ON THE CENTER OF SOME FINITE LINEAR GROUPS

HARVEY I. BLAU

ABSTRACT. This note proves two results, one in characteristic $p$ and the other in characteristic zero, which restrict the order of the center of some finite linear groups of degree less than a prime $p$ which divides the group order.

$G$ denotes a finite group, $p$ a fixed odd prime, $P$ a Sylow $p$-subgroup of $G$. $Z$ is the center of $G$ and $z = |Z|$.

Theorem 1. Assume $G = G'$, $G$ is not of type $L_2(p)$, $P$ is cyclic, and for some field $K$ of characteristic $p$, there is a faithful, indecomposable $KG$-module $L$ of dimension $d < p$. If $d$ is odd then $d \geq \frac{z}{z+2}(p+1)$. If $d$ is even then

\[ d \geq \frac{z}{z+2}(p+1) \quad (z \text{ odd}) \]
\[ d \geq \frac{z}{z+4}(p+1) \quad (z \text{ even}). \]

Theorem 2. Assume $G = G'$, $P$ has order $p$ and is not normal in $G$, the number $t$ of conjugate classes of $p$-elements of $G$ is at least 3, and $G$ has a faithful irreducible complex character $\chi$ of degree $d < p - 1$. Let $e = \frac{p-1}{t}$. Then $z \leq 2d(e+1)$.

Remarks. (i) Theorem 1 supplements [1, Theorem 5.11]. While the fractional multiples of $p$ given in [1, Theorem 5.11] are a little better than in Theorem 1, an annoying (especially for large values of $z$) remainder term in the earlier result is dispensed with here. One consequence is the following: It is known that $z|d$ under the hypotheses of Theorem 1. As a corollary of the theorem, we have that if $z = d$, then $d \geq p - 3$.

(ii) Theorem 2 is proved by exploiting the methods of [2], which were themselves a variation on those of [8]. The numerical case $p = 31$, $d = z = 28$, $e = 3$ listed in [1, 8], and not ruled out by previous results, is eliminated by Theorem 2. For in that case the modular representation involved in [1] lifts to an ordinary representation to which Theorem 2 can be applied.
(iii) Apparently, no groups are known which satisfy either the hypotheses of Theorem 1 with \( p \geq 13 \) and \( d < p - 2 \), or the hypotheses of Theorem 2 with \( p > 7 \) and \( d < p - 2 \). If such groups do exist, their \( p \)-local structure is quite restricted, as our results indicate.

**Proof of Theorem 1.** Since \( L_p \) is indecomposable \([7]\) and remains indecomposable under all field extensions (as \( P \) is cyclic), we may assume \( K \) is a splitting field for all subgroups of \( G \). Let \( d = p - s \). By \([1, (5.3)]\), the nonprojective summands of \( L \otimes L \) are \( L_i, 0 \leq i \leq s - 1 \), of dimensions \( 2i + 1 + m_i p \), with \( \sum_{i=0}^{s-1} m_i \leq p - 2s \). Now \( z \mid d \) \([1, Proposition 5.1]\) and by \([1, (5.10)]\),

\[
(1) \quad z \mid 2(2i + 1 + m_i p), \quad 0 \leq i \leq s - 1.
\]

For any integer \( i \) with \( 0 \leq i < (s - 1)/2 \), let \( i' = s - 1 - i \). Then (1) implies

\[
(2) \quad z \mid 2(2s + (m_i + m_{i'})), \quad 0 \leq i < (s - 1)/2.
\]

Suppose \( d \) is odd. Then \( z \) is odd, and (2) yields

\[
(m_i + m_{i'}) p \equiv -2s \pmod{z}, \quad 0 \leq i \leq s/2 - 1.
\]

Since \( p \equiv s \pmod{z} \), and \( (s, z) = 1 \), we have

\[
m_i + m_{i'} \equiv -2 \pmod{z}, \quad 0 \leq i \leq s/2 - 1.
\]

Thus \( m_i + m_{i'} \geq z - 2, 0 \leq i \leq s/2 - 1 \), so that

\[
p - 2s \geq \sum_{i=0}^{s-1} m_i \geq \sum_{i=0}^{s/2-1} (m_i + m_{i'}) \geq (s/2)(z - 2).
\]

It follows that \( s \leq (2/(z + 2))p \), whence \( d \geq (z/(z + 2))p \).

