Math. Z. 128, 297–304 (1972)

Groups with a Steinberg Character

Forrest A. Richen

Let G be a finite group and p a rational prime. If G is a simple Lie type group of characteristic p then G has the following property. G has an absolutely irreducible character χ whose degree is the order of a p-Sylow subgroup of G, and all other characters are in the principal p-block, $B_0(p)$. (χ is called the Steinberg character. See [4, 5, 9] and [12].) For simple groups G, this property seems to hold only if G has Lie type of characteristic p.

The most general conjecture that can be made from this observation, namely that the above property about the characters of G forces G to be of Lie type at characteristic p, seems too difficult at present. In fact to prove anything in this direction, I have had to make arithemtical assumptions about G as well as assumptions about a subgroup which ultimately corresponds to the normalizer of a torus. In Section 4 I will indicate why such assumptions may be inevitable.

Theorem. *Let G be a finite group and p a prime such that $|G|=p g'$, $(p, g')=1$. Suppose that G has an irreducible character χ of degree p and that all other characters of G are in the principal p-block, $B_0(p)$. Let P be a p-Sylow subgroup and let $N(P)=HP$ where $H\cap P=\{1\}$. Suppose that H is a TI set and $|N(H)|=2|H|$. Then G is isomorphic to $PSL_2(p)$.*

(Recall a subgroup A of a group G is a TI set if $A\cap A^g\neq\{1\}$ implies $g\in N(A)$.)

The following corollary is related to a theorem of Ito [11].

Corollary. *Let G be a transitive permutation group of prime degree, p. Suppose G has a unique character χ whose degree is divisible by p and that $\chi(1)=p$. Suppose that if the normalizer of a p-Sylow subgroup P of G is HP where $H\cap P=\{1\}$ then H is a TI set and $|N(H)|=2|H|$. Then $p=5$, 7 or 11 and $G\cong PSL_2(p)$.*

The proof of the theorem is carried out in Sections 1–3 and the corollary is proved and discussed in Section 4. I assume familiarity with elementary finite group theory and character theory including the theory of blocks. (Gorenstein's book [8], Huppert's book [10] and Curtis and Reiner's book [3] will serve as general references.) At a crucial point detailed information about B_0 (p) is needed for groups containing p to the first power (Brauer [1]), but that information is fully stated in the text.

§ 1. Some Subgroups of G

Let G be a group that satisfies the hypotheses of the theorem. Let P be a p-Sylow subgroup, $B=N(P)=HP$ where $H\cap P=1$, and $N=N(H)$. Since the characters of G are $\{\chi\}\cup B_0(p)$, G has exactly one block of defect 1. Brauer's first main theorem gives $C(P)\subseteq P$ (or see Theorem 3 in Brauer [2]). Thus $H\cong N(P)/C(P)$ is a cyclic group whose order e divides $p-1$. Since $|N|=2e$, $e=1$ would give $|G|=2$ and $p=2$ contrary to the assumption that G has a character of degree 2. Thus $e>1$. This together with Burnside's fusion theorem (7.1.1, [8]) gives the following fact.

(1.1) *B is a Frobenius group of order pe with cyclic complement H of order $e>1$. G has $t=(p-1)/e$ classes of p-elements.*

(1.2) *G is a non abelian simple group.*

Proof. Suppose $1\neq S\vartriangle G$ and $p\,\big|\,|G:S|$. Then $S\leqq O_{p'}(G)$ which is just $\bigcap\{\ker\zeta\colon \zeta\in B_0(p)\}$. (Theorem 1, Brauer [2].) Thus the characters of $G/O_{p'}(G)$ are just the characters of $B_0(p)$. Then summing the squares of the degrees of the characters of G gives

$$|G|=\sum_{\zeta\in B_0(p)}\zeta(1)^2+p^2=|G\colon O_{p'}(G)|+p^2.$$

The only solution to this equation is $|G|=(p+1)\,p$. But $e\,|\,(p-1)$ and $e\,|\,(p+1)\,p$ forces $e=1$ against (1.1).

