ON FINITE GROUPS WITH A CYCLIC SYLOW SUBGROUP[1]

BY
MARCEL HERZOG

Introduction

The purpose of this paper is to prove the following

THEOREM 1. *Let G be a finite group, and suppose that G contains a subgroup M of order m, satisfying the following conditions*:

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

(ii) *for some fixed prime p, the Sylow p-subgroup of M is cyclic and nontrivial*;

(iii) $q = [N_G(M):M] \neq 1, p - 1$;

(iv) *if z is an element of M of order p, and if $xy = z$, where x and y are elements of G of order p, then $x \in M$, except possibly in the case that both x and y are conjugate to z^{-1} in G_0, where G_0 is the minimal normal subgroup of G containing M.*

Then one of the following statements is true.

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

(II) *$N_G(M)/M$ is a cyclic group, M is cyclic of odd order, and if K denotes the Fitting subgroup of G, then*

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

In particular, G is solvable.

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

(IV) *G is isomorphic to $SL(2, 2^{4w+2})$, $w \geq 1$, $m = 2^{4w+2} + 1$, $q = 2$, $p = 5$.*

Groups corresponding to statements (I), (II), (III) and (IV) will be called of type (I), (II), (III) and (IV), respectively. It is not hard to check that the simple groups of types (III) and (IV) indeed satisfy the assumptions of Theorem 1. As an immediate corollary we get

COROLLARY. *Let G be a non-solvable finite group, and suppose that G contains a subgroup M satisfying conditions* (i)–(iv). *Then G is a simple group, either of type* (III) *or of type* (IV).

In three recent works, finite simple groups G with a subgroup M containing the centralizer in G of each of its nonunit elements were investigated under the condition that $q = [N_G(M):M] = 2$. M. Suzuki [7] has shown, that if it is also known that the centralizer of an involution of G has order $|M| - 1$, then G is isomorphic to $SL(2, 2^n)$, $|M| = 2^n + 1 > 3$. W. B. Stewart [6] has shown, that if $3 \mid |M|$, then G is isomorphic to $PSL(2, r)$ for some r. K. Harada [1] has shown, that if $|G| \leq 4(|M| + 1)^{*}$, then G is isomorphic to

Received January 15, 1968.
[1] This work was supported in part by a National Science Foundation grant.

$PSL(2, r)$ for some r, and if G contains two non-conjugate subgroups satisfying the conditions imposed on M, then G is isomorphic to $SL(2, 2^n)$, $2^n > 2$. As a variation on that theme, we will prove the following.

THEOREM 2. *Let G be a simple finite group, and suppose that G contains a subgroup M of order m, such that*

(a) *for all $h \in M^{\#}$, $C_G(h) \subseteq M$,*

(b) $q = [N_G(M):M] = 2$.

Assume, also, that M satisfies condition (iv) *for some prime divisor p of m. Then one of the following statements is true.*

(A) $p = 3$, *G is isomorphic to $PSL(2, r)$, where $r = mk \pm 1, k = (r - 1, 2)$.*

(B) $p = 5$, *G is isomorphic to $SL(2, 2^{4w+2})$, $w \geq 0$, where $m = 2^{4w+2} + 1$.*

Conditions (i)–(iii) of Theorem 1 exclude the case $p = 2$. If $p = 3$, the above mentioned theorem of Stewart shows that if G is simple and $q \neq 1$, then assumptions (i) and (ii) alone force G to be isomorphic to some $PSL(2, r)$. Finally, if no exceptions are allowed in condition (iv) of Theorem 1, then it follows from [4], Theorem 5, that G is either of type (I) or of type (II).

Theorem 1 and its corollary generalize the results of [2]. While in [2] the subgroup M was assumed to be cyclic of prime order p, in the present paper the corresponding restriction on M is that its Sylow p-subgroup is cyclic and nontrivial. This generalization forces a more extensive use of previous results and notation than was necessary in [2]. Therefore, although all the necessary notation is summarized below, and the partial results of [3] and [4] which are used in the proof of Theorems 1 and 2 are clearly indicated, the reader is expected to be familiar with the above mentioned papers.

