PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 43, Number 2, April 1974

SOME CRITERIA FOR THE NONEXISTENCE OF CERTAIN FINITE LINEAR GROUPS

HARVEY I. BLAU

ABSTRACT. Let p be a prime and G a finite group, not of type $L_2(p)$, with a cyclic Sylow p-subgroup P. Assume that $G=G'$. The purpose of this note is to put some rather stringent lower bounds on the degree d of a faithful indecomposable representation of G over a field of characteristic p given certain conditions on the normalizer N and the centralizer C of P in G. In particular, if the center of G has order 2 and $|N:C|=p-1$, then $d\geqq p-1$.

This paper began when the author realized that some of the methods in [**1**] were more powerful than he originally believed. Consequently, elements of the argument below appeared in slightly less general form (and with weaker application) in [**1**, §5]. Although the blanket hypotheses of that section do not exactly coincide with those of our assertions (we do not assume here that $p\geqq 13$ or that G is not of type $L_2(p)$ in Lemma 1 below), it should be clear that the results we quote from [**1**, §5] are indeed valid in the context where they are applied.

Throughout the paper G denotes a finite group, p an odd prime, P a Sylow p-subgroup of G. N and C are, respectively, the normalizer and centralizer of P in G, $e=|N:C|$, $t=(p-1)/e$, and z is the order of Z, the center of G. K is a field of characteristic p which is a splitting field for all subgroups of G. If M is a KG-module, M^* denotes its dual. The linear character $\alpha: N/P\rightarrow K$ is as defined in [**1**]. ν_2 is the usual 2-adic valuation on the rationals.

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

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

Hypothesis B implies Hypothesis A by [**2**]. If group G and module L satisfy Hypothesis B, then so do J and L_J, where J is the intersection of the derived series of G. So the assumption $G=G'$ is not a severe restriction.

Presented to the Society, January 16, 1974; received by the editors August 13, 1973.

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

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

Our first result generalizes [**1**, Lemma 5.15], and has almost the same proof.

LEMMA 1. *Assume Hypothesis* A *and that* $G=G'$. *Suppose there exist indecomposable* KG-*modules* L *and* M *of dimension* d *with* $p/2<d<p$ *such that* $M\not\approx L^*$ *but the nonprojective summands of* $L\otimes M$ *are self-dual. Then*

$$\begin{aligned} d &\geqq p-t \qquad (t \text{ odd}),\\ &\geqq p-t+1 \quad (t \text{ even}). \end{aligned}$$

PROOF. Let $L_N=V_d(\lambda)$, $M_N=V_d(\gamma)$ as in [**1**, §4]. Let $s=p-d$. $M\not\approx L^*$ implies $\lambda\gamma\alpha^s\neq 1$ [**1**, Lemma 2.3]. As in [**1**, §5], the nonprojective summands of $L\otimes M$ are L_i, $0\leqq i\leqq s-1$, where dim $L_i=2i+1+m_ip$ and

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

As remarked in [**1**, §5], the L_i are self-dual if and only if $(\lambda\gamma\alpha^s)^2=1$.

Suppose m_i is odd. Then, as in the proof of [**1**, Lemma 5.5], there is an odd number of $j\equiv 0 \pmod e$ in $\mathscr{S}_i$ if t is even, and an odd number of $j\equiv e/2 \pmod e$ in $\mathscr{S}_i$ if t is odd. Suppose m_i is even. Then $2i+1+m_ip$ is odd, so [**1**, (5.6)] and $(\lambda\gamma\alpha^s)^2=1$ imply

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

Since $\lambda\gamma\alpha^s\neq 1$, there must exist $j\in\mathscr{S}_i$ with $j\not\equiv 0 \pmod e$, $2j\equiv 0 \pmod e$. Hence e is even and $j\equiv e/2 \pmod e$. Furthermore, there must be an odd number of such j in $\mathscr{S}_i$. Since m_i is even, there must also be $j\in\mathscr{S}_i$ with $j\equiv 0 \pmod e$. So each $\mathscr{S}_i$ contains some $j\equiv 0 \pmod e$ if t is even, or $j\equiv e/2 \pmod e$ if t is odd. Since $|\langle\alpha\rangle|=e$, [**1**, (5.2)] implies $s\leqq t$ if t is odd, and $s\leqq t-1$ if t is even.

