TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 203, 1975

UNDER THE DEGREE OF SOME FINITE LINEAR GROUPS. II

BY

HARVEY I. BLAU

ABSTRACT. Let G be a finite group with a cyclic Sylow p-subgroup for some prime $p \geqslant 13$. Assume that G is not of type $L_2(p)$, and that G has a faithful indecomposable modular representation of degree $d \leqslant p$. Some known lower bounds for d are improved, in case the center of the group is trivial, as a consequence of results on the degrees (mod p) of irreducible Brauer characters in the principal p-block.

1. **Introduction.** This paper continues the work of [3], [1], [2] on groups which, for a fixed prime p, are not of type $L_2(p)$, and which have a cyclic Sylow p-subgroup and a faithful indecomposable representation of degree $d \leqslant p$ over a field of characteristic p. Information on the degrees (modulo p) of irreducible Brauer characters in the principal p-block is obtained, and then used to improve some known lower bounds for d in case the center of the group is trivial.

Throughout the paper, G is a finite group, p a fixed prime, P a Sylow p-subgroup of G. N and C are respectively, the normalizer and centralizer of P in G. Z is the center of G, $z = |Z|$, $e = |N : C|$ and $t = (p-1)/e$. K is a field of characteristic p which is a splitting field for all subgroups of G, and B_0 is the principal p-block of G.

Hypothesis A. *$|P| = p$ and N/P is abelian.*

Hypothesis B. *P is cyclic, $p \geqslant 13$, G is not of type $L_2(p)$, and there is a faithful indecomposable KG-module L of dimension $d = p - s \leqslant p$.*

Hypothesis B implies Hypothesis A by [3]. When Hypothesis A holds, we freely use the notation and terminology of [1]. In particular, if X is a nonprojective indecomposable KG-module, $X = L(n, \gamma)$ means that the Green correspondent of X is the KN-module $V_n(\gamma)$; or, equivalently, that γ, a linear character from N/P to K, is the npmv of X, and $\operatorname{rem} X = n$. α is the linear character: $N/P \to K$ defined by $x^{-1}yx = y^{\alpha(x)}$ all $y \in P, x \in N$. We denote $\gamma = \alpha^i$ for

Received by the editors August 7, 1973.

AMS (MOS) subject classifications (1970). Primary 20C20, 20C05; Secondary 20D05.

Key words and phrases. Indecomposable modular representation, small degree, cyclic Sylow p-subgroup, main value.

some i with $j \leqslant i \leqslant k$ (j, k integers) by $\gamma \in [j, k]$. Since $|\langle\alpha\rangle| = e$, $\gamma \in [j, k]$ if and only if $\gamma \in [j + re, k + re]$ for all integers r.

2. Statement of results.

THEOREM 1. *Assume Hypothesis* B. *Let* X *be an irreducible KG-module in* B_0 *with* $X \not\approx X^*$. *Let* $m = p - x = \text{rem } X$.

(a) *If* $\text{rem } X > p/2$ *then* $x \leqslant \max\{t, (e/2) - s + t\}$. *If* $\text{rem } X < p/2$ *then* $m \leqslant \max\{t, ((e + 1)/2) - s + t\}$.

(b) *Suppose* $z \mid 2$ *and* $L \not\approx L^*$. *Then* $\text{rem } X > p/2$ *implies* $x \leqslant \max\{t, (2e - 6s + 7t + 2)/3\}$, *and* $\text{rem } X < p/2$ *implies* $m \leqslant \max\{t, (2e - 6s + 7t + 4)/3\}$.

(c) *Suppose* $z \mid 2$, $L \not\approx L^*$, e *is even, and* $s > t$. *Then* $\text{rem } X > p/2$ *implies* $x \leqslant \max\{t, (2e - 6s + 4t + 5)/3\}$. *If* $\text{rem } X < p/2$, *then* $m \leqslant \max\{t, (2e - 6s + 4t + 7)/3\}$.

(d) *Suppose* $L \approx L^*$ *and* e *is even. Then* $\text{rem } X > p/2$ *implies* $x \leqslant \max\{1, (e/2) - s + 1\}$, *and* $\text{rem } X < p/2$ *implies* $m \leqslant \max\{1, (e/2) - s + 1\}$.

THEOREM 2. *Assume Hypothesis* B. *Let* X *be an irreducible KG-module in* B_0 *with* $X \approx X^*$. *Assume* $m = p - x = \text{rem } X$ *is even. Then* e *is odd. If* $\text{rem } X > p/2$ *then* $x \leqslant e - 2s + 2t$. *If* $\text{rem } X < p/2$ *then* $m \leqslant e - 2s + 2t + 1$.

