LINEAR GROUPS

BY
HARVEY I. BLAU[1]

Abstract. Let G be a finite group with a cyclic Sylow p-subgroup P for some prime $p \geqq 13$. Assume that G is not of type $L_2(p)$, and that G has a faithful indecomposable modular representation of degree $d \leqq p$. This paper offers several improvements of the known bound $d \geqq (7p)/10 - 1/2$. In particular, $d \geqq 3(p-1)/4$. Other bounds are given relative to the order of the center of G and the index of the centralizer of P in its normalizer.

1. **Introduction.** A finite group is of *type* $L_2(p)$ if each of its composition factors is either a p-group, a p'-group or isomorphic to $PSL(2, p)$. Feit [5] proved

THEOREM 1. *Let G be a finite group with a cyclic S_p-subgroup P for some prime p. Assume that G is not of type $L_2(p)$. Suppose that there is a faithful indecomposable KG-module L of dimension $d \leqq p$, where K is a field of characteristic p. Then $p \neq 2$, $|P| = p$, $L|_P$ is indecomposable, and $\mathscr{C}_G(P) = P \times \mathscr{Z}(G)$. Furthermore $d \geqq 2(p-1)/3$ and $d \geqq (7p)/10 - \frac{1}{2}$ in case $p \geqq 13$.*

If $p < 13$, all relevant groups with faithful indecomposable KG-modules of dimension less than $p-2$ are known, including the Janko group of degree 7 where $p = 11$ [11]. The question of whether there exist any groups satisfying Theorem 1 with $p \geqq 13$ and $d < p-2$ remains open. Should any occur, they would lead to new simple groups.

This paper offers several improvements of the lower bound $(7p)/10 - \frac{1}{2}$ for the dimension of L when $p \geqq 13$. We easily show $d \geqq 3(p-1)/4$ (Theorem 5.7). If $d = 3(p-1)/4$ then L is self-dual, $|\mathscr{Z}(G)| = 2$, and $|\mathscr{N}_G(P) : \mathscr{C}_G(P)| = (p-1)/2$ (Theorem 6.4). Other theorems relate d to $|\mathscr{Z}(G)| = z$ and $|\mathscr{N}_G(P) : \mathscr{C}_G(P)| = e = (p-1)/t$. In particular, if e is even and z odd then d is either odd or equal to $p-1$ (Theorem 5.12). $d \geqq p - (e/2 + 1)$ if e is even, and $d \geqq p - ((e-1)/2 + t)$ if e is odd (Theorem 7.1). This last result serves to improve an inequality due to Brauer [3] for groups with a complex representation of degree less than $p-1$. (See the remarks in §7.)

Received by the editors May 18, 1970.

AMS 1969 *subject classifications*. Primary 2025, 2080; Secondary 2075.

Key words and phrases. Indecomposable modular representation, small degree, cyclic Sylow p-subgroup, symmetric decomposition, skew decomposition, irreducible complex representation.

[1] Most of the results in this paper were part of the author's doctoral dissertation, written under the direction of Walter Feit and submitted to Yale University. This research was partially supported by the Army Research Office (Durham).

The methods of [5] are exploited, beginning with a generalized local theory in §2. The result in §3 on symmetric and skew decomposition is used in several proofs in the sequel. A theorem of Feit on invariants and the Green correspondence is combined with the structure theory of a block with cyclic defect group in §4, providing some useful information. The main results are established in §§5, 6, 7. Finally, a table is given for the *possible* values of d when $13 \leqq p \leqq 31$.

G denotes a finite group, K a field, P a S_p-subgroup of G, $N=\mathcal{N}_G(P)$ and $C=\mathcal{C}_G(P)$. If M and W are KG-modules, $M+W$ means their direct sum and M^* is the dual of M. Further notation and terminology are either standard or explained en route.

2. **Local theory.** A mild generalization of results of Thompson [14] and Feit [5] is presented. The proofs in these sources for the prototypes of Lemmas 2.1–2.6 below carry over virtually unchanged, so we omit those proofs here.

In this section, P is a cyclic group of order $q=p^n$ for some fixed prime p, and $P \triangleleft PH$ where H is an abelian p'-group. Let K be a field of characteristic p which is a splitting field for H, so that the $|H|$ irreducible (linear) characters of H are afforded by K-representations. Let char $H=\{\lambda_i\}$ be the set of all such characters.

LEMMA 2.1. *For each integer s with $1 \leqq s \leqq q$ and each $\lambda \in \text{char } H$, there is an indecomposable KPH-module $V_s(\lambda)$ such that $\dim_K V_s(\lambda)=s$, $V_s(\lambda)|_P$ is indecomposable, and if U is the unique submodule of $V_s(\lambda)$ with $\dim U=1$, then $uh=\lambda(h)u$ for all $u \in U$, $h \in H$. Every indecomposable KPH-module is isomorphic to some $V_s(\lambda)$; $V_s(\lambda) \approx V_t(\mu)$ if and only if $s=t$ and $\lambda=\mu$; $V_s(\lambda)$ is projective if and only if $s=q$. Furthermore for each $1 \leqq i \leqq s$, each $V_s(\lambda)$ has a unique submodule U_i with $\dim U_i=i$; $U_i \approx V_i(\lambda)$.*

Let α be the linear character: $H \to K$ given by

$$h^{-1}yh = y^{\alpha(h)}, \quad \text{all } y \in P,\ h \in H.$$

Then $\alpha(H) \subseteq F-\{0\}$, where F is the prime subfield of K. In the sequel, $V_s(\lambda)$ is defined as in Lemma 2.1. Set $V_0(\lambda)=0$ for all $\lambda \in \text{char } H$. If $H=\langle 1 \rangle$, set $V_s(\lambda)=V_s$. If $h \in H$, $\det_s(\lambda)(h)$ means the determinant of h acting as a linear transformation on $V_s(\lambda)$.

LEMMA 2.2. *Let $V_i(\lambda) \approx U_i \subseteq V_s(\lambda)$ for $0 \leqq i \leqq s$. Then $V_s(\lambda)/U_i \approx V_{s-i}(\lambda\alpha^{-i})$.*

As a corollary there is

LEMMA 2.3. $V_s(\lambda)^* \approx V_s(\lambda^{-1}\alpha^{s-1})$ *and* $\det_s(\lambda)(h)=\lambda^s\alpha^{-s(s-1)/2}(h)$ *for all* $h \in H$.

LEMMA 2.4. *Assume $|P|=p$. If $1 \leqq s \leqq t$ and $s+t \leqq p$, then*

$$V_s(\lambda) \otimes V_t(\mu) \approx \sum_{i=0}^{s-1} V_{s+t-1-2i}(\lambda\mu\alpha^{-i}).$$

LEMMA 2.5. *Assume $|P|=p$. $V_s(\lambda) \otimes V_p(\mu) \approx \sum_{i=0}^{s-1} V_p(\lambda\mu\alpha^{-i})$ for $1 \leqq s \leqq p$.*

LEMMA 2.6. *Assume* $|P|=p$. *If* $1\leqq b\leqq c$ *and* $b+c\leqq p$, *then*

$$V_{p-b}(\beta)\otimes V_c(\gamma)\approx\sum_{i=0}^{b-1}V_{p-b-c+1+2i}(\beta\gamma\alpha^{-c+1+i})+\sum_{j=0}^{c-b-1}V_p(\beta\gamma\alpha^{-j}).$$

The following lemma is proved with a technique due to Green [10] and employed by Feit in [5].

LEMMA 2.7. *If* $M\approx V_q(\pi)+V_t(\tau)$, $V_s(\sigma)\approx S\subseteq M$ *and* $M/S\approx V_r(\rho)$ *where* $t, r, s<q$, *then* $\sigma=\pi$ *and* $\rho=\tau=\pi\alpha^{r-1}$.

Proof. First observe that in any direct sum $V_j(\mu)+V_i(\lambda)$, the elements fixed by P form a space of K-dimension two. Hence any submodule is a direct sum of at most two indecomposable summands. Since $s+r=q+t$ where $r<q$, then $s>t$. Thus, $S\cap V_q(\pi)\neq\{0\}$, hence S and $V_q(\pi)$ share a one-dimensional KPH-module, so $\sigma=\pi$. Also $S\cap V_1(\tau)=\{0\}$ implies the image of $V_1(\tau)$ is nonzero in M/S, hence $\rho=\tau$. Observe

$$(2.8)\qquad \begin{aligned} &V_q(\rho\alpha^{1-r})/V_{q-r}(\rho\alpha^{1-r})\approx V_r(\rho)\quad\text{and}\\ &(V_q(\pi)+V_q(\tau\alpha^{1-t}))/X\approx V_q(\pi)+V_t(\tau),\quad\text{where } X\approx V_{q-t}(\tau\alpha^{1-t}).\end{aligned}$$

Hence there exists W with $(V_q(\pi)+V_q(\tau\alpha^{1-t}))\supseteq W\supseteq X$, $W/X\approx S$ and

$$(2.9)\qquad (V_q(\pi)+V_q(\tau\alpha^{1-t}))/W\approx V_r(\rho).$$

Combining (2.8) and (2.9) with Schanuel's theorem [10, (1.6e)] gives

$$(2.10)\qquad W+V_q(\rho\alpha^{1-r})\approx V_{q-r}(\rho\alpha^{1-r})+V_q(\pi)+V_q(\tau\alpha^{1-t}).$$

Thus W has a projective summand and W, X satisfy hypotheses similar to those on M, S so $V_q(\tau\alpha^{1-t})\subseteq W$. Then by (2.10) and the Krull-Schmidt theorem, $V_q(\rho\alpha^{1-r})\approx V_q(\pi)$. Hence $\rho=\pi\alpha^{r-1}$.

