A CHARACTERIZATION OF THE SIMPLE GROUPS $PSL(2, p)$, $p > 3$

BY

MARCEL HERZOG

ABSTRACT

Let G be a finite group, containing a self-centralizing subgroup of prime order p. If G is non-solvable, contains more than one class of conjugate elements of order p, and satisfies an additional condition, then G is isomorphic to $PSL(2,p)$, $p > 3$.

Introduction. The purpose of this paper is to prove the following

THEOREM. *Let G be a finite group containing a cyclic subgroup M of prime order p and satisfying the following conditions:*

(i) $C_G(m) \subseteq M$ *for all* $m \in M^{\#}$

(ii) $[N_G(M): M] \neq p-1$

(iii) *If* $z \in M^{\#}$ *and* $xy = z$, *where* $x^p = y^p = 1$, *then* $x \in M$, *except possibly in the case that both* x *and* y *are conjugate to* z^{-1} *in* G.

Then one of the following statements is true.

(I) *G is a Frobenius group with M as the kernel.*

(II) *There exists a nilpotent normal subgroup K of G such that:*

$$G = N_G(M)K, \ K \cap N_G(M) = 1.$$

(III) *G is isomorphic to $PSL(2,p)$, $p > 3$.*

As an immediate consequence of the theorem we get the following characterization of the simple groups $PSL(2,p)$, $p > 3$, which are known to satisfy the assumptions of the theorem.

COROLLARY. *Let G be a finite non-solvable group containing a cyclic subgroup M of prime order p which satisfies conditions* (i)–(iii). *Then G is isomorphic to $PSL(2,p)$ and $p > 3$.*

Conditions (i) and (ii) certainly exclude the case $p = 2$, and if $p = 3$ they allow only the trivial situation $N_G(M) = M$, thus forcing G to be of type (II). However,

Received December 21, 1966.

the case $p = 3$ was investigated by W. Feit and J. G. Thompson in [3], under the single assumption (i). They classified the groups in question and proved that if G is a simple group, then it is isomorphic to either $PSL(2,5)$ or $PSL(2,7)$.

If no exceptions are allowed in condition (iii), then it follows from [5], Theorem 5 that G is either of type (I) or of type (II).

Groups G containing a subgroup M of order p which satisfies condition (i) were studied by R. Brauer in [1]. Among other results he proved that if $G = G'$ and $[G: N_G(M)] < p(p+3)/2 + 1$ then G is isomorphic either to $PSL(2,p)$, $p > 3$ or to $PSL(2, p-1)$, where $p - 1 = 2^n$, $n > 1$. In our proof this result serves as the concluding argument.

The methods of this paper are similar to those applied in [4] and [5], which rely heavily on the work of W. Feit [2]. But in the present case the results of Brauer [1] are available, simplifying the necessary notation as well as many of the arguments. We therefore repeat the necessary definitions from [4] and [5] (not always identically) and prove everything except for the results form [1] and [2], which are summarized. Consequently, this work can be read independently of [4] and [5].

If T is a subset of a group G, $C_G(T)$, $N_G(T)$, $|T|$ and $T^\#$ will denote respectively: the centralizer, normalizer, number of elements and the non-unit elements of T. The subscript G will be dropped in cases where it is clear from the context which group is involved. The commutator subgroup of G will be denoted by G', and 1 will be the notation for the trivial subgroup.

Proof of the Theorem. It will be assumed that G satisfies the assumptions of the theorem, but is not of type (I) or (II). It suffices to show that G satisfies (III).

M is certainly a trivial -intersection- set in G and it follows easily from (i) that M is a Sylow p-subgroup of G. Since G is not of type (II), $N_G(M) \neq M$. Thus the results of W. Feit [2, §2] and R. Brauer [1, pp. 59–60] are applicable, and the relevant ones will be summarized below, together with the corresponding notation.

