A GENERALIZATION OF FEIT'S THEOREM

BY

J. H. LINDSEY II

Abstract. This paper is part of a doctoral thesis at Harvard University. The title of the thesis is Finite linear groups in six variables.

Using the methods of this paper, I believe that I can prove that if \( p \) is a prime greater than five with \( p \equiv -1 \pmod{4} \), and \( G \) is a finite group with faithful complex representation of degree smaller than \( 4p/3 \) for \( p > 7 \) and degree smaller than 9 for \( p = 7 \), then \( G \) has a normal \( p \)-subgroup of index in \( G \) divisible at most by \( p^2 \). These methods are particularly effective when there is nontrivial intersection of \( p \)-Sylow subgroups. In fact, if the current work people are doing on the trivial intersection case can be extended, it should be possible to show that, for \( p \) a prime and \( G \) a finite group with a faithful complex representation of degree less than \( 3(p - 1)/2 \), \( G \) has a normal \( p \)-subgroup of index in \( G \) divisible at most by \( p^2 \). (It may be possible to show that the index is divisible at most by \( p \) if the representation is primitive and has degree unequal to \( p \).)

Introduction. In this paper all representations are assumed to be over \( \mathbb{C} \), the complex numbers. We use standard mathematical notation without comment. If \( X \) is a representation of the group \( G \) on the vector space \( V \), we call a subspace \( U \) of \( V \) a homogeneous space for \( G \) if \( F \) is invariant for \( G \) and \( U \) is maximal with the property that the irreducible constituents of the representation of \( G \) on \( U \) are equivalent. The representation \( X \) is called quasiprimitive if it is irreducible, and for all normal subgroups \( N \) of \( G \), \( X|N \) has just the homogeneous subspace \( V \). For \( x \in G \) and \( \gamma \in C \), \( C_{\gamma}(\gamma^{-1}x) = \langle v \mid v \in V, X(x)v = \gamma v \rangle \) and for \( H \subseteq G \), \( C_{\gamma}(H) = \bigcap_{h \in H} C_{\gamma}(h) \). The term \( i_{\Pi} \) is defined in the following theorem. This theorem generalizes the theorem in [5]. Equality is allowed by \( C \).

Theorem. Let \( \Pi \) be a set of primes and let \( X \) be a faithful representation on the vector space \( V \) of the finite group \( G \) of degree \( n \) over the complex numbers. Define \( i_{\Pi}(G) = |G|^{|\Pi|}/|O_{\Pi}(G)| \). Assume that \( p \leq n + 1 \), \( p \geq 7 \) for all \( p \in \Pi \). Assume that \( G \) has a \( \Pi \)-Sylow subgroup, \( H \). Then either:

I. \( i_{\Pi}(G) \) is not composite.

II. \( X \) is imprimitive or reducible on the spaces \( V_1 \) and \( V_2 \) of dimension \( n/2 \) where \( V = V_1 \oplus V_2 \). Also, \( n + 1 = p \in \Pi \) for some \( p \). There exists a normal subgroup \( M \) of
$G$ of index 1 or 2 having the $V_i$ as invariant, irreducible subspaces. There exist subgroups $T_i$ of $M$ with $M = \mathbb{Z}(M)(T_1 \times T_2)$; $C_V(T_i) = V_i$; and

$$T_i \simeq \text{PSL}(2, p), \quad p \equiv -1 \pmod{4},$$

$$\simeq \text{SL}(2, p), \quad p \equiv 1 \pmod{4}, \quad \text{for } i = 1, 2.$$

The theorem generalizes [5] when $n+1 \in \Pi$. When $n+1 \notin \Pi$, an abelian $\Pi$-Sylow subgroup of $G$ was guaranteed by Blichfeldt. When $n+1 \in \Pi$, the existence of a $\Pi$-Sylow subgroup must be assumed (such a group is abelian by Lemma 7). For example $\text{SL}(2, 13)$ has a representation of degree 6, but has no subgroup of order $(7)(13)$. When $n+1 \notin \Pi$, our proof uses only Lemmas 1 and 2 and furnishes a short proof of Feit's Theorem. Furthermore, when for $p \in \Pi$, $p \geq 2n+1$, we may use our proof to prove that $i_n(G) = 1$ or $p = 2n+1 \in \Pi$ for some $p$ and $G/Z(G) \simeq \text{PSL}(2, p)$, the result of [6], by induction on $n$. Here, only Lemma 1 is needed. Also, (E) and (H) follow immediately from the stronger induction hypothesis that $i_n(G_0) = 1$ when $G_0$ has a faithful representation of degree $n_0 < n$. Then only steps (A), (B), (C), (F), (I), and (J) are needed to complete the proof, since [2] can be applied if $|G|_n$ is prime.

**Lemma 1.** If $G$ is a finite group and $\Pi$ is a set of primes, define $i_n(G) = |G|_n/|O_n(G)|$. Then if $H$ is a homomorphic image or a subgroup of $G$, $i_n(H)|i_n(G)$. Furthermore, if $K$ and $L$ are finite groups, $i_n(K \times L)/(|i_n(K)||i_n(L)|)$. Finally, $i_n(G) = i_n(G/Z(G))$.

**Proof.** If $\alpha$ is a homomorphism from $G$ onto $H$ with kernel $K$, then $\alpha(O_n(G)) \subset O_n(H)$ and

$$|H|_n/|\alpha(O_n(G))| = [(|G|_n/|K|_n)/(|O_n(G)|/|K \cap O_n(G)|)]$$

which divides $|G|_n/|O_n(G)|$. If $H \subset G$ and $\beta$ is the natural homomorphism from $G$ to $G/O_n(G)$, then $H \cap O_n(G) \subset O_n(H)$ and $H/H \cap O_n(G) \simeq \beta(H) \subset G/O_n(G)$. The middle statement of Lemma 1 follows from $O_n(K) \times O_n(L) \subset O_n(K \times L)$. We have already shown that $i_n(G/Z(G))|i_n(G)$. Let $\gamma$ be the natural homomorphism of $G$ into $G/Z(G)$. Let $M = \gamma^{-1}(O_n(G/Z(G)))$. Then $Z(G) = [Z(G)]_n \times [Z(G)]_n$, where $[Z(G)]_n$ is characteristic in $Z(G)$ and is a normal $\Pi$-Sylow of $M$. By Schur-Zassenhaus, there exists $N$, a $\Pi$-Sylow subgroup of $M$. As $M = N \times [Z(G)]_n$, $N$ is characteristic in $M$ which is normal in $G$. Therefore, $N \subset O_n(G)$. As $|G|_n/|N| = |G/M|_n = |G/Z(G)|_n/|O_n(G/Z(G))|$, this concludes the proof of Lemma 1.