DEFINITION. If $U\approx V_1(\lambda)$ is an irreducible constituent of a KPH-module M, then we say that λ is an *H-value* of M. This is equivalent to $\lambda(h)$ being an eigenvalue of h acting on M, for all $h\in H$. λ is a *main H-value* (mv) if there is $x\neq 0$ in M with $xh=\lambda(h)x$ and $xy=x$ for all $h\in H$, $y\in P$.

The H-values of $V_s(\lambda)$ are $\lambda, \lambda\alpha^{-1},\ldots,\lambda\alpha^{-s+1}$ by Lemma 2.2, and the unique mv of $V_s(\lambda)$ is λ. Considering the set of elements fixed by P immediately gives

PROPOSITION 2.11. *Let* $M=\sum_{i=1}^n V_{d_i}(\lambda_i)$ *where* $1\leqq d_i\leqq q$ *and* $\lambda_i\in\operatorname{char} H$ *for* $1\leqq i\leqq n$. *The H-values of M are* $\bigcup_{i=1}^n\{\lambda_i,\lambda_i\alpha^{-1},\ldots,\lambda_i\alpha^{-d_i+1}\}$ *and the mv's are the* λ_i.

The H-values of $V_{d_i}(\lambda_i)$ are called *projective H-values* (pv) (resp. *nonprojective H-values* (npv)), and λ_i is *projective main value* (pmv) (resp. *nonprojective main value* (npmv)) if $d_i=q$ (resp. $d_i<q$). Of course, a given λ may be both a pv and a npv of M.

3. **Symmetric and skew decomposition.** If K is a field of characteristic not equal to two, and L a KG-module with $\dim_K L=d$, then $L\otimes L=A+B$, where A is the

subspace of symmetric tensors and B the subspace of skew-symmetric tensors. A and B are KG-modules with $\dim_K A=d(d+1)/2$ and $\dim_K B=d(d-1)/2$. For any subgroup H of G, $A|_H$ and $B|_H$ are the symmetric, resp. skew, summands of $L|_H \otimes L|_H$. If $\{x_i\}$ is a K-base for L, then

$$(3.1)\qquad A = \langle x_i \otimes x_j + x_j \otimes x_i\rangle, \qquad B = \langle x_i \otimes x_j - x_j \otimes x_i\rangle.$$

Suppose $\{x_i\}$ consists of eigenvectors with respective eigenvalues ε_i for some $g \in G$. Then by (3.1), the eigenvalues of g on A consist exactly of $\{\varepsilon_i^2\}$ plus the eigenvalues of g on B.

For the rest of this section, let field K and group PH satisfy the hypotheses of §2, with $|P|=p$. Then for any integer d with $p/2<d<p$, and $s=p-d$, Lemma 2.6 says, for any $\lambda \in \text{char } H$,

$$(3.2)\qquad V_d(\lambda) \otimes V_d(\lambda) \approx \sum_{i=0}^{s-1} V_{2i+1}(\lambda^2\alpha^{s+i}) + \sum_{i=s}^{p-1-s} V_p(\lambda^2\alpha^{s+i}).$$

LEMMA 3.3. *Let $s=p-d$, where $p/2<d<p$. Let $A+B$ be the decomposition of $V_d(\lambda) \otimes V_d(\lambda)$ into symmetric and skew parts. Then A is the direct sum of exactly those summands in* (3.2) (*projective and nonprojective*) *with $i \equiv s$* (mod 2). *B is the direct sum of the summands in* (3.2) *with $i \equiv s-1$* (mod 2).

Proof. By the Krull-Schmidt theorem, the summands of (3.2) are distributed between A and B. The remarks above and Lemma 2.2 show that

$$(3.4)\qquad (H\text{-values of } A) = \{\lambda^2, (\lambda\alpha^{-1})^2, \ldots, (\lambda\alpha^{-d+1})^2\} \cup (H\text{-values of } B).$$

Assume first that PH is a Frobenius group with Frobenius kernel P (so that α is faithful on H and char $H=\langle\alpha\rangle$), and that $|H|=p-1$. Since $|H|$ is even, it makes sense to distinguish between even and odd powers of α. Since $d>p/2$, $\{\lambda^2, (\lambda\alpha^{-1})^2, \ldots, (\lambda\alpha^{-d+1})^2\}$ covers each even power at least once, and $|H|=p-1$ implies

$$(3.5)\qquad \{\lambda^2\alpha^{s\pm i} \mid 0 \leqq i \leqq s-1\} \cap \{\lambda^2\alpha^{s+i} \mid s \leqq i \leqq p-s-1\} = \varnothing.$$

The two sets given in (3.5) are the H-values of the nonprojective summands and the mv's of the projective summands, respectively. Each $\gamma \in \text{char } H$ is an H-value of $V_p(\pi)$ twice if $\gamma=\pi$, but exactly once if $\gamma \neq \pi$.

Of the $p-2s$ projective summands, suppose more lie in B than in A. Then each of $\lambda^2\alpha^{s+i}$, $s \leqq i \leqq p-s-1$, occurs more times in B than in A as an H-value which is not a mv, and the majority of them occur additionally in B as pmv's. (3.5) shows they are *not* balanced by nonprojective H-values, and this contradicts (3.4). So more projective summands lie in A than in B.

Now $\lambda^2\alpha^{2s-1}$ is an H-value of only $V_{2s-1}(\lambda^2\alpha^{2s-1})$ among the nonprojective summands, and is a non-mv just once for each $V_p(\lambda^2\alpha^{s+i})$, $s \leqq i \leqq p-s-1$. So if $V_{2s-1}(\lambda^2\alpha^{2s-1}) \subseteq A$, (3.4) implies there is one more projective summand in B than in A in order that the odd powers of α balance as H-values, a contradiction. Hence,

$V_{2s-1}(\lambda^2\alpha^{2s-1})\subseteq B$. To balance $\lambda^2\alpha^{2s-1}$, there is exactly *one* more projective summand in A.

Similarly, $\lambda^2\alpha^{2s-2}$ is an H-value of only $V_{2s-1}(\lambda^2\alpha^{2s-1})$, $V_{2s-3}(\lambda^2\alpha^{2s-2})$ and each projective. $V_{2s-1}(\lambda^2\alpha^{2s-1})$ with the projectives leaves $\lambda^2\alpha^{2s-2}$ balanced between A and B. This is an even power of α, so (3.4) implies $V_{2s-3}(\lambda^2\alpha^{2s-2})\subseteq A$.

Consider $V_{2j+1}(\lambda^2\alpha^{s+j})$ for $0\leqq j<s-2$, and suppose for all $j<k\leqq s-1$,

$$\begin{aligned} V_{2k+1}(\lambda^2\alpha^{s+k}) &\subseteq B \quad \text{if } k\equiv s-1 \pmod 2,\\ &\subseteq A \quad \text{if } k\equiv s \pmod 2. \end{aligned}$$

$\lambda^2\alpha^{s+j}$ is an H-value of only $V_{2j+1}(\lambda^2\alpha^{s+j})$, $V_{2k+1}(\lambda^2\alpha^{s+k})$ for each $k>j$, and of each projective. If $j\equiv s-1 \pmod 2$ then our inductive assumption implies the $V_{2k+1}(\lambda^2\alpha^{s+k})$ and the projectives give an extra $\lambda^2\alpha^{s+j}$ as an H-value to A. So (3.4) implies $V_{2j+1}(\lambda^2\alpha^{s+j})\subseteq B$. If $j\equiv s \pmod 2$, our assumption says that the $V_{2k+1}(\lambda^2\alpha^{s+k})$ and the projectives distribute $\lambda^2\alpha^{s+j}$ evenly between A and B. Hence, $V_{2j+1}(\lambda^2\alpha^{s+j})\subseteq A$. Induction downwards shows

$$(3.6)\qquad \begin{aligned} A &= \sum_{0\leqq i\leqq s-1;\, i\equiv s \pmod 2} V_{2i+1}(\lambda^2\alpha^{s+i})+(p-2s+1)/2 \text{ projectives},\\ B &= \sum_{0\leqq i\leqq s-1;\, i\equiv s-1 \pmod 2} V_{2i+1}(\lambda^2\alpha^{s+i})+(p-2s-1)/2 \text{ projectives}. \end{aligned}$$