On the other hand suppose $p\,\big|\,|S|$ and $S\vartriangle G$. Then $P\leqq S$, and the Frattini Lemma (1.3.7, [8]) gives $G=SB$. Hence $G/S\cong B/S\cap B$ is cyclic of order prime to p. Thus $G'\subseteq S$ and we may assume $p\,\big|\,|G'|$. Now $\chi\varphi$ is an irreducible character of degree p if φ is a linear character of G. Since χ is the unique irreducible character of degree p, $\chi\varphi=\chi$. Thus χ vanishes on $G-G'$. Hence

$$\begin{aligned}(\chi|_{G'},\chi|_{G'})&=\frac{1}{|G'|}\sum_{x\in G'}|\chi(x)|^2\\&=\frac{1}{|G'|}\sum_{x\in G}|\chi(x)|^2\\&=|G\colon G'|.\end{aligned}$$

Now Clifford's Theorem (V, 17.3 in [10]) gives

$$\chi|_{G'}=e\sum_{i=1}^{n}\lambda_i$$

where e is some positive integer and the λ_i's are the distinct G-conjugates of some irreducible character λ_1 of G'. Taking degrees shows $p=e\,n\,\lambda_1(1)$.

Taking the inner product of $\chi|_{G'}$ with itself shows $|G\colon G'|=e^2 n$. Thus $e=n=1$ and $G'=G$. Hence $S=G$ proving (1.2).

To determine the structure of N we need a lemma.

Lemma. *If $x\in G$ and $\chi(x)\neq 0$, and u and v are involutions then $x=u_1 v_1$ for some u_1 and v_1 conjugate to u and v respectively. There is one class of involutions.*

Proof. Suppose not. Then if u and v are any involutions in G,

$$0=\sum \frac{\zeta(u)\,\zeta(v)\,\overline{\zeta(x)}}{\zeta(1)}$$

where the sum is over all irreducible characters ζ of G (p. 315, [8]). Since $\chi(1)=p$ and u and v are involutions $\chi(u)\,\chi(v)\neq 0$. Moreover (1.2) implies that χ is faithful so that $\chi(u)\,\chi(v)\,\overline{\chi(x)}$ is non zero and relatively prime to p. Also since χ is the unique character of G of degree p, χ is integer valued. This gives

$$-\ell\big(\chi(u)\,\chi(v)\,\overline{\chi(x)}\big)=p\left(\ell \sum_{\zeta\in B_0(p)} \frac{\zeta(u)\,\zeta(v)\,\overline{\zeta(x)}}{\zeta(1)}\right)$$

where $\ell = l\,c\,m\,\{\zeta(1)\colon\ \zeta\in B_0(p)\}$ is relatively prime to p. The left side is an integer prime to p and the right side is an algebraic integer divisible by p. This contradiction proves the first sentence.

Since G is a simple group, G contains an element x of prime order q different than 2 and p (Burnside's Theorem 4.3.3, [8]). If q_0 is a prime ideal in the ring of algebraic integers containing q then $\chi(x)\equiv\chi(1)\equiv p \pmod{q_0}$. Thus $\chi(x)\neq 0$. Thus if u and v are involutions in G, they have conjugates u_1 and v_1 respectively such that $u_1 v_1=x$. Hence u_1 and v_1 are conjugate in the dihedral group $\langle u_1, x\rangle$, and so u and v are conjugate.

(1.3) *N is dihedral of order $2e$.*

Proof. Since B is a Frobenius group B has t non-linear characters $\varphi_1, \dots, \varphi_t$ of degree e and e linear characters $\mu_1, \dots, \mu_e$. Each $\varphi_i=(\xi_i)^B$ for some non-identity character ξ_i of P. (See 4.5.3, [8] for example.) Now χ is fixed under field automorphisms since it is the unique character of G of degree p. Since each ξ_i is algebraically conjugate to ξ_1, we have

$$a=(\chi|_P, \xi_1)_P=(\chi|_P, \xi_i)_P$$

for all i. Moreover since χ is faithful $a\neq 0$. Thus by Frobenius reciprocity $a=(\chi|_B, \varphi_i)_B$ for all i. Since $\chi(1)=p$ and $\varphi_i(1)=e$, $a=1$. Thus

$$\chi|_B-\sum_{i=1}^{t}\varphi_i$$

is some linear character μ of B.