**Lemma 2.** Let $X$ be a faithful irreducible representation of a finite group $G$ which affords the character $\chi$. Let $p \geq 5$ be a prime. Let $H = (O^p(G))'$ and let $P$ be a $p$-Sylow subgroup of $H$. Assume that $i_p(G) = p$ and $n = \chi(1) < p - 1$. Then

(i) $X$ is primitive, $n \geq (p-1)/2$, $p \nmid |H|$, $i_p(H) = p$ and $O^p(G) \leq HZ(G)$.

(ii) $X|H$ is irreducible.

(iii) $\chi|P$ is the sum of distinct linear characters. The principal character of $P$ is contained in this sum if and only if $n > (p-1)/2$.

(iv) If $x$ is a $p$-element of $G$ then either $X(x)$ is scalar or has distinct eigenvalues.
Proof. By [6], \(i_p(G) \neq 1\) implies that \(n \geq (p-1)/2\). If \(X\) is imprimitive on the spaces \(V_1, \ldots, V_n\), let \(K\) be the subgroup of \(G\) fixing the \(V_i\). As \(\dim V_i = n/m < (p-1)/2\), the constituent \(X_i(K)\) of \(X(K)\) acting on \(V_i\) satisfies \(i_p(X_i(K)) = 1\) for \(i = 1, \ldots, m\). As \(|G/K| = m!\) and \(O_p(K)\) is characteristic in \(K\) which is normal in \(G\), \(O_p(K)\) is a normal \(p\)-Sylow subgroup of \(G\), a contradiction.

Using Blichfeldt's method of replacing a generator \(X(x)\) by

\[Y(y) = [\det(x)]^{-1/n}X(x),\]

one may find a finite group \(L\) with a unimodular representation \(Y\) of degree \(n\) with \(Y(L)(ZGL(n, C)) = X(G)(ZGL(n, C))\). Then \(Y\) is primitive. Furthermore,

\[L/Z(L) \cong Y(L)(ZGL(n, C))/ZGL(n, C) = X(G)(ZGL(n, C))/ZGL(n, C) \cong G/Z(G)\]

By Lemma 1, \(i_p(L) = i_p(G) = p\). As \(n < p-1\), \(O_p(L)\) is abelian by Lemma 7. As \(O_p(L)\) is normal in \(L\), \(Y(L)\) permutes the homogeneous spaces of \(Y\) on \(O_p(L)\) (the sums of spaces on which identical constituents of \(Y\) on \(O_p(L)\) act). Therefore, all constituents of \(Y\) on \(O_p(L)\) are identical and \(Y\) consists of scalars of the form \(\alpha I_n\). Then \(\alpha\) is a \(p\)-th root of unity for some \(t\) and \(\alpha^p = \det(\alpha I_n) = 1\). As \(n < p-1\), \(\alpha = 1\) and \(O_p(L) = \langle 1 \rangle\). Therefore, \(p \| |L|\). Then Lemma 3.1 of [5] applies to \(L\) and implies that \((O^p(L))' = O^p(L)\). If \(x\) is a \(p\)-element in \(G\), then there exists \(z \in ZGL(n, C)\) with \(zX(x) = Y(y)\) for some \(y\) in \(L\). As \(\langle X(x), Y(y) \rangle \leq \langle z, X(x) \rangle\), an abelian subgroup, \(z = Y(y)^{-1}X(x)\) is of finite order. Then \([z]_p X(x) = [zX(x)]_p = [Y(y)]_p\) is a power of \(Y(y)\), and replacing \(z\) by \([z]_p\), we may take \(y\) to be a \(p\)-element. This and the symmetric argument show that \(X(O^p(G))ZGL(n, C) = Y(O^p(L))ZGL(n, C)\). Then \(X(H) = (X(O^p(G)))' = (Y(O^p(L)))' = Y(O^p(L))\). Therefore, \(p \| |H|\), \(i_p(H) = p\), \(X(O^p(G)) \subseteq Y(O^p(L))ZGL(n, C) = X(H)ZGL(n, C)\), and \(O^p(G) \subseteq HZ(G)\). By [6], irreducible constituents \(X_i(H)\) of \(X|H\) with \(i_p(X_i(H)) = p\) have degree \(\geq (p-1)/2\). As \(n < p-1\), there is at most one such constituent. By Lemma 1, there is at least one such constituent. If \(W\) is the space on which this constituent acts and \(x \in G\), then \(H = xHx^{-1}\) has \(xW\) as an irreducible invariant space for some constituent \(U\) of \(X|Hx^{-1}\) and \(i_p(U(xHx^{-1})) = p\). Therefore, \(xW = W\) and by irreducibility of \(X\), \(\dim W = n\) and \(X|H\) is irreducible. The statement in Lemma 2 about \(\chi|P\) follows from Lemma 3.1 of [5] applied to \(Y(O^p(L)) = X(H)\). The final statement of Lemma 2 follows from our previous step where for \(x\) a \(p\)-element in \(G\) there exist \(y \in L\) and \(z \in ZGL(n, C)\) with \([z]_p X(x) = [Y(y)]_p\), which is \(I_n\) or has distinct eigenvalues.

The remaining lemmas are needed in the proof of our theorem only in the case where we have a proper generalization of Feit's Theorem \((n + 1 \in \Pi)\). Some of the proofs of these lemmas require Feit's Theorem.