The author is grateful to the referee for pointing out a mistake in the original manuscript. In the original version of this paper, the exceptional case of condition (iv) was stated in the form "unless both x and y are conjugate to z^{-1} in G". However, this condition does not necessarily hold for a normal subgroup of G containing M, a fact which is needed in the proof. As now stated, condition (iv) holds for every normal subgroup of G containing M. Indeed, it is easily seen that M is a Hall subgroup of G. Since $N_G(M)$ is a Frobenius group, M is nilpotent. Thus by [8], M is conjugate in G to $A(M)$, where A is any automorphism of G. It follows that G_0 is a characteristic sugbroup of G, and therefore if G_1 is a normal subgroup of G containing M, then G_0 is the minimal normal subgroup of G_1 containing M. Unfortunately, a similar slip occurs in [2] and [4]. In both papers, condition (iv) (in our notation) should be modified to read as stated in this work.

The proof of Theorems 1 and 2 requires a slightly more general result than those stated in [4]. It has been mentioned in that work that the results of [3] with respect to the prime number 3 hold for an arbitrary odd prime, provided that we assume condition (iv) to hold, and under the additional assumption that M is noncyclic. However, the only place where the noncyclicity of M is used in [3] is in the proof of Corollary 4.1, which clearly requires only the fact that G is not of type (II). Therefore, if G is not of type (II), and if condition (iv) holds for some prime p, then the results of [3] can be applied to that p.

We use the standard notation $C_G(T)$, $N_G(T)$, $|T|$ and $T^{\#}$, where T is a subset of the group G, to denote respectively: the centralizer, normalizer, number of elements and the nonunit elements of T. The commutator subgroup of G will be denoted by G', and $T \triangleleft G$ means: T is a normal subset in G.

Proof of Theorem 1. If $m = p$, then the result follows from the theorem of [2]. Although conclusion (II) was stated there differently, it is easy to see that the two forms of (II) are equivalent. Therefore, from now on, it will be assumed that $m > p$.

As $N_G(M)$ is a Frobenius group, q divides $p - 1$, hence $q \leq (p-1)/2$, and for each prime factor u of m, q divides $u - 1$. It follows that $q < (m-1)^{1/2}$.

Before proceeding, the necessary notation will be introduced, following that of [3] and [4] as closely as possible. By [3], Theorem 2.3, the order of G, g, is given by the formula $g = qm(nm+1)$. The t conjugate classes of G meeting $M^{\#}$ are denoted by $C_1, C_2, \cdots, C_t$, of which the first t_0 contain elements of order p; $t_0 = (p-1)/q$. The conjugate classes of $N_G(M)$ meeting $M^{\#}$ are $C_i \cap M$, $i = 1, \cdots, t$. The elements $h_1, \cdots, h_t$ of M are representatives of the C_i's and also of the $C_i \cap M$'s. The irreducible characters of $N_G(M)$, vanishing outside M, are denoted by ζ_i, $i = 1, \cdots, t$. At least one of the characters ζ_i, say ζ_1, is of degree q. The exceptional characters of G associated with the ζ_i's are X_i, $i = 1, \cdots, t$. If $h \in M^{\#}$, $X_i(h) = \varepsilon\zeta_i(h) + z_i c$, where ε and c are integers independent of i and h, $\varepsilon = \pm 1$ and $z_i = \zeta_i(1)/q$. The degree of X_1, which is associated with the above mentioned ζ_1, will be denoted by x, and is given by the formula

$$x = am + q(\varepsilon - vc)$$

where a is a nonnegative integer and $v = (m-1)/q$. Those nonexceptional irreducible characters of G which do not vanish on $M^{\#}$ are denoted by θ_i, $i = 1, \cdots, d$, and each of them takes a constant integral value c_i on $M^{\#}$. θ_1 is the principal character of G. The following notation will also be needed:

$$T = \textstyle\sum_i c_i^2, \qquad S = \sum_i c_i^3/\theta_i(1),$$

where i ranges over $1, \cdots, d$;

$$B_{ijk} = \sum_s \frac{\zeta_s(h_i)\zeta_s(h_j)\zeta_s(h_k^{-1})}{\zeta_s(1)}, \qquad 1 \leq i, j, k \leq t,$$

where s ranges over $1, \cdots, t$; and finally

$$B = \{(i, i, i^*) \mid 1 \leq i \leq t_0\}, \qquad E = \{(i, j, k) \mid 1 \leq i, j, k \leq t_0\}$$