As $N = N_G(M) \neq M$, N is a Frobenius group with M as its kernel and it is well known that there exists a subgroup Q of N such that:

$$N = QM, \quad Q \cap M = 1.$$

Let the order of Q be q; then q divides $p-1$, and $t = (p-1)/q$ is the number of conjugate classes $\tilde{C}_i$ of elements of order p in N. Since M is a Sylow subgroup of G, t is also the number of conjugate classes C_i of elements of order p in G and $\tilde{C}_i = C_i \cap M$ after rearrangement, if necessary. Let $m_1, \cdots, m_t$ be a set of representatives of $\tilde{C}_i$, $i = 1, \cdots, t$; they also represent the C_i, $i = 1, \cdots, t$. It follows from the Sylow Theorem that order g of G can be expressed by the formula $g = qp(np+1)$. As G is not of type (I) $n > 0$ and consequently

$$g > qp^2. \tag{1}$$

The irreducible characters of N fall under two categories. The first one consists of t characters ξ_i, $i = 1, \cdots, t$ of degree q, vanishing outside M. The second category consists of q linear characters which contain M in their kernel. It follows that

$$\sum_s \xi_s(m_i)\xi_s(m_j^{-1}) = \delta_{ij}p - q$$

$$\sum_s \xi_s(m_i) = -1$$

where $1 \leqq i, j \leqq t$ and the summation ranges over $s = 1, \cdots, t$. The index of summation s will have the above meaning throughout this paper.

The exceptional characters of G associated with ξ_i will be denoted by X_i, $i = 1, \cdots, t$. We have:

$$X_i(1) = x = (wp + \delta)/t$$

where w is a positive integer and $\delta = \pm 1$; hence $x \geqq q$. Also:

$$X_i(m) = \varepsilon\xi_i(m) + c \text{ for all } m \in M^{\#}, \quad i = 1, \cdots, t$$

where c is a rational integer and $\varepsilon = \pm 1$.

The non-exceptional irreducible characters of G non-vanishing on $M^{\#}$ will be denoted by R_i, $i = 1, \cdots, q$. Each of these characters is constant on $M^{\#}$, the values being either 1 or -1. Let $R_i(1) = r_i$ and let $R_i(m) = c_i$ for all $m \in M^{\#}$. Then $c_i = \pm 1$ and $r_i \equiv c_i \pmod p$. R_1 will denote the principal character of G.

Since all the remaining irreducible characters of G vanish on $M^{\#}$, none of them is linear; hence $[G: G'] \leqq q + t$.

We will need also the following inequalities. It follows immediately from the fact that if $c_i = -1$ then $r_i \geqq p - 1$ that

$$S = \sum_{i=1}^{q} c_i^3/r_i \geqq 1 - (q-1)/(p-1). \tag{2}$$

Suppose that $c_i = -1$, $i = 2, \cdots, q$. Then:

$$O = \sum_{i=1}^{t} X_i(m_1)x + \sum_{i=1}^{q} c_i r$$

$$= x(tc - \varepsilon) + 1 - \sum_{i=2}^{q} r_i$$

and therefore $tc - \varepsilon \geqq 0$. Thus if $tc - \varepsilon < 0$ then at least two c_i are equal to 1. Consequently

$$S \geqq 1 - (q-2)/(p-1) \quad \text{if} \quad tc - \varepsilon < 0 \tag{3}$$

Let s_{ijk}, $1 \leqq i,j,k \leqq t$ denote the coefficient of $\bar{C}_k$ in $\bar{C}_i\bar{C}_j$ and let c_{ijk}, $1 \leqq i,j,k \leqq t$ denote the coefficient of C_k in C_iC_j. Then it is well known that for all $1 \leqq i,j,k \leqq t$

$$s_{ijk} = (qp/p^2)(B_{ijk} + q) = (q/p)(B_{ijk} + q) \tag{4}$$

$$c_{ijk} = (g/p^2)(A_{ijk} + S) \tag{5}$$

where

$$B_{ijk} = (1/q) \sum_s \xi_s(m_i)\xi_s(m_j)\xi_s(m_k^{-1})$$

$$A_{ijk} = (1/x) \sum_s X_s(m_i)X_s(m_j)X_s(m_k^{-1}).$$

Let finally

$$\delta(i,j,k) = \delta_{ik} + \delta_{jk} + \delta_{ij^*} \quad 1 \leqq i,j,k \leqq t$$

$$K = tc^3 - 3c^2\varepsilon - 3cq$$

$$E = \{(i,j,k) \mid 1 \leqq i,j,k \leqq t, \ (i,j,k) \neq (i,i,i^*)\}$$

where $C_{i^*} = C_i^{-1}$.

We proceed by proving three lemmas, first of which summarizes some auxilary formulas. In each lemma the assumptions on the group G are those mentioned at the beginning of the proof.

