Pacific Journal of Mathematics

TWO SOLVABILITY THEOREMS

I. Martin (Irving) Isaacs

Vol. 23, No. 2 April 1967

PACIFIC JOURNAL OF MATHEMATICS
Vol. 23, No. 2, 1967

TWO SOLVABILITY THEOREMS

I. M. ISAACS

In this paper we prove two theorems which have certain similarities.

THEOREM I. **Let G be a group with a cyclic S_p subgroup P such that every p'-subgroup of G is abelian. Then either G has a normal p-complement or else $P \Delta G$.**

THEOREM II. **Let G be a group and let $p \neq 2$ and q be primes dividing $|G|$. Suppose for every $H < G$ which is not a q-group or a q'-group that $p \,||\, H|$. If q^a is the q-part of $|G|$ and $p > q^a - 1$ or if $p = q^a - 1$ and an S_p of G is abelian then no primes but p and q divide $|G|$.**

Both theorems are proved by studying minimal counter-examples and in both cases contradictions are obtained for $p > 3$ without the use of character theory. When $p = 3$ both minimal counterexamples satisfy the hypotheses of the same character theoretic proposition which is actually a special case of Theorem II, and this yields the desired contradictions.

Both theorems imply that the respective groups in question are solvable. In the first case the Schur-Zassenhaus Theorem (see 9.3.6 of [5]) is used and in the second case Burnside's p^iq^j theorem (see 12.3.3 of [5]) yields the solvability.

1. In this section we prove the character theoretic proposition which is a special case of Theorem II and which is used to prove both of our main results. We begin by giving a lemma which is a restatement of some of the restlts of § II of [1].

LEMMA 1. *(Brauer-Fowler) Let G be a group of even order which has only one class of involutions K_0 with $m = |K_0|$. Let K_i, $1 \leqq i \leqq r$ be the remaining nonidentity real classes in G. Then*

$$m^2 = um + \sum_{i=1}^{r} v_i \,|\, K_i \,|$$

where u is the number of involutions in the centralizer of an involution and v_i is the number of involutions which transform x to x^{-1} when $x \in K_i$.

PROPOSITION. Let G be a group with an abelian S_3 subgroup P with the properties

(1) $|\mathfrak{N}_G(P)| = 4\,|P|$, $|\mathfrak{C}_G(P)| = 2\,|P|$,

(2) $\mathfrak{C}_G(P)$ is a *T.I.* set and

(3) if $H < G$ has even order then $|H| \mid (4|P|)$.

Then G is not simple.

Proof. Suppose G is simple. It is clear that the order of an S_2 of G is 4 and thus by Burnside's theorem it must be elementary and all of its involutions are conjugate in its normalizer. Put

$$S = \mathfrak{C}_G(P) = P \times \langle s \rangle \quad \text{and} \quad N = \mathfrak{N}_G(P) = S\langle t \rangle ,$$

where s and t are commuting involutions. Since G is simple and P is abelian, we have $P \cap \mathfrak{Z}(\mathfrak{N}(P)) = 1$ by 13.5.5 of [5] and thus $\mathfrak{C}_P(t) = 1$ and t acts on P with no nontrivial fixed points. Therefore t transforms every element of P and thus also of S into its inverse. Clearly $S \triangle N$ and $P \triangle \mathfrak{N}_G(S)$ and thus $N = \mathfrak{N}_G(S)$. If two elements of S are conjugate in G they are conjugate in N since S is a *T. I.* set and if they are distinct they are inverses. Since the only elements of S equal to their inverses are s and 1, the remaining $2|P| - 2$ elements of S span $|P| - 1$ classes of G.

If $y \neq 1$ is a real element of G which is not an involution then $\mathfrak{N}_G(\langle y \rangle) < G$ has even order and thus y has order divisible by 3 and centralizes some element of order 3. By taking conjugates we may suppose that this element is in P and therefore $y \in N$. Since no element of $N - S$ centralizes any element $\neq 1$ in P, we conclude that $y \in S$. Therefore the $|P| - 1$ classes spanned be the nonself-inverse elements of S are the classes K_i of the lemma and $r = |P| - 1$.