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

We will proceed now with the proof. If $M \triangleleft G$, then (I) holds. Therefore, from now on, we will also assume that $g > qm$. By Theorem 3.1 of [3], the assumption that $q < (m-1)^{1/2}$ yields $c = 0$, $T = q$. By Theorem 1 of [5], we have $c_i = \pm 1$, $i = 1, \cdots, q = d$.

Finally, it will also be assumed that G satisfies neither conclusion (II), nor conclusion (IV), and G is of minimal order satisfying all the above mentioned conditions. Since G does not satisfy conclusion (II), it is easily seen that $N_G(M)$ has no normal complement in G. It will be our aim to derive a contradiction from these assumptions.

From the minimality of G it follows easily that $G' = G$. Indeed, by Theorem 2.3, parts e and f, of [3], $G' \supset M$, $M \not\triangleleft G'$, $M \neq N_{G'}(M)$, $G = G'N_G(M)$ and G' does not satisfy conclusion (II) of the theorem. Since $M \subset G' \triangleleft G$, G' satisfies condition (iv). If $G' \neq G$, then by the minimality of G, $G' \cong SL(2, 2^{4w+2})$, $p = 5$. But then q divides 4 and by (iii) $q < 4$; hence $q = 2$ and $N_G(M) \subseteq G'$, $G = G'$, a contradiction.

It has been mentioned in the introduction, that the results of [3], Sections 4 and 5, are also applicable to the present situation, after replacing the number 3 by the odd prime p, as long as G does not satisfy conclusion (II), which is one of our assumptions. Therefore we will refer to the hypotheses and the results of [3] in the above mentioned sense.

It follows from the assumptions (i)–(iii) that $t_0 = (p - 1)/q > 1$ and hence $E-B$ is a non-empty set. It is easy to check that G satisfies Hypothesis B of [3], and therefore it follows from Corollary 4.5 there, that $\varepsilon = -1$ and for each $(i, j, k) \in E - B$ the following holds:

$$g = qm(B_{ijk} + q)(-qB_{ijk}/x + S)^{-1}.$$

By Corollary 4.4 of [3], for all $(i, j, k) \in E\text{-}B$,

$$B_{ijk} = mA/q - q$$

where A is a positive integer given by

$$\begin{aligned} A &= (q-1)/t_0 \quad \text{if} \quad t_0 = 2, \qquad 2 \nmid q \\ &= q/t_0 \qquad\qquad \text{otherwise.} \end{aligned}$$

The above formulas yield

$$g = m^2A[(-mA + q^2)/x + S]^{-1}, \tag{1}$$

where x is the degree of the exceptional character X_1 of G. By the formula mentioned for x and in view of the fact that $c = 0$ and $\varepsilon = -1$,

$$x = am - q, \tag{2}$$

where a is a positive integer.

Since $c_i = \pm 1$ for all i, $T = q$ and $G' = G$, the definition of S and the formulas for $\theta_i(1)$ in section 3 of [3] yield the following inequalities:

$$1 - (q-1)/(m-1) \leq S \leq 1 + (q-1)/(m+1). \tag{3}$$

We notice, furthermore, that the denominator in formula (1) is a positive real number, and by the definition of A, $q^2 < Am$. Consequently, in view of (2) and (3), we get

$$(mA - q^2)/(ma - q) < S \leq 1 + (q-1)/(m+1)$$

yielding

$$\frac{m(A-a)+q-q^2}{ma-q} < \frac{q-1}{m+1}. \tag{4}$$

A contradiction will be derived now separately for the following two complementary cases: $a \leq A-1$ and $a \geq A$.