COROLLARY 3. *Assume Hypothesis* B *with* $z = 1$ *and* $L \not\approx L^*$. *Then*

$$s \leqslant \min\{\tfrac{1}{2}(t + (e/2)), (2e + 7t + 2)/9\}.$$

Furthermore, if e *is even then* $s \leqslant \max\{t, (2e + 4t + 5)/9\}$.

COROLLARY 4. *Assume Hypothesis* B *with* $z = 1$, d *even, and* $L \approx L^*$. *Then* $s \leqslant (e + 2t)/3$.

The next result eliminates the case $p = 31, d = 27, z = 1, e = 6$ listed in [1, §8].

COROLLARY 5. *Assume Hypothesis* B *with* $z = 1, G = G'$, t *odd and* $L \approx L^*$. *Then* $s \leqslant (e + 2)/3$.

[2, Corollary 2], [1, Theorem 5.7] show that under Hypothesis B with $t \geqslant 3$, we have $d \geqslant 5(p - 1)/6$. Our final corollary partially extends this result to the case $t = 2$, with the additional restriction that $z = 1$.

COROLLARY 6. *Assume Hypothesis* B *with* $z = 1$ *and* $t = 2$. *Then* $d \geqslant (5p - 7)/6$ *unless* $L \approx L^*$ *and* d *is odd.*

3. **Proofs.**

LEMMA 7. *Assume Hypothesis* A. *Let* $X = L(m, \gamma)$ *be a nonprojective irreducible KG-module,* $x = p - m$, *and let* μ: $N/P \to K$ *be a linear character. Let* u, r *be positive integers such that* $u < r \leq (p + 3)/4, m > u$ *(if* rem $X < p/2$), *or* $x > u$ *(if* rem $X > p/2$). *Assume that* $\gamma^{-1}\alpha^{-x}$ *occurs as a main value of* $\Sigma_{i=0}^{r-1} L(2i + 1, \mu\alpha^i)$ *at most* u *times.*

(a) *If* rem $X > p/2$, *then* $r \leq (x + 1)/2$ *implies* $\gamma\mu \notin [-(r-1)+u, (r-1)-u]$, *and* $r > (x + 1)/2$ *implies* $\gamma\mu \notin [-y, (r-1)-u]$ *where* $y = \min\{[(x-u-1)/2], (r-1)-u\}$.

(b) *If* rem $X < p/2$, *then* $r \leq (m + 1)/2$ *implies* $\gamma\mu \notin [-(r-1)+u, (r-1)-u]$, *and* $r > (m + 1)/2$ *implies* $\gamma\mu \notin [-(r-1)+u, y']$ *where* $y' = \min\{[(m-u-1)/2], (r-1)-u\}$.

PROOF. Let $L_i = L(2i + 1, \mu\alpha^i)$, $0 \leq i \leq r - 1$. Since $\gamma^{-1}\alpha^{-x}$ is the npmv of X^* [1, Lemma 2.3], then $X^* \subseteq L_i$ implies $\gamma^{-1}\alpha^{-x}$ is a main value of L_i. So X^* is a submodule of at most u of the L_i.

If $X \otimes L_i$ has 1 as an npmv, then $X \otimes L_i$ has an invariant by [1, Theorem 4.1]. Since $X \otimes L_i \approx \mathrm{Hom}_K(X^*, L_i)$ as a KG-module, it would follow that $X^* \subseteq L_i$.

(a) *Suppose* rem $X > p/2$.

If $r \leq (x + 1)/2$, then for all i with $0 \leq i \leq r - 1$, the npmv's of $X \otimes L_i$ are $\gamma\mu\alpha^{i-w}$, $0 \leq w \leq 2i$ [1, Lemma 2.4]. Thus if $\gamma\mu = \alpha^k$ with $|k| \leq r - 1 - u$, then 1 is an npmv of $L_{|k|}, L_{|k|+1}, \ldots, L_{r-1}$. Hence, X^* is a submodule of at least $u + 1$ of the L_i, a contradiction. So we may assume $r > (x + 1)/2$.

Suppose $\gamma\mu = \alpha^k, 0 \leq k \leq r - 1 - u$. Note that $u + k \leq r - 1$. If $k \geq [(x + 1)/2]$, then for any j with $k \leq j \leq u + k$, the npmv's of $X \otimes L_j$ are $\gamma\mu\alpha^{-j+w}$, $0 \leq w \leq x - 1$ [1, Lemma 2.6]. Since $x \geq u + 1$ implies $j - x + 1 \leq k \leq j$, 1 is an npmv of $X \otimes L_j$. Hence X^* is contained in each of the $u + 1$ modules $L_k, L_{k+1}, \ldots, L_{k+u}$, a contradiction.

