FINITE LINEAR GROUPS OF PRIME DEGREE

DAVID B. WALES

1. Introduction and notation. If G is a finite group which has a faithful complex representation of degree n it is said to be a linear group of degree n. It is convenient to consider only unimodular irreducible representations. For $n \leqq 4$ these groups have been known for a long time. An account may be found in Blichfeldt's book (**1**). For $n = 5$ they were determined by Brauer in (**4**). In (**4**), many properties of linear groups of prime degree p were determined for p a prime greater than or equal to 5.

In a forthcoming series of papers these results will be extended and the linear groups of degree 7 determined. In the first paper, some general results on linear groups of degree p, $p \geqq 7$, will be given. These results will later be applied to the prime $p = 7$.

We only consider linear groups which are primitive. This means that for a prime degree p the representation cannot be written in monomial form. Equivalently, the group has no normal abelian subgroups not contained in the centre. If G is an imprimitive linear group of degree p, there is a normal abelian subgroup K such that G/K is isomorphic to a subgroup of S_p, the symmetric group on p elements.

In § 2 a bound is obtained for the order of a p-Sylow group of a primitive linear group of degree p. In § 3 a certain configuration described in (**4**) is shown to exist only in a trivial case. In § 4, it is shown that the character of the representation is rational or at least real when restricted to certain p-regular elements. This is used to restrict the power of certain primes other than p in the group order. Finally, in § 5 we prove a short theorem which states that for primes $p/2 < q < p$ and $q \geqq 7$ the q-Sylow group is abelian. This is also true if $q = 5$ but the proof is more involved. As it is only needed for $p = 7$, it is treated later when linear groups of degree 7 are considered explicitly.

Notation. Let G be a finite group with a faithful irreducible representation X of degree p over the complex numbers. We denote by χ the character associated to X. Here X will be assumed primitive and unimodular; p is a prime greater than 5. If S is a subset of G, we let $|S|$ be the cardinality of S, $N(S)$ the normalizer of S, and $C(S)$ the centralizer of S. If H is a subgroup, the centre of H, $C(H) \cap H$, is denoted by $Z(H)$. The centre of G, $Z(G)$, is denoted by Z. Let $|G| = g = p^a \cdot g_0$, $(p, g_0) = 1$. It was shown in (**4**, § 4) that if $a = 1$,

Received August 11, 1967. This work was part of the author's Ph.D. thesis at Harvard University in 1967. It was supported by a Canadian National Research Council Special Scholarship.

then $Z = e$; if $a > 1$, then Z is cyclic of order p. If q is a prime, then a q-Sylow group is denoted by P_q. If $q = p$ we drop the subscript and write P.

Let A be an abelian group and Γ a faithful representation of it. Suppose that $\Gamma = \sum_{i=1}^{m} a_i \xi_i$, with a_i integers and ξ_i distinct linear characters of A. The number m is called the variety of A.

We denote by K the splitting field of G given by Q with the gth roots of unity adjoined. As is standard, we let $O_p(G)$ $(O_{p'}(G))$ be the maximal normal p-group (p'-group), of G and $O^p(G)$ $(O^{p'}(G))$ the minimal normal group whose quotient is a p-group (p'-group).

Acknowledgement. I wish to thank Professor R. Brauer for his help and encouragement.

2. A bound for the value a. Our goal in this section is to show that $a \leqq \frac{1}{2}(p + 1)$. This is done by showing that there is an element ξ in a p-Sylow group P of G such that $X(\xi)$ has $\frac{1}{2}(p - 1)$ eigenvalues $\epsilon = e^{2\pi i/p}$, $\frac{1}{2}(p - 1)$ eigenvalues $\bar{\epsilon}$, and one eigenvalue 1. For $p \geqq 7$ this contradicts Blichfeldt's theorem (**1**, p. 96). Blichfeltd's theorem states that if G is primitive, the eigenvalues of $X(\xi)$ for any ξ in $G - Z$ cannot all lie within 60° of any particular eigenvalue of $X(\xi)$.

We need notation for some standard concepts. If t is an integer not congruent to 0 (mod p) let σ_t be the permutation of the set $\{1, 2, \ldots, p\}$ mapping j onto $\sigma_t(j)$, where $\sigma_t(j) \equiv tj \pmod p$. Here $j = 1, 2, \ldots, p$. Let D be the set of diagonal $p \times p$ matrices with diagonal entries complex numbers. If $(d) \in D$, let $(d)_{ii}$ be the number in the ith row and ith column of (d). Let R_t be the map of D to itself defined by

$$(R_t(d))_{i,i} = (d)_{\sigma_t(i),\sigma_t(i)}.$$

It is clear that R_t permutes the diagonal entries of d. One sees easily that if d_1 and d_2 are in D and $u \not\equiv 0 \pmod p$, then

$$R_t(d_1 d_2) = R_t(d_1)R_t(d_2), \qquad R_{tu}(d_1) = R_t\{R_u(d_1)\}.$$

We assume now in this section that $a \geqq 4$. The structure of a p-Sylow group P of G has been determined in (**4**, § 4). These results show that P contains normal abelian subgroups A_i, $i = 1, 2, \ldots, a - 1$, with $|A_i| = p^{a-i}$. There are independent elements $\xi_1, \xi_2, \ldots, \xi_{a-1}$ of order p such that A_i is generated by $\xi_{a-i}, \xi_{a-i+1}, \ldots, \xi_{a-1}$ for each $i = 1, 2, \ldots, a - 1$. We denote A_1 by A. A basis for the representation space can be chosen so that

$$(X(\xi_{a-k}))_{ij} = \delta_{ij}\epsilon^{\binom{j-1}{k-1}}.$$

Here

$$\epsilon = e^{2\pi i/p}, \qquad \binom{r}{s} = \frac{r(r-1)\ldots(r-s+1)}{s!}, \qquad \binom{r}{0} = 1,$$

$$k = 1, 2, \ldots, a - 1, \quad \text{and} \quad i, j = 1, 2, \ldots, p.$$

Also, $(X(\xi))_{ij}$ denotes the element in the ith row and jth column of the matrix $X(\xi)$ with respect to this basis.

Let D_1 be the subset of D consisting of matrices $X(\xi)$ for $\xi \in A$. The map R_t is a group homomorphism of D_1 onto a set $R_t(D_1)$. We will show that, in fact, $R_t(D_1)$ is D_1 itself and hence R_t is a group homomorphism of D_1 to D_1. In fact, we show the stronger statement that $R_t\{X(A_j)\} = \{X(A_j)\}$ for $j = 1, 2, \ldots, a-1$.

THEOREM 2.1. *For each j, $j = 1, 2, \ldots, a-1$, there are integers $S_{j1}, S_{j2}, \ldots, S_{jj}$ such that $R_t(X(\xi_{a-j})) = X(\xi'_{a-j})$, where $\xi'_{a-j} = (\xi_{a-1})^{S_{j1}}(\xi_{a-2})^{S_{j2}} \ldots (\xi_{a-j})^{S_{jj}}$. Furthermore, $S_{j1}, \ldots, S_{jj}$ are unique* (mod p) *with $S_{jj} \equiv t^{j-1}$* (mod p).

Proof. We recall that

$$(X(\xi_{a-j}))_{ii} = \epsilon^{\binom{i-1}{j-1}}.$$

If we replace σ_t by σ, we have:

$$(R_t(X(\xi_{a-j})))_{ii} = \epsilon^{\binom{\sigma(i)-1}{j-1}}, \qquad i = 1, 2, \ldots, p.$$

We must find integers $S_{j1}, \ldots, S_{jj}$ such that

$$\epsilon^{\binom{\sigma(i)-1}{j-1}} = \epsilon^{\binom{i-1}{0}S_{j1}}\epsilon^{\binom{i-1}{1}S_{j2}} \ldots \epsilon^{\binom{i-1}{j-1}S_{jj}} \tag{2.1}$$

for $i = 1, \ldots, p$; $j = 1, \ldots, a-1$. This is equivalent to

$$\binom{\sigma(i)-1}{j-1} \equiv \binom{i-1}{0}S_{j1} + \binom{i-1}{1}S_{j2} + \ldots + \binom{i-1}{j-1}S_{jj} \pmod{p}. \tag{2.1*}$$

Let x be an indeterminant over the integers. Consider the polynomial equation

$$(j-1)!\binom{xt-1}{j-1} = (j-1)!\left\{\binom{x-1}{0}S_{j1} + \binom{x-1}{1}S_{j2} + \ldots + \binom{x-1}{j-1}S_{jj}\right\}. \tag{2.2}$$

The coefficients are all integers as each side is multiplied by $(j-1)!$. Here, $j = 1, 2, \ldots, a-1$. Since $a \leqq p-1$, $(j-1)! \not\equiv 0$ (mod p). Suppose that (2.2) is satisfied for integers $S_{j1}, \ldots, S_{jj}$. By letting $x = i = 1, 2, \ldots, p$ and reducing (mod p), we see that (2.1)* is satisfied as $\sigma(i) \equiv it$ (mod p). It is only then necessary to show that (2.2) can be satisfied.