LEMMA 1. *For all* $(i,j,k) \in E$

$$s_{ijk} = c_{ijk} \tag{6}$$

$$A_{ijk} = (1/x)(\varepsilon q B_{ijk} + c\delta(i,j,k)p + K) \tag{7}$$

$$tc^2 = 2\varepsilon c \tag{8}$$

Proof. Since M is a trivial-intersection-set in G, condition (iii) implies that $s_{ijk} = c_{ijk}$ whenever $(i,j,k) \in E$. To prove (7) notice that:

$$\begin{aligned} xA_{ijk} &= \sum_s (\varepsilon\xi_s(m_i) + c)(\varepsilon\xi_s(m_j) + c)(\varepsilon\xi_s(m_k^{-1}) + c) \\ &= \varepsilon \sum_s \xi_s(m_i)\xi_s(m_j)\xi_s(m_k^{-1}) \\ &\quad + c\sum_s [\xi_s(m_i)\xi_s(m_j) + \xi_s(m_i)\xi_s(m_k^{-1}) + \xi_s(m_j)\xi_s(m_k^{-1})] \\ &\quad + \varepsilon c^2 \sum_s [\xi_s(m_i) + \xi_s(m_j) + \xi_s(m_k^{-1})] + c^3 t \\ &= \varepsilon q B_{ijk} + c(\delta_{ij^*}p + \delta_{ik}p + \delta_{jk}p - 3q) - 3c^2\varepsilon + c^3 t \\ &= \varepsilon q B_{ijk} + c\delta(i,j,k)p + K. \end{aligned}$$

Finally (8) follows from:

$$\begin{aligned} p = |C_G(m_1)| &= \sum_s X_s(m_1)X_s(m_1^{-1}) + q \\ &= \sum_s (\varepsilon\bar{\xi}_s(m_1) + c)(\varepsilon\bar{\xi}_s(m_1^{-1}) + c) + q \\ &= p - q - 2\varepsilon c + tc^2 + q. \end{aligned}$$

LEMMA 2. *$q = (p-1)/2$ and $G' = G$.*

Proof. Suppose that $q < (p-1)/2$; then $t \geqq 3$ and by (8) $c = 0$. Hence by (6) and (7) all B_{ijk}, $(i,j,k) \in E$, satisfy the same linear equation:

$$qB_{ijk} + q^2 = g(\varepsilon qB_{ijk} + xS)/px. \tag{9}$$

Since $q = g\varepsilon q/px$ would imply that $g = px \leqq p\sqrt{g}$, $g \leqq p^2$ in contradiction to (1), all B_{ijk}, $(i,j,k) \in E$, are equal to each other. Let $C_3 \neq C_1, C_1^{-1}$; then:

$$q = \sum_{i=1}^{t} s_{i13} = t(qB_{113} + q^2)/p.$$

Therefore $qB_{113} + q^2 = pq/t$, which when inserted into (9) yields:

$$g = \frac{p^2qx}{(pq - tq^2)\varepsilon + txS} = \frac{p^2q^2}{(q^2\varepsilon/x) + (p-1)S}.$$

As $x \geqq q$, $(p-1)S \geqq p - 1 - (q-1) = p - q$ and $p > 3q$, it follows that:

$$g \leqq p^2q^2/(-q + p - q) \leqq p^2q$$

in contradiction to (1). Thus $q = (p-1)/2$.

As $[G: G'] \leqq q + t < p$, the order of G' is of the form $q'p(np+1)$. That follows from the fact that the number of Sylow p-subgroups of G' equals to that of G. If G' satisfies (I), then obviously G satisfies (I), in contradiction to our assumptions. If G' is of type (II), then the normalizer N_1 of M in G' has a nilpotent normal complement K in G'. Let F be the Fitting subgroup of G'; then clearly $K \subset F$ and $M \cap F = 1$. Since $G' = N_1K$, $F = (N_1 \cap F)K$. Let $x \in N_1 \cap F$, $m \in M^{\#}$; then $x^{-1}m^{-1}xm \in M \cap F = 1$, hence $x \in C_G(m) \cap F = M \cap F = 1$. Thus $F = K$ and K is characteristic in G', hence normal in G. It follows that G is of type (II), again a contradiction. Therefore G' satisfies the same assumptions as G does, and consequently by the first part of this proof $q' = (p-1)/2 = q$, $G' = G$.