If $k \leq [(x-1)/2]$ then $k \leq i \leq [(x-1)/2]$ implies the npmv's of $X \otimes L_i$ are $\gamma\mu\alpha^{i-w}$, $0 \leq w \leq 2i$, whence $X^* \subseteq L_i$. There are $[(x-1)/2] - k + 1$ of the L_i here, so we may assume $[(x-1)/2] - k + 1 \leq u$. Consider any integer j with $0 \leq j \leq u + k - [(x-1)/2] - 1$. Then

$$[(x + 1)/2] + j \leq [(x + 1)/2] + u + k - [(x - 1)/2] - 1 = u + k \leq r - 1,$$

and $x \geq u + 1$ implies

$$[(x + 1)/2] + j - x + 1 \leq u + k - x + 1 \leq k.$$

Now the npmv's of $X \otimes L_{[(x+1)/2]+j}$ are $\gamma\mu\alpha^{-j-[(x+1)/2]+w}$, $0 \leqslant w \leqslant x-1$, whence 1 is an npmv and $X^* \subseteq L_{[(x+1)/2]+j}$. So X^* is contained in $[(x-1)/2] - k + 1 + u + k - [(x-1)/2] = u + 1$ of the L_i, a contradiction.

Suppose $\gamma\mu = \alpha^{-k}$, $0 \leqslant k \leqslant y, y = \min\{[(x-u-1)/2], r-1-u\}$. Then as above, $X^* \subseteq L_k, L_{k+1}, \ldots, L_{[(x-1)/2]}$. We may assume $[(x-1)/2] - k + 1 \leqslant u$. Consider any integer j with $0 \leqslant j \leqslant u - [(x-1)/2] + k - 1$. Then $[(x+1)/2] + j \leqslant u + k \leqslant r - 1$ and $k \leqslant (x-u-1)/2$ implies $[(x+1)/2] + j - x + 1 \leqslant u + k - x + 1 \leqslant -k$. Therefore 1 is an npmv of $X \otimes L_{[(x+1)/2]+j}$, so that $X^* \subseteq L_{[(x+1)/2]+j}$, $0 \leqslant j \leqslant u - [(x-1)/2] + k - 1$. Then X^* is again contained in $u+1$ of the L_i, a contradiction.

(b) *Suppose* rem $X < p/2$.

If $r \leqslant (m+1)/2$ and $\gamma\mu = \alpha^k$ with $|k| \leqslant r - 1 - u$, then as in part (a), X^* is a submodule of $L_{|k|}, L_{|k|+1}, \ldots, L_{r-1}$, a contradiction. So we may assume $r > (m+1)/2$.

Suppose $\gamma\mu = \alpha^{-k}$, $0 \leqslant k \leqslant r - 1 - u$. If $k \geqslant [(m+1)/2]$, then for any j with $k \leqslant j \leqslant u + k \leqslant r - 1$, the npmv's of $X \otimes L_j$ are $\gamma\mu\alpha^{j-w}$, $0 \leqslant w \leqslant m-1$. Since $u < m$ implies $j - m + 1 \leqslant k \leqslant j$, 1 is an npmv of $X \otimes L_j$. Hence, X^* is contained in each of the $u+1$ modules $L_k, L_{k+1}, \ldots, L_{k+u}$, a contradiction.

If $k \leqslant [(m-1)/2]$, then $k \leqslant i \leqslant [(m-1)/2]$ implies the npmv's of $X \otimes L_i$ are $\gamma\mu\alpha^{i-w}$, $0 \leqslant w \leqslant 2i$, so that $X^* \subseteq L_i$. We may assume $[(m-1)/2] - k + 1 \leqslant u$. For any integer j with $0 \leqslant j \leqslant u + k - [(m-1)/2] - 1$, then $[(m+1)/2] + j \leqslant u + k \leqslant r - 1$ and $m > u$ implies $[(m+1)/2] + j - m + 1 \leqslant u + k - m + 1 \leqslant k$. Since the npmv's of $X \otimes L_{[(m+1)/2]+j}$ are $\gamma\mu\alpha^{[(m+1)/2]+j-w}$, $0 \leqslant w \leqslant m-1$, 1 is an npmv and $X^* \subseteq L_j$. Again, X^* is contained in $u+1$ modules L_i, another contradiction.