We now show that S_{jr} can be defined inductively to satisfy (2.2) in terms of S_{jk}, $k < r$. For $r = 1$, set $x = 1$. Equation (2.2) is then

$$(j-1)!\binom{t-1}{j-1} = (j-1)!S_{j1}.$$

This shows that $S_{j1} = \binom{t-1}{j-1}$. In general, setting $x = r$, (2.2) becomes

$$(j-1)!\binom{rt-1}{j-1} = (j-1)!\left\{\binom{r-1}{0}S_{j1} + \binom{r-1}{1}S_{j2} + \ldots + S_{jr}\right\}.$$

This shows that S_{jr} can be defined inductively. The values S_{jr} obtained for $r = 1, 2, \ldots, j$ satisfy (2.2) for $x = 1, 2, \ldots, j$. Furthermore, (2.2) is a polynomial equation in x of degree $j - 1$. As both sides agree for j values of x, both sides agree for all values of x. We note that the coefficient of x^j on the left of (2.2) is t^{j-1}. On the right it is S_{jj}. This shows that $S_{jj} = t^{j-1}$. The values $S_{j1}, \ldots, S_{jj}$ can be seen to be unique (mod p) by noticing, as for (2.2), that S_{jr} can be defined inductively in terms of S_{jk}, $k = 1, 2, \ldots, r - 1$. The proof of the theorem is complete.

We can now define a homomorphism S_t of A to A in the following way. If $\xi \in A$, then $S_t(\xi) = \xi'$, where $R_t(X(\xi)) = X(\xi')$. This is well-defined as X is faithful. Furthermore, R_t has kernel I, where I is the identity $p \times p$ matrix. This means that S_t has kernel e, the identity of G. We see that S_t is an automorphism of A. Since $R_tR_u = R_{tu}$, we have $S_tS_u = S_{tu}$, where $t, u \not\equiv 0 \pmod p$.

The automorphism S_t can be considered as a linear transformation of the vector space A. Here A is a vector space of dimension $a - 1$ over the integers (mod p). As usual for linear transformations we can describe S_t by a matrix (S_t). We use the basis $(\xi_{a-1}, \ldots, \xi_1)$. The jth row of (S_t) is $(S_{j1}, \ldots, S_{jj}, 0, \ldots, 0)$. Let $y_1, \ldots, y_{a-1}$ be integers (mod p). If the element

$$(\xi_{a-1})^{y_1}(\xi_{a-2})^{y_2}\ldots(\xi_1)^{y_{a-1}}$$

is denoted by $(y_1, \ldots, y_{a-1})$, S_t maps $(y_1, \ldots, y_{a-1})$ onto $(y_1, \ldots, y_{a-1})(S_t)$. We now come to the main theorem of this section.

THEOREM 2.2 (cf. **4**, 4C). *If* $|G| = p^a g_0$, $p \geqq 7$, *then* $a \leqq \frac{1}{2}(p + 1)$.

Proof. Suppose that $a \geqq \frac{1}{2}(p + 3)$. Let t be a primitive root (mod p). The matrix (S_t) has eigenvalues $1, t, t^2, \ldots, t^{a-2}$. The matrix $(S_t)^2$ has eigenvalues $1, t^2, t^4, \ldots, t^{(a-2)2}$. Since $a \geqq \frac{1}{2}(p + 3)$, there are at least $\frac{1}{2}(p + 1)$ rows in $(S_t)^2$. The eigenvalue in the $\frac{1}{2}(p + 1)$st row is $t^{\frac{1}{2}(p-1)^2} = 1$. This means that $(S_t)^2$ has two eigenvalues 1. As the eigenvalues of S_t are distinct, S_t can be diagonalized. This means that $(S_t)^2$ can be diagonalized, and hence there are two independent eigenvalues with eigenvalue 1. This also follows since (S_t) has order prime to p. One of the eigenvectors is $(1, 0, \ldots, 0)$. Let an independent eigenvector be $(\tau_1, \ldots, \tau_{a-1})$. The element ξ in A corresponding to this vector satisfies $S_{t^2}(\xi) = \xi$, or $R_t(X(\xi)) = X(\xi)$. The permutation σ_{t^2} is the permutation $(1, t^2, \ldots, t^{\frac{1}{2}(p-3)})(t, t^3, \ldots, t \cdot t^{\frac{1}{2}(p-3)})$. This means that the coefficients of $X(\xi)$ in rows $1, t^2, t^4, \ldots, t^{\frac{1}{2}(p-3)}$ are equal. The same is true for the rows $t, t^3, \ldots, t \cdot t^{\frac{1}{2}(p-3)}$. An appropriate element $\xi^r(\xi_{a-1})^s$ has one eigenvalue 1, $\frac{1}{2}(p - 1)$ eigenvalues ϵ, and $\frac{1}{2}(p - 1)$ eigenvalues $\bar{\epsilon}$. Here, $\epsilon = e^{2\pi i/p}$. This contradicts Blichfeldt's theorem (**2**, p. 96) and shows that $a \leqq \frac{1}{2}(p + 1)$.

3. Non-abelian Sylow intersection groups. We now turn to a discussion of the case described in (**4**) for which non-abelian p-Sylow intersection groups occur. In this situation there are two p-Sylow groups P and P^μ, $\mu \in G$, such that $P \cap P^\mu = D$. Here D is non-abelian of order p^3 and $N(D)/D \cong \mathrm{SL}(2, p)$. The following theorem shows that this case arises only in the special case that $N(D) = G$.

The idea for the proof of the following theorem was suggested by D. Gorenstein of Northeastern University.

THEOREM 3.1. *If G contains a non-abelian Sylow intersection group D, then $a = 4$, $D \lhd G$, and $G/D \cong \mathrm{SL}(2, p)$.*

The following proof holds for $p = 5$ as well. The theorem for $p = 5$ can also be found in (**4**, 9A).

Proof. The proof is in several parts. The idea is to consider $C(\eta)$, where η is an involution in $N(D)$. We will show that the only involution in $C(\eta)$ is η itself. This shows that a 2-Sylow group of G contains only one involution. Results of (**6**) can be applied to yield $a = 4$ and $D \lhd G$.

(1) Set $M = N(D)$. We will show in this part that M contains a subgroup M_0 isomorphic to $\mathrm{SL}(2, p)$. By (**4**, 5C) we have $M/D \cong \mathrm{SL}(2, p)$. Let η be an involution in M. Clearly, η is not in D as $|D| = p^3$. As M/D has exactly one involution, it must be $\bar{\eta}$, where $\bar{\eta}$ is the image of η under the canonical homomorphism of M into M/D. Any involution in M must therefore be of the form ηd, where $d \in D$.

Let D^* be the group $\langle D, \eta\rangle$ of order $2p^3$. Clearly, $\langle\eta\rangle$ is a 2-Sylow group, and hence all involutions in D^* are conjugate to η by an element of D. The number of such conjugates must be $|D|/|C_D(\eta)|$. Here $C_D(\eta) = C(\eta) \cap D$. The isomorphism $M/D \cong \mathrm{SL}(2, p)$ is obtained by noting the way in which any element of M transforms D/Z under conjugation. The involution η inverts elements in G/Z. Its matrix is

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The only elements in D centralized by η are the elements of Z. The number of conjugates of η in D^* is therefore $p^3/p = p^2$. This means that there are p^2 conjugates of η in M.