Lemma 3. Let \(X\) be a faithful, irreducible representation of a finite group \(G\) of degree \((p-1)/2\) for \(p\), a prime greater or equal to 5. Suppose \(G\) does not have a normal \(p\)-Sylow subgroup. Then \(G = G'Z(G)\) where \(G' \simeq PSL(2, p)\) if \((p-1)/2\) is odd.
and \( G' \simeq SL(2, p) \) if \((p - 1)/2\) is even. There are exactly two distinct irreducible representations of \( G' \) of degree \((p - 1)/2\).

**Proof.** As in the proof of Lemma 2, there exists a finite group \( L \) with a faithful, unimodular \((p - 1)/2\)-dimensional representation \( Y \) with \( Y(L) \mathbb{Z}GL(n, C) = X(G) \mathbb{Z}GL(n, C) \) and the following properties: \( i_p(L) = p, p \parallel |L| \). By [2], \( L/\mathbb{Z}(L) \simeq PSL(2, p) \). Then \((X(G))' = (Y(L))' \simeq PSL(2, p)\) or \( SL(2, p) \) by [11]. Furthermore, 
\[
(X(G))' \mathbb{Z}GL(n, C) = (Y(L))' \mathbb{Z}GL(n, C) = Y(L) \mathbb{Z}GL(n, C) = X(G) \mathbb{Z}GL(n, C).
\]
Therefore, \( G = G' \mathbb{Z}(G) \). The remainder of the lemma follows from the classification in [11] of projective representations of \( PSL(2, p) \).

**Lemma 4.** Let \( L \) be a subgroup of a finite group \( G \) and \( i_p(L) = i_p(G) = p \) for a prime \( p \geq 5 \). Let \( X \) be a faithful, irreducible representation over \( C \) of \( G \) of degree \( n < p - 1 \). Let \( Y \) be the unique constituent of \( X|L \) which is irreducible and satisfies \( i_p(Y(L)) = p \). Let \( m = \deg Y \). Then \( m = n \) or \( m = n - 1 = (p - 1)/2 \). (Actually, by [12], \( m = n \).)

**Proof.** Let \( X|L = W \oplus Y \) for some constituent \( W \) of \( Y|L \). Then \( i_p(W(L)) = 1 \), by Lemma 1. By [1], \( O^p(W(L)) = O_p(W(L)) \) is abelian and \( (O^p(W(L)))' = \langle 1 \rangle \). For any \( p \)-element \( M \) in \( Y(L) \) we may find \( x \in L \) with \( Y(x) = M \). Then \( Y([x]_p) = [Y(x)]_p \) and we may take \( x \) to be a \( p \)-element. Therefore, \( Y(O^p(L)) = O^p(Y(L)) \). Then by Lemma 2, we may find \( y \in (O^p(L))' \) with \( Y(y) \) having order \( p \) and \( m \) distinct eigenvalues, one of which is 1 if and only if \( m \geq (p - 1)/2 \). Also, \( W(y) \in (O^p(W(L)))' = \langle 1 \rangle \). Applying Lemma 2 to \( y \in G \) and the representation \( X \), we see that \( X(y) \) has distinct eigenvalues. This implies the conclusion of Lemma 4.

**Lemma 5.** Let \( X \) be a faithful, reducible representation of the finite group \( G \). Let \( X = X_1 \oplus X_2 \) where \( \deg X_1 \leq (p + 1)/2, \deg X_2 < p - 1, p \) is a prime greater than 4, \( X_1 \) is irreducible and \( i_p(X_1(G)) = p \) for \( i = 1, 2 \); and \( i_p(G) > p \). Then there exists \( x \in (O^p(G))' \cap \ker X_2 \) of order \( p \) with \( X_1(x) \) having exactly \((p - 1)/2\) eigenvalues unequal to 1. Furthermore, if \( \deg X_1 = \deg X_2 = (p - 1)/2 \), then \( G = Z(G)(G_1 \times G_2) \) where for \( i = 1, 2 \), \( G_i \subset \ker X_i \cap O^p(G) \) and \( G_i \simeq PSL(2, p) \) if \((p - 1)/2 \) is odd, \( G_1 \simeq SL(2, p) \) if \((p - 1)/2 \) is even.

**Proof.** Let \( \alpha \) be the natural homomorphism \( G \rightarrow Y_1(G) \times Y_2(G) \) where \( Y_i(G) = X_i(G)/Z(X_i(G)) \) for \( i = 1, 2 \). Then \( \ker \alpha = Z(G) \) and by Lemma 1, \( i_p(\alpha(G)) = i_p(G) > p \). By Lemma 2, \( p \parallel |Y_i(G)| \) for \( i = 1, 2 \). Then \( p^2 \parallel |\alpha(G)|_p = |Y_2(G)|_p(\ker Y_2)/Z(G)|_p \) and \( p \parallel |\ker Y_2/Z(G)| \). Let \( K = \ker Y_2 \). Then \( K < G, Y_1(K) \subset Y_1(G), \) and \( X_2(K) \subset Z(X_2(K)) \). Since \( p \parallel |Y_1(K)| \), by Lemma 2, \( O^p(Y_1(G)) \subset Y_1(K) \) and \( O^p(X_1(G)) \subset X_1(K)Z(X_1(G)) \). Then \( K' \subset \ker X_2 \) and \( X_1(K') \simeq (O^p(X_1(G)))' \) which by Lemma 2 contains an element \( x \) of order \( p \) with exactly \((p - 1)/2\) eigenvalues unequal to 1. If \( \deg X_1 = (p - 1)/2 \), then by Lemma 3, \( (O^p(X_1(G)))' \simeq PSL(2, p) \) and \( X_1(G) = (O^p(X_1(G)))'Z(X_1(G)) \). Defining \( G_2 = K' \) and reversing the roles of \( X_1 \) and \( X_2 \) for \( \deg X_1 = \deg X_2 = (p - 1)/2 \) finishes the proof of Lemma 5.
Lemma 6. Let \( p \) be a prime \( \geq 5 \) and \( G \) be a finite group with a faithful representation \( X \) of degree \( n = p - 1 \). Let \( L \subseteq G \) with \( L/Z(L) \cong PSL(2, p) \), \( (|Z(L)|, p) = 1 \), and \( X|L = X_1 \otimes I_2 \) with deg \( X_1 = (p - 1)/2 \). Let \( P \) be a \( p \)-Sylow subgroup of \( L \) and \( A \) be an abelian subgroup of \( G \) with \( P \subseteq A \). If \( AZ(G) \) (or \( A \)) is a trivial intersection set of \( G/Z(G) \) (or \( G \)), then \( X|\langle A, L \rangle \) is reducible.