Now let x be a generator of H.

$$\chi(x)=\mu(x)+\sum_{i=1}^{t}\varphi_i(x)=\mu(x)\neq 0,$$

since $\varphi_i=\xi_i^B$ implies that φ_i vanishes off of P. Thus the lemma implies that there is an involution $u\in G$ such that $x^u=x^{-1}$. Thus $\langle x,u\rangle$ is a dihedral subgroup of N of order $2e$ and so is equal to N.

§ 2. Some Characters of G

Recall that if A is a subgroup of G which is a TI set then the mapping from the set of generalized characters of $N(A)$ whose support is contained in $A-\{1\}$ to generalized characters of G, $\alpha\mapsto\alpha^G$, the induced character, is an isometry (4.4.6, [8]).

(2.1) *Suppose $e>4$. Then there are two irreducible characters, λ_1,λ_2 of N of degree 2 which are induced from linear characters of H. λ_1 and λ_2 are real valued. There exist irreducible characters γ_1,γ_2,α of G and integers ε and δ of absolute value 1 so that*

$$1_H^G-\lambda_i^G=1-\varepsilon\gamma_i+\delta\alpha.$$

$\gamma_1(x)=\gamma_2(x)$ unless x is conjugate to an element of $H-\{1\}$.

Proof. The first two sentences are elementary since N is a dihedral group. A proof of the last, which is well known, is included. Frobenius reciprocity gives $(\Gamma_i^G,1_G)=1$ where $\Gamma_i=1_H^N-\lambda_i$. Applying the isometry to Γ_i gives $(\Gamma_i^G,\Gamma_j^G)_G=2+\delta_{ij}$. Thus

$$\Gamma_i^G=1+\delta\alpha+\varepsilon_i\gamma_i$$

where α,γ_1,γ_2 are distinct irreducible characters and $\delta,\varepsilon_1,\varepsilon_2$ are integers of absolute value 1. Moreover $\varepsilon_1\gamma_1-\varepsilon_2\gamma_2=\Gamma_1^G-\Gamma_2^G$ has degree zero while $\gamma_i(1)>0$. Thus $\varepsilon_1=\varepsilon_2$ proving (2.1) if we set $\varepsilon=-\varepsilon_1$.

We now must recall some facts about the principal block of G, $B_0(p)$. No assumption about e is made. Brauer's paper [1] is the reference. (Alternatively see [13].)

(2.2) *There are $e+t$ characters in $B_0(p)$. The first e of them $\zeta_1,\ldots,\zeta_e$ have the property that ζ_i has constant value a_i on all p-elements and a_i is either 1 or -1. As a result $\zeta_i(1)\equiv a_i \pmod p$. The remaining t make up the so called exceptional class, $\theta_1,\ldots,\theta_t$. If $g\in G$ has order prime to p, then $\theta_i(g)=\theta_j(g)$. $\sum_{i=1}^{t}\theta_i$ has constant value a on the p-elements, $a=1$ or -1, and as a result $t\,\theta_i(1)\equiv\sum\theta_i(1)\equiv a \pmod p$. Moreover $a\theta_1+\sum_{i=1}^{e}a_i\zeta_i$ vanishes on p-regular elements. $B_0(p)$ gives a tree T in the following way.*

The vertices of T are the characters $\zeta_1, \ldots, \zeta_e$, $\theta = \sum \theta_i$, and two vertices are joined by an edge if and only if they have a modular constituent in common. Two vertices are joined by at most one edge. If two vertices are joined by an edge, they take different values on p-elements.