Let $M_1 = C_M(\eta) = C(\eta) \cap M$. As there are p^2 conjugates of η in M, we see that $|M:M_1| = p^2$. Since $D \cap M_1 = Z$, this yields $M_1D = M$. By the isomorphism theorem, $\mathrm{SL}(2, p) \cong M/D \cong M_1D/D \cong M_1/(M_1 \cap D) \cong M_1/Z$. We can use Grün's theorem (**14**, p. 173) on M_1 to obtain a subgroup $M_0 = M_1'$ such that $M_0 \cong \mathrm{SL}(2, p)$. Grün's theorem on M_1 yields a normal subgroup M_0 of index p as $Z \in Z(M_1)$. This subgroup could not contain Z, otherwise M_1' would be a p'-group and thus M_1 would be p-solvable. Clearly, $M_1 \cong M_0 \times Z$, and therefore $M_0 = M_1'$ and $M_0 \cong M_1/Z \cong \mathrm{SL}(2, p)$. Clearly $\eta \in M_0$.

(2) Again consider the group $D^* = \langle D, \eta \rangle$. Since $X|D$ is irreducible, $X|D^*$ is irreducible. Since $|D^*| = 2p^3$, X is of 2 defect 1 and thus has $\langle \eta \rangle$ as a cyclic defect group. This implies that $\chi(\eta) = \pm 1$. A more elementary way to see this is to note that the centralizer in D^* of η has order $2p$. If $\chi(\eta) \neq \pm 1$, the sum $(\chi(\eta))^2$ over the $p - 1$ conjugates of χ is greater than $2p$.

The sign of $\chi(\eta)$ can be determined by the unimodularity of $X(\eta)$. We see that $X(\eta)$ must have $\frac{1}{2}(p + \delta)$ eigenvalues 1 and $\frac{1}{2}(p - \delta)$ eigenvalues -1. Here, $\delta = 1$ if $p \equiv 1 \pmod 4$ and $\delta = -1$ if $p \equiv 3 \pmod 4$. This implies that $\chi(\eta) = \delta$.

(3) Let ξ be an element of order p in M_0. We can assume that ξ is in P. The notation of (**4**) will be used. Here $D = \langle \tau, \xi_{a-2}, \xi_{a-1} \rangle$. Furthermore, $A = \langle \xi_{a-1}, \xi_{a-2}, \ldots, \xi_1 \rangle$ and $Z = \langle \xi_{a-1} \rangle$. We have the relations $(\tau)^{\xi_{a-t}} = \tau(\xi_{a-t+1})^{-1}$ for $t = 2, 3, \ldots, a - 1$. Since $\xi \in C(\eta)$, we have $\chi(\xi) \neq 0$ for if $\chi(\xi) = 0$, the constituents of $X(\xi)$ are all distinct and so by (**4**, 3F), $2 \nmid |C(\xi)|$. This implies that $\xi \in A$, as for elements $\xi \in P - A$, $\chi(\xi) = 0$. Let $x_1, x_2, \ldots, x_{a-1}$ be integers, $0 \leqq x_i \leqq p - 1$, such that

$$\xi = (\xi_{a-1})^{x_1}(\xi_{a-2})^{x_2} \ldots (\xi_1)^{x_{a-1}}.$$

We know that ξ normalizes D as $\xi \in M$. Our relations yield

$$\tau^{\xi} = \tau(\xi_{a-1})^{-x_2}(\xi_{a-2})^{-x_3} \ldots (\xi_2)^{-x_{a-1}}.$$

Since $D = \langle \tau, \xi_{a-1}, \xi_{a-2} \rangle$ and $\tau^{\xi} \in D$, we must have $x_4 = x_5 = \ldots = x_{a-1} = 0$. This means that $\xi \in A_{a-3} = \langle \xi_{a-1}, \xi_{a-2}, \xi_{a-3} \rangle$. By (**4**, 4E), the characteristic roots of $X(\xi)$ have multiplicity at most 2.

(4) Let $W_1 = C(\eta)$. Clearly $M_0 \subseteq M_1 \subseteq W_1$. Since $\eta \in Z(W_1)$ and $X(\eta)$ has $\frac{1}{2}(p + \delta)$ eigenvalues 1, $\frac{1}{2}(p - \delta)$ eigenvalues -1, $X|W_1$ must split into components Y_1 and Y_2 of degrees $\frac{1}{2}(p + 1)$ and $\frac{1}{2}(p - 1)$, respectively. $Y_1(\eta)$ has eigenvalues δ; $Y_2(\eta)$ has eigenvalues $-\delta$.

Since $M_0 \subseteq W_1$, we can consider $Y_i|M_0$, $i = 1, 2$. These are representations of $M_0 \cong \mathrm{SL}(2, p)$. There are five irreducible characters of $\mathrm{SL}(2, p)$ whose degrees are smaller than $p - 1$. These are in two p-blocks, $B_0(p)$ and $B_1(p)$. In $B_0(p)$ there is the principal character and two p-conjugate characters of degree $\frac{1}{2}(p + \delta)$. The kernel of these p-conjugate characters is $\langle \eta \rangle$. In $B_1(p)$ there are two p-conjugate characters of degree $\frac{1}{2}(p - \delta)$. These characters are faithful.

Let t be a primitive root mod p and

$$\omega_1 = \sum_{s=0}^{\frac{1}{2}(p-3)} \epsilon^{(t)^{2s}}, \qquad \omega_2 = \sum_{s=0}^{\frac{1}{2}(p-3)} \epsilon^{(t)^{2s+1}}.$$

The exceptional characters have value ω_1 or ω_2 on a p-element if the degree is $\frac{1}{2}(p - 1)$ and $\omega_1 + 1$ or $\omega_2 + 1$ if the degree is $\frac{1}{2}(p + 1)$. In each case, the corresponding eigenvalues are all distinct.

The representations $Y_i|M_0$, $i = 1, 2$, must have characters corresponding to sums of these characters. Let y_i be the character of Y_i. The eigenvalues of

$X(\xi)$ have multiplicity at most two and are not all distinct. If any of the $Y_i|M_0$ are the identity, the multiplicity is greater than 2 except in the case $p = 5$. In the case $p = 5$, if $Y_2|M_0$ is the identity, η is in the kernel of X. The value of $\chi(\xi)$ must be $y_1(\xi) + y_2(\xi)$ which can only be $1 + \omega_1 + \omega_1$ or $1 + \omega_2 + \omega_2$. By replacing X by a conjugate or ξ by a power, we can assume that $\chi(\xi) = 1 + 2\omega_1$. Clearly $y_1(\xi) = 1 + \omega_1$, $y_2(\xi) = \omega_1$. We know that $Y_1(\eta) = \delta I$, $Y_2(\eta) = -\delta I$. The representation $Y_i|M_0$ such that $Y_i(\eta) = -I$ must be irreducible and in $B_1(p)$. The other component $Y_j|M$ must then correspond to an exceptional character and, by comparing degrees, be irreducible. It is in $B_0(p)$.

Let L and $K(C)$ be the $\frac{1}{2}(p - 1) \times \frac{1}{2}(p - 1)$ matrices

$$L = \begin{bmatrix} \epsilon & 0 & \cdot & \cdot & & \cdot & \cdot & 0 \\ 0 & \epsilon^{t^2} & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & 0 & & & & & & \cdot \\ \cdot & \cdot & & & & & & \cdot \\ & & & & & & & \\ & & & & & & & \cdot \\ \cdot & & & & & & & \cdot \\ \cdot & & & & & & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & \epsilon^{t^{(p-3)}} \end{bmatrix};$$

$$K(C) = \begin{bmatrix} 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdot & \cdot & & & 0 \\ \cdot & & & & & & & & \cdot \\ \cdot & & & & & & & & \cdot \\ & & & & & & & & \cdot \\ & & & & & & & & \cdot \\ \cdot & & & & & & & 0 & 0 \\ \cdot & & & & & & 0 & 1 & 0 \\ 0 & \cdot & \cdot & & & \cdot & \cdot & 0 & 1 \\ C & 0 & \cdot & \cdot & & \cdot & \cdot & 0 & 0 \end{bmatrix}.$$

There is an element ϕ in M_0 such that $\xi^\phi = \xi^{t^{p-3}}$. If ξ has the representation in SL$(2, p)$ as $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ we can let ϕ be $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{p-2} \end{smallmatrix}\right)$. The basis for the representation spaces can be chosen so that

$$\begin{aligned} &Y_2(\xi) = L, && Y_1(\xi) = L \oplus 1; && \\ &Y_2(\phi) = K(-1), && Y_1(\phi) = K(1) \oplus -1 && \text{if } p \equiv 1 \pmod 4; \\ &Y_2(\phi) = K(1), && Y_1(\phi) = K(-1) \oplus -1 && \text{if } p \equiv 3 \pmod 4. \end{aligned}$$

Each $Y_i|M_0$ is irreducible, and hence each Y_i is irreducible on W_1.