Finally, suppose $\gamma\mu = \alpha^k$, $0 \leqslant k \leqslant y'$, where $y' = \min\{[(m-1-u)/2], r-u-1\}$. As before, $X^* \subseteq L_k, L_{k+1}, \ldots, L_{[(m-1)/2]}$, and we may assume $[(m-1)/2] - k + 1 \leqslant u$. For any j with $0 \leqslant j \leqslant u - [(m-1)/2] + k - 1$,

$$[(m+1)/2] + j \leqslant u + k \leqslant r - 1$$

and $k \leqslant (m-1-u)/2$ implies

$$[(m+1)/2] + j + 1 - m \leqslant u + k + 1 - m \leqslant -k.$$

So 1 is an npmv of $X \otimes L_{[(m+1)/2]+j}$ and $X^* \subseteq L_{[(m+1)/2]+j}$, $0 \leqslant j \leqslant u - [(m-1)/2] + k - 1$. Thus X^* is contained in $u+1$ of the L_i, which is again a contradiction.

LEMMA 7′. *Assume Hypothesis* A. *Let* $X = L(m, \gamma)$ *be a nonprojective* *irreducible KG-module,* $x = p - m$, *and let* $\mu\colon N/P \longrightarrow K$ *be a linear character. Let* r *be an integer such that* $1 < r \leqslant (p+3)/4$. *Let* $m > 1$ *if* $\operatorname{rem} X < p/2$, *or* $x > 1$ *if* $\operatorname{rem} X > p/2$. *Assume that for no integer* i *with* $0 \leqslant i < r - 1$ *does* $\gamma^{-1}\alpha^{-x}$ *occur as a main value of both* $L(2i+1, \mu\alpha^i)$ *and* $L(2i+3, \mu\alpha^{i+1})$.

(a) *If* $\operatorname{rem} X > p/2$, *then* $r \leqslant (x+1)/2$ *implies* $\gamma\mu \notin [-r+2, r-2]$ *and* $r > (x+1)/2$ *implies* $\gamma\mu \notin [-[(x-2)/2], r-2]$.

(b) *If* $\operatorname{rem} X < p/2$, *then* $r \leqslant (m+1)/2$ *implies* $\gamma\mu \notin [-r+2, r-2]$ *and* $r > (m+1)/2$ *implies* $\gamma\mu \notin [-r+2, [(m-2)/2]]$.

The proof is similar to that of Lemma 7 and is omitted.

PROPOSITION 8. *Assume Hypothesis* A. *Let* $X = L(m, \gamma)$ *be a nonprojective irreducible KG-module with* $X \not\approx X^*$. *Let* $m = p - x$. *Assume* $x > 1$ *if* $\operatorname{rem} X > p/2$, *or* $m > 1$ *if* $\operatorname{rem} X < p/2$.

(a) *If* $\operatorname{rem} X > p/2$ *then* $\gamma^2 \notin [-2x+1, -1]$ *so that* $\gamma \notin [-x+1, -1]$ *and* $\gamma \notin [-x+1+[e/2], [(e+1)/2]-1]$.

(b) *If* $\operatorname{rem} X < p/2$ *then* $\gamma^2 \notin [0, 2m-2]$, *so that* $\gamma \notin [0, m-1]$ *and* $\gamma \notin [[(e+1)/2], m-1+[e/2]]$.

PROOF. $X \not\approx X^*$ and X irreducible imply there is no nonzero KG-homomorphism from X^* to X. Thus $X \otimes X$ has no invariants, so [1, Theorem 4.1] implies 1 is not an npmv of $X \otimes X$.

If $\operatorname{rem} X > p/2$, the npmv's of $X \otimes X$ are $\gamma^2\alpha^{x+i}$, $0 \leqslant i \leqslant x-1$. Hence, $\gamma^2 \notin [-2x+1, -x]$. The same argument applied to X^* gives $(\gamma^{-1}\alpha^{-x})^2 \notin [-2x+1, -x]$, whence $\gamma^2 \notin [-x, -1]$.

If $\operatorname{rem} X < p/2$, the npmv's of $X \otimes X$ are $\gamma^2\alpha^{-i}$, $0 \leqslant i \leqslant m-1$. Hence, $\gamma^2 \notin [0, m-1]$. The same argument for X^* yields $(\gamma^{-1}\alpha^{m-1})^2 \notin [0, m-1]$, so that $\gamma^2 \notin [m-1, 2m-2]$.

PROOF OF THEOREM 1. Let $X = L(m, \gamma)$. $\gamma \in \langle\alpha\rangle$ by [1, Proposition 4.6]. The discussion of [1, §4] shows that X, X^* separate a total of either $2x$ ($\operatorname{rem} X > p/2$) or $2m$ ($\operatorname{rem} X < p/2$) vertices from the real stem of the graph of B_0. Hence, $\operatorname{rem} X > p/2$ implies $x \leqslant [e/2]$ and $\operatorname{rem} X < p/2$ gives $m \leqslant [e/2]$. So we may assume $d < p - 1$, and, in the proof of (a), (b) that $s > t$. By [1, Theorem 5.7], $s \leqslant (p+3)/4$.