Since $\mathfrak{C}_G(s) \supseteqq N$ and $|\mathfrak{C}_G(s)| \mid (4|P|)$ we must have $\mathfrak{C}(s) = N$. Every element of $N - S$ is an involution and therefore in the lemma we have $u = 2|P| + 1$. Since $\mathfrak{C}(s) = N, m = [G : N] = |G|/4|P|$. If $x \in S$ and $x \neq 1$, s then $\mathfrak{C}_G(x) = S$ and $|K_i| = [G : S] = 2m$. Finally, the only involutions transforming x to x^{-1} are the elements of $N - S$ and hence each $v_i = 2|P|$ and the lemma yields

$$m^2 = (2|P| + 1)m + (|P| - 1)(2|P|)(2m)$$

and therefore $m = 4|P|^2 - 2|P| + 1$ and $|G| = 4|P|m$.

Now G has $|P| + 1$ real classes and thus by Theorem 12.4 of [4] it has $|P|$ irreducible, nonprincipal real valued characters, χ_i, $1 \leqq i \leqq |P|$. Since G has m involutions,

$$m = \sum_{i=1}^{|P|} \chi_i(1)\varepsilon_i$$

where $\varepsilon_i = \pm 1$ by Theorem 3.6 of [4]. Therofore $m \leqq \sum_{i=1}^{|P|} \chi_i(1)$ and we have

$$m^2 \leqq \left[\sum_{i=1}^{|P|} \chi_i(1)\right]^2 \leqq |P| \sum_{i=1}^{|P|} \chi_i(1)^2 = |P|\,[|G| - \sum \psi_j(1)^2 - 1]$$

where the ψ_j are the irreducible nonreal valued characters. Thus

$$|P| \sum \psi_j(1)^2 \leqq |P|\,(|G| - 1) - m^2 \leqq m(4|P|^2 - m)$$

since $|G| = 4|P|m$. Since $4|P|^2 - m = 2|P| - 1 < 2|P|$, we have $\sum \psi_j(1)^2 < 2m$. Because G contains elements of order prime to 6, not every class of G is real and thus some ψ exists with $\psi \neq \bar{\psi}$ and hence $\psi(1)^2 < m$.

Now $[N:S] = 2$ and S is abelian and thus all nonlinear irreducible characters of N have degree 2. Since t acts without fixed points on P, it is clear that $N' = P$ and N has exactly 4 linear characters and thus has $|P| - 1$ distinct irredudcible characters of degree 2, say $\lambda_1, \cdots, \lambda_{|P|-1}$. Since $[N:S] = 2$ and $\lambda_i \mid S$ is reducible, it follows that λ_i vanishes on $N - S$ and we may apply Theorem 38.16 of [3] since S is a $T.\ I.$ set. Therefore G has irreducible characters

$$\zeta_1, \zeta_2, \cdots, \zeta_{|P|-1}$$

and there is $\varepsilon = \pm 1$ with $\lambda_i^G - \lambda_j^G = \varepsilon(\zeta_i - \zeta_j)$. Since each λ_i^G is real valued, the same is true of the ζ_i and thus we have the inner product $[\psi, (\lambda_i^G - \lambda_j^G)] = 0$. Therefore

$$[\psi, \lambda_i^G] = [\psi, \lambda_j^G]$$

and by Frobenius Reciprocity, $[\psi \mid N, \lambda_i] = [\psi \mid N, \lambda_j]$. We conclude that the multiplicities of each λ_i in $\psi \mid N$ are equal. Since ψ is faithful and N is nonabelian, $\psi \mid N$ has some nonlinear constituent and thus this common multiplicity is $\geqq 1$ and therefore $\psi(1) \geqq 2(|P| - 1)$. Since $\psi(1)^2 < m < 4|P|^2$, we have $\psi(1) < 2|P|$ and thus

$$\psi(1) = 2|P| - 2 \quad \text{or} \quad 2|P| - 1\,.$$

Let q be the largest prime divisor of $\psi(1)$. If $q = 2$ then since $\psi(1) \mid |G|$ we must have $\psi(1) = 4 = 2|P| - 2$ and $|P| = 3$. In this situation $m = 31$ and $|G| = 12 \cdot 31$ and since no simple group can have this order, we have a contradiction. Thus $q \neq 2$ and since $3 \mid |P|$, $q > 3$. Since $q \mid |G|$ we must have $q \mid m$ and $4|P|^2 - 2|P| + 1 \equiv 0$ mod q. Since $2|P| \equiv 1$ or 2 mod q, we have $4|P|^2 - 2|P| + 1 \equiv 1$ or 3 mod q. Since $q > 3$ this is our final contradiction.