(5) Let P_0 be a p-Sylow group of W_1 containing ξ and Z. If ξ_0 is in P_0, then

ξ_0 commutes with η and thus $\chi(\xi_0) \neq 0$ (**4**, 3F). Let Q be a p-Sylow group of G containing P_0, say $Q = P^{\mu_1}$ with $\mu_1 \in G$. If ρ is in Q and not in A^{μ_1}, $\chi(\rho) = 0$. This shows that $P_0 \subseteq A^{\mu_1}$. We see that P_0 must be abelian since A^{μ_1} is abelian. Elements in P_0 therefore commute with ξ. This means that $Y_i(\xi)$ commutes with $Y_i(\xi_0)$ and since the eigenvalues of $Y_i(\xi)$ are all distinct, the matrix $Y_i(\xi_0)$ must be diagonal. Let

$$Y_2|P_0 = \oplus \sum_{i=1}^{\frac{1}{2}(p-1)} \lambda_i$$

with the λ_i linear characters of P_0.

As η centralizes P_0, $X|P_0$ must have a multiple constituent (**4**, 3F). We know that $Y_i(\xi)$ has distinct constituents and so $Y_i|P_0$ must have distinct constituents. This means that $Y_1|P_0$ and $Y_2|P_0$ must have a constituent in common. In the basis chosen, we can apply the matrix $Y_i(\phi)$, $\frac{1}{2}(p-1)$ times, to obtain:

$$(3.1) \qquad Y_1|P_0 = \oplus \sum_{i=1}^{\frac{1}{2}(p-1)} (\lambda_i \oplus \lambda_p), \qquad Y_2|P_0 = \oplus \sum_{i=1}^{\frac{1}{2}(p-1)} \lambda_i.$$

Here λ_p is a linear character of P_0.

(6) Let L_i be the kernel of Y_i, $i = 1, 2$. Suppose that $\xi_0 \in P_0 \cap L_2$. We have $Y_2(\xi_0) = I$, and hence $\lambda_j(\xi_0) = 1, j = 1, 2, \ldots, \frac{1}{2}(p-1)$. This implies that $\lambda_p(\xi_0) = 1$, and thus $\xi_0 = e$. If $\xi_0 \in P_0 \cap L_1$, we have $\lambda_j(\xi_0) = 1$, $j = 1, 2, \ldots, \frac{1}{2}(p-1), p$, and again $\xi_0 = e$. This shows that $P_0 \cap L_i = e$, $i = 1, 2$. Consequently, $p \nmid |L_i|$. Furthermore, we know that $L_1 \cap L_2 = e$ since $Y_1 \oplus Y_2 = X|W_1$ is faithful.

(7) In this section we show that $|P_0| = p^2$. Suppose then that $|P_0| = p^b$, $b > 2$. Y_1 and Y_2 are representations of W_1 of degree less than $p - 1$ and thus Feit's theorem (**8**) can be applied. Here Y_i is a faithful representation of W_1/L_i. We set $|W_1/L_i| = p^b\omega_i$, where $(p, \omega_i) = 1$. Feit's theorem gives two normal subgroups R_i such that $L_i \lhd R_i \lhd W_i$, $|R_i/L_i| = p^b$ or p^{b-1}. If $|R_i/L_i| = p^b$, there would be a normal series $e \lhd L_i \lhd R_i \lhd W_1$ and W_1 would be p-solvable. This is impossible since $M_0 \subseteq W_1$, and $M_0 \cong \mathrm{SL}(2, p)$ is a p-unsolvable group. This means that $|R_i/L_i| = p^{b-1}$.

Clearly, $|R_1R_2|$ is divisible by p^{b-1} as $|R_1|$ is divisible by p^{b-1}. Suppose that $p^b \mid |R_1R_2|$. This would imply that a full p-Sylow group of W_1 would be contained in R_1R_2 and so M_0 would be in R_1R_2. This would imply that R_1R_2 was p-unsolvable. However, we have

$$R_1R_2 \rhd \underbrace{R_2 \rhd}_{p^{b-1}} \underbrace{L_2 \rhd}_{p'} e, \qquad \underbrace{R_1 \rhd}_{p^{b-1}} \underbrace{L_1 \rhd}_{p'} e,$$

$$R_1R_2/R_2 \cong R_1/(R_1 \cap R_2).$$

Clearly, R_1R_2 is p-solvable. This shows that

$$|R_1R_2| = p^{b-1}r, \qquad (r, p) = 1.$$

Since R_1 and R_2 are normal in R_1R_2, R_1 and R_2 must have the same p-Sylow groups. For if not, let r be a p-element in R_1 not in R_2. This element permutes the p-Sylow groups of R_2. As the number of p-Sylow groups is congruent to 1 (mod p), there must be a fixed 1. This implies that $p^b \mid |R_1R_2|$, a contradiction. Therefore any p-element in R_1 is in R_2. Similarly, p-elements of R_2 are contained in R_1.

Let T be the subgroup of R_1R_2 generated by these p-Sylow groups. Clearly $|T| = p^{b-1}t$, $(p, t) = 1$. We will show that $T = Z$ which will be a contradiction as we are assuming that $b > 2$.

Since T is characteristic in R_i and $R_i \lhd W_1$, we have $T \lhd W_1$. We have $|R_i/L_i| = p^{b-1}$, $p^{b-1} \mid |T|$, $T \subseteq R_i$ and thus $TL_i = R_i$. Furthermore, $T/(T \cap L_i) \cong TL_i/L_i = R_i/L_i$. This implies that $T \cap L_i = O_{p'}(T)$. We see that $T \cap L_1 = T \cap L_2$. Since $L_1 \cap L_2 = e$, $T \cap L_1 = T \cap L_2 = e$. This shows that $R_i/L_i \cong T$ and so $|T| = p^{b-1}$. We know that T is abelian and $T \lhd W_1$.

We can apply Clifford's Theorem to $Y_i|T$. By (3.1), we have

$$Y_1|T = \{\lambda_1 \oplus \ldots \oplus \lambda_{(p-1)/2} \oplus \lambda_p\}|T,$$
$$Y_2|T = \{\lambda_1 \oplus \ldots \oplus \lambda_{(p-1)/2}\}|T.$$

The characters $\lambda_1, \ldots, \lambda_{(p-1)/2}, \lambda_p$ restricted to T must all be conjugate in W_1. The number of distinct conjugates divides $\frac{1}{2}(p+1)$ and $\frac{1}{2}(p-1)$. This number can only be one. We have $X|T = (\epsilon)^r I$ and thus $T \subseteq Z$. Clearly, $T = Z$ and we have a contradiction. We now assume that $b = 2$.

(8) Grün's theorem can be used to obtain a subgroup $W_0 \subseteq W_1$ such that $W_1 = W_0 \times Z$, $|W_0| = p\omega$ with $(p, \omega) = 1$. We know that $M_0 \subseteq W_1$. Either $M_0W_0 = W_1$ or W_0. Suppose that $M_0W_0 = W_1$. Then

$$Z \cong W_1/W_0 \cong M_0W_0/W_0 \cong M_0/(M_0 \cap W).$$

This is impossible since $M_0 \cong \mathrm{SL}(2, p)$. We must have $M_0W_0 = W_0$ and thus $M_0 \subseteq W_0$.

(9) We now consider the group W_0. Here $Y_i|W_0$ is irreducible since $Y_i|M_0$ is irreducible. Furthermore, $Y_i(M_0)$ has no normal p-Sylow group and thus $Y_i(W_0)$ has no normal p-Sylow group. We can apply the results of (**13**) to the linear groups $Y_i(W_0)$. This shows that for $p \neq 7$ there are normal subgroups B_i such that $W_0/B_i \cong \mathrm{LF}(2, p)$. For $p = 7$ there are normal subgroups B_i such that $W_0/B_1 \cong \mathrm{LF}(2, 7)$ or A_7, $W_0/B_2 \cong \mathrm{LF}(2, 7)$. The case $W_0/B_1 \cong A_7$ is impossible here since a composition series would have factors A_7 and $\mathrm{LF}(2, 7)$, and thus 7^2 would divide $|W_0|$. The $Y_i(B_i)$ are scalar matrices.