Proof. By [11], \( X_1 |N_L(P) \) is irreducible. By [4, Lemma 5.2], \( C_{GL(n, \mathbb{C})}(X(N_L(P))) = I_{n/2} \otimes GL(2, \mathbb{C}) = C_{GL(n, \mathbb{C})}(X(L)) \). Therefore, \( X|N_L(P) \) and \( X|L \) have the same invariant subspaces. As \( P \subseteq A \), \( P \not\subseteq Z(G) \), and \( AZ(G) \) (or \( A \)) is a T. I. S. of \( G/Z(G) \) (or \( G \), it follows that \( N_L(P) \subseteq N(AZ(G)) \). Furthermore,

\[
|\langle N_L(P), AZ(G) \rangle/\langle AZ(G) \rangle| \geq |N_L(P)/P| = (p - 1)/2.
\]

By Clifford’s Theorem, \( X|\langle N_L(P), AZ(G) \rangle \) has an invariant space of dimension less than or equal to \( (p - 1)/2 \). As this space is invariant for \( N_L(P) \), it is invariant for \( L \) and for \( \langle L, A \rangle \).

Lemma 7. Let \( \Pi \) be a set of primes, all of which are greater than \( n \). Let \( G \) be a finite \( \Pi \)-group with a faithful representation \( X \) of degree \( n \). Then \( G \) is abelian. 

Proof. Degrees of irreducible constituents of \( X \) divide \(|G| = |G|_\Pi \) and are no larger than \( n \). Such degrees are 1, and \( G \) is abelian.

Lemma 8. Let \( G \) have a faithful representation \( X \). Let \( K \) be a normal subgroup of \( G \) with \( X|K \) irreducible. Let \( x \in G \) have order \( p \), an odd prime not dividing \(|K| \). Then there exists \( \gamma \in C \) with \( \gamma^p = 1 \) and the primitive \( p \)th roots of 1 appearing equally often as eigenvalues of \( \gamma X(x) \).

Proof. There are \( p \) extensions of \( X|K \) to \( \langle K, x \rangle \). Let \( Y \) be one of these. Then they are all of the form \( Y \otimes A^i \) where \( A \) is a faithful linear representation of \( \langle K, x \rangle/K \). Since the character of \( X \) does not vanish on \( x \) (as \( \deg X \neq 0 \) (mod \( p \)) and since the Galois group \( \langle \sigma \rangle \) of the \( p \)th roots of 1 permutes these \( p \) representatives \( Y \otimes A^i \) it follows that exactly one of them has a rational character, since \( Y \otimes A^i = \sigma(Y \otimes A^i) = (Y \otimes A^p) \otimes A^i = Y \otimes A^{K+i} \) can be solved for \( i \).

Lemma 9. Let \( X \) be a faithful, irreducible, quasiprimitive representation of a finite group \( G \) on an \( n \)-dimensional vector space \( V \). Let \( H \) be a subgroup of \( G \) with \( H/Z(H) \cong PSL(2, p) \) for \( p \) a prime greater than four. Suppose that \( \dim C_V(H) = n - (p - 1)/2 \). Then \( \dim C_V(H) \leq 1 \).

Proof. By Lemma 3, we may replace \( H \) by \( H' \) with \( H \cong (P)SL(2, p) \). Assume that \( C_V(H) > 1 \). There are two overlapping cases:

Case 1. \( (p - 1)/2 \) is even. In this case \( H \cong SL(2, p) \). Let \( P = \langle x \rangle \) be a \( p \)-Sylow subgroup of \( H \). By [13] we may write \( X \) in matrix form in the ring of local integers of some algebraic number field for a prime ideal dividing \( (2) \). As \( (2, |P|) = 1 \), by
[13] and [10], we may further take $X|P$ to be diagonal. Let $z$ be the involution in $Z(H)$. By Lemma 2, $X(x)$ has $n-(p-1)/2$ eigenvalues 1 and $(p-1)/2$ distinct eigenvalues $e_1, \ldots, e_{(p-1)/2}$ unequal to 1. We may write

$$X(x) = \text{diag}(1, \ldots, 1, e_1, \ldots, e_{(p-1)/2}).$$

As $z \in C(x)$ and $C_r(P) = C_r(H) \subset C_r(z)$, there exist $\gamma_1$ with

$$X(z) = \text{diag}(1, \ldots, 1, \gamma_1, \ldots, \gamma_{(p-1)/2}).$$

Let $Y$ be the modular representation obtained by taking coefficients in $X$ modulo the prime ideal dividing 2. Then $z \in K$, the kernel of $Y$. By [3], $K$ is a two group. By quasiprimitivity, we may change coordinates to write $X(K)=U(K) \otimes I_m$ for some irreducible representation $U$ of $K$ and some integer $m$. By [8, Satz 3], there exist functions $V$ and $W$ from $G$ to $GL(n/m, C)$ and $GL(m, C)$ respectively with $X(g)=V(g) \otimes W(g)$ for all $g \in G$. We may also take $V(x)$ to have order $p$. Then $V(x)$ normalizes $U(K)$. By Lemma 8, $V(x)$ is scalar or has as many as $(p-1)$ distinct eigenvalues. As $X(x)$ has only $(p+1)/2$ distinct eigenvalues, $V(x)$ is scalar. As $e_1$ occurs only once as an eigenvalue of $X(x)$, $\dim V=1$. Then $X(z)$ is scalar, a contradiction.