For any group P of odd prime order p, the Frobenius group PH as above may be constructed. By restriction to P, our results imply that if $V_d\otimes V_d=A'+B'$, decomposition into symmetric and skew parts, then

$$(3.7)\qquad \begin{aligned} A' &= \sum_{0\leqq i\leqq s-1;\, i\equiv s \pmod 2} V_{2i+1}+((p-2s+1)/2)V_p,\\ B' &= \sum_{0\leqq i\leqq s-1;\, i\equiv s-1 \pmod 2} V_{2i+1}+((p-2s-1)/2)V_p. \end{aligned}$$

Now make no special assumption about PH. $V_d(\lambda)\otimes V_d(\lambda)$ contains a unique indecomposable summand of dimension $2i+1$, for each i with $0\leqq i\leqq s-1$. So restricting to P and applying (3.7) shows that (3.6) remains true. Finally, it now follows that the projective summands distribute between A and B as in the statement of this lemma in order that (3.4) be satisfied.

In the same way (and with less trouble), one obtains the following results: If $2s\leqq p$, then Lemma 2.4 says $V_s(\lambda)\otimes V_s(\lambda)\approx\sum_{i=0}^{s-1} V_{2i+1}(\lambda^2\alpha^{1-s+i})$.

LEMMA 3.8. *Let $2s\leqq p\neq 2$. Let $A+B$ be the decomposition of $V_s(\lambda)\otimes V_s(\lambda)$ into symmetric and skew parts. Then A is the direct sum of the $V_{2i+1}(\lambda^2\alpha^{1-s+i})$ with $i\equiv s-1 \pmod 2$, $0\leqq i\leqq s-1$; B is the direct sum of the $V_{2i+1}(\lambda^2\alpha^{1-s+i})$ with $i\equiv s \pmod 2$, $0\leqq i\leqq s-2$.*

4. **Blocks and the Green correspondence.** Here is a special case of the Green correspondence (see Thompson [14]): Let K be a field of characteristic p and G a

finite group with a S_p-subgroup P which is a T.I. set. There is a one-to-one correspondence between all nonprojective indecomposable KG-modules X, and all nonprojective indecomposable KN-modules V: $X \leftrightarrow V$ if and only if V is the unique nonprojective indecomposable summand of $X|_N$, or equivalently, X is the unique nonprojective summand of V^G. If $X \leftrightarrow V$, then $X^* \leftrightarrow V^*$.

A nonzero element x of a KG-module is called an *invariant* if $xg = x$, all $g \in G$.

THEOREM 4.1 (FEIT). *If $X \leftrightarrow V$ as above, then X has invariants if and only if V has invariants.*

Proof. Let Q_0 be the projective indecomposable KG-module whose socle is the trivial one-dimensional KG-module. Q_0 is, of course, a direct summand of KG with socle $K(\sum_{g\in G} g)$. If X contains a nonzero element of the form $\sum_{g\in G} yg$ for some $y \in X$, then the map f: $KG \to X$ defined by $f(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g yg$, where $a_g \in K$, induces a KG-isomorphism of Q_0 into X, a contradiction. Thus, $N_{G,\langle 1\rangle}(X) = 0$, so that $H^0(G, \langle 1\rangle, X) = \mathrm{Inv}_G(X)$ (see [7, II.3]). Similarly, $H^0(N, \langle 1\rangle, V) = \mathrm{Inv}_N(V)$. Since $H^0(G, \langle 1\rangle, X) \approx H^0(N, \langle 1\rangle, V)$ [7, III.5.9], the theorem follows.

Now let $|P| = p$, let $\mathcal{O}$ be the ring of integers in a p-adic number field k, $\mathcal{P}$ the maximal ideal of $\mathcal{O}$, $K = \mathcal{O}/\mathcal{P}$, and assume all irreducible kG and KG modules are absolutely irreducible. B will denote a p-block of defect 1.

Each block B is associated with a tree (see Brauer [1], Dade [4], Rothschild [13]). Say that the graph of B has e edges, corresponding to irreducible modular characters (and to their corresponding projective indecomposables), and hence $e+1$ vertices, corresponding to p-conjugate families of ordinary irreducible characters. In only one family, said to lie on the *exceptional* vertex, is there more than one character (there are $(p-1)/e$). If $e = p-1$, we pick the "exceptional" vertex arbitrarily.

DEFINITION. If M is an irreducible KG-module in B, the *remainder* of M (rem M) is the unique integer m with $1 \leq m < p$ and $\dim_K M \equiv m \pmod p$. The *separation* of M (sep M) is the number of vertices the edge M separates from the exceptional. (If $e = p-1$, sep M depends on our choice of the exceptional vertex.)

An argument of Rothschild shows there is an integer $r \not\equiv 0 \pmod p$ with

$$r(\text{sep } M) \equiv \pm \text{rem } M \pmod p \tag{4.2}$$

where the result alternates along paths to the exceptional. As a consequence, all remainders in B are congruent (mod p) to elements of

$$\{r, 2r, \ldots, er\} \cup \{-er, -(e-1)r, \ldots, -r\}.$$

Results of Brauer [2, I] give

$$\text{If } N/P \text{ is abelian, then } e = |N:C| \text{ and } r = 1. \tag{4.3}$$

The correspondence $L \to L^*$, where L is an irreducible kG- or KG-module, gives an incidence preserving map of the tree for B to the tree for a block B'. If B contains an ordinary or modular irreducible which is isomorphic to its dual (Brauer

[1, Theorem 13] shows that the latter implies the former), then the map sends B to itself. The same theorem of Brauer implies that those modular (resp. ordinary) irreducibles equal to their duals lie on the edges (resp. vertices) of a single *real stem* across which the map $L \to L^*$ reflects the tree. The exceptional vertex in such a block, if $e<p-1$, must also lie on the stem. (This discussion is given by Tuan [15] in the case of the principal block.)

For the rest of §4, assume $N=PH$ where H is an abelian p'-group. Then (4.3) and §§2, 3 apply. λ is called an H-value of a KG-module L if and only if it is an H-value of $L|_N$.

PROPOSITION 4.4. *For any $\lambda \in \operatorname{char} H$, there is at most one irreducible KG-module X such that $X \leftrightarrow V_t(\lambda)$ by the Green correspondence for some positive integer $t<p$.*

Proof. Suppose X and Y are distinct irreducibles with $X \leftrightarrow V_t(\lambda)$ and $Y \leftrightarrow V_s(\lambda)$ $\operatorname{Hom}_{KG}(X, Y)=0=\operatorname{Hom}_{KG}(Y, X)$, so by Theorem 4.1, there are no invariants in the nonprojective summands of $V_t(\lambda)^* \otimes V_s(\lambda)$ or of

$$V_s(\lambda)^* \otimes V_t(\lambda) = V_s(\lambda^{-1}\alpha^{s-1}) \otimes V_t(\lambda).$$

Without loss, assume $s \leqq t$. If $s+t \leqq p$,

$$V_s(\lambda^{-1}\alpha^{s-1}) \otimes V_t(\lambda) \approx \sum_{i=0}^{s-1} V_{s+t-1-2i}(\lambda^{-1}\alpha^{s-1}\lambda\alpha^{-i}) = \sum_{i=0}^{s-1} V_{s+t-1-2i}(\alpha^{s-1-i}),$$

by Lemma 2.4. But one of the npmv's is $\alpha^0=1$, a contradiction. If $s+t>p$, let $t=p-b$. Then $b<s$ and

$$V_s(\lambda^{-1}\alpha^{s-1}) \otimes V_{p-b}(\lambda) \approx \sum_{i=0}^{b-1} V_{p-b-s+1+2i}(\lambda^{-1}\alpha^{s-1}\lambda\alpha^{1-s+i}) + (\text{projectives})$$

by Lemma 2.6, and α^0 is a npmv, a contradiction.

The following result is proven by Feit (not yet published) in a more general setting.

PROPOSITION 4.5. *Let M, W and R be nonprojective indecomposable KG-modules with $M \leftrightarrow V_m(\mu)$, $W \leftrightarrow V_w(\gamma)$, $R \leftrightarrow V_r(\rho)$, $M \subseteq W$ and $W/M \approx R$. Then*

(a) *$m+r<p$ implies $m+r=w$ and $\rho=\mu\alpha^{-m}$, $\gamma=\mu$;*

(b) *$m+r>p$ implies $m+r=p+w$ and $\rho=\gamma=\mu\alpha^{r-1}$.*

Furthermore, if one of R or M is irreducible, then it is uniquely determined by the other and one of conditions (a) *or* (b).