Clearly $p \nmid |B_i|$ as $p \mid |\mathrm{LF}(2, p)|$. Therefore $p \nmid |B_1B_2|$; $B_1 \subseteq B_1B_2 \subseteq W_0$. Since W_0/B_1 is simple, $B_1B_2 = B_1$. Similarly, $B_2 = B_1B_2$. Set $B = B_1 = B_2$.

Since $B \cap M_0 \subseteq M_0$ we have:

$$M_0/(B \cap M_0) \cong \begin{cases} \mathrm{SL}(2, p), \\ \mathrm{LF}(2, p), \\ e. \end{cases}$$

Here e is impossible as it would imply that $M_0 \subseteq B$ and so $p \mid |B|$. Furthermore, $M_0/(B \cap M_0) \cong M_0B/B \subseteq W_0/B \cong \mathrm{LF}(2, p)$. This shows that $M_0/(B \cap M_0) \cong \mathrm{LF}(2, p)$, which implies that $M_0B/B \cong \mathrm{LF}(2, p)$ and so $M_0B = W_0$.

(10) Again we fix i such that Y_i maps M_0 isomorphically, j such that Y_j maps $M_0/\langle\eta\rangle$ isomorphically. We will now show that η is the only involution in W_1. Suppose then that σ is an involution in W_1, $\sigma \neq \eta$. Certainly σ is in W_0, as elements in W_1 not in W_0 have order divisible by p.

Suppose first that $\sigma \in B$. This means that $Y_i(\sigma) = \pm I$, $Y_j(\sigma) = \pm I$, since the $Y_i(B)$, $Y_j(B)$ are scalar matrices. In either case, det $Y_i(\sigma)$ is 1 as Y_i has even degree. Since Y_j has odd degree, $Y_j(\sigma) = I$. This means that $Y_i(\sigma) = -I$. We see that $\sigma = \eta$ and so have a contradiction. We can assume that $\sigma \notin B$.

(11) Since $M_0B = W_0$, we have $\sigma = \tau_1 b$ with $b \in B$, $\tau_1 \in M_0$, $\tau_1 \neq e$ and since σ is an involution, $(\tau_1 b)^2 = (\tau_1)^2(b)^2 = \sigma^2 = e$. This follows since τ_i and b commute. We see that $Y_i(\tau_1^2)Y_i(b^2) = I$, $Y_j(\tau_1^2)Y_j(b^2) = I$. Since $Y_i(b^2)$ and $Y_j(b^2)$ are scalar matrices, $Y_i(\tau_1^2)$ and $Y_j(\tau_1^2)$ are scalar matrices also.

The only scalar matrix in $Y_j|M_0$ is I and thus $Y_j(b^2) = I$. This shows that $Y_j(b) = \pm I$. The only scalar matrices in $Y_i|M_0$ are I and $-I$. If $Y_i(\tau^2) = I$, then $Y_i(b^2) = I$, $Y_i(b) = \pm I$. In this case, $b = \eta$ or $b = e$. This means that $\sigma \in M_0$ and implies that $\sigma = \eta$. We see that $Y_i(\tau_1^2) = -I$. In turn, $Y_i(b^2) = -I$ and thus $Y_i(b) = \pm iI$.

This element b has order 2^2 and $X|\langle b\rangle$ has variety 2 (see introduction). By (**4**, 3D), $\langle b\rangle \cap Z$ is not e and we have a contradiction. This shows that the only involution in $C(\eta) = W_1$ is η itself.

(12) This result implies that η is the only involution in a 2-Sylow group S_2 of G. For if not, there is a 2-element r not in W_1 which normalizes some 2-Sylow group of W_1. Since η is the only involution in W_1, r centralizes η and hence is in W_1. This is a contradiction.

The theorem of Brauer-Suzuki (**6**) can now be applied to G. Let $K = O_{2'}(G)$. This theorem states that $\bar{\eta}$ is in the centre of G/K. Here $\bar{\eta}$ is the image of η in G/K.

Clearly $Z \subseteq K$. If $Z = K$, $\bar{\eta}$ would be in $Z(G/K)$. However, $\tau^\eta \equiv \tau^{-1} \pmod Z$ and therefore $\bar{\eta} \notin Z(G/K)$. Therefore $K > Z$. Suppose that $Z = O_p(K)$. Since K is of odd order it is solvable (**9**) and thus $O_{pp'}(K) > Z$. This implies that $O_{pp'}(K) = Z \times O_{p'}(K)$ and hence $O_{p'}(K) > e$. This is impossible by the primitivity of X. We see then that $O_p(K) > Z$ and $O_p(G) > Z$. Set $P_1 = O_p(G)$. Clearly P_1 is in all p-Sylow groups of G. Since $P \cap P^\mu = D$, we have $P_1 \subseteq D$. If $P_1 = D$, we have $G = N(D)$ and thus by (**4**), $a = 4$, $G/D \cong \mathrm{SL}(2, p)$. If $P_1 \neq D$, $|P_1| = p^2$. All such groups in D are of the form $\langle(\tau)^r(\xi_{a-2})^s, Z\rangle$. The only such group normal in P is $\langle\xi_{a-2}, Z\rangle = A_{a-2}$. However, $N(A_{a-2}) = N(P)$ (**4**, 5C). This shows that $P \lhd G$, a contradiction since $P^\mu \neq P$. The proof is complete.

Remark. This theorem in conjunction with (**4**, 5A, 5C, 6A, 6B) shows that the only p-Sylow intersection groups of P are P, Z, and A. It is mentioned in (**4**, § 7) that for $p \geqq 13$, A cannot be a p-Sylow intersection group. If A is not a p-Sylow intersection group, the p-Sylow groups of $\bar{G}$ form a $T - I$ set.

4. Some results on the rationality of χ. In this section we show that in many cases χ is rational or at least real when restricted to p-regular elements. We only consider the case $a \geqq 3$. It is assumed that the case of § 3 does not occur, that is, G has no non-abelian p-Sylow intersection groups. The only p-Sylow intersection groups contained in P are therefore P, Z, and A. We know from results of (**4**) that the only p-defect groups in P are then P, Z, or A. Clearly A cannot be one as $C(A) = A$ and hence there is no p-regular element R such that A is a p-Sylow group of $C(R)$ (**2**; **10**). Since $C(P) = Z$, there is only one block of full p-defect $B_0(p)$. All other blocks have p-defect 1. This proves part of the following lemma. Here $\bar{G} = G/Z$.

LEMMA 4.1. *If $a \geqq 4$, $B_0(p)$ is the only block of full p-defect. All other blocks are of defect 1 with defect group Z. Each p-block of G corresponds to a unique block $\bar{B}$ of $\bar{G}$ with defect one less* (**2**). *If y^* is an irreducible character of $\bar{G}$ in $\overline{B_0(p)}$, $y^*(\xi_{a-2})$ is not* 0.

Proof. If G is not the group described in § 3, all statements are clear except the last. If G is the group described in § 3, D cannot be a p-defect group as there is no p-regular element centralizing D except e. The last statement follows since $\bar{\xi}_{a-2}$ is the centre of a p-Sylow group and thus

$$y^*(\bar{\xi}_{a-2})/\deg y^* \not\equiv 0 \pmod p.$$

THEOREM 4.2. *Suppose that $a \geqq 4$ and G is not the group described in Theorem* 3.1. *Let $H = O^{p'}(G)$. The representation $X|H$ is primitive. Either χ is rational on q-elements or there is an element of order pq in $\bar{H} = H/Z$. Here q is an odd prime other than p.*

COROLLARY 4.3. *If there are no elements of order pq in $\bar{H}$ and $g = p^a q^b g_1$ with $(g_1, q) = 1$, then $b \leqq [p/(q-1)] + [p/q(q-1)] + \dots$.*

Proof. As χ is rational on q-elements, this follows by a theorem of Schur (**12**).