**Case 2.** Here $(p-1)$ is not a power of 2. In this case, there exists $q$, an odd prime dividing $p-1$. Let $P=\langle x \rangle$ be a $p$-Sylow subgroup of $H$. Then there exists $y$ of order $q$ in $N_H(P)$. The normal subgroup $P^q$ generated by $P$ contains $H$. If it is reducible, then some constituent of $X|P^q$ has $H$ in the kernel, contrary to quasiprimitivity. Conjugates of $X(x)$ cannot permute spaces of imprimitivity nontrivially, for that would imply that $|\text{trace } X(x)| \leq n-p$. Therefore, $X|P^q$ is primitive. We may replace $G$ by $P^q$ and assume $G=P^q$. Then $\langle y \rangle^q \supseteq H$, $\langle y \rangle^q \supseteq H^q \supseteq P^q=H$, and $G=\langle y \rangle^q$. Write $X|H=X_1 \oplus X_2$ where $H$ is in the kernel of $X_1$ and $\deg X_2=(p-1)/2$. The constituents of $X_2|P$ are distinct and nonprincipal. Also, $y$ fixes only principal characters of $P$. Therefore, $X_2(y)=0$ and the eigenvalue 1 occurs $(p-1)/2q$ times in $X_2(y)$ and $n-((p-1)/2)-(p-1)/2q$ times in $X(y)$. If $u$ is any conjugate of $y$ in $G$ and $H_u=\langle H, u^{-1}Hu \rangle$, then

$$n-\dim C_r(H_u) \leq n-\dim C_r(\langle H, u \rangle)$$

$$= n-\dim C_r(H) \cap C_r(u) \leq n-\dim C_r(H)+n-\dim C_r(u)$$

$$= (p-1)/2+(p-1)/2-(p-1)/2q < p-1.$$

As $(p-1)/2+(p-1)/2+\dim C_r(H_u)>n$, by [6], $X|H_u$ has at most one constituent, say $X_u$ acting on the subspace $V_u$, with $i_p(X_u(H_u)) \neq 1$. By [5], $i_p(X_u(H_u)) \leq p$. Since $i_p(H)=p$, by Lemma 1, such an $X_u$ exists, $i_p(X_u(H))=i_p(X_u(u^{-1}Hu))=p$, and $X_u$ contains the nonprincipal constituent of $X|H$ and the nonprincipal constituent of $X|u^{-1}Hu$. Let $Y_u$ be a complement to $X_u$ for $X|H_u$. Then $X|H_u=Y_u \oplus X_u$. As $H$ and $u^{-1}Hu$ are in the kernel of $Y_u$, $H_u$ is in the kernel of $Y_u$ and $V=C_r(H_u) \oplus V_u$. By Lemma 4 applied to $X_u$ and $H_u$:

$$\deg X_u = (p+1)/2 \quad \text{and} \quad \dim C_r(H_u) = n-(p+1)/2.$$
If \( \text{deg} \ X_u = (p-1)/2 \), then \( u^{-1}C_v(H) = C_v(u^{-1}Hu) = C_v(Hu) = C_v(H) \). As \( C_v(H) \) is not invariant for \( G = \langle y \rangle \), we may find \( u_0 \) conjugate to \( y \) with \( \text{deg} \ X_{u_0} = (p+1)/2 \) (actually, \( \text{deg} \ X_{u_0} = (p+1)/2 \) is impossible by [12]), but we go on, anyway) and \( \dim \ C_v(H_{u_0}) = n - (p+1)/2 > 0 \). Since \( G = H^a \) and \( G = \langle y \rangle \), \( G = \langle v^{-1}Hv \rangle = u_1 \cdot \cdot \cdot u_r \), where \( u_i \) is a conjugate of \( y \) in \( G \) for \( i = 1, \ldots, r \). As \( C_v(H_{u_0}) \) is not invariant under \( X(G) \), we may find \( v = u_1 \cdot \cdot \cdot u_r \) conjugate to \( y \) for \( i = 1, \ldots, r \), with \( C_v(H_{u_0}) \) not invariant under \( v^{-1}Hv \). Then \( C_v(H_{u_0}) \neq C_v(v^{-1}Hv) \) and \( C_v(v^{-1}Hv, H_{u_0}) \neq C_v(H_{u_0}) \). Take \( v \) so that \( C_v(v^{-1}Hv, H_{u_0}) \neq C_v(H_{u_0}) \) and \( r \) is minimal. Then \( r \geq 1 \). Define \( w = u_1^{-1} = u_1 \cdot \cdot \cdot u_{r-1} \). Then \( C_v(w^{-1}Hw, H_{u_0}) = C_v(H_{u_0}) \). Letting \( w^{-1}Hw \) play the role of \( H \) and \( u_r \) play the role of \( u \), we have

\[
C_v(v^{-1}Hw, w^{-1}Hv) = C_v(w^{-1}Hw, u_r^{-1}(w^{-1}Hw)u_r) = n - (p+1)/2.
\]

As \( C_v(v^{-1}Hw, v^{-1}Hv) \subseteq C_v(w^{-1}Hw) \) and \( C_v(H_{u_0}) \subseteq C_v(w^{-1}Hw) \),

\[
\dim \ C_v(v^{-1}Hw, H_{u_0}) \geq \dim \ C_v(v^{-1}Hw, v^{-1}Hv) \cap C_v(H_{u_0})
\]

\[
\geq \dim \ C_v(w^{-1}Hw, v^{-1}Hv) + \dim \ C_v(H_{u_0}) - \dim \ C_v(w^{-1}Hw)
\]

\[
\geq n - (p+1)/2 + n - (p+1)/2 - (n - (p-1)/2) > n - (p-1).
\]

As with \( X_u \), by [6], \( X(v^{-1}Hv, H_{u_0}) \) has exactly one irreducible constituent \( W \) acting on \( U_w \) with \( i_p(W(v^{-1}Hv, H_{u_0})) \neq 1 \). By [5], \( i_p(W(v^{-1}Hv, H_{u_0})) = p \). This constituent \( W \) contains the nonprincipal constituents of \( X(v^{-1}Hv, H_{u_0}) \) so \( V = C_v(v^{-1}Hv, H_{u_0}) \oplus U_w \). By Lemma 4 applied to \( W \) and \( H_{u_0} \subset \langle v^{-1}Hv, H_{u_0} \rangle \):

\[
\text{deg} \ W = (p+1)/2, \ \dim \ C_v(v^{-1}Hv, H_{u_0}) = n - (p+1)/2 = \dim \ C_v(H_{u_0}), \ \\
C_v(v^{-1}Hv, H_{u_0}) = C_v(H_{u_0}),
\]

a contradiction.