(2.3) *Suppose $e > 4$. Then $\alpha = \chi$; γ_1 and γ_2 are real valued characters of degree $p+1$.*

Proof. At least one γ_i is not in the exceptional family of $B_0(p)$ for if they both were, then (2.1) and (2.2) would say that they are equal everywhere contrary to $\gamma_1 \neq \gamma_2$. Let $x = \gamma_1(1)$ and $a = \alpha(1)$. Then (2.1) implies $0 = 1 - \varepsilon x + \delta a$, and (2.2) implies that $\varepsilon x \equiv \pm 1 \pmod p$. If $\varepsilon x \equiv 1 \pmod p$, then $p \mid a$ and so $\alpha \notin B_0(p)$. Thus $\alpha = \chi$. If $\varepsilon x \equiv -1 \pmod p$ then $\delta a \equiv -2 \pmod p$. Since $e > 4$ and $e \mid p-1$, $p \geqq 7$. Thus $\delta a \not\equiv \pm 1$ and so α must belong to the exceptional family of $B_0(p)$. But then $t \delta a \equiv \pm 1 \pmod p$ which gives $-2t \equiv \pm 1 \pmod p$. Hence $p \leqq 2t + 1$. But $e > 4$ and $e t = p - 1$ yield $4t < 2t$ a contradiction.

Since $\alpha = \chi$, (2.1) gives that

$$\gamma_i = \varepsilon(1 + \delta \chi - \Gamma_i^G).$$

χ is rational valued since it is the only character of degree p, and (2.1) says that λ_i and hence Γ_i^G are real valued. Thus γ_i is real valued. Its degree $\varepsilon(1 + \delta \chi(1)) = \varepsilon + \varepsilon \delta p$. Since this must be a positive number, $\varepsilon \delta = 1$. Thus $\gamma_i(1)$ is $p-1$ or $p+1$.

Suppose $\gamma_i(1) = p-1$. Then $\gamma_i(g) = -1$ if g is a p-element, and so $\gamma_{i|P} + 1_P$ is the regular character of P. In the notation of the proof of (1.3) we then have $1 = (\gamma_{i|P}, \xi_j)_P = (\gamma_{i|B}, \varphi_j)_B$ by Frobenius reciprocity, and so $\gamma_{i|B} = \sum_{j=1}^{t} \varphi_j$ which vanishes on $H - \{1\}$. But if x is a generator of H we have $\gamma_i(x) = -1 + \chi(x) - 1_H^G(x) + \lambda_i^G(x) = -3 + \chi(x) + \lambda_i^G(x)$. But $\chi(x)$ is a rational root of unity from the proof of (1.3), and $\lambda_i^G(x)$ is easily computed to be a real number < 2. Thus $0 = \gamma_i(x) < -3 + 1 + 2 = 0$ a contradiction. Thus $\gamma_i(1) = p+1$ proving (2.3).

For the remainder of this section assume $e > 4$. By a theorem of Tuan (Theorems A and B, [14]) the tree T described in (2.2) can be drawn so that it is symmetric with respect to a stem (an open polygonal subgraph) and so that mapping a character to its contragredient is the automorphism of the tree which is reflection through the stem. Thus a character is real valued if and only if it is a vertex on the stem. The trivial character is one end point of the stem. Both of γ_1 and γ_2 are on the stem and so least one of them, γ_1 say, has more than one modular constitutent. No modular constituent of γ_1 is the trivial modular representation since $\gamma_1(g) = 1$ for a p-element g by (2.2). Thus one of the modular constituents of γ_1 is a faithful irreducible representation of G in a field of characteristic

p of degree no larger than $(p+1)/2$. Feit's theorem (Theorem 1, [6]) implies that G is of type $L_2(p)$ and so (1.2) implies that $G \cong PSL_2(p)$.

§3. $e \leqq 4$

It is possible to reduce the cases $e=2,3$ and 4 to high powered classification theorems, but with very little extra effort these cases can be disposed of by elementary methods.