COROLLARY 4.4. *If A is not a p-Sylow intersection group and there is an element of order pq^c in $\bar{H}$, then $q^c|p-1$.*

Proof. Since there are no p-Sylow intersection groups contained in P except P and Z, an element $\bar{R}$ which centralizes an element in $\bar{P}$ must normalize $\bar{P}$. Therefore $R \in N(P)$. Since A is characteristic in P, $N(A) \supseteq N(P)$ and since A is abelian, $X|N(P)$ is monomial. The diagonal matrices come from A and thus $N(P)/A$ is a subgroup of S_p with a normal p-Sylow group. It follows that q^c, the order of R in $N(P)/A$, divides $p - 1$ since the order of the normalizer of a p-Sylow group of S_p is $p(p-1)$.

https://doi.org/10.4153/CJM-1969-114-0 Published online by Cambridge University Press

Proof of Theorem 4.2. The proof consists of several parts.

(1) Let $H = O^{p'}(G)$. Since $P \subseteq H$, $X|H$ is irreducible. If $X|H$ is not primitive, there is a normal abelian subgroup K of H such that H/K is isomorphic to a subgroup of S_p. Let P_0 be a p-Sylow group of K. Since K is abelian, P_0 is characteristic in K and hence normal in H. It is therefore in all p-Sylow groups of H. This means that it is in all p-Sylow groups of G. Its order must be p^{a-1} or p^a. Since K is abelian, P_0 is abelian and thus $|P_0| = p^{a-1}$, $P_0 = A$. This shows that $A \lhd G$, contradicting the primitivity of X. This shows that $X|H$ is primitive. From now on we replace G by H in our considerations and thus we can assume that $O^{p'}(G) = G$.

(2) We again assume that a basis is chosen for the representation space as in (**4**). Let $\psi = \chi|P$. Suppose that

$$\psi\bar{\psi} = 1 + \sum_{i=2}^{e} a_i\eta_i. \tag{4.1}$$

The η_is are irreducible characters of P, the a_i integers. Since $Z \in \ker \psi\bar{\psi}$, we have $Z \in \ker \eta_i$. Let η_i^* be the corresponding character of $\bar{P}$. We see that $\psi\bar{\psi}$ represents $\bar{P}$ faithfully since an element ξ in the kernel of $\psi\bar{\psi}$ satisfies $|\psi(\xi)| = p$ and thus $\xi \in Z$. The η_i have degree 1 or p since $\bar{P}$ is a p-group and $p^2 > p^2 - 1$. It also follows from Ito's Theorem (**11**) that all irreducible characters of P have degree 1 or p. We know that $\chi(\xi_{a-2}) = 0$, and therefore $\psi\bar{\psi}(\xi) = 0$. In particular, the eigenvalues of $X \otimes \bar{X}(\xi_{a-2})$ are the pth roots of 1 all taken with multiplicity p.

Suppose that ξ_{a-2} is in the kernel of some η_i of degree p. This means that $X \otimes \bar{X}(\xi)$ has at least $p + 1$ eigenvalues 1, giving a contradiction. Therefore ξ_{a-2} is not in the kernel of any η_i of degree p. On the other hand, since $P' = A_2 \supset \langle \xi_{a-2} \rangle$, ξ_{a-2} is in the kernel of each linear character η_i.

The group $\bar{P}$ is non-abelian since $a \geqq 4$. In fact, the centre of $\bar{P}$ is generated by $\bar{\xi}_{a-2}$. There must be some non-linear character η_i occurring in (4.1). For this η_i, $\eta_i(\xi_{a-2}) = p\epsilon^t$ for some t, $1 \leqq t \leqq p - 1$. Since

$$1 + \sum_{j=2}^{e} a_j\eta_j(\xi_{a-2}) = 0,$$

there must be $p - 1$ characters η_j of degree p each conjugate to η_i on ξ_{a-2}. We label these $\eta_1, \ldots, \eta_{p-1}$. The remaining characters in (4.1) are all linear. We label them $\xi_1, \ldots, \xi_{p-1}$. Equation (4.1) becomes

$$\psi\bar{\psi} = 1 + \sum_{i=1}^{p-1} \eta_i + \sum_{i=1}^{p-1} \xi_i. \tag{4.2}$$

(3) We now assume that q is a prime for which there are no elements of order pq in $\bar{G}$ and for which there is a q-element R such that $\chi(R)$ is not rational. Let $g = p^a q^b g_1$, where $(g_1, q) = 1$. The splitting field K is Q with the gth root of unity attached. Let K_1 be Q with the $p^a g_1$th roots of unity attached. Suppose that there is an element σ of $G(K/K_1)$, the Galois group of K over K_1, for which $\chi^\sigma\bar{\chi}(R)$ is not rational.

Clearly, $\chi^\sigma\bar{\chi}|P = \chi\bar{\chi}|P = \psi\bar{\psi}$ since σ keeps the pth roots of unity fixed. Suppose that $\chi^\sigma\bar{\chi} = \sum_{i=1}^k a_i y_i$, the y_i are irreducible characters of G. Again, since $Z \in \ker \chi^\sigma\bar{\chi}$, the y_i can be considered as linear characters y_i^* of $\bar{G}$. We consider the possibilities for this decomposition.

(4) Let $z = \sum_{i=1}^k b_i y_i$, $b_i \leqq a_i$, and assume that $z|P$ contains only linear characters. Let $K = \ker z$. Clearly $\xi_{a-2} \in K$. Clearly $K \lhd G$ and $\chi^\sigma\bar{\chi}|K = z|K + \ldots = (\deg z) \cdot 1_K + \ldots$, where 1_K is the trivial character on K. If $\deg z > 1$, this implies that $\chi|K$ is reducible by the primitivity and thus $K \subseteq Z$. This is not true since $\xi_{a-2} \in K$. This shows that $\deg z = 1$. We see that there is at most one y_i such that $y_i|P$ contains only linear characters and this y_i is linear itself.

(5) Suppose that $y_j|P$ is rational. If y_j is not linear, $y_j|P$ cannot contain only linear constituents and thus must contain at least one non-linear constituent η_r, $r = 1, 2, \ldots, p-1$. Since $y_j(\xi_{a-2})$ is rational, all η_r, $r = 1, 2, \ldots, p-1$, must occur in $y_j|P$. This implies that $\chi^\sigma\bar{\chi} - y_j|P$ has only linear constituents and therefore is linear. This means that $\chi^\sigma\bar{\chi} = y_i + y_j$, where y_i is linear, or $\chi^\sigma\bar{\chi} = y_j$. In the latter case, y_j^* is in $B_0(p)$ as its degree is p^2. However, $y_j^*(\bar{\xi}_{a-2}) = 0$, a contradiction to Lemma 4.1. This means that if $y_j|P$ is rational, it is either linear or $\chi^\sigma\bar{\chi} = y_i + y_j$ with y_i linear.

(6) Suppose that ξ_{a-2} is not in the kernel of some y_i, $i = 1, 2, \ldots, k$. If $K = \ker y_i$, $K \cap P$ is a normal subgroup of P not containing ξ_{a-2}. The only such subgroup is Z (**4**, 4D). However, this implies that $K = K_0 \times Z$, where $K_0 = O_{p'}(K)$. This implies that $K_0 = e$ since χ is primitive. We know that $Z \subseteq K$ and thus y_i acts faithfully on $\bar{G}$.

(7) Assume now that there are no linear characters among the y_i, $i = 1, 2, \ldots, k$. We have seen in (5) that this implies that $y_i|P$ is irrational. We know that $\xi_{a-2} \notin \ker y_i$ by (4), since $\xi_{a-2} \in \ker y_i$ implies $y_i|P$ has only linear constituents. Furthermore, since $\chi^\sigma\bar{\chi}(R)$ is irrational, some $y_j(R)$ is irrational. This shows that there is a y_j which is irrational on R and P. Since $\xi_{a-2} \notin \ker y_j$, y_j is faithful on $\bar{G}$. Since there are no elements of order pq in $\bar{G}$, this is a contradiction by (**3**; **7**). This shows that some y_i is linear.

Let y_1 be a linear character. We have

$$\chi^\sigma\bar{\chi} = y_1 + \sum_{i=2}^k a_i y_i.$$

Let $K = \ker y_1$. Since $O^{p'}(G) = G$, we have G/K a p-group. Clearly $Z \not\supseteq K$ since $\xi_{a-2} \in K$. This means that $\chi|K$ is irreducible by primitivity. Furthermore, $\chi^\sigma\bar{\chi}|K$ has a constituent 1_K and hence $\chi^\sigma|K = \chi|K$. Since R is a q-element, $R \in K$. We see that $\chi\bar{\chi}(R) = \chi^\sigma\bar{\chi}(R)$. In particular, $\chi\bar{\chi}(R)$ is irrational.