Let $L = L(d, \lambda)$. Then

$$(L \otimes L^*)_N \approx \sum_{i=0}^{s-1} V_{2i+1}(\alpha^i) + \sum_{i=s}^{p-s-1} V_p(\alpha^i)$$

[1, Lemma 2.3, Lemma 2.6]. So $L \otimes L^*$ is the direct sum of $\Sigma_{i=0}^{s-1} L(2i+1, \alpha^i)$ and (possibly) a projective KG-module. Since $p - s \leqslant p - 1 = te$, no linear character: $N/P \to K$ occurs as a main value of $\Sigma_{i=0}^{s-1} L(2i+1, \alpha^i)$ more than t times.

[1, Lemma 2.6] also gives

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

So $L \otimes L$ is the direct sum of $\Sigma_{i=0}^{s-1} L(2i+1, \lambda^2\alpha^{s+i})$ and perhaps a projective module, and no linear character: $N/P \to K$ occurs as a main value of $\Sigma_{i=0}^{s-1} L(2i+1, \lambda^2\alpha^{s+i})$ more than t times. Note that $z \mid 2$ implies $\lambda^2\alpha^s \in \langle\alpha\rangle$. If e is even, [1, Lemma 3.3] implies for all integers i with $0 \leqslant i < s-1$, $L(2i+1, \lambda^2\alpha^{s+i})$ and $L(2i+3, \lambda^2\alpha^{s+i+1})$ have no main values in common.

Let $T = \bigcap_n G^{(n)}$, the intersection of the derived series. G not p-solvable implies $P \subseteq T$. L_P is indecomposable [3], hence T and L_T satisfy Hypothesis B. Then $d < p-1$ and [1, Proposition 6.1] imply L_T is irreducible. It follows that L is irreducible.

(a) Suppose first that rem $X > p/2$. We may assume $x > t$. Then by Lemma 7 with $\mu = 1, u = t$ and $r = s$, $\gamma \notin [0, s-1-t]$. Applying Lemma 7 to X^* gives $\gamma^{-1}\alpha^{-x} \notin [0, s-1-t]$, so $\gamma \notin [-x-s+1+t, -x]$. $X \not\approx X^*$ implies $\gamma \notin [-x+1, -1]$ by Proposition 8. Thus

$$\gamma \notin [-x-s+1+t, s-1-t].$$

Since Proposition 8 also says $\gamma \notin [-x+1+[e/2], [(e+1)/2]-1]$, we must have

$$\text{either} \quad s-t < -x+1+[e/2] \quad \text{or} \quad [(e+1)/2]-1 < e-x-s+t.$$

Both these inequalities are equivalent to $x < [e/2]-s+t+1$, i.e. $x \leqslant [e/2]-s+t$. Note that

$$\begin{aligned} &s-t < -x+1+[e/2] \leqslant [(e+1)/2]-1 < e-x-s+t, \\ &\gamma \in [s-t, [e/2]-x] \quad \text{or} \quad [[(e+1)/2], e-x-s+t]. \end{aligned} \tag{9}$$

If rem $X < p/2$, we may assume $m > t$. Lemma 7 and Proposition 8 give $\gamma \notin [-s+1+t, m+s-t-2]$. Proposition 8 implies

$$\gamma \notin [[(e+1)/2], m-1+[e/2]],$$

so that

$$\text{either} \quad m+s-t-1 < [(e+1)/2] \quad \text{or} \quad m-1+[e/2] < e-s+t.$$

Hence $m \leqslant [(e+1)/2]-s+t$. Note

$$\begin{aligned} &m+s-t-1 < [(e+1)/2] \leqslant m-1+[e/2] < e-s+t, \\ &\gamma \in [m+s-t-1, [(e-1)/2]] \quad \text{or} \quad [m+[e/2], e-s+t]. \end{aligned} \tag{10}$$

(b) Assume first that rem $X > p/2$. We may assume $x > t$ and $x >$

$(2e - 6s + 7t + 2)/3$. Suppose $x \geqslant 2s - t$. By (a), $x \leqslant (e/2) - s + t$. Therefore, $2s - t \leqslant (e/2) - s + t$ implies $s \leqslant (e/6) + (2t/3)$. Then

$$\begin{aligned} x &> (2e/3) - 2s + (7t/3) + (2/3) \\ &\geqslant (2e/3) - s - (e/6) - (2t/3) + (7t/3) + (2/3) \\ &= (e/2) - s + (5t/3) + (2/3). \end{aligned}$$

Hence, $(e/2) - s + t > (e/2) - s + (5t/3) + (2/3)$, a contradiction. So we may assume $x \leqslant 2s - t - 1$, hence $(x - t - 1)/2 \leqslant s - t - 1$.