By (2.2) there are $e+t$ characters in $B_0(p)$ and there is just one other, the Steinberg character χ. Hence G has exactly $e+t+1$ conjugacy classes. By (1.1) t of these classes are classes of p-elements and there is one class for the identity. Writing $|G|=(1+rp)ep$, where $1+rp=|G\colon N(P)|$, each p-element g is in a class of size $|G\colon C(g)|=[(1+rp)ep]/p=(1+rp)e$. Thus there are $(1+rp)et=(1+rp)(p-1)$ p-elements in G. Let $x_1, \ldots, x_e$ be the orders of the elements in each of the remaining e-classes and $c_1, \ldots, c_e$ the orders of the centralizers of these elements. Summing the orders of the conjugacy classes we get

$$(1+rp)ep=1+(1+rp)(p-1)+(1+rp)ep\left[\frac{1}{c_1}+\cdots+\frac{1}{c_e}\right]$$

or

$$(*) \qquad 1=\frac{1+r(p-1)}{1+rp}\cdot\frac{1}{e}+\frac{1}{c_1}+\cdots+\frac{1}{c_e}.$$

Suppose $e=2$. Then N is the centralizer of an involution and has order 4. Since G is simple, G has a prime q different from 2 and p in its order. The centralizer of a q-element is a power of q, since G has only 3 classes of p-regular elements. Thus we may write $c_1=q^n$ and $c_2=4$. Eq. $(*)$ becomes

$$1=\frac{1+r(p-1)}{1+rp}\cdot\frac{1}{2}+\frac{1}{q^n}+\frac{1}{4}.$$

This forces $q^n<4$ and $q^n=3$ first of all and then forces $r=1$ and $p=5$. Thus $|G|=60$ and so $G\cong PSL_2(5)$. (See [7] for example.)

Suppose $e=3$. Since N has order 6 and is dihedral the three elements are self centralizing and conjugate to their inverses. This says that the 3-Sylow subgroups have order 3 and that there is one class of 3-elements. By the lemma of Section 2 there is one class of involutions. Thus we may write $c_3=x_3=3$, $x_2=2$ and $c_2\geqq 4$. Eq. $(*)$ yields that

$$1<\frac{1}{3}+\frac{1}{c_1}+\frac{1}{4}+\frac{1}{3}$$

which gives $c_1<12$. By the above $c_1 \neq 2, 3, 6$, or 9. c_2 cannot be 10 because then G would contain elements of order 5 and 10, and there are not enough classes for this. Neither can c_1 be 5, 7 or 11 because if $c_1=x_1=q$

for a prime q, then a q-Sylow subgroup Q has order q, and its normalizer induces the full automorphism group of Q since there is only one class of q-elements. This forces G to contain an element of order $q-1$ and there are not enough classes for such an element. Thus $c_2=2^a$ and $c_1=2^b$, a and $b \geqq 2$. The only solution consistent with $*$ is $c_1=4$ and $c_2=8$. Applying $(*)$ again yields $r=1$ and $p=7$ giving $|G|=168$. Thus $G \cong PSL_2(7)$. (See [7] for example.)

Finally suppose $e=4$ for purposes of obtaining a contradiction. Since H is characteristic in N, and N is dihedral of order 8, N is a 2-Sylow subgroup of G and H is self centralizing. Moreover there is just one class of elements of order 4 by Sylow's theorem. By the lemma of Section 2 there is just one class of involutions. Thus we may wirte $x_2=2$ and $c_2 \geqq 8$, $x_4=c_4=4$ and $c_3 \geqq c_1 \geqq 3$ with neither c_1 nor c_3 being 4. Eq. $(*)$ gives

$$1<\frac{1}{4}+\frac{2}{c_1}+\frac{1}{4}+\frac{1}{8}$$

which says that $c_1=3$ or 5. Hence $x_1=c_1=q$ where q is 3 or 5. Thus a q-Sylow subgroup has order q and $c_2=8$.

This gives just two possibilities for c_3 and x_3. Either $c_3=x_3=q$ or $x_3=s$ a prime different from p, 2 and q and $c_3=s^n$ for some n. If $c_3=q$ then Eq. $(*)$ becomes

$$1=\frac{1}{4}\left(\frac{1+r(p-1)}{1+rp}\right)+\frac{2}{q}+\frac{1}{4}+\frac{1}{8}$$

with q either 3 or 5. $q=3$ gives no positive integer solutions to r and p while $q=5$ implies $r=1$ and $p=9$ a contradiction.