2. In this section we prove the first of our main results. We begin with a lemma.

LEMMA 2. *Let H be an abelian group with a collection of proper subgroups $\{K_i\}$ such that $H = \bigcup K_i$ and $K_i \bigcap K_j = 1$ if $i \neq j$. Then*

H is an elementary abelian p-group for some prime p.

Proof. If $x, y \in H^{\#}$ have different orders m and n respectively, with $m > n$, choose K_i with $x \in K_i$. Then $1 \neq (xy)^n = x^n \in K_i$. If $xy \in K_j$ then $(xy)^n \in K_i \cap K_j$ and therefore $i = j$ and $xy \in K_i$. Thus $y \in K_i$. If $z \in H^{\#}$ is arbitrary then the order of z is different from at least one of m and n and thus $z \in K_i$. Thus $K_i = H$ and this contradiction shows that all elements of $H^{\#}$ have equal orders and the result follows.

THEOREM I. *Let G be a group with a cyclic S_p subgroup P such that every p'-subgroup of G is abelian. Then G has a normal p-complement or else $P \triangle G$.*

Proof. Suppose the theorem is false and let G be a minimal counterexample. Let $N = \mathfrak{N}_G(P)$ and let K be an $S_{p'}$ (p-complement) of N whose existence is guaranteed by the Schur-Zassenhaus Theorem (9.3.6 of [5]). If any element $x \in K$ centralizes a nonidentity element of P, then because P is cyclic, x centralizes all of P. (See for instance 20.1 of [4]).

Every proper subgroup of G satisfies the hypotheses and thus has either a normal S_p or $S_{p'}$. If $L \triangle G$ and $p \nmid |L|$ then G/L satisfies the hypotheses and does not have a normal $S_{p'}$ and therefore if $L > 1$, $PL \triangle G$. By Burnside's theorem, $K \not\triangle N$ and thus NL does not have a normal $S_{p'}$ and if $NL < G$, L normalizes P and P is characteristic in PL and thus is normal in G. This contradiction shows that $NL = G$. Now put $M = \bigcap_{x \in G} N^x \triangle G$. Since $x = uv$ for some $u \in N$ and $v \in L$ we have $N^x = N^{uv} = N^v \supseteqq K^v$. However KL is a p'-subgroup and thus is abelian and $K^v = K$. Since x was arbitrary, $M \supseteqq K$ and thus $M \supseteqq K^u$ for all $u \in N$. Since K is an $S_{p'}$ of the solvable group M we may conclude that K^u is conjugate to K in M by P. Hall's theorem (9.3.10 of [5]) and therefore there exists $w \in M$ with $uw^{-1} \in \mathfrak{N}_N(K)$. If $\mathfrak{N}_N(K) > K$ then $\mathfrak{N}_P(K) > 1$. This group is normalized and thus centralized by K and thus all of P is also. This contradiction shows that $\mathfrak{N}_N(K) = K, uw^{-1} \in K$, and thus $N = MK$. Since $p \nmid |K|, P \subseteqq M$ and we have $M = N$ and thus all N^x are equal and $N \triangle G$. Thus $P \triangle G$ and we have a contradiction. Our assumption on the existence of L is therefore invalid and $\mathfrak{O}_{p'}(G) = 1$.

If $P_0 \triangle G$ is a p-group, put $C = \mathfrak{C}_G(P_0) \triangle G$. If $C = G$ then K centralizes P_0 and therefore K centralizes all of P and we have a contradiction. Thus $C < G$ and since $P \subseteqq C$, C does not have a normal S_p. Therefore C is not a p-group and has a normal $S_{p'}$ and this contradicts $\mathfrak{O}_{p'}(G) = 1$ and we conclude that $\mathfrak{O}_p(G) = 1$. If $L \neq 1$

is any proper normal subgroup of G then either an S_p or an $S_{p'}$ of L is normal in G and is >1 and this contradiction shows that G is simple.