**Proof of the theorem.** We use induction on \( n = \text{deg} \ X \) and assume that the finite group \( G \) with representation \( X \) is a counterexample to the theorem with \( n \) minimal for a fixed set of primes, \( \Pi \). By Lemma 7 we may let \( H \) be an abelian \( \Pi \)-Sylow subgroup of \( G \).

(A). If \( L \subset G \) and \( X|L \) is reducible, then \( L \) satisfies the conclusion of the theorem. In particular \( X|G \) is irreducible.

**Proof.** Let \( L \) contradict (A) and \( X|L = Y_1 \oplus Y_2 \). Then \( \text{deg} \ Y_i < n \leq p - 1 \) for all \( p \in \Pi \) and \( i = 1, 2 \). By the minimality of \( n \), \( i_{p}(Y_i(L)) \) is not composite for \( i = 1, 2 \). If for \( i = 1 \) or 2, \( \text{deg} \ Y_i < (p-1)/2 \) for all \( p \in \Pi \), then by [6], \( i_{p}(Y_i(L)) = 1 \), and by Lemma 1, \( i_{p}(L) \) is not composite. Therefore, \( \text{deg} \ Y_i = n/2 = p - 1 \) for some \( p \in \Pi \) and \( i_{p}(Y_i(L)) = p \) for \( i = 1, 2 \). Then \( i_{p}(L) = p \), or Lemma 5 applied to \( L \) gives the conclusion.

(B). We may choose \( X \) and \( G \) so that \( X \) is unimodular. Then \( H \cap Z(G) = \langle 1 \rangle \).

**Proof.** By [1], we may find a finite group \( L \) with a faithful, unimodular representation \( Y \) of dimension \( n \) with \( X(G)ZGL(n, C) = Y(L)ZGL(n, C) \). Then \( Y \) is irreducible.
Now $G$ has a $\Pi$-Sylow subgroup and $L/Z(L) \cong G/Z(G)$ has a $\Pi$-Sylow subgroup. Let $U \supseteq Z(L)$ and $UZ(L)$ be a $\Pi$-Sylow subgroup of $L/Z(L)$. As $[Z(L)]_W$ is a normal $\Pi'$-Sylow subgroup of $UZ(L)$, by Schur-Zassenhaus, $UZ(L)$ has a $\Pi$-Sylow subgroup, and this is a $\Pi$-Sylow subgroup for $L$. Now $i^n(G) = i^n(G/Z(G)) = i^n(L/Z(L)) = i^n(L)$ is composite. If $V = V_1 \oplus V_2$ gives spaces of imprimitivity for $Y(L)$, then $X(G)$ has the same spaces of imprimitivity and a normal subgroup $K$ of index 1 or 2 leaves $V_1$ and $V_2$ invariant. As $O_n(K)$ is characteristic in $K$ and $K < G$, $O_n(K) \subseteq O_n(G)$. Then $G$ satisfies whichever alternative of the conclusion of the theorem that $K$ satisfies by (A). Therefore, $Y$ and $L$ are a counterexample to the theorem and may be used to replace $X$ and $G$. Then $X$ may be taken to be unimodular. Then if $x \in H \cap Z(G)$, $X(x) = y\gamma n$ where $\gamma^n = 1$, and $\gamma$ must be 1.

(C). We may further choose $G$ with $G = O^\Pi(G) = H^G$, and with $X$ being primitive.

Proof. Both $O^p(L)$ and $H^G$ are the subgroup of $G$ generated by all $\Pi$-elements. Also, $H \subseteq H^G$. If $i^n(H^G)$ is not composite, then as $O_n(H^G)$ is characteristic in $H^G \trianglelefteq G$, $O_n(H^G) \subseteq O_n(G)$, and $i^n(G)$ is not composite, a contradiction. Suppose that $V = V_1 \oplus V_2$ and $O_n(H^G)$ is imprimitive on the $V_i$, $i = 1, 2$. As a subgroup of $H^G$ of index 2 contains all $\Pi$-elements of $H^G$ and, hence of $G$ and must equal $H^G$, it follows that $V_1$ and $V_2$ are invariant for $H^G$. As $i^n(H^G)$ is composite, by (A), $X(H^G)$ satisfies II of the theorem. As $V_1$ and $V_2$ are the unique invariant subspaces of dimension $n/2$ for $H^G < G$, $G$ is imprimitive on the $V_i$, $i = 1, 2$; and satisfies II of the theorem, a contradiction. As $O^\Pi(O^\Pi(G))$ contains all $\Pi$-elements of $O^\Pi(G)$ and of $G$, $O^\Pi(O^\Pi(G)) = O^\Pi(G)$. As $O^\Pi(G)$ is a contradiction to the theorem, we may replace $G$ by $O^\Pi(G)$. Then we have $G = O^\Pi(G) = H^G$. If $V_1, \ldots, V_m$ form spaces of imprimitivity for $G$, then $m \leq n < p$ for all $p \in \Pi$ and $\Pi$-elements must fix the $V_i$. Then $G = H^G$ fixes the $V_i$. Then, by (A), $m = 1$.

(D). If $x$ is a $\Pi$-element with an eigenvalue occurring more than $n/2$ times in $X(x)$, then $x = 1$.