Proof. Treat the problem locally. All projective summands of $M|_N$ appear in $W|_N$, and in addition so do those of $R|_N$. Factor out the former, split off the latter, and hence assume $M|_N=V_m(\mu)$, $R|_N=V_r(\rho)$, so $\dim_K W=m+r$. If $m+r<p$, then $W|_N=V_w(\gamma)+$no projectives, with $m+r=w$. $V_{m+r}(\gamma)/V_m(\mu) \approx V_r(\rho)$ implies $\gamma=\mu$ and $\rho=\mu\alpha^{-m}$ by Lemma 2.2. If $m+r>p$, then $W|_N=V_w(\gamma)+V_p(\pi)$, and we apply Lemma 2.7 to obtain $\pi=\mu$ and $\rho=\gamma=\mu\alpha^{r-1}$.

Suppose R is irreducible. If $m+r<p$, then $\rho=\mu\alpha^{-m}$, which depends only on M, and which by Proposition 4.4 determines R. If $m+r>p$, let $R=S^*$, so that where $S\leftrightarrow V_r(\sigma)$, $V_r(\rho)=V_r(\sigma)^*=V_r(\sigma^{-1}\alpha^{r-1})$ by Lemma 2.3. Then $\sigma^{-1}\alpha^{r-1}=\mu\alpha^{r-1}$, so $\sigma=\mu^{-1}$, and by Proposition 4.4 again, S (hence $R\approx S^*$) is determined by M. If M is irreducible, consider the dual $W^*\supseteq R^*$ and $W^*/R^*\approx M^*$.

PROPOSITION 4.6. *The npmv's of the indecomposable KG-modules in a single block B of defect* 1 *all lie in a single coset of* char $(H/\mathscr{C}_H(P))$ *in* char H.

Proof. Let U be the unique maximal submodule of an arbitrary projective indecomposable KG-module Q in B. There is a chain of submodules $W=W_0\subseteq W_1\subseteq\cdots\subseteq W_n=U$ such that W is the unique minimal submodule of U, hence all the W_i are indecomposable, and the W_i/W_{i-1}, $0\leqq i\leqq n$, include all the distinct irreducible constituents of Q. Let W_i/W_{i-1} have npmv λ_i and W_i have npmv γ_i. By Proposition 4.5, γ_i is either γ_{i-1} or λ_i, and $\lambda_i=\gamma_{i-1}\alpha^{j_i}$ for some integer j_i. Since $\alpha|_{\mathscr{C}_H(P)}=1$, the λ_i are all in a single coset of char $(H/\mathscr{C}_H(P))$. Since projective indecomposables on adjacent edges of the tree have irreducible constituents in common, the proposition is true for all the modular irreducibles in B.

Let $X\leftrightarrow V_s(\sigma)$, $0<s<p$, be any indecomposable KG-module in B. Let M be a maximal submodule of X. By induction on the dimension of X, we may assume that the npmv's of M and of the irreducible constituents of M are in the same coset of char $(H/\mathscr{C}_H(P))$. We may also assume that σ is not a npmv of M, $M|_N=\sum_i V_{m_i}(\mu_i)$ where each $m_i<p$, and dim $X/M<p$. Now $\sigma\neq\mu_i$ for any i implies $V_i(\sigma)\cap M|_N=\langle 0\rangle$. Thus $V_s(\sigma)\subseteq(X/M)|_N$, so that σ is the npmv of irreducible X/M. The proposition follows.

The following result is partially contained in [2].

COROLLARY 4.7. *There is one block of defect* 1 *for each coset of* char $(H/\mathscr{C}_H(P))$ *as in Proposition* 4.6, *and for each* $\lambda\in$ char H *there is exactly one irreducible KG-module L with npmv* λ.

Proof. This follows from the fact that there are $|\mathscr{C}_H(P)|$ blocks of full defect (since H is abelian), Proposition 4.6 and (4.3).

PROPOSITION 4.8. *Every modular irreducible in a block B of defect* 1 *may be written in the prime subfield F of K if and only if one of them may be so written.*

Proof. Let L be a modular irreducible in B with $L\leftrightarrow V_t(\lambda)$. L may be written in F if and only if $L^T=L$ for all automorphisms T of K if and only if $V_t(\lambda)^T=V_t(\lambda)$ if and only if $\lambda^T=\lambda$ for all $T\in$ Aut (K). Since $\alpha(H)\subseteq F$, $\lambda^T=\lambda$ if and only if $(\lambda\alpha^i)^T=\lambda\alpha^i$ for all integers i. Apply Proposition 4.6.

REMARKS. (1) Tuan's result [15] that every modular irreducible in B_0, the principal block, can be written in F, follows immediately. (2) If $|H|\,|\,p-1$, then $\lambda(H)\subseteq F$ for all $\lambda\in$ char H and in this case *all* modular irreducibles in blocks of defect 1 are written in F.

PROPOSITION 4.9. *If $\mathscr{C}_H(P)$ is cyclic, there are at most two blocks containing a real stem.*

Proof. If B has a real stem, then B contains a modular irreducible $L \leftrightarrow V_d(\lambda)$ and its dual $L^* \leftrightarrow V_d(\lambda^{-1}\alpha^{d-1})$. $\lambda^{-1}\alpha^{d-1}=\lambda\alpha^k$ for some integer k by Proposition 4.6. Thus $\lambda^2|_{\mathscr{C}_H(P)}=1$. But if $\mathscr{C}_H(P)$ is cyclic then $\lambda^2|_{\mathscr{C}_H(P)}=1$ if and only if λ is in one of at most two fixed cosets of char $(H/\mathscr{C}_H(P))$ in char H. Apply Corollary 4.7.

REMARK. One of these blocks will be B_0, the principal block. Denote the other, if it exists, by B_2. B_2 may have a real stem consisting of a single vertex only.

The local theory easily yields the well-known

PROPOSITION 4.10. *If L is a nonprojective indecomposable KG-module and $T \in \text{Aut } K$, then $(L^T)^* \approx (L^*)^T$.*

Proof. Say $L \leftrightarrow V_d(\lambda)$. Then

$$(L^T)^* \leftrightarrow V_d(\lambda^T)^* = V_d((\lambda^T)^{-1}\alpha^{d-1}) = V_d((\lambda^{-1}\alpha^{d-1})^T) \leftrightarrow (L^*)^T.$$

§4 is concluded with a proposition of a general nature. The easy proof is omitted.

PROPOSITION 4.11. *Let L be an indecomposable but not irreducible KG-module with $L\approx L^*$ and socle $L=W_1+W_2+\cdots+W_t$. Then socle $L\subseteq$radical L and W_1^*, $W_2^*,\ldots, W_t^*$ are the constituents of $L/\text{rad } L$.*

5. **Lower bounds.** We assume for the rest of this paper that group G and module L satisfy the hypotheses of Theorem 1 with $p\geqq 13$ and $\dim_K L=d<p$. Let $T=\bigcap_n G^{(n)}$, the intersection of the derived groups. Since G is not of type $L_2(p)$, T and $L|_T$ also satisfy Theorem 1. Thus with no loss we assume $G=G'$.

If X is a KG-module such that $X|_P$ is indecomposable, either X is the trivial one-dimensional module or $\dim X\geqq(7/10)p-\frac{1}{2}$. $N=PH$, where H is an abelian p'-group, so §2 applies: $L|_N=V_d(\lambda)$ for some $\lambda\in\text{char }(H)$.

We use the following notation:

$s=p-d$;

$e=|N:C|=(p-1)/t$;

$Z=\mathscr{Z}(G)$ and $z=|Z|$.

If X is an indecomposable KG-module, write $X=X(u,\gamma)$ if and only if $X\leftrightarrow V_u(\gamma)$ by the Green correspondence.

1_0=the trivial one-dimensional KG-module.

PROPOSITION 5.1. *Z is cyclic and $z|d$.*

Proof. If $y\in Z$, y acts on L as the $d\times d$ scalar matrix $(\lambda(y))$. Thus L faithful implies λ is faithful on Z. Then $\lambda(Z)\subseteq K$ implies Z is cyclic. Det $(\lambda(y))=\lambda^d(y)=1$ since $G=G'$. Hence $z|d$.