Let $\chi\bar{\chi} = y_1' + \sum_{i=2}^{k'} a_i' y_i'$, where the y_i' are irreducible characters of G, y_1' is 1. We have seen in (4) that none of the y_i' with $i \geqq 2$ are linear. Suppose that $k' > 2$. None of the $y_i'|P$, $i \geqq 2$, can be rational. For, if one were, by (4), it would contain all of the η_i and the others would contain only linear characters ξ_i. This is also impossible by (5). For at least one i, $y_i'(R)$ is not rational since $\chi\bar{\chi}(R)$ is not rational. Furthermore, ξ_{a-2} is not in the kernel of y_i' since $y_i'|P$ does not have linear constituents. This shows, by (6), that y_i' is faithful on $\bar{G}$. Again, as there are no elements in $\bar{G}$ of order pq, we have a contradiction to (**3**; **7**). This shows that $i = 2$, $\chi\bar{\chi} = y_1' + y_2'$.

Since $\chi\bar{\chi}(R)$ is not rational and $y_1'(R) = 1$, we see that $y_2'(R)$ is not rational. Let σ_1 be in $G(K/K_1)$ such that $y_2'(R)^{\sigma_1} \neq y_2'(R)$. Since

$$\chi^{\sigma_1}\bar{\chi}\overline{\chi^{\sigma_1}\bar{\chi}} = \chi\bar{\chi}\chi^{\sigma_1}\overline{\chi^{\sigma_1}} = (1 + y_1')(1 + y_1'^{\sigma_1}) = 1 + \ldots$$

with no further constituents 1, we see that $\chi^{\sigma_1}\bar{\chi}$ is irreducible. The character $\chi^{\sigma_1}\bar{\chi}$ can be considered as a character of $\bar{G}$. It is in $\bar{B}_0(p)$ and $\chi^{\sigma_1}\bar{\chi}(\xi_{a-2}) = 0$, contradicting Lemma 4.1.

We have shown that $\chi^{\sigma}\bar{\chi}(R)$ irrational leads to a contradiction and thus $\chi^{\sigma}\bar{\chi}(R)$ is always rational.

(8) Let $\chi(R) = \mu$. We know that μ is not rational but $\mu^{\sigma}\bar{\mu}$ is always rational. Let σ_2 be an element of $G(K/K_1)$ such that $\mu^{\sigma} = \bar{\mu}$. This is possible since μ is a sum of $(q)^b$th roots of unity. We know that $\bar{\mu}\bar{\mu}$ is rational and thus μ^2 is rational. The minimal equation of μ is $x^2 - r = 0$, where $\mu^2 = r$. This shows that μ has exactly one conjugate, $-\mu$.

Let $\rho_1 = e^{2\pi i/q^b}$. The Galois group $G(K/K_1)$ is isomorphic to the Galois group $G(Q[\rho_1]/Q)$ by the natural restriction from K to $Q[\rho_1]$. For $q \neq 2$, it is cyclic of order $(q-1)q^{b-1}$. If s_1 is a primitive root (mod q^b), $G(Q[\rho_1]/Q)$ is generated by σ, where $\sigma(\rho_1) = \rho_1^{s_1}$. There is therefore a unique extension of degree 2, the fixed field of σ^2. Let ρ be $e^{2\pi i/q}$ and let s be a primitive root (mod q). Set $\omega = \sum_{i=1}^{\frac{1}{2}(q-1)}(\rho)^{s^{2i}}$. Clearly, $\omega^{\sigma^2} = \omega$. Also as is well known, ω is irrational and thus $Q[\omega]$ is the fixed field. The algebraic integers in $Q[\omega]$ are of the form $a + b\omega$, where a and b are integers. This follows since the algebraic integers in $Q[\rho]$ are in $Z[\rho]$ and the conjugates of ω are linearly independent. We see then that $\mu = a + b\omega$. Furthermore, $\omega + \omega^{\sigma} + 1 = 0$. In our case, $\mu^{\sigma} = a + b\omega^{\sigma} = a - b(1 + \omega) = -a - b\omega$. This shows that $2a - b = 0$ and $\mu = a(1 + 2\omega)$. Let I be a prime ideal of the algebraic integers in $Z[\rho_1]$ containing q. Since ω is a sum of $\frac{1}{2}(q-1)$ qth roots of 1 all of which are congruent to 1 (mod I) we see that $1 + 2\omega \equiv 0$ (mod I). This means that $\mu \equiv 0$ (mod I). However, since χ has degree p, $\mu \equiv p$ (mod I), giving a contradiction. This completes the proof of the theorem.

We now discuss the case $a = 3$, $|G| = p^3g_0$. The methods above do not apply since $\bar{P}$ is now abelian. However, we can apply the character theory described in (**4**; **5**) to this case. We first show that except for a trivial case, $O^{p'}(G)/Z$ is simple.

THEOREM 4.5. *If G does not have a normal p-Sylow group, Z is the only non-trivial normal subgroup of $O^{p'}(G)$, and thus $O^{p'}(G)/Z$ is simple.*

Proof. We assume that G does not have a normal p-Sylow group. Let $H = O^{p'}(G)$. Let K be a non-trivial normal subgroup of H. The proof consists of several steps.

https://doi.org/10.4153/CJM-1969-114-0 Published online by Cambridge University Press

(1) If K is a p'-group, then $O_{p'}(H) \neq e$. Therefore $O_{p'}(G) \neq e$, contradicting the primitivity of χ. This means that K is not a p'-group.

(2) Let P be a p-Sylow group of G. Clearly $P \subseteq H$. Let $P_0 = P \cap K$. If $\xi \in P_0$, $\xi \notin Z$, there is a $\tau \in P$ such that $\xi^\tau = \xi(\xi_2)^r$, $\langle \xi_2 \rangle = Z$, for any r, $0 \leqq r \leqq p - 1$. This implies that $Z \subseteq P_0$. Suppose that $P_0 = Z$. Then $K = Z \times K_0$, where $K_0 = O_{p'}(K)$. Since $K \neq Z$, $K_0 \neq e$. This gives a normal non-trivial p'-subgroup K_0, contradicting (1). Therefore $P_0 \supsetneqq Z$. If $P_0 = P$, then $K = H$, giving a contradiction. We see that $|P_0| = p^2$.

(3) Suppose that $P \subseteq H_1 \subseteq H$. We will compute $O^p(\bar{H}_1)$. Since $\bar{P}$ is abelian, we use Grün's theorem (**14**) to see that $\bar{H}_1/O^p(\bar{H}_1) \cong \bar{P} \cap C(N_{\bar{H}_1}(\bar{P}))$. If $N_{\bar{H}}(\bar{P}) \neq \bar{P}$, then $C(N_{\bar{H}_1}(\bar{P})) = \bar{Z}$ by (**4**, 7A). This means that $O^p(\bar{H}_1) = \bar{H}_1$. If we know that $O^p(\bar{H}_1) \neq \bar{H}_1$, this implies that $N_{\bar{H}_1}(\bar{P}) = \bar{P}$ and hence $N_{H_1}(P) = P$.

(4) Consider the group PK. Clearly $|PK| = p^3 r_0$, where $|K| = p^2 r_0$. Certainly, PK/K is cyclic of order p. This shows that $O^p(PK) \neq PK$ and thus $O^p(\overline{PK}) \neq \overline{PK}$. Applying part (3) with $H_1 = PK$, we have $N_{PK}(P) = P$. As $P_0 = P \cap K$ is not a p-Sylow intersection group (**4**, 7A), $N_K(P_0) = P_0$ since any element of K normalizing P_0 must normalize P. Since P_0 is abelian, $P_0 \subset C_K(N_K(P_0))$. By Burnside's theorem (**14**, p. 169), K has a normal p-complement. This normal p-complement is then normal in G, contradicting the primitivity of χ unless it is e. We see then that $K = P_0$, $P_0 \lhd G$. Again, since there are no p-Sylow intersection groups, $P \lhd G$, contradicting the hypothesis. This completes the proof of the theorem.

The following theorem is a collection of several properties of $O^p(G)$.