On the other hand if $x_3=s$ then the normalizer of an s-Sylow subgroup is a Frobenius group of order $(s^n-1)\,s^n$. (This follows from the Burnside fusion theorem and the fact that $c_3=s^n$.) Inspecting the possible Frobenius complements (see 10.3.1, [8] for example) yields that $s^n-1=2$ or 4 and so $c_3=3$ or 5. Thus we may assume $c_1=3$, $c_2=8$, $c_3=5$, and $c_4=4$, and equation $(*)$ has no solution with these values for the c_i. This completes the proof of the theorem.

§ 4. The Corollary

The corollary follows directly from the theorem. Since G is a transitive permutation group of degree p where p is a prime, G is isomorphic to a subgroup of the symmetric group on p letters. Thus p divides $|G|$ only once and the p-Sylow groups of G are self centralizing. But a p-Sylow subgroup being self centralizing implies that every character whose degree is prime to p belongs to $B_0(p)$ (Theorem 3, [2]). Thus the hypotheses of the theorem hold for G and p, and so $G \cong PSL_2(p)$. Since G has a subgroup of index p, a theorem of Galois implies that $p=2, 3, 5, 7$ or 11 (II, 8.28, [10]), and $p=2$ and 3 are excluded since G is simple.

Ito proves the following related result (Theorem, [11]). Suppose G is a transitive permutation group of prime degree p. (A) Suppose $(p-1)/2=q$ is a prime. (B) Suppose exactly one character of G has degree divisible by p. Then $p=5, 7$, or 11 and $G \cong PSL_2(p)$.

Hypothesis (B) is weaker than the corresponding hypothesis about the Steinberg character in the corollary. However hypothesis (A) is certainly stronger than the corollary's hypothesis about H. In fact it is not hard to prove that if G is a simple transitive permutation group of degree $p=2q+1$ with p and q primes and if H is defined as in the corollary, then H is a TI set and $|N(H)|=2|H|$. Thus perhaps some strong assumption on H is inevitable.

References

1. Brauer, R.: On groups whose order contains a prime number to the first power I. Amer. J. Math. **64**, 401–420 (1942).
2. Brauer, R.: Some applications of the theory of blocks of characters of finite groups I. J. Algebra **1**, 152–167 (1964).
3. Curtis, C. W., Reiner, I.: Representation theory of finite groups and associative algebras. New York: Interscience 1962.
4. Curtis, C.W.: The Steinberg character of a finite group with a (B, N)-pair. J. Algebra **4**, 433–441 (1966).
5. Dagger, S.W.: On the blocks of the Chevalley groups. J. London Math. Soc. (2) **3**, 21–29 (1971).
6. Feit, W.: Groups with a cyclic Sylow subgroup. Nagoya Math. J. **27**, 571–584 (1966).
7. Frobenius, G.: Über Gruppen des Grades p oder $p+1$. Sitzber. Preuß. Akad. Wiss., (1902), 351–369.
8. Gorenstein, D.: Finite groups. New York: Harper and Row 1968.
9. Humphreys, J.E.: Defect groups for finite groups of Lie type. Math. Z. **119**, 149–152 (1971).
10. Huppert, B.: Endliche Gruppen I. Berlin-Heidelberg-New York: Springer 1967.
11. Ito, N.: A note on transitive permutation groups of degree $p=2q+1$, p and q being prime numbers. J. Math. Kyoto. Univ. **3-1**, 111–113 (1963).
12. Richen, F.: Blocks of defect 0 of a split (B, N)-pair. J. Algebra **21**, 275–279 (1972).
13. Thompson, J.G.: Vertices and sources. J. Algebra **6**, 1–6 (1967).
14. Tuan, H.F.: On groups whose orders contain a prime to the first power. Ann. of Math. **45**, 110–140 (1944).

Prof. F.A. Richen
Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48104
USA

(Received November 23, 1971)