Let $M=M(d,\gamma)$ be another (not necessarily distinct) KG-module with $\dim M = \dim L$ (in the sequel, M is usually L or L^*). $M|_N=V_d(\gamma)$, so Lemma 2.6 implies

$$(5.2)\qquad (L\otimes M)|_N = \sum_{i=0}^{s-1} V_{2i+1}(\lambda\gamma\alpha^{s+i})+\sum_{i=s}^{p-s-1} V_p(\lambda\gamma\alpha^{s+i}).$$

Then by the Green correspondence, $L\otimes M=\sum_{i=0}^{s-1} L(2i+1,\lambda\gamma\alpha^{s+i})+Q$, where Q is projective. By (5.2), for each integer i with $0\leqq i\leqq s-1$, we may choose a set of integers $\mathscr{S}_i$ such that $\mathscr{S}_i\cap\mathscr{S}_k=\varnothing$ if $i\neq k$, $\bigcup_{i=0}^{s-1}\mathscr{S}_i$ is contained in the set of integers j such that $s\leqq j\leqq p-s-1$, and

$$L(2i+1,\lambda\gamma\alpha^{s+i})|_N = V_{2i+1}(\lambda\gamma\alpha^{s+i})+\sum_{j\in\mathscr{S}_i} V_p(\lambda\gamma\alpha^{s+j}).$$

Let $m_i=|\mathscr{S}_i|$. Of course, $\mathscr{S}_i$ and m_i are also functions of λ, γ, and s. We have

$$(5.3)\qquad \dim L(2i+1,\lambda\gamma\alpha^{s+i}) = 2i+1+m_ip,\quad\text{and}\quad \sum_{i=0}^{s-1} m_i\leqq p-2s.$$

$m_i>0$ for $1\leqq i\leqq s-1$, since $2i+1<(7/10)p-\frac{1}{2}$, and $m_0=0$ if and only if $\lambda\gamma\alpha^s=\alpha^0$ if and only if $\gamma=\lambda^{-1}\alpha^{-s}$, which says $M\approx L^*$.

Using Lemma 2.3 and the assumption $G=G'$, we have, for $0\leqq i\leqq s-1$,

$$(5.4)\qquad \begin{aligned} 1 &= \det L(2i+1,\lambda\gamma\alpha^{s+i})\quad\text{on } H\\ &= (\lambda\gamma\alpha^s)^{2i+1}\prod_{j\in\mathscr{S}_i}(\lambda\gamma\alpha^s)^p\alpha^j\alpha^{-(p-1)/2}\\ &= (\lambda\gamma\alpha^s)^{2i+1+m_ip}\alpha^{-m_i(p-1)/2}\prod_{j\in\mathscr{S}_i}\alpha^j. \end{aligned}$$

Now $L(2i+1,\lambda\gamma\alpha^{s+i})\approx L(2i+1,\lambda\gamma\alpha^{s+i})^*$ if and only if $(\lambda\gamma\alpha^{s+i})^2=\alpha^{2i}$ (by Lemma 2.3) if and only if $(\lambda\gamma\alpha^s)^2=1$. Thus either none or all of the nonprojective indecomposable summands of $L\otimes M$ are self-dual.

LEMMA 5.5. *Suppose the nonprojective indecomposable summands of $L\otimes M$ are self-dual. The number of summands $L(2i+1,\lambda\gamma\alpha^{s+i})$ of* $\dim 2i+1+m_ip$ *with m_i odd is less than or equal to*

$t-1$ *if t is even,*
t *if t is odd,*
$t-2$ *if t is odd but $s>e/2$.*

Proof. If $V_p(\mu)$ is a summand of $L(2i+1,\lambda\gamma\alpha^{s+i})|_N$, so is $V_p(\mu)^*=V_p(\mu^{-1})$. $\mu=\lambda\gamma\alpha^{s+j}$ implies $\mu^{-1}=\lambda\gamma\alpha^{s-j}$. Then for any i with $0\leqq i\leqq s-1$, (5.4) implies

$$(5.6)\qquad 1 = (\lambda\gamma\alpha^s)^{2i+1+m_ip}\alpha^{-m_i(p-1)/2}\prod_{j\in\mathscr{S}_i;\,2j\equiv 0\ (\mathrm{mod}\ e)}\alpha^j.$$

If m_i is odd, then $2i+1+m_ip$ even gives $(\lambda\gamma\alpha^s)^{2i+1+m_ip}=1$, so that

$$\alpha^{m_i(p-1)/2} = \alpha^{(p-1)/2} = \prod_{j\in\mathcal{S}_i;\, 2j\equiv 0 \pmod e} \alpha^j.$$

There is an odd number of such j. If t is even, then $(p-1)/2\equiv 0 \pmod e$ and there is an odd number of $j\equiv 0 \pmod e$ in $\mathcal{S}_i$. If t is odd, then $(p-1)/2\equiv e/2 \pmod e$, and there is an odd number of $j\equiv e/2 \pmod e$ in $\mathcal{S}_i$. (5.2) establishes the lemma.

THEOREM 5.7. $d\geqq \max\{p-e, 3(p-1)/4\}$.

Proof. If d is taken to be minimal, L may be assumed absolutely irreducible. $d<p$ implies L is in a block of defect 1. Theorem 1 says $d\geqq(7/10)p-\frac{1}{2}$, so by (4.3), $d\geqq p-e$. If $e\leqq(p-1)/4$ then $d\geqq(3p+1)/4$. If $e=(p-1)/3$ and $s\leqq e/2$ then $d\geqq(5p+1)/6$. So we may assume $t\leqq 3$ and if $t=3$ then $s>e/2$.

Let $M=L^*$. Then $\gamma=\lambda^{-1}\alpha^{-s}$, so $\lambda\gamma\alpha^s=1$. Lemma 5.5 implies at most one m_i is odd. By (5.3),

$$1+2(s-2) \leqq \sum_{i=1}^{s-1} m_i \leqq p-2s,$$

whence $s\leqq(p+3)/4$.

PROPOSITION 5.8. *If z is odd then either $d>p-e$ or $e=2$.*

Proof. By Theorem 5.7 we may assume $d=p-e$ and L is absolutely irreducible. $e<p-1$ implies $\operatorname{sep} L=e$, so that L lifts to an ordinary irreducible which is exceptional. Then a theorem of Feit [6] gives $e=2$.

Now let $M=L$. (5.4) gives, for $0\leqq i\leqq s-1$,

$$1 = (\lambda^2\alpha^s)^{2i+1+m_ip}\alpha^{m_i(p-1)/2}\prod_{j\in\mathcal{S}_i}\alpha^j. \tag{5.9}$$

Since α is trivial on Z, $(\lambda^2)^{2i+1+m_ip}|_Z=1$. Since L is faithful, λ is faithful on Z, so that

$$z\,|\,2(2i+1+m_ip), \qquad 0\leqq i\leqq s-1. \tag{5.10}$$

The next theorem shows that d is bounded below at least as a function of the order of Z.

THEOREM 5.11. *If $b|z$ with b an odd integer, set $s=bq+r$, q and r integers with $0\leqq r<b$. Then*

$$s \leqq (2/(b+5))(p+r(b-r)/2).$$

If $4c|z$, set $s=cw+u$, c, w, and u integers with $0\leqq u<c$. Then all the m_i (from $L\otimes L$) are odd and

$$s \leqq (1/(c+2))(p+u(c-u)).$$

Proof. If odd $b|z$, then (5.10) implies $b|2i+1+m_ip$, $0\leqq i\leqq s-1$, so for any $0\leqq i$, $j\leqq s-1$, $b|2(i-j)+p(m_i-m_j)$. Hence if $|i-j|<b$, $b\nmid i-j$ so $b\nmid m_i-m_j$. In particular $m_i\neq m_j$. Thus

$$\sum_{b \text{ consecutive integers } i} m_i \geqq \sum_{j=1}^{b} j = b(b+1)/2,$$

$$p-2s \geqq \sum_{i=0}^{s-1} m_i \geqq qb(b+1)/2+r(r+1)/2$$
$$= (s-r)(b+1)/2+r(r+1)/2.$$

Solving for s proves the first statement.

If $4c|z$, then $2c|2i+1+m_ip$, $0\leqq i\leqq s-1$, by (5.10), so each m_i is odd. $2c|2(i-j)+p(m_i-m_j)$ for $0\leqq i,j\leqq s-1$. So if $|i-j|<c$, $c\nmid m_i-m_j$ and

$$\sum_{c \text{ consecutive integers } i} m_i \geqq \sum_{j=1}^{c} 2j-1 = c^2,$$

$$p-2s \geqq \sum_{i=0}^{s-1} m_i \geqq wc^2+u^2 = (s-u)c+u^2.$$

Solve for s to complete the proof.

If $e=|\text{char }(H/Z)|=|\langle\alpha\rangle|$ is even, then we may sensibly speak of the parity of an element of $\langle\alpha\rangle$ as an odd or even power of α.