If P and P^* are two S_p subgroups of G and $P_0 = P \cap P^* > 1$, then since P is cyclic, $U = \mathfrak{N}_G(P_0) \supseteqq N$ and $U < G$. Since N fails to have a normal $S_{p'}$, the same is true of U and thus the S_p P of U is normal and $P = P^*$. Therefore P is a T. I. set. Now let

$$S = \mathfrak{C}_G(P) \subseteqq N .$$

If P^* is another S_p of G and $S^* = \mathfrak{C}(P^*)$, suppose that $S_0 = S \cap S^* > 1$. Now S_0 is not a p-group for otherwise $S_0 \subseteqq P \cap P^* = 1$, and thus there is some $x \neq 1$ in S_0 which is a p'-element. Since

$$P, P^* \subseteqq \mathfrak{C}_G(x) < G,$$

$\mathfrak{C}_G(x)$ has a normal $S_{p'}$ L. Since x is a p'-element of N we may suppose that $x \in K$ and hence $K \subseteqq \mathfrak{C}(x)$ because K is abelian. Thus $K \subseteqq L$ and $K = \mathfrak{N}_L(P)$. Since P normalizes L, it also normalizes K and this is a contradiction. Therefore $S_0 = 1$ and S is a T. I. set.

Now let A be any maximal p'-subgroup of G and B a p'-subgroup with $A \cap B \neq 1$. If $V = \mathfrak{C}_G(A \cap B) < G$ then $A, B \subseteqq V$. If V has a normal $S_{p'}$ L then $A \subseteqq L$ and by maximality $A = L$ and $B \subseteqq A$. If V has a normal S_p P_0 then V has a possibly not normal $S_{p'}$ L and since V is solvable, we may suppose that $A \subseteqq L$ by P. Hall's theorem. Thus $A = L$ and some conjugate of B is contained in A. In this situation, since A normalizes P_0 and P is a T. I. set we may conclude that A normalizes some S_p of G.

If q is a prime, $q \mid |A|$, let Q be an S_q of G with $Q \cap A \neq 1$. Then some conjugate of Q is $\subseteqq A$ and thus A is a Hall subgroup of G. If A^* is another maximal p'-subgroup of G with $q \mid |A^*|$ then A^* meets some conjugate of A and we may conclude that A^* is conjugate to A and $|A| = |A^*|$. If A does not normalize an S_p of G then A is disjoint from all other maximal p'-subgroups of G and A is a T. I. set. In this situation let $Q \subseteqq A$ be an S_q of G. Since A is abelian, $Q \triangle \mathfrak{N}_G(A)$ and since A is a $T.$ $I.$ set, $\mathfrak{N}_G(Q) = \mathfrak{N}_G(A)$ and thus by Burnside's theorem, $\mathfrak{N}_G(A) > A$. By the maximality of A it follows that $p \mid |\mathfrak{N}(A)|$ and some element of order p normalizes A.

Continuing with the situation where A does not normalize an S_p of G, suppose some element y of order p centralizes some $a \neq 1$ in A. We may suppose $y \in P$ and since $y \in P^a$ also, we conclude that $P = P^a$ and we may suppose $a \in K$. Then $K \cap A \neq 1$ and therefore $K \subseteqq A$. Since A is a $T.$ $I.$ set, y normalizes A and $K = \mathfrak{N}_A(\langle y \rangle)$ and thus y normalizes and hence centralizes K and therefore K centralizes all of P and we have a contradiction. Thus no $a \in A$ different from

1 commutes with any element of order p and since A is normalized by such an element we have $|A| \equiv 1 \bmod p$.