Now $L \not\approx L^*$ implies $\lambda^2\alpha^s = \alpha^c$ where $|c| > s - 1$ by Proposition 8. We may take $s \leqslant c \leqslant e - s$. Since $(\lambda^{-1}\alpha^{-s})^2\alpha^s = \alpha^{-c}$, replacing L by L^* (if necessary) we may assume $e/2 \leqslant c \leqslant e - s$. Lemma 7 applied to X for $\mu = 1, \alpha^c, \alpha^{-c}$ gives $\gamma\mu \notin [-[(x - t - 1)/2], s - 1 - t]$, and applied to X^* yields $\gamma^{-1}\alpha^{-x}\mu^{-1} \notin [-[(x - t - 1)/2], s - 1 - t]$, whence $\gamma\mu \notin [-x - s + 1 + t, [(x - t - 1)/2] - x]$. In particular,

$$(11) \qquad \begin{aligned} &\gamma \notin [c - x + 1 + t - s, c + [(x - t - 1)/2] - x] \quad \text{and} \\ &\gamma \notin [-c - [(x - t - 1)/2], -c + s - 1 - t]. \end{aligned}$$

Since $c \geqslant e/2$ and $x > t$, we have

$$(12) \qquad c + [(x - t - 1)/2] - x \geqslant [e/2] - x.$$

If $e - c + s - 1 - t < [e/2] - x$, then $c \leqslant e - s$ implies $x < c + [e/2] - e - s + t + 1 \leqslant [e/2] - 2s + t + 1$ which says

$$(2e/3) - 2s + (7t/3) + (2/3) < [e/2] - 2s + t + 1.$$

Hence, $(7t/3) + (2/3) < t + 1$ which implies $4t < 1$, a contradiction. So

$$(13) \qquad e - c + s - 1 - t \geqslant [e/2] - x.$$

If either $c - x + 1 + t - s$ or $e - c - [(x - t - 1)/2]$ is less than or equal to $s - t$, then (9), (11), and (12) or (13) imply $\gamma \in [[(e + 1)/2], e - x - s + t]$. But the same argument applied to X^* gives $\gamma^{-1}\alpha^{-x} \in [[(e + 1)/2], e - x - s + t]$, hence $\gamma \in [s - t, [e/2] - x]$, a contradiction. Therefore

$$(14) \qquad c - x + 1 + t - s > s - t \quad \text{and} \quad e - c - [(x - t - 1)/2] > s - t.$$

Adding these two inequalities, we have $e - x - [(x - t - 1)/2] + 1 + t - s > 2s - 2t$, which says $e - 3s + 3t + 1 > x + [(x - t - 1)/2]$, whence $x + (x - t)/2 \leqslant e - 3s + 3t + 1$. The desired inequality follows.

The case $\operatorname{rem} X < p/2$ is similar. We may assume $m > t$ and $m > (2e - 6s + 7t + 4)/3$. If $m \geqslant 2s - t$, then (a) yields

$$((e + 1)/2) - s + t > (e/2) - s + (5t/3) + (7/6),$$

a contradiction. So we may assume $(m - t - 2)/2 \leqslant s - t - 1$.

Let $\lambda^2\alpha^s = \alpha^c$, where we may assume $s \leqslant c \leqslant e/2$. Lemma 7 applied to X, X^*, with $\mu = \alpha^c$, gives

$$(15)\qquad \begin{gathered} \gamma \notin [-c - s + 1 + t, -c + [(m - t - 1)/2]] \text{ and} \\ \gamma \notin [c + m - 1 - [(m - t - 1)/2],\ c + m + s - t - 2]. \end{gathered}$$