Proof. Otherwise, we may take $x \in H$ of order $p$, a prime, with $X(x)$ having eigenvalues $\sigma, \sigma, \ldots, \sigma, \sigma_1, \sigma_1, \ldots, \sigma_m$, $m < n/2$. If $\langle x \rangle^G$ is abelian, then by quasiprimity, (C), $X(\langle x \rangle^G)$ has identical linear constituents and $\langle x \rangle^G \subseteq Z(G)$, a contradiction. Therefore, we may find $y$, a conjugate of $x$ not in $C(x)$. Let $K = \langle x, y \rangle$. By Lemma 7, $K$ is not a $p$-group, and $i_p(K) \neq 1$. Therefore, by Lemma 1, there exists an irreducible constituent $Y$ of $X|K$ with $i_p(Y(K)) > 1$. Now, $C_\nu(\alpha^{-1}x) \cap C_\nu(\alpha^{-1}y)$ is a sum of linear constituents for $X|K$. Also,

$$n - \dim C_\nu(\alpha^{-1}x) \cap C_\nu(\alpha^{-1}y) \leq n - \dim C_\nu(\alpha^{-1}x) + n - \dim C_\nu(\alpha^{-1}y) \leq 2n - 2m < n.$$ 

Therefore, $\deg Y < n$ and by minimality of $n$, $i_p(Y(K)) = p$. As $Y(x) \notin Z(Y(K))$, by Lemma 2, $Y(x)$ has distinct eigenvalues. Let $d$ be the number of $\alpha_1, \ldots, \alpha_m$ occurring as eigenvalues in $Y(x)$.

Then

$$n/2 \leq (p-1)/2 \leq \deg Y = \var(Y(x)) \leq 1 + d \leq 1 + m < 1 + (n/2).$$
Then \((p - 1)/2 = \deg Y = \text{var } X = 1 + d = 1 + m\). Replacing \(x\) by \(y\) above, we see that a complement \(U\) to \(Y\) for \(X/K\) has \(U(x) = U(y) = aI_{n-(p-1)/2}\). By Lemma 2 applied to \(Y(K)\), there exists \(u\) of order \(p\) in \(K'\) with \(Y(x)Y(u^{-1}) \in Z(Y(K))\) and \(Y(u)\) having \((p - 1)/2\) distinct eigenvalues, all unequal to 1. As \(u \in K'\), \(U(u) = I_{n-(p-1)/2}\). Then \(\text{var } X(u) = 1 + (p - 1)/2\). As \(Y(xu^{-1})\) and \(U(xu^{-1})\) are both scalar of order dividing \(p\), \(\text{var } X(xu^{-1}) \leq 2\). As \(X\) is primitive and \(p \geq 7\), by [1], \(X(xu^{-1})\) is scalar. Then

\[
\text{var } X(x) = \text{var } X(u) = 1 + (p - 1)/2 \geq 1 + n/2 > 1 + m,
\]

a contradiction.

(E). If \(x\) is a nonidentity \(\Pi\)-element, then \(i_{\Pi}(C(x)) = 1\).

**Proof.** Otherwise, by Lemma 1, \(X|C(x)\) has an irreducible constituent \(Y\) with \(i_{\Pi}(Y(C(x))) \neq 1\). By [6], \(\deg Y \geq (p - 1)/2\) for some \(p \in \Pi\). Then some eigenvalue occurs in \(X(x)\) with multiplicity \(m \geq (p - 1)/2 \geq n/2\). By (D), \(m = (p - 1)/2 = n/2\) and \(n + 1 \in \Pi\). Let \(U\) be a complementary constituent to \(Y\) for \(X|C(x)\). If \(U(C(x))\) does not have a normal abelian \(p\)-Sylow subgroup, then by [6], \(U\) is irreducible, \(\text{var } X(x) \leq 2\), \(\text{var } X(x) = 1\) by [1] and primitivity, \(x \in Z(G)\), and by (B) \(x = 1\), a contradiction. Therefore, \((O^\Pi(C(x)))'\) is in the kernel of \(U\). By Lemma 3,

\[
Y((O^\Pi(C(x)))') \simeq (P)\text{SL}(2, p).
\]

Then \((O^\Pi(C(x)))'\) contradicts Lemma 9.

(F). \(H\) is a trivial intersection set (T. I. S.) in \(G\).

**Proof.** Let \(x \in H^\# \cap g^{-1}Hg\). Then \(H, g^{-1}Hg \in C(x)\). By (E), \(i_{\Pi}(C(x)) = 1\). Then \(H = O_{\Pi}(C(x)) = g^{-1}Hg\).

(G). If \(K \leq G\) and \(O_{\Pi}(K) \neq \langle 1 \rangle\), then \(i_{\Pi}(K) = 1\).

**Proof.** Let \(K\) contradict (G). If \(x\) is a \(\Pi\)-element of \(K\), then \(\langle x, O_{\Pi}(K) \rangle\) is a \(\Pi\)-group, and by Lemma 7, \(x \in C(O_{\Pi}(K))\). Therefore, \(O_{\Pi}(K) \subset C(O_{\Pi}(K)) \subset C(y)\) for some nonidentity \(\Pi\)-element \(y\) in \(O_{\Pi}(K)\). By (E) and Lemma 1, \(i_{\Pi}(O_{\Pi}(K)) = 1\). Then \(O_{\Pi}(K)\) is a normal \(\Pi\)-Sylow subgroup of \(K\).

(H). If \(x \notin Z(G)\), then \(i_{\Pi}(C(x)) = 1\).

**Proof.** As \(C([x]_{\Pi}) \supseteq C(x)\), by (E) and Lemma 1, we may assume that \(x\) is a \(\Pi\)-element contradicting (H). By (G), \(O_{\Pi}(C(x)) = \langle 1 \rangle\). By (A) applied to \(C(x)\), \(i_{\Pi}(C(x)) = p\) for some \(p \in \Pi\); otherwise, the \(\Pi\) of the theorem gives a subgroup contradicting Lemma 9. Therefore, \(|C(x)|_{\Pi} = p\). Replacing \(x\) by a conjugate of \(x\) there exists a \(p\)-Sylow subgroup \(P = \langle y \rangle\) of \(C(x)\) contained in \(H\).