Case 1. Suppose that $a \leq A-1$. Since in this case $A-a \geq 1$, inequality (4) yields

$$(m-q^2)/(mA-m-q) < q/(m+1).$$

Consequently

$$m-q^2+1 < qA-q$$

and

$$q/2 \geq q/t_0 \geq A > m/q-q,$$

$$3q^2/2 > m. \tag{5}$$

However, since $t_0 \geq 2$ and $m > p$, $2q < p < m/q$, in contradiction to (5). Thus Case 1 cannot occur.

Case 2. Suppose that $a \geq A$. It follows then from (1), (2), and (3) that

$$\begin{aligned} g &\leq m^2A[(-mA+q^2)/(mA-q)+1-(q-1)/(m-1)]^{-1} \\ &= \frac{mA(mA-q)(m-1)}{(q-1)(q-A)}. \end{aligned}$$

As $A \leq q/t_0 \leq q/2$, we get

$$g \leq \frac{qm(m-2)(m-1)}{2(q-1)}. \tag{6}$$

Since $g = qm(nm+1)$, where n is a positive integer, inequality (6) yields

$$n \leq m/q. \tag{7}$$

As $G = G'$, it follows from the Corollary in [5], that either $m = p$, $G \cong PSL(2, p)$ or $q = 2$, $m = 2^b+1 > 3$ and $G \cong SL(2, 2^b)$. Since $m > p$, the former possibility cannot occur. In the latter case, it would follow from the fact that $A = q/t_0$ is an integer and $t_0 \geq 2$, that $p = t_0 q + 1 = 5$, hence $b = 4w+2$, and $G \cong SL(2, 2^{4w+2})$, $w \geq 1$, in contradiction to our assumptions. Thus Case 2 cannot occur, and the proof of Theorem 1 is complete.

Proof of Theorem 2. Since M is an abelian group, the number of elements of M of order p equals $p^n - 1$, for some positive n. Let t_0 be the number of conjugate classes of G, containing elements of order p; then $t_0 = (p^n-1)/q$.

Suppose first that $2 = q \geq (p^n-1)^{1/2}$. Then, either $p^n = 5$ or $p^n = 3$. In each case the Sylow p-subgroup of M is cyclic. In the former case, G is of type (B) by Theorem 1, ($PSL(2, 5) \cong SL(2, 4)$), and in the latter case G is of type (A) by [6].

It remains to deal with the case $q < (p^n-1)^{1/2} \leq (m-1)^{1/2}$, $t_0 \geq 2$. But then, by Corollary 4.4 of [3] (in the general sense, as mentioned in the introduction), t_0 divides q, and therefore $t_0 = 2$, $p^n - 1 = 4$, $p^n = 5$ and again by Theorem 1 G is of type (B).

References

1. K. Harada, *A characterization of the groups $LF(2, q)$*, Illinois J. Math., vol. 11 (1967), pp. 647–659.
2. M. Herzog, *A characterization of the simple groups $PSL(2, p)$*, Israel J. Math., vol. 5 (1967), pp. 79–85.
3. ——, *On finite groups which contain a Frobenius subgroup*, J. Algebra, vol. 6 (1967), pp. 192–221.
4. ——, *A characterization of some projective special linear groups*, J. Algebra, vol. 6 (1967), pp. 305–308.
5. ——, *On finite groups, containing a CCT-subgroup with a cyclic Sylow subgroup*, Pacific J. Math., vol. 25 (1968), pp. 523–531.
6. G. Higman, *Odd characterizations of finite groups*, Notes, Oxford Univ., January 1967.
7. M. Suzuki, *An abelian subgroup which is the centralizer of its nonidentity elements*, Lecture, Midwestern Conference on Group Theory and Number Theory, Columbus, Ohio, March 30–April 2, 1966.
8. H. Wielandt, *Zum Satz von Sylow*, Math. Zeitschr., vol. 60 (1954), pp. 407–408.

University of California
Santa Barbara, California