THEOREM 5.12. *Assume e is even. If either* (i) *z is odd and d is even, or* (ii) $z=2$ *and λ^2 is even, then $d=p-1$ and $p\equiv 1$* (mod 4). *If $z=4$, then $d>(4p)/5$.*

Proof. Lemma 3.3 implies that if $j\in\mathscr{S}_i$ for $M=L$ in (5.2), then $j\equiv i$ (mod 2). If $(p-1)/2$ is even and i is odd, then $\alpha^{m_i(p-1)/2}$ is even and $\prod_{j\in\mathscr{S}_i}\alpha^j$ has the same parity as m_i. If $(p-1)/2$ is odd and i is even, then $\prod_{j\in\mathscr{S}_i}\alpha^j$ is even and $\alpha^{m_i(p-1)/2}$ has the same parity as m_i. Thus if $(p-1)/2\equiv i+1$ (mod 2), $\alpha^{m_i(p-1)/2}\prod_{j\in\mathscr{S}_i}\alpha^j$ has the same parity as m_i. Furthermore, d is even under any of the hypotheses, so $\alpha^{s(2i+1+m_ip)}$ has opposite parity from m_i. Then (5.9) implies $(\lambda^2)^{2i+1+m_ip}$ is odd for all $0\leqq i\leqq s-1$ with $i\equiv(p+1)/2$ (mod 2).

$\lambda^z\in\langle\alpha\rangle$. By (5.10), $(\lambda^2)^{2i+1+m_ip}$ is *even* for *all* $0\leqq i\leqq s-1$ if either (i) or (ii) hold. Then in this event, $(p-1)/2$ is even and $s=1$. The first statement is proved.

Suppose $4|z$. Then all m_i are odd, $0\leqq i\leqq s-1$. If $i\equiv(p-1)/2$ (mod 2), then $\alpha^{s(2i+1+m_ip)}\alpha^{m_i(p-1)/2}\prod_{j\in\mathscr{S}_i}\alpha^j$ is even, and hence so is $(\lambda^2)^{2i+1+m_ip}$ by (5.9). Assume $d<p-1$. Then $(\lambda^2)^{2i+1+m_ip}$ is odd for some $i\leqq s-1$. (5.10) implies λ^z is odd. It follows that, for $0\leqq i\leqq s-1$,

$$2(2i+1+m_ip)/z \equiv i+(p-1)/2 \pmod 2.$$

If $z=4$, $2(2i+1+m_ip)/z=(2i+1+m_i+m_i(p-1))/2=(m_i+1)/2+i+m_i(p-1)/2\equiv(m_i+1)/2+i+(p-1)/2$ (mod 2). Thus $m_i\equiv 3$ (mod 4), $0\leqq i\leqq s-1$. Then by (5.3), $3s\leqq\sum_{i=0}^{s-1}m_i\leqq p-2s$. This proves the second statement.

Remark 5.13. The nonprojective summands of $L \otimes L$ are self-dual if and only if $(\lambda^2\alpha^s)^2=1$. This implies $z|4$.

Theorem 5.14. *If* $z=4$ *and* $(\lambda^2\alpha^s)^2=1$ *then*

$$d \geqq p-1 \text{ and } p \equiv 1 \pmod 4 \quad \text{if } e \text{ is even,}$$
$$\geqq p-t+1 \quad \text{if } e \text{ is odd.}$$

Proof. All the m_i (from $L \otimes L$), $0 \leqq i \leqq s-1$, are odd by Theorem 5.11. Then Lemma 5.5 implies $d \geqq p-t+1$ if e is odd. The proof of Lemma 5.5 shows that for all $0 \leqq i \leqq s-1$, there is some $j \equiv (p-1)/2 \pmod e$ in $\mathscr{S}_i$. If $j \in \mathscr{S}_i$ then $j \equiv i \pmod 2$ by Lemma 3.3. If e is even, then $(p-1)/2 \equiv i \pmod 2$ for all $0 \leqq i \leqq s-1$. Hence $s=1$ and $(p-1)/2$ is even.

Lemma 5.15. *Suppose* $L \approx L^*$ *and* $M=M(d,\gamma) \approx M^* \not\approx L$ *are in the same p-block with* dim $M=d$. *Then*

$$s \leqq t-1 \quad \text{if } t \text{ is even,}$$
$$\leqq t \quad \text{if } t \text{ is odd,}$$
$$\leqq t-2 \quad \text{if } t \text{ is odd and } s > e/2.$$

Proof. $\gamma^2=\lambda^2=\alpha^{d-1}$, and by Proposition 4.6, $\gamma\lambda^{-1} \in \langle\alpha\rangle$. Hence $\gamma=\lambda\alpha^{e/2}$ and $\lambda\gamma\alpha^s=\alpha^{e/2}$. Thus the nonprojective summands of $L \otimes M$ are self-dual, and (5.6) implies, for all $0 \leqq i \leqq s-1$,

$$(5.16)\quad \begin{aligned} 1 &= (\alpha^{e/2})^{2i+1+m_ip}\alpha^{m_i(p-1)/2} \prod_{j\in\mathscr{S}_i;\,2j\equiv 0 \pmod e} \alpha^j \\ &= \alpha^{e/2+m_i(e/2-(p-1)/2)} \prod_{j\in\mathscr{S}_i;\,2j\equiv 0 \pmod e} \alpha^j. \end{aligned}$$

If m_i is odd, then as in Lemma 5.5, t even implies there is an odd number of $j \equiv 0 \pmod e$ in $\mathscr{S}_i$, and t odd implies there is an odd number of $j \equiv e/2 \pmod e$ in $\mathscr{S}_i$. If m_i is even, there is an even number of $j \in \mathscr{S}_i$ with $2j \equiv 0 \pmod e$, and (5.16) gives

$$1 = \alpha^{e/2} \prod_{j\in\mathscr{S}_i;\,2j\equiv 0 \pmod e} \alpha^j.$$

Hence there is an odd number of $j \equiv e/2 \pmod e$ in $\mathscr{S}_i$, and thus also an odd number of $j \equiv 0 \pmod e$. Done by (5.2).

Lemma 5.17. *Let* L *be self-dual,* $z=2$ *and* e *be even. Then* H *is cyclic.*

Proof. H/Z is cyclic and $z=2$. Thus if H is not cyclic, $H=E\times Z$ where $E \approx H/Z$ acts faithfully on P. Since $L|_N=V_d(\lambda)$, $L|_{PE}=V_d(\lambda|_E)=V_d(\alpha^k)$ for some integer k. $L \approx L^*$ implies $\lambda^2=\alpha^{d-1}$, whence $(\lambda|_E)^2=\alpha^{2k}=\alpha^{d-1}$. Since e is even, $d-1$ must be even and d is odd. But $2=z|d$, a contradiction.

THEOREM 5.18. *Let L be self-dual, $z=2$ (so that $L\in B_2$) and $e=(p-1)/t$ where t is odd. Then L has an algebraic conjugate in B_2 and $d\geqq p-t$.*

Proof. Let Q be the Sylow 2-subgroup of H. Since $|H|=z(p-1)/t$, where $z=2$ and t is odd, $\nu_2(|Q|)=\nu_2(p-1)+1$. By the above lemma, H, and hence Q, is cyclic. Thus, λ faithful on Z implies λ is faithful on Q, so $\lambda(Q)\nsubseteq F$, the prime subfield of K. Then there exists $T\in \mathrm{Aut}(K)$ with $\lambda^T\neq\lambda$, and hence $L^T=L(d,\lambda^T)\not\approx L$. Since $(\lambda^T)^2=(\lambda^2)^T=\alpha^{d-1}$, $(L^T)^*\approx L^T$. T preserves B_0, hence L and $L^T\in B_2$ by Proposition 4.9. Lemma 5.15 implies $d\geqq p-t$.

6. **A minimal case.** After dispensing with some elementary facts, we extract further information when L has the smallest degree allowed by Theorem 5.7, that is, $3(p-1)/4$.

PROPOSITION 6.1. *If $d<p-1$, then L is irreducible.*

Proof. $L|_P=V_d$ has a unique one-dimensional space of invariants, so the socle of L is irreducible and every submodule of L is indecomposable. If 1_0 occurs twice consecutively in a composition series for L, then Proposition 4.5 implies $1=1\alpha^{-1}$, so $e=1$, a contradiction. Then L has a unique nontrivial constituent $R\leftrightarrow V_r(\rho)$. If L has composition series 1_0, R, 1_0 then $\lambda=1$ and $1=1\alpha^{-(r+1)}$ by Proposition 4.5. Hence $d=r+2\equiv 1 \pmod e$, so $d>r\geqq p-e$ implies $d=p$, a contradiction.

Thus L has composition series either 1_0, R or R, 1_0. Replacing L by L^* if necessary, we may assume the former. Then $\lambda=1$, $\rho=\alpha^{-1}$, and R is a constituent of Q_0, the projective indecomposable with socle 1_0. R is adjacent to 1_0 in the graph of B_0. If $R\not\approx R^*$ then sep $R=r$ and R, R^* and 1_0 separate $2r+1$ vertices from the exceptional. Hence, $p-1\geqq e\geqq 2r+1\geqq 3(p-1)/2+1$, a contradiction. If $R\approx R^*$ then $\alpha^{-2}=\rho^2=\alpha^{r-1}$. Hence $r\equiv -1 \pmod e$. But $r\geqq p-e$ gives $r=p-2$ and $d=p-1$.