If \(X|C(x)\) has two constituents \(X_1\) and \(X_2\) with \(i_p(X_1(C(x))) = p\) for \(i = 1, 2\), then, by [6], \(X|C(x) = X_1 \oplus X_2\) with \(p = (n + 1) \in \Pi\), \(\deg X_i = (p - 1)/2\), and \(X_i(C(x))/Z(X_i(C(x))) \simeq (P)\text{SL}(2, p)\) for \(i = 1, 2\). By Lemma 3, there is a subgroup \(K\) of \(C(x)\) with \(K \simeq (P)\text{SL}(2, p)\), and \(X_i\) are either the two distinct \((p - 1)/2\) dimensional representations of \((P)\text{SL}(2, p)\) or are identical. In the first case, \(X(y)\) has mutually distinct eigenvalues and \(C(y)\) is abelian. Then \(\langle H, x \rangle \subseteq C(y)\) and \(H \subseteq C(x)\) contrary to \(|C(x)_{\Pi}| = p\). In the second case, we may change coordinates to write
$X|K = X_1 \otimes I_2$ and apply Lemma 6 with $A = H, L = K$ to conclude that $X|\langle H, K \rangle$ is reducible. We may apply (A) to $\langle H, K \rangle$. As II of the theorem gives a subgroup contradicting Lemma 9, $i_{n}(\langle H, K \rangle)$ is not composite, $O_{n}(\langle H, K \rangle) \neq \langle 1 \rangle$. By (G), $i_{n}(\langle H, K \rangle) = 1$. Then $p \leq i_{n}(K) \leq i_{n}(\langle H, K \rangle) = 1$, a contradiction.

Therefore, $X|C(x)$ has exactly one irreducible constituent, say $Y$ acting on the subspace $S$, with $i_{p}(Y(C(x))) \neq 1$. Let $U$, acting on the subspace $T$, be a complement to $Y$ for $X|C(x)$. Let $K = (O_{p}'(C(x)))'$. Then $K \leq \ker U$. By Lemma 2, there exists $u$ of order $p$ in $K$ with $Y(u)$ having $m \geq (p-1)/2$ eigenvalues unequal to 1. As $|C(x)|_p = p$, we may choose $u$ to be $y$. Let $W = \sum_{\beta \neq \gamma} C_{p}(\beta^{-1}y)$. Then $W \subseteq S$. Also, $m = \dim W$, and $m \geq (p-1)/2$. Furthermore, $X(x)$ acts as a scalar on $S$, and, therefore, also on $W$. As $\langle H, x \rangle \subseteq C(y)$, $W$ is invariant under $\langle H, x \rangle$. For any $h \in H$, $X((h, x))$ acts as a scalar on $W$ and $X((h, x))$ has at least $m$ eigenvalues equal to 1. As $H$ is a T. I. S. and $y \in H \cap C(x)$, $x \in N(H)$ and $(h, x) \in H$. By (D), $(p-1)/2 \leq m \leq n/2$ or $(h, x) = 1$. Therefore, $2m+1 = p = (n+1) \in \Pi$ or $H \subseteq C(x)$. As $|C(x)|_p = p$, $2m+1 = p = (n+1) \in \Pi$. Then $\deg Y = (p+1)/2$, otherwise, $K$ contradicts Lemma 9. Now $T \oplus S = V = C_{p}(y) \oplus W$ with $C_{p}(y)$ and $W$ invariant under $\langle H, x \rangle$. By Lemma 2, $Y \mid K$ is reducible. Let $h$ be any element of $H$. Then $C_{p}(h^{-1}Kh) = h^{-1}C_{p}(K) \subseteq h^{-1}(C_{p}(y)) = C_{p}(y)$. Then

$$\dim C_{p}(h^{-1}Kh) = \dim C_{p}(K) \cap C_{p}(h^{-1}Kh) \geq \dim C_{p}(K) + \dim C_{p}(h^{-1}Kh) - \dim C_{p}(y) = (p-3)/2 + (p-3)/2 - (p-1)/2 = (p-5)/2 > 0.$$ 

Then by [6] and Lemma 1, $X|\langle K, h^{-1}Kh \rangle$ has at most one constituent $R$ with $i_{p}(R(\langle K, h^{-1}Kh \rangle)) \neq 1$. The constituent $R$ must contain the constituent $Y$ for $R|K$. As $\deg R < n$, by minimality of $n$, $i_{p}(R(\langle K, h^{-1}Kh \rangle)) = p$. By Lemma 4 applied to $R$ and $K \subseteq \langle K, h^{-1}Kh \rangle$, $\deg R = \deg Y$. Then $S$ is invariant under $X(h)$. As $X(x)$ is scalar on $S$, $S \subseteq C_{p}(h, x)$ and by (D), $(h, x) = 1$. Then $H \subseteq C(x)$ a contradiction.

(I). Let $N_0 = \{\bigcup_{1 \neq \gamma \in \gamma} C(y)\} - Z(G)$. Then if $g \notin N(H), N_0 \cap g^{-1}N_0 g$ is empty.

**Proof.** Let $x \in N_0 \cap g^{-1}N_0 g$. Then there exist $h, k \neq 1, h, k \in H$ with $h, g^{-1}kg \in C(x)$. By (H), $i_{n}(C(x)) = 1$, so $h, g^{-1}kg \in O_{n}(C(x))$. By Lemma 7, $O_{n}(C(x)) \subseteq C(h), C(g^{-1}kg)$. As $H$ is a T. I. S., $O_{n}(C(x)) \subseteq N(H), N(g^{-1}Hg)$. Then $O_{n}(C(x))$, $H \cap g^{-1}Hg$ are $\Pi$-groups, and $\langle h \rangle \subseteq O_{n}(C(x)) \subseteq H \cap g^{-1}Hg$. Then $H = g^{-1}Hg$.

(II). By (C) and (I), $H \subseteq G$ satisfies the hypothesis of Lemma 4.2 of [5], by which $n+1 > |H|^{1/2} \geq p$ for some $p$ in $\Pi$, a contradiction.

**BIBLIOGRAPHY**


The RAND Corporation, Santa Monica, California 90406