LEMMA 3. *If $q = (p-1)/2$ is odd, then:*

$$g = \frac{p^2(p-3)x}{-2(q+1) + 4xS}, \quad 2c - \varepsilon = -1. \tag{10}$$

If $q=(p-1)/2$ *is even, then*:

$$g=\frac{p^2(p-1)x}{-2q+4xS},\qquad 2c-\varepsilon=1. \tag{11}$$

Proof. By (6), (4), (5), and (7) for all $(i,j,k)\in E$

$$qB_{ijk}+q^2=g(\varepsilon qB_{ijk}+K+\delta(i,j,k)cp+xS)/px. \tag{12}$$

As $t=2$, it is easy to check that if q is odd then $\delta(i,j,k)=2$ for all $(i,j,k)\in E$ and if q is even then $\delta(i,j,k)=1$ for all $(i,j,k)\in E$. Since $q\neq g\varepsilon q/px$, in each case all the B_{ijk} are equal to each other for all $(i,j,k)\in E$; so are the corresponding s_{ijk}. Thus if q is odd

$$q=1+s_{122}+s_{222},(qB_{122}+q^2)/p=s_{122}=(q-1)/2=(p-3)/4$$

and (12) yields

$$g=\frac{p^2(p-3)x}{\varepsilon[p(p-3)-(p-1)^2]+4K+8cp+4xS}.$$

If q is even, then:

$$q=s_{212}+s_{112},(qB_{112}+q^2)/p=s_{112}=q/2=(p-1)/4.$$

Consequently, (12) yields:

$$g=\frac{p^2(p-1)x}{\varepsilon[p(p-1)-(p-1)^2]+4K+4cp+4xS}.$$

We will now show that (11) holds; the proof of (10) is similar and it is left to the reader. It suffices to show that:

$$\varepsilon(p-1)+4K+4cp=-2q=1-p \text{ and } 2c-\varepsilon=1.$$

Now $K=2c^3-3c^2\varepsilon-3cq$ and $c^2=c\varepsilon$; hence:

$$4K=-4c^2\varepsilon-12cq=-4c^2\varepsilon-6cp+6c=2c-6cp$$

and

$$\varepsilon(p-1)+4K+4cp=(\varepsilon-2c)p+(2c-\varepsilon).$$

Thus it suffices to show that $2c-\varepsilon=1$. But

$$(2c-\varepsilon)^2=4c^2-4c\varepsilon+1=1$$

and consequently it remains to prove that $2c-\varepsilon\neq-1$. Suppose that $2c-\varepsilon=-1$ then:

$$g=\frac{p^2(p-1)x}{p-1+4xS}\leqq\frac{p^2(p-1)}{4[1-(q-1)/(p-1)]}<(p-1)p^2/2=qp^2$$

in contradiction to (1). The proof of the lemma is complete.

We will continue now with the proof of the theorem. Lemmas 2 and 3 yield, in view of (2), (3) and the fact that $x \geqq q$, that:

$$g \leqq \frac{p^2(p-1)}{[-2(q+1)/q] + 4[1-(q-2)/(p-1)]} = (p-1)^2 p^2/4.$$

As $g = (p-1)p(np+1)/2$, it follows that $n < (p-1)/2$. Consequently by Brauer [1, Corollary, p. 70] either G is isomorphic to $PSL(2,p)$, $p > 3$ or it is isomorphic to $PSL(2,p-1)$, where $p - 1 = 2^m > 2$. Since $q = (p-1)/2$, the second case may occur only if $q = 2$, $p = 5$. But $PSL(2,4)$ is isomorphic to $PSL(2,5)$; hence $p > 3$ and G is isomorphic to $PSL(2,p)$ for all p. The proof of the theorem is complete.

References

1. R. Brauer, *On permutation groups of prime degree and related classes of groups*, Ann. of Math. **44** (1943), 55–79.

2. W. Feit, *On a class of doubly transitive permutation groups*. Ill. J. Math. **4** (1960), 170–186.

3. W. Feit and J. G. Thompson, *Finite groups which contain a self-centralizing subgroup of order* 3. Nagoya J. Math. **21** (1962), 185–197.

4. M. Herzog, *On finite groups which contain a Fröbenius subgroup*. To appear in Journal of Algebra.

5. M. Herzog, *A characterization of some projective special linear groups*. To appear.

University of Illinois,
Urbana, Illinois