PROPOSITION 6.2. *$\lambda^2\alpha^s=\alpha^c$ for some integer c with $|c|\leqq s-1$ if and only if $c=0$ (i.e., $L\approx L^*$).*

Proof. $L\approx L^*$ if and only if there are invariants in $(L^*)^*\otimes L=L\otimes L$ (and equivalently in $L^*\otimes L^*$), since L is irreducible for $d<p-1$. This follows from there being invariants in $\sum_{i=0}^{s-1} V_{2i+1}(\lambda^2\alpha^{s+i})$ or $\sum_{i=0}^{s-1} V_{2i+1}(\lambda^{-2}\alpha^{-s+i})$ by Theorem 4.1. This says $\lambda^2\alpha^s=\alpha^c$ for some c with $|c|\leqq s-1$. When $L\approx L^*$, $\lambda^2\alpha^s=1$, and $\alpha^c=1$ for some c with $|c|\leqq s-1$ if and only if $c=0$, since $s\leqq e$.

LEMMA 6.3. *Suppose $z|2$ and $(\lambda^2\alpha^s)^2\neq 1$, so that (replacing L by L^* if necessary) $\lambda^2\alpha^s=\alpha^k$ with $e/2<k<e$. If there exist integers $0\leqq b$, $c<s$ such that $k+b+c\geqq e$ and $|b-c|\leqq e-k$ then* $\mathrm{Hom}_{KG}(L(2c+1,\alpha^c), L(2b+1,\lambda^2\alpha^{s+b}))\neq 0$.

Proof. If one of b or c is less than $(p-1)/4$ then $2(b+c)+2\leqq p$, so by Lemma 2.4 $V_{2c+1}(\alpha^c)\otimes V_{2b+1}(\lambda^2\alpha^{s+b})$ has main H-values $\alpha^{k+b+c}, \alpha^{k+b+c+1},\ldots,\alpha^{k+|b-c|}$ and hence has invariants. If $b=c=(p-1)/4$ then $s=(p+3)/4$ implies $k\geqq e/2+1$ (since $e\geqq(p-1)/3$ and $4|p-1$ says e is even), so $V_{2c+1}(\alpha^c)\otimes V_{2b+1}(\lambda^2\alpha^{s+b})$ has npmv's

$\alpha^{k+(p-1)/2}\alpha^{-((p-1)/2+1)+1+i}=\alpha^{k+i}$, $0\leqq i\leqq (p-1)/2-1$, by Lemma 2.6. So in either case, there are invariants in $L(2c+1, \alpha^c)^* \otimes L(2b+1, \lambda^2\alpha^{s+b})$ by Theorem 4.1.

THEOREM 6.4. *If* $d=3(p-1)/4$ *then* $L\approx L^*$, $z=2$, *and* $e=(p-1)/2$.

Proof. Let $L_i=L(2i+1, \alpha^i)$ and $N_i=L(2i+1, \lambda^2\alpha^{s+i})$ for $0\leqq i\leqq s-1$. These are the nonprojective summands of $L\otimes L^*$ and $L\otimes L$, respectively. Set $\dim L_i=2i+1+m_i p$ and $\dim N_i=2i+1+n_i p$.

L is irreducible. By Theorem 5.7 and its proof we may assume $t\leqq 3$, one $m_i=1$ and all the others are 2 for $1\leqq i\leqq s-1$. By Theorem 5.11, $z|4$. Since $4|p-1$, e is even. Then Theorem 5.12 implies $z|2$.

First, suppose $L\not\approx L^*$.

(i) Suppose $(\lambda^2\alpha^s)^2=1$. Since $t\leqq 3$, and $t=3$ implies $s>e/2$, Lemma 5.5 says the number of odd n_i is less than or equal to 1. Then

$$2(s-1)+1 \leqq \sum_{i=0}^{s-1} n_i \leqq p-2s,$$

so $s\leqq (p+1)/4$, a contradiction.

(ii) Suppose $(\lambda^2\alpha^s)^2\neq 1$. $z|2$ implies L, L^* are both in the same block B by Corollary 4.7. B must have a real stem, and L, L^* separate a total of $2s=(p+3)/2$ vertices from the exceptional. So $e=p-1$. $\lambda^2\alpha^s=\alpha^k$ where $e/2+1\leqq k<e$. Then $k+(s-1)+(s-2)=k+(p-1)/2-1\geqq e$, so Lemma 6.3 implies there exist nonzero KG-homomorphisms from L_{s-1} to N_{s-1} and to N_{s-2}.

Since all $m_i\leqq 2$, $\dim L_{s-1}\leqq 2p+2s-1=2p+(p+1)/2<4(3/4)(p-1)$. Hence L_{s-1} has at most three nontrivial irreducible constituents. Since L_{s-1} has no invariants, by Theorem 4.1, and is self-dual, Proposition 4.11 implies L_{s-1} has a unique minimal submodule $W\neq 1_0$ and a unique maximal submodule M with $\dim M=ap+m$, $0<m<p$. $W^*=L_{s-1}/M$, so if W^* has a pmv, then it is a mv of any nonzero KG-homomorphic image of L_{s-1}, hence of N_{s-1} and N_{s-2}. But the mv's of all the N_i are distinct when $e=p-1$, by (5.2), a contradiction. Thus $3(p-1)/4\leqq \dim W=w<p$, and W has a unique mv γ. Let $\gamma^*=\gamma^{-1}\alpha^{w-1}$, the mv of W^*. Then γ^* is *not* a mv of some N_u, $u=s-1$ or $s-2$. Since $(p+1)/2=2s-1<w$, $m+w>p$, so Proposition 4.5 implies $\gamma^*=\alpha^{s-1}$, the npmv of L_{s-1}.

Let S be the kernel of the homomorphism $L_{s-1}\to N_u$. Then W^* is not a submodule of L_{s-1}/S, $S\neq\{0\}$, and N_u has no invariants, so L_{s-1}/S has a unique minimal submodule R, where $R\approx R^*$ is the third nontrivial constituent of L_{s-1}. Thus L_{s-1}/S has composition series R, W^* or R, 1_0, W^* and each submodule of L_{s-1}/S is indecomposable. γ^* cannot be a mv of L_{s-1}/S, so rem $R+\dim W<p$ by Proposition 4.5. Then $\dim R>p$. But $\dim R\leqq (5p+1)/2-3(p-1)/2=p+2$.

Since L_{s-1} has unique minimal submodule W, L_{s-1} is properly contained in the projective indecomposable with socle W. Then all constituents of L_{s-1} lie on edges adjacent to W in the tree of B_0, and $e=p-1$ implies none occurs more than once in L_{s-1}. Thus $W \not\approx W^*$ and on the graph

$$\begin{array}{c|c} W & \underline{\;R\;} \\ W^* & \end{array}.$$

Take the vertex pictured as the exceptional. dim $W \geqq 3(p-1)/4$ implies sep $W = p$-rem W. Then sep $R=p$-rem $R \geqq p-2$, a contradiction.

Second, suppose $L \approx L^*$.

Let $L \otimes L = A+B$, the symmetric and skew decomposition. Lemma 3.3 gives $\sum_{i \equiv s \pmod 2} L_i \subseteq A$, $\sum_{i \equiv s-1 \pmod 2} L_i \subseteq B$.

If $z=1$, $L \in B_0$. e is even, so s is even by Theorem 5.12. Then

$$\sum_{i \equiv s-1 \pmod 2} m_i = m_1 + m_3 + \cdots + m_{s-1} \leqq (p-2s-1)/2$$

by Lemma 3.3. Hence $2(s/2)-1 \leqq (p-2s-1)/2$, since all but one $m_i=2$. This gives $s \leqq (p+1)/4$, a contradiction.

It follows that $z=2$. Theorem 5.18 implies $e=(p-1)/2$.

Actually, a good deal more is known in this situation. Each of the L_i (except perhaps L_1) is irreducible, and the degree of the exceptional characters in B_0 is either $(3p+1)/2$ or $(5p+1)/2$ ([0, Theorems 9.3, 9.4] and other unpublished results of the author). Of course, the existence of such a group is not at all certain.