THEOREM 2. *Assume Hypothesis* B *and* $G=G'$. *Suppose there is a positive integer* n *such that* $ze|2(p^n-1)$ *but* $ze\nmid p^n-1$. *Then*

$$\begin{aligned} d &\geqq p-t \qquad (t \text{ odd}),\\ &\geqq p-t+1 \quad (t \text{ even}). \end{aligned}$$

PROOF. Let $q=p^n$, and σ be the isomorphism of K into K given by $x^\sigma=x^q$, all $x\in K$. Let $\mathscr{L}$ be a representation of G with underlying module L, and for each $g\in G$, let $\mathscr{L}(g)^\sigma$ be the matrix obtained by replacing each entry a_{ij} of $\mathscr{L}(g)$ by a_{ij}^σ. Then $g\to\mathscr{L}(g)^\sigma$ defines a representation of G with an underlying indecomposable KG-module of dimension d which we will call L^σ. If $L_N=V_d(\lambda)$, then $(L^\sigma)_N=V_d(\lambda^\sigma)$, where $\lambda^\sigma=\lambda^q$. $(L^*)_N=V_d(\lambda^{-1}\alpha^{-s})$ [**1**, Lemma 2.3]. Note that $\lambda^\sigma(\lambda^{-1}\alpha^{-s})\alpha^s=\lambda^{q-1}$.

Since $ze=|N/P|$ [2] and λ is a linear character: $N/P\to K$, $ze|2(q-1)$ implies $\lambda^{2(q-1)}=1$. It follows that the nonprojective summands of $L^\sigma\otimes L^*$ are self-dual. The conditions $ze|2(q-1)$, $ze\nmid q-1$ imply

$$\nu_2(z)+\nu_2(e)=1+\nu_2(q-1). \tag{3}$$

Since $e|p-1$, it follows that z is even and hence d is even by [**1**, Proposition 5.1].

Suppose $\lambda^{q-1}=1$. Since λ is faithful on cyclic Z [**1**, Proposition 5.1], $z|q-1$. If e is odd, we have $\nu_2(z)=1+\nu_2(q-1)$, a contradiction, so e is even. Then the first paragraph of the proof of [**1**, Theorem 5.12] shows that $(\lambda^2)^{2i+1+m_ip}$ is an odd power of α for all $0\leqq i\leqq s-1$ with $i\equiv(p+1)/2 \pmod 2$, where $2i+1+m_ip$ is the dimension of the summand of $L\otimes L$ with Green correspondent $V_{2i+1}(\lambda^2\alpha^{s+i})$. Since we may assume $d<p-1$, there exist such i. Because $z|2(2i+1+m_ip)$ [**1**, (5.10)] and $\lambda^z\in\langle\alpha\rangle$, it follows that λ^z is an odd power of α. Now since $1=(\lambda^z)^{(q-1)/z}$, we have $\nu_2((q-1)/z)\geqq\nu_2(e)$ which contradicts (3). Hence, $\lambda^{q-1}\neq 1$, so $L^*\not\approx(L^\sigma)^*$ and Lemma 1 may be applied.

REMARKS. (i) [**1**, Theorem 5.18] is a special case of Theorem 2, with $z=2$, t odd, and the (now unnecessary) restriction $L\approx L^*$.

(ii) The following numerical cases listed in [**1**, §8] are eliminated by Theorem 2 (each 4-tuple is an instance of p, d, z, e): (29, 24, 8, 7), (29, 24, 4, 14), (29, 26, 26, 28), (31, 24, 2, 30).