Since $c \leqslant [e/2]$ and $m > t$,

$$(16)\qquad c + m - 1 - [(m - t - 1)/2] \leqslant [e/2] + m - 1.$$

If $e - c - s + 1 + t > m - 1 + [e/2]$, then $c \geqslant s$ implies $m < e - [e/2] - c - s + 2 + t \leqslant e - [e/2] - 2s + 2 + t$, which gives

$$(2e/3) - 2s + (7t/3) + (4/3) < [(e + 1)/2] - 2s + 2 + t.$$

Hence, $(7t/3) + (4/3) < 2 + t$ and $t < 1/2$, a contradiction. So

$$(17)\qquad e - c - s + 1 + t \leqslant m - 1 + [e/2].$$

If either $c + m + s - t - 2 \geqslant e - s + t$ or $e - c + [(m - t - 1)/2] \geqslant e - s + t$, then (10), (15), and (16) or (17) imply $\gamma \notin [m + [e/2], e - s + t]$. But also $\gamma^{-1}\alpha^{m-1} \notin [m + [e/2], e - s + t]$, whence $\gamma \in [m + [e/2], e - s + t]$, a contradiction. Hence

$$(18)\qquad c + m + s - t - 2 < e - s + t \text{ and } e - c + [(m - t - 1)/2] < e - s + t.$$

Adding these two inequalities yields $m + [(m - t - 1)/2] < e - 3s + 3t + 2$, hence $m + (m - t)/2 \leqslant e - 3s + 3t + 2$ and (b) follows.

(c) Suppose rem $X > p/2$. We may assume $x > t$ and $x > (2e - 6s + 4t + 5)/3$. Suppose $x \geqslant 2s - 1$. Then arguing as in (b), we see that (a) forces $(e/2) - s + t > (e/2) - s + t + (4/3)$, a contradiction. Hence, $s > (x + 1)/2$.

Assume $\lambda^2\alpha^s = \alpha^c, e/2 \leqslant c \leqslant e - s$. Lemma 7′, with $\mu = \alpha^c$, applied to X^* and X, gives

$$(19)\qquad \begin{gathered} \gamma \notin [c - x - s + 2, c - x + [(x - 2)/2]] \text{ and} \\ \gamma \notin [-c - [(x - 2)/2], -c + s - 2]. \end{gathered}$$

The argument proceeds as in (b), with (19) replacing (11). We arrive at $c - x - s + 2 > s - t$ and $e - c - [(x - 2)/2] > s - t$. Adding these inequalities yields the desired result.

If rem $X < p/2$, we may assume $m > t$ and $m > (2e - 6s + 4t + 7)/3$. If $m \geqslant 2s - 1$, then (a) implies $((e + 1)/2) - s + t > (e/2) - s + t - 1/2 + (7/3)$, a contradiction. So $s > (m + 1)/2$.

Assume $\lambda^2\alpha^s = \alpha^c, s \leqslant c \leqslant e/2$. Apply Lemma 7′ to X and X^* to obtain

$$(20)\qquad \begin{gathered} \gamma \notin [-c - s + 2, -c + [(m - 2)/2]] \text{ and} \\ \gamma \notin [c + m - 1 - [(m - 2)/2], c + m + s - 3]. \end{gathered}$$

Argue as in (b), with (20) replacing (15), to reach $c + m + s - 3 < e - s + t$ and $e - c + [(m - 2)/2] < e - s + t$. Adding these inequalities completes the proof of (c).

(d) If $\operatorname{rem} X > p/2$, we may assume $x > 1$. Then by Lemma 7′, with $\mu = 1 = \lambda^2\alpha^s$, $\gamma \notin [0, s - 2]$. Likewise, $\gamma^{-1}\alpha^{-x} \notin [0, s - 2]$, so that $\gamma \notin [-x-s+2, -x]$. Then Proposition 8 implies either $s-1 < -x+1+(e/2)$ or $(e/2) - 1 < e - x - s + 1$. Each is equivalent to $x < (e/2) - s + 2$, hence $x \leqslant (e/2) - s + 1$.

If $\operatorname{rem} X < p/2$, we may assume $m > 1$. Then Lemma 7′, with $\mu = 1 = \lambda^2\alpha^s$, applied to X and X^*, gives $\gamma \notin [-s + 2, 0]$ and $\gamma \notin [m - 1, s + m - 3]$. Proposition 8 implies either $s + m - 2 < e/2$ or $m - 1 + (e/2) < e - s + 1$. Both inequalities are equivalent to the desired result, and Theorem 1 is proved.

Proof of Theorem 2. $X \approx X^*$ implies $\gamma^2 = \alpha^{m-1}$ [1, Lemma 2.3]. $X \in B_0$ implies $\gamma \in \langle\alpha\rangle$. Thus $m - 1$ odd forces e to be odd.

Since $x \leqslant e$ if $\operatorname{rem} X > p/2$ and $m \leqslant e$ if $\operatorname{rem} X < p/2$ by Rothschild's argument [1, §4], it suffices to assume $s > t$. Let $\operatorname{rem} X > p/2$. Suppose $e - 2s + 2t < x \leqslant t$. Then $2s \geqslant e + t + 1$. But [2, Corollary 2] says $2s \leqslant \max\{e + 5, e + t - 1\}$. It follows that $t + 1 \leqslant 5$, so $t \leqslant 4$. If $t = 4$, then m even implies $x \leqslant 3$ and $e - 2s + 8 < 3$, so that $2s > e + 5$, a contradiction. If $t = 2$ then $e - 2s + 2t < 2$ implies $s > (e + 2)/2 = (p + 3)/4$, again a contradiction. So we may assume $x > t$.