Let $A_0, A_1, \cdots, A_s$ be a collection of maximal p'-subgroups of G with all $|A_i|$ distinct and including all posibilities and with $K \subseteqq A_0$. If $q \mid |G|$ and $q \neq p$ then some A_i contains an S_q of G and if $q \mid |A_j|$ also, then A_j meets some conjugate of A_i and as we have seen this implies that $|A_j| = |A_i|$ and thus $j = i$. Therefore

$$|G| = |P| \prod_{i=0}^{s} |A_i| .$$

Since $K \subseteqq A_0$, no A_i for $i > 0$ can normalize an S_p of G and if $A_0 > K$, the same is true of A_0. In this situation no p-element commutes with a p'-element nontrivially and thus $\mathfrak{C}_G(P) = P$ and K is isomorphic with a subgroup of the automorphisms of P and since P is cyclic and $p \nmid |K|, |K| \leqq p - 1$. Continuing with the assumption that $A_0 > K$ we see that all $|A_i| \equiv 1 \bmod p$ and thus $|G|/|P| \equiv 1 \bmod p$. By Sylow's theorem, $|G|/|K||P| \equiv 1 \bmod p$ and therefore $1 \equiv |G|/|P| \equiv |K| \bmod p$. Since $|K| < p$ we must have $|K| = 1$ and this is a contradiction by Burnside's theorem. Therefore $A_0 = K$ and K is a maximal p'-subgroup.

Let $Z = \mathfrak{C}_K(P) < K$ and let Q be an S_q of K. Clearly, $K \subseteqq \mathfrak{N}_G(Q)$ and thus by Burnside's theorem, $K < \mathfrak{N}_G(Q)$ and hence $p \mid |\mathfrak{N}(Q)|$. Since $Z < K$ we may choose q with $Q \nsubseteqq Z$. If $\mathfrak{N}(Q)$ has a normal S_p P_0 then Q centralizes P_0 and therefore Q centralizes all of some S_p subgroup of G. It follows that Q is contained in some conjugate of Z and thus $Q^u \subseteqq Z$. However Q^u is therefore an S_q of the abelian K and $Q^u = Q$. This contradicts $Q \nsubseteqq Z$ and thus $\mathfrak{N}(Q)$ fails to have a normal S_p and hence has a normal $S_{p'}$ L and $L \supseteqq K$. By the maximality of $K, K = L$ and K is normalized by an element x of order p. If $x \in P^*$, an S_p of G, suppose $K \subseteqq \mathfrak{N}(P^*)$. Then $K \subseteqq \mathfrak{N}(\langle x \rangle)$ and thus x centralizes K and therefore K centralizes all of P^*. Since $KP^* = N_G(P^*)$ we have a contradiction and no S_p containing x is normalized by K. In particular, $x \notin P$. We conclude that each of $P, P^x, \cdots, P^{x^{p-1}}$ is normalized by K and they are all distinct. Now $\mathfrak{C}_K(P^{x^i}) = Z^{x^i}$ and since $\mathfrak{C}_G(P)$ is a $T.\ I.$ set $Z^{x^i} \cap Z^{x^j} = 1$ unless $i = j$.

Put $|Z| = c$. Since the direct product $Z \times Z^x \subseteqq K$ we have $c^2 \mid |K|$ and we set $|K| = c^2 t$. We have $|K - \bigcup Z^{x^i}| = c^2 t - p(c-1) - 1$. Now K/Z is a p'-group isomorphic with a subgroup of the automorphisms of P and thus is cyclic of order dividing $p - 1$. Since $[K : Z] = ct$, we have $ct \mid (p - 1)$.

If x centralizes any $a \neq 1$ in K then a normalizes and thus centralizes a full S_p P^* of G with $x \in P^*$. If $b \in K$ then $a^b = a$ centralizes

$(P^*)^b$ and thus $P^* = (P^*)^b$ because $\mathfrak{C}_G(P^*)$ is a $T.\ I.$ set and thus K normalizes P^*. We have seen that this is impossible and thus x acts without nontrivial fixed points on K and $p \mid (c^2t - 1)$.

We have then, $p \mid (p - 1 + c^2t)$ and since $ct \mid (p - 1)$,

$$p \mid \left[\frac{p-1}{ct} + c\right].$$

Since both $p - 1/ct$ and c divide $p - 1$, we have $(p - 1)/ct + c < 2p$ and thus $(p - 1)/ct + c = p$. This implies that $c \mid ((p - 1)/ct - 1)$ and $p - 1/ct \mid (c - 1)$. It follows that either $p - 1/ct = 1$ or $c = 1$. If $c = 1$ then $t = 1$ and thus $|K| = 1$ and this is a contradiction and therefore $p - 1/ct = 1$. This yields $t = 1$ and $c = p - 1$ and thus $|K| = (p - 1)^2$. We have then $|K - \bigcup Z^{x^i}| = c^2t - p(c - 1) - 1 = 0$ and thus $K = \bigcup Z^{x^i}$. We may therefore apply Lemma 2 to K and conclude that K is an elementary abelian q-group for some prime q. Since K/Z is cyclic of order $ct = p - 1$, we conclude that $p - 1 = q$ and thus $p = 3$ and $q = 2$. Therefore $|\mathfrak{N}_G(P)| = |P|\,|K| = 4\,|P|$ and