7. Functions of $|N:C|$.

THEOREM 7.1.

$$\begin{aligned} d &\geqq p-(e/2+1) && (e \text{ even}) \\ &\geqq p-((e-1)/2+t) && (e \text{ odd}). \end{aligned}$$

Proof. We may assume $e<p-1$. Let B' be the block in which lie all the non-projective indecomposable summands of $L \otimes L$. We denote these by

$$N_i = L(2i+1, \lambda^2\alpha^{s+i}), \qquad 0 \leqq i \leqq s-1.$$

Let χ be an exceptional ordinary irreducible character in B'. $\chi(1) \equiv \varepsilon e \pmod p$, where $\varepsilon = \pm 1$. Thompson [14, Theorem 1] has shown that there is an $\mathcal{O}$-free $\mathcal{O}G$-module X affording χ such that $W=X/\mathcal{P}X$ has irreducible socle. If M is an irreducible KG-module which is a constituent of W, then M appears just once in any composition series for W. If $\varepsilon=1$, then Rothschild's argument shows $\sum$ rem $M = e$, where the sum is taken over all constituents of W. If $\varepsilon=-1$, then rem $M = p$-sep M and $\sum$ sep $M=e$. So if we sum over any subset containing, say, n of the constituents of W,

$$np > \sum \text{rem } M > (n-1)p. \tag{7.2}$$

A result of Janusz [12, Theorem 7.1] implies that W is uniserial. (This can also be proved directly, using Proposition 4.5.)

Let $Y=W/\text{rad } W$. Y is irreducible. Let R be any nonzero KG-homomorphic image of W. Then $Y\approx R/\text{rad } R$. Let $S=\text{rad } W/\text{rad }(\text{rad } W)$.

If $\varepsilon=1$, let $Y\leftrightarrow V_{p-y}(\gamma)$, where $y=\text{sep } Y$. By (7.2) and Proposition 4.5, γ is the unique npmv of each of the R.

If $\varepsilon=-1$, either Y has a pmv τ or $Y=1_0$. If the former is true, then τ is a pmv of each R. If the latter case holds then $0\neq S\neq 1_0$ and S has a pmv σ. Then either $R\approx 1_0$ or R has S as a constituent and σ as a pmv.

We conclude that all modules which are nonzero KG-homomorphic images of W and which are not equal to 1_0 have a main value in common.

Suppose $s\geqq(e+1)/2$. W has Green correspondent either $V_e(\lambda^2\alpha^k)$ if $\varepsilon=1$, or $V_{p-e}(\lambda^2\alpha^k)$ if $\varepsilon=-1$, for some integer k. For each i with $(e-1)/2\leqq i<s$, the npmv's of $V_e(\lambda^2\alpha^k)^*\otimes V_{2i+1}(\lambda^2\alpha^{s+i})$ are $\alpha^{-k-1+s+i-j}$, $0\leqq j\leqq e-1$, by Lemma 2.4. The npmv's of $V_{p-e}(\lambda^2\alpha^k)^*\otimes V_{2i+1}(\lambda^2\alpha^{s+i})$ are $\alpha^{-k+s-i+j}$, $0\leqq j\leqq e-1$, by Lemma 2.6. Since $|\langle\alpha\rangle|=e$, in either case $W^*\otimes N_i$ has npmv α^0. By Theorem 4.1, there exists a nonzero KG-homomorphism from W into N_i, for all $(e-1)/2\leqq i<s$. Since no such N_i has invariants, the homomorphic image is never 1_0. It follows that all the N_i with $(e-1)/2\leqq i<s$ have a main value in common.

Suppose e is even. Then Lemma 3.3 implies for $0\leqq i, j<s$, N_i and N_j have *no* main values in common unless $i\equiv j \pmod 2$. Thus if $s>e/2+1$, the existence of $N_{e/2}$ and $N_{(e/2)+1}$ as summands of $L\otimes L$ forces a contradiction. So if e is even, $d\geqq p-(e/2+1)$.

Suppose e is odd. By (5.2) for $L\otimes L$, a given $\gamma\in\text{char } H$ can be a npmv of at most one N_i, and a pmv of at most $t-1$ of the N_i, $0\leqq i\leqq s-1$. Since all the N_i with $(e-1)/2\leqq i\leqq s-1$ have a main value in common, it follows that $t\leqq s-(e-1)/2$. Therefore $d\geqq p-((e-1)/2+t)$.

REMARKS. Let G be a finite group with a Sylow p-subgroup P of prime order p. Assume that P is not a normal subgroup of G, and that G has a faithful irreducible complex representation of degree $n<p-1$. Then if $p>7$, either $G/Z\approx PSL(2,p)$ with $n=(p\pm 1)/2$, or G satisfies the hypotheses of Theorem 1, with $d=n=p-e$ and $t=(p-1)/e\geqq 3$ [2, II], [3], [6], [15]. Assume the latter possibility. If $d<p-2$, then z is even [6, Theorem 1]. In particular, e must be odd and t even, which also follows from Theorem 7.1 above. Theorem 7.1 also shows $p-e\geqq p-((e-1)/2+t)$ which gives $p\leqq 2t^2-t+1$. This improves Brauer's inequality $p\leqq t^3-t+1$ [3]. We will show in a separate paper that in fact $p\leqq t^2-3t+1$.

8. **Small primes.** The results and methods of this paper have been applied to primes p, $13\leqq p\leqq 31$, to eliminate some possibilities for $d<p-2$, where $L=L(d,\lambda)$ satisfies Theorem 1 and $G=G'$. The chart below lists all cases remaining open. From over 300 numerical possibilities for $e|p-1$, $d\geqq\max\{3(p-1)/4, p-e\}$, and $z|d$, exactly 98 still remain. Work in progress may soon eliminate more cases. On the other hand, some new groups may arise.

	d	z	e
$p = 13$:	10	2	6
$p = 17$:	13	1	16
	14	2	4, 8
		14	4, 8, 16
$p = 19$:	15	1	18
		3	9, 18
		5	9
	16	1	9
		2	3, 6, 9
		4	3, 6, 18
		8	3, 6
$p = 23$:	17	1	22
	18	2	11
	19	1	11, 22
	20	1, 2, 5, 10, 20	11
$p = 29$:	22	2	14
	23	1	28
	24	2, 12	7, 14
		3, 8	7
		4	14
		6	7, 14, 28
	25	1, 5	7, 14, 28
	26	1	7
		2	4, 7, 14
		13	7
		26	4, 7, 14, 28
$p = 31$:	23	1	30
	24	2	15, 30
	25	1	15, 30
	26	1, 2	15
	27	1, 3, 9	5, 6, 10, 15, 30
	28	1	5, 15
		2	3, 5, 6, 15
		4	3, 5
		7	3, 5, 15
		14	3, 5, 6, 10, 15, 30
		28	3, 5, 15

References

0. H. Blau, *On the degree of some finite linear groups*, Ph.D. Thesis, Yale University, New Haven, Conn., 1969.

1. R. Brauer, *Investigations on group characters*, Ann. of Math. (2) **42** (1941), 936–958. MR **3**, 196.

2. ———, *On groups whose order contains a prime number to the first power*. I, II, Amer. J. Math. **64** (1942), 421–440. MR **4**, 1; MR **4**, 2.

3. ———, *Some results on finite groups whose order contains a prime to the first power*, Nagoya Math. J. **27** (1966), 381–399. MR **33** #7402.

4. E. C. Dade, *Blocks with cyclic defect groups*, Ann. of Math. (2) **84** (1966), 20–48. MR **34** #251.

5. W. Feit, *Groups with a cyclic Sylow subgroup*, Nagoya Math. J. **27** (1966), 571–584. MR **33** #7404.

6. ———, *On finite linear groups*, J. Algebra **5** (1967), 378–400. MR **34** #7632.

7. ———, *Modular representations of finite groups*, Lecture Notes, Yale University, New Haven, Conn., 1969.

8. J. A. Green, *On the indecomposable representations of a finite group*, Math. Z. **70** (1958/59), 430–445. MR **24** #A1304.

9. ———, *Blocks of modular representations*, Math. Z. **79** (1962), 100–115. MR **25** #5114.

10. ———, *The modular representation algebra of a finite group*, Illinois J. Math. **6** (1962), 607–619. MR **25** #5106.

11. Z. Janko, *A new finite simple group with abelian Sylow* 2*-subgroups and its characterization*, J. Algebra **3** (1966), 147–186. MR **33** #1359.

12. G. J. Janusz, *Indecomposable modules for finite groups*, Ann. of Math. (2) **89** (1969), 209–241. MR **39** #5622.

13. B. Rothschild, *Degrees of irreducible modular characters of blocks with cyclic defect groups*, Bull. Amer. Math. Soc. **73** (1967), 102–104. MR **34** #4381.

14. J. G. Thompson, *Vertices and sources*, J. Algebra **6** (1967), 1–6. MR **34** #7677.

15. H. F. Tuan, *On groups whose orders contain a prime number to the first power*, Ann. of Math. (2) **45** (1944), 110–140. MR **5**, 143.

Northern Illinois University,
De Kalb, Illinois 60115