THEOREM 4.6. *Let $a = 3$, $H = O^{p'}(G)$. Suppose that $H \neq P$. Then the character $\chi|H$ is primitive. If $\sigma \in G(K/Q(\epsilon))$ and $\chi^\sigma|H \neq \chi|H$, then $\bar{\chi}\chi^\sigma|H$ is irreducible. In this case $\chi\bar{\chi} = 1 + \chi_2$, χ_2 is irreducible, $\chi_2^\sigma \neq \chi_2$. Furthermore, $\chi|H$ is real on p-regular elements.*

Proof. The primitivity of $\chi|H$ follows from Theorem 4.5 as there are no non-trivial normal subgroups except Z. From now on in this theorem we replace G by $O^{p'}(G)$.

(1) We first show that if $\chi^\sigma\bar{\chi}$ is irreducible for all $\sigma \in G(K/Q(\epsilon))$ with $\chi^\sigma \neq \chi$, then χ is real on p-regular elements. Suppose that $\chi \neq \bar{\chi}$ on some p-regular element. There is an element in $G(K/Q(\epsilon))$ such that $\chi^\sigma = \bar{\chi}$ for p-regular elements. We know that $\chi^\sigma \neq \chi$ and so $y = \chi^\sigma\bar{\chi}$ is irreducible. Let y^θ be the modular character corresponding to y. Since y has degree p^2, it is of p-defect 1. However, $Z \in \ker y$ and thus y can be considered as a character of $\bar{G}$. Here it is of p-defect 0 and hence is modularly irreducible. However, $(\chi^\sigma)^\theta = \bar{\chi}^\theta$ since $\chi^\sigma = \bar{\chi}$ on p-regular elements. Certainly, $\bar{\chi}^\theta\bar{\chi}^\theta$ is not irreducible since the characters corresponding to the symmetric and skew symmetric tensors are summands. This shows that $(\chi^\sigma\bar{\chi})^\theta$ is not irreducible, giving a contradiction. We see that χ is real on p-regular elements.

https://doi.org/10.4153/CJM-1969-114-0 Published online by Cambridge University Press

(2) We now show that $\chi^\sigma\bar{\chi}$ is irreducible if $\chi^\sigma \neq \chi$. The results of (**5**) are applied. These are described in (**4**; § 8). We use the notation of (**4**) here.

Suppose that $\chi^\sigma\bar{\chi}$ is reducible. Since all of the constituents of $\chi^\sigma\bar{\chi}$ have degrees at most $p^2 - 1$, they are all in $B_0(p)$. We can therefore write

$$\chi^\sigma\bar{\chi} = \sum_{i=1}^{e} a_i\chi_i + a_0\left(\sum_{k=1}^{t} \chi_0^{\,k}\right).$$

Since χ is zero on $P - Z$, the multiplicities of $\chi_0^{\,k}$, $k = 1, 2, \ldots, t$, are all the same. We use an argument similar to (**4**, § 8).

Suppose that $a_i \neq 0$, $b_i > 0$. Since $\chi_i(1) \equiv b_i \pmod{p^2}$, $\chi_i(1) \leqq p^2 - 1$, we see that $\chi_i(1) = b_1$. This means that $P \subseteq \ker \chi_i$, which implies that G is in the kernel of χ_i and that $\chi_i = 1$. Further, $\chi^\sigma = \chi$, contradicting the hypothesis.

Suppose that $a_i \neq 0$, $b_i < 0$. As in (**4**), $\{|b_i| + \chi_i\}|\bar{P} = m\rho_{\bar{P}}$, $m > |b_i|$, where $\rho_{\bar{P}}$ is the regular representation of $\bar{P}$. We have $p^2 - 1 \geqq \chi_i(1) = mp^2 - |b_i| \geqq |b_i|(p^2 - 1)$. This yields $b_i = -1$, $\chi_i(1) = p^2 - 1$. This means that $\chi^\sigma\bar{\chi}$ has a linear constituent which can only be 1 by the choice of G. Again $\chi^\sigma = \chi$, giving a contradiction.

Finally, we have $\chi^\sigma\bar{\chi} = a_0(\sum_{k=1}^{t} \chi_0^{\,k})$. However, $(\sum_{k=1}^{t} \chi_0^{\,k}(\xi)) \neq 0$, and thus $a_0 = 0$ also. We have seen then that $\chi^\sigma\bar{\chi}$ must be irreducible.

(3) Suppose that $\chi\bar{\chi} = 1 + y$. If y and y^σ had a common constituent, we would have

$$\chi^\sigma\bar{\chi}\overline{\chi^\sigma\bar{\chi}} = \chi\bar{\chi}\chi^\sigma\overline{\chi^\sigma} = (1 + y)(1 + y^\sigma) = 1 + (y_1y^\sigma) + \ldots = 1 + 1 + \ldots.$$

This implies that $\chi^\sigma\bar{\chi}$ is reducible. This means that in (**4**, § 8, Case II), $y = \sum_{k=1}^{t} \chi_0^{\,k}$. If y and y^σ have no common constituents, $\chi_0^{\,k}$ and $(\chi_0^{\,k})^\sigma$ are all distinct. This is inconsistent with the results of (**4**, § 8; **5**). We see that (**4**, § 8, Case I) occurs and $\chi\bar{\chi} = 1 + \chi_2$ with χ_2 irreducible. Furthermore, $\chi_2^{\,\sigma} \neq \chi_2$.

5. Abelian Sylow groups. If q is a prime, $p/2 < q < p$, the q-Sylow group must be abelian. This is easy to show if q is greater than five but difficult for $q = 5$. We will prove it in this section for $q \geqq 7$ and save the proof for $q = 5$ for a later paper in which linear groups of degree 7 are treated explicitly (see p. 1042 of this issue). The proof does not depend on the fact that G is of prime degree and so we prove it in general. The proof seems to be well known.

THEOREM 5.1. *If G has a faithful primitive irreducible representation X of degree n and q is a prime, $n/2 < q < n$, $7 \leqq q$, then a q-Sylow group of G is abelian.*

Proof. If a q-Sylow group P_q is non-abelian, $X|P_q$ must have a constituent of degree q and $n - q$ linear constituents. Let ξ be an element in $Z(P_q) \cap P_q'$. For an appropriate power ξ^r the eigenvalues of $X(\xi^r)$ are $e^{2\pi i/q}$ repeated q times and 1 repeated $n - q$ times. This contradicts Blichfeldt's theorem (**1**, p. 96) since $q \geqq 7$ and shows that P_q is abelian.

References

1. H. F. Blichfeldt, *Finite collineation groups* (Univ. Chicago Press, Chicago, Illinois, 1917).
2. R. Brauer, *Zur Darstellungstheorie der Gruppen endlicher ordnung*, I; II. Math. Z. *63* (1956), 406–444; *72* (1959), 25–46.
3. ——— *A note on theorems of Burnside and Blichfeldt*, Proc. Amer. Math. Soc. *15* (1964), 31–34.
4. ——— *Über endliche lineare Gruppen von Primzahlgrad*, Math. Ann. *169* (1967), 73–96.
5. R. Brauer and H. S. Leonard, Jr., *On finite groups with an abelian Sylow group*, Can. J. Math. *14* (1962), 436–450.
6. R. Brauer and M. Suzuki, *On finite groups of even order whose 2-Sylow group is a quaternion group*, Proc. Nat. Acad. Sci. *45* (1959), 1757–1759.
7. W. Burnside, *Theory of groups of finite order*, 2nd ed. (Cambridge Univ. Press, Cambridge, 1911).
8. W. Feit, *Groups which have a faithful representation of degree less than $p - 1$*, Trans. Amer. Math. Soc. *112* (1964), 287–303.
9. W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math. *13* (1963), 775–1029.
10. J. A. Green, *Blocks of modular representations*, Math. Z. *79* (1962), 100–115.
11. N. Ito, *On the degrees of irreducible representations of a finite group*, Nagoya Math. J. *3* (1951), 5–6.
12. I. Schur, *Über ein Klasse von endlichen Gruppen linearer Substitutionen*, Sitzber. Preuss. Akad. Wiss. Berlin *1905*, 77–91.
13. H. F. Tuan, *On groups whose orders contain a prime to the first power*, Ann. of Math. (2) *45* (1944), 110–140.
14. H. J. Zassenhaus, *The theory of groups*, 2nd ed. (Chelsea, New York, 1958).

California Institute of Technology,
Pasadena, California

https://doi.org/10.4153/CJM-1969-114-0 Published online by Cambridge University Press