Since e and x are odd, $\gamma^2 = \alpha^{-x}$ implies $\gamma = \alpha^{(e-x)/2}$. By Lemma 7 with $\mu = 1$, $\gamma \notin [0, s - 1 - t]$. Hence $(e - x)/2 \geqslant s - t$ and $x \leqslant e - 2s + 2t$.

Let $\operatorname{rem} X < p/2$. If $e - 2s + 2t + 1 < m \leqslant t$, then $2s > e + t + 1$. Since $e + t + 1$ is even, $2s \geqslant e + t + 3$. By [2, Corollary 2], $5 \geqslant t + 3$ so $t = 2$. Then $e - 2s + 2t < 2$ implies $s > (e + 2)/2 = (p + 3)/4$, a contradiction. Then it suffices to assume $m > t$.

$X \approx X^*$ implies $\gamma^2 = \alpha^{m-1}$. Then $\gamma = \alpha^{(e+m-1)/2}$. By Lemma 7 with $\mu = 1$, $\gamma \notin [-s + 1 + t, 0]$. Therefore $(e + m - 1)/2 \leqslant e - s + t$, so $m \leqslant e - 2s + 2t + 1$.

It suffices to assume, in proving the corollaries, that $d < p - 1$. Then, as in the proof of Theorem 1, L is irreducible. If $z = 1$, $L \in B_0$ [1, Corollary 4.7].

Proof of Corollary 3. Let $L = X$ in Theorem 1, $L \not\approx L^*$ implies $s \leqslant e/2$, hence $(e/2) - s + t \geqslant t$. Then (a) gives $s \leqslant (e/2) - s + t$, so $s \leqslant \frac{1}{2}((e/2) + t)$.

If $t \geqslant s > (2e + 7t + 2)/9$, then $9t > 2e + 7t + 2$ implies $t > e + 1$. Then $s > (2e + 7(e + 1) + 2)/9 = e + 1$, a contradiction. So if $s >$

$(2e + 7t + 2)/9$, then $s > t$. Theorem 1(b) yields $s \leqslant (2e - 6s + 7t + 2)/3$, whence $s \leqslant (2e + 7t + 2)/9$.

If e is even and $s > t$, Theorem 1(c) gives $s \leqslant (2e - 6s + 4t + 5)/3$ and $s \leqslant (2e + 4t + 5)/9$.

PROOF OF COROLLARY 4. Let $L = X$ in Theorem 2. Then $s \leqslant e - 2s + 2t$, whence the result.

PROOF OF COROLLARY 5. Since $G = G'$, the determinant of the linear transformation on L given by the action of each element of G is 1. Then [1, Lemma 2.3] implies $\lambda^d = \alpha^{d(d-1)/2}$, where $L = L(d, \lambda)$. $L \approx L^*$ gives $\lambda^2 = \alpha^{d-1}$. Since d is odd, $\lambda = \alpha^{(d-1)/2}$. Now t odd (and hence e even) gives

$$(d - 1)/2 = (p - 1 - s)/2 = (te - s)/2 = (te/2) - (s/2) = (e - s)/2.$$

By Lemma 7$'$, with $X = L$, $r = s$, $\mu = \lambda^2\alpha^s = 1$, we have $\lambda \notin [0, s - 2]$. Hence $s - 1 \leqslant (e - s)/2$, which implies $s \leqslant (e + 2)/3$.

PROOF OF COROLLARY 6. If $L \not\approx L^*$, Corollary 3 implies $s \leqslant (p + 15)9 \leqslant (p + 7)/6$ for all $p \geqslant 13$. If $L \approx L^*$ and d is even, Corollary 4 gives $s \leqslant (e + 2t)/3 = (p + 7)/6$ and we are done.

REFERENCES

1. H. I. Blau, *Under the degree of some finite linear groups*, Trans. Amer. Math. Soc. **155** (1971), 95–113; Errata, ibid. **162** (1971), 475. MR **43** #367; **44** #329.

2. ———, *Finite groups where two small degrees are not too small*, J. Algebra **28** (1974), 551–555.

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

DEPARTMENT OF MATHEMATICS, NORTHERN ILLINOIS UNIVERSITY, DEKALB, ILLINOIS 60115