(iii) The assumptions of Theorem 2 are satisfied if we have Hypothesis B, $G=G'$, t odd, and $z=2^k$, where either $p\equiv 1 \pmod 4$ and k is any positive integer, or $p\equiv 3 \pmod 4$ and $k=1$ or $k>\nu_2(p+1)$. In particular, if $t=1$ and $z=2$, then $d\geqq p-1$. This bound is best possible, as there is a group $G=G'$ satisfying Hypothesis B, with $p=7$, $z=2$, and $e=d=6$, such that G/Z is the Hall-Janko group of order 604,800 [3]. Feit has shown, in work not yet published, that there is no $G=G'$ satisfying Hypothesis B with $p=11$, $z=2$, and $e=d=10$. For $p>11$, the existence of relevant groups with $z=2$ and $e=d=p-1$ is apparently unknown.

Some notation is needed to state the next theorem. Assume Hypothesis B and $G=G'$. Let $L_N=V_d(\lambda)$. Define the integer x $(=x(L)$, unique modulo $e)$ by $\lambda^z=\alpha^{[z(d-1)/2]+x}$ where square brackets denote the greatest integer symbol. Since the determinant of the action of each element of G on L is 1, [**1**, Lemma 2.3] implies $\lambda^d=\alpha^{d(d-1)/2}$ Now $z|d$, so when z is even, $\lambda^d=(\lambda^z)^{d/z}$ implies $xd/z\equiv 0 \pmod e$.

THEOREM 4. *Assume Hypothesis* B *with* $G=G'$, *t odd, and d even. Suppose there is an odd positive integer n such that* $p^n\equiv\pm 1 \pmod z$ *and* $x(p^n\mp 1)/z\equiv 0 \pmod e$. *Then* $d\geqq p-t$.

PROOF. Let $q=p^n$, and let σ be as in Theorem 2 (so $(L^\sigma)_N=V_d(\lambda^q)$). Since we may assume $d<p-1$, [**1**, Theorem 5.12] implies z is even.

Suppose $q\equiv 1 \pmod z$ and $x(q-1)/z\equiv 0 \pmod e$. Then

$$\begin{aligned}\lambda^{q-1} &= (\lambda^z)^{(q-1)/z} = \alpha^{((q-1)(d-1)/2)+(x(q-1)/z)} \\ &= \alpha^{((q-1)/2)(d-1)} = \alpha^{((p-1)/2)(\text{odd integer})} = \alpha^{e/2}\end{aligned}$$

since d is even and n, t are odd. Thus $\lambda^{q-1}\neq 1$, $(\lambda^{q-1})^2=1$. It follows that L^σ and L^* satisfy the hypotheses of Lemma 1.

Suppose $q\equiv -1 \pmod z$ and $x(q+1)/z\equiv 0 \pmod e$. Then

$$\lambda^{q+1} = (\lambda^z)^{(q+1)/z} = \alpha^{((q+1)(d-1)/2)+(x(q+1)/z)} = \alpha^{((q-1)(d-1)/2)+(d-1)} = \alpha^{(e/2)-s}.$$

So $\lambda^q\lambda\alpha^s\neq 1$, $(\lambda^q\lambda\alpha^s)^2=1$, whence L^σ and L satisfy the hypotheses of Lemma 1.

COROLLARY 5. *Assume Hypothesis* B *with* $G=G'$, t *odd, and* d *even. Suppose there is an odd positive integer* n *such that* $p^n\equiv\pm 1 \pmod d$. *Then* $d\geqq p-t$.

MORE REMARKS. (iv) Theorem 4 eliminates the cases (17, 14, 14, 16) and (31, 28, 14, 30) from [**1**, §8].

(v) The numerical assumptions of Corollary 5 hold if t is odd and $d=2r$, r a prime such that $r\equiv 3 \pmod 4$.

REFERENCES

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

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

3. J. H. Lindsey II, *On a six dimensional projective representation of the Hall-Janko group*, Pacific J. Math. **35** (1970), 175–186. MR **42** #7769.

DEPARTMENT OF MATHEMATICAL SCIENCES, NORTHERN ILLINOIS UNIVERSITY, DEKALB, ILLINOIS 60115