Suppose \( d \) is even. If \( z \) is odd, again we have

\[
m_i + m_{i'} \equiv -2 \pmod{z}, \quad 0 \leq i < (s - 1)/2.
\]

Also, \( z \mid 2(s + pm_{(s - 1)/2}) \) implies \( m_{(s - 1)/2} \equiv -1 \pmod{z} \). Thus

\[
p - 2s \geq m_{(s - 1)/2} + \sum_{i=0}^{(s-3)/2} (m_i + m_{i'}) \geq z - 1 + (z - 2)(s - 1)/2.
\]

It follows that \( s \leq (2/(z + 2))p - z/(z + 2) \), hence

\[
(3) \quad d \geq (z/(z + 2))p + z/(z + 2) = (z/(z + 2))(p + 1).
\]

If \( z \) is even, (2) implies the above congruences are still valid modulo \( z/2 \). So we may replace \( z \) by \( z/2 \) in (3) to obtain \( d \geq (z/(z + 4))(p + 1) \).
Proof of Theorem 2. Assume the hypotheses of Theorem 2. Then $d = p - e$ [5]. If $p = 7$, no such groups exist [6], so we may assume $p > 7$.

Feit's reduction argument [8, (6.1)] shows that $G$ is not of type $L_2(p)$. Then by [8, (2.1)], $G$ satisfies conditions $(\ast)$ of [8], and $z|d$. If $e = 1$ then $d = p - 1$, a contradiction. If $e = 2$ then $G \cong SL_2(2^a)$ and $z = 1$ [9]. So we may assume $2 < e < (p - 1)/2$. Also, [8, Theorem 1] implies $z$ is even, hence $e$ is odd.

Let $F$ be a $p$-adic number field with ring of integers $R$ such that $F$ and $R/f(R) = K$ are splitting fields for all subgroups of $G$. Let $M$ be an $R$-free $RG$-module such that $M \otimes_F F$ affords $\chi$ and $L = M/f(R)M$ is indecomposable [10]. $P \not\in G$ implies $L$ is faithful, so the situation of Theorem 1 holds with $s = e$.

Let $N$ be the normalizer of $P$ in $G$, and let $L_N = V_{p-e}(\lambda)$ (cf. [1, §3]), where $\lambda$ is a linear character: $N \rightarrow K$. Let $L_i$ be as above, $0 \leq i \leq e - 1$. $L_i$ has Green correspondent $V_{2i+1}(\lambda^2 \alpha_1^{e+1})$ [1, §3]. Let $\chi_L = \chi(1)\eta$ a faithful linear character: $Z \rightarrow F$. Now $\eta(Z) \subseteq R$, and if $\tilde{\eta}$ denotes $\eta$ composed with the canonical homomorphism: $R \rightarrow K$, then $\tilde{\eta} = \lambda_2$. There is a one-one correspondence between the $p$-blocks of positive defect and the distinct powers of $\eta$: an irreducible character $\zeta$ of $G$ is in block $B$ if and only if $\zeta = \zeta(1)\eta^n$ [4]. Thus $\chi, L$ are in $B_1$ and the $L_i$ are all in $B_2$ [1, §4].

Let $\zeta_j, 1 \leq j \leq t$, be the exceptional characters in $B_2$. Then $\zeta_{jz} = \zeta_j(1)\eta^2$. By [8, (4.1)], $\zeta_j(1) = mp + e$ for some positive integer $m$, independent of $j$.

We may assume $F$ is sufficiently large so that for each $i$ with $0 \leq i < (e - 1)/2$, there is an $R$-free $RG$-module $X_i$ such that $X_i/f(R)X_i \cong L_i \oplus L_{e-i-1}$ [3, Lemma 2.1]. Also, there is an $R$-free $RG$-module $Y$ such that $Y/f(R)Y \cong L_{(e-1)/2}$. Now the $\zeta_j$ occur in the character afforded by each $X_i$ with total multiplicity at least 2, and in the character afforded by $Y$ with multiplicity at least 1 [3, Lemma 2.2]. Hence

$$\dim_{K} L \otimes L \geq \text{rank}_{R} \left(Y \bigoplus \sum_{i=0}^{(e-3)/2} X_i \right) \geq 2\zeta_1(1)(e - 1)/2 + \zeta_1(1) = e\zeta_1(1).$$

Therefore $(p - e)^2 \geq e(mp + e)$. It follows that $m \leq (p - 2e)/e = t - 2 + 1/e$, whence $m \leq t - 2$.

Since $\zeta_{jz} = \zeta_j(1)\eta^2$, we set the determinant of the appropriate scalar matrices equal to 1 (as $G = G'$) to see that $\eta^{2(mp + e)} = 1$. Since $\eta$ is faithful on the cyclic group $Z$, it follows that $z|2(mp + e)$, hence $mp + e \equiv 0 \pmod{z/2}$. Now $z|p - e$ implies $me + e \equiv 0 \pmod{z/2}$ and $(z, e) = 1$ yields $m + 1 \equiv 0 \pmod{z/2}$. Therefore $t - 2 \geq m \geq z/2 - 1$. Hence $z \leq 2t - 2 = 2(d - 1)/e < 2d/e$. Since $z|d$, we have $z \leq 2d/(e + 1)$.
REFERENCES

3. ———, Finite groups where two small degrees are not too small, J. Algebra 28 (1974), 541–555.

DEPARTMENT OF MATHEMATICS, NORTHERN ILLINOIS UNIVERSITY, DE KALB, ILLINOIS 60115