$$|\mathfrak{C}_G(P)| = |P|\,|Z| = 2\,|P|.$$

If $H < G$ has even order then so does an $S_{p'}$ of H and thus a maximal p'-subgroup containing it has even order and this order must equal $|A_0| = |K| = 4$ and therefore $|H| \mid (4\,|P|)$. Since $\mathfrak{C}_G(P)$ is a $T.\ I.$ set, the proposition applies and G is not simple. This contradiction proves the theorem.

We note here that an alternate method of completing the proof is to use the theorem of Brauer, Suzuki and Wall [2] instead of the proposition given here in § 1. While there are some similarities in the proofs of these two results, the Brauer-Suzuki-Wall theorem is considerably deeper.

3. Here we prove our second theorem.

THEOREM II. *Let G be a group and let $p \neq 2$ and q be primes dividing $|G|$. Suppose for every $H < G$ which is not a q-group or a q'-group that $p \mid |H|$. If q^a is the q-part of $|G|$ and $p > q^a - 1$ or if $p = q^a - 1$ and an S_p of G is abelian then no primes but p and q divide $|G|$.*

Proof. If the theorem is false, let G be a minimal counter-example. Every $H < G$ which is neither a q-group nor a q'-group satisfies the hypotheses and thus none has order divisible by any prime different from p and q. Suppose $N \triangle G$ with $1 < N < G$. If $q \mid |N|$ then no other prime but p can also divide it and thus some prime

$r \neq p$, q divides $[G:N]$. If Q is an S_q of N then $\mathfrak{N}_G(Q)N = G$ and since $r \nmid |N|$, $r \mid |\mathfrak{N}_G(Q)|$ and thus G has a subgroup of order $r\,|Q|$. This contradiction shows that $q \nmid |N|$. If any $r \neq p$ divides $|N|$, let R be an S_r of N. Then $\mathfrak{N}_G(R)N = G$ and since $q \nmid |N|$, $q \mid |\mathfrak{N}_G(R)|$ and G has a subgroup of order $q\,|R|$. This contradiction shows that N must be a p-group.

If Q is any q-subgroup of G then $\mathfrak{N}_G(Q) < G$ and thus is not divisible by any prime different from p or q. If for every $Q > 1$, $\mathfrak{N}_G(Q)/\mathfrak{C}_G(Q)$ is a q-group then by Frobenius' theorm (see for instance 21.8 of [4]) G has a normal $S_{q'}$ which must be a p-group and this is a contradiction. Thus for some Q, an S_p of $\mathfrak{N}_G(Q)$ fails to centralize Q and in particular is not normal. Thus an S_p of G is not normal and Q is normalized by an element x of order p^b which does not centralize it. Some orbit of the elements of Q thus has size $\geqq p$ and $q^a \geqq |Q| \geqq p + 1 \geqq q^a$. We have equality and thus $p + 1 = q^a$ and Q is a full S_q of G, all of whose nonidentity elements are conjugate under x. Thus since $p \neq 2$, $q = 2$ and all 2-elements of G are involutions and in one class. Furthermore, by hypothesis, an S_p subgroup P of G is abelian.

If G has the proper normal subgroup N then we have seen that N is a p-group but since G does not have a normal S_p, $p \mid [G:N]$. If $N \subseteqq H < G$ and $q \mid [H:N]$ then the only other prime which can divide $[H:N]$ is p and thus G/N satisfies the hypothesis and if $N > 1$ we have a contradiction. This shows that G is simple.

If $H < G$ has even order and an S_2 of H is not normal then H does not have a normal p-complement. If P_0 is an S_p of H then by Burnside's theorem, P_0 is properly contained in its normalizer in H. Therefore $[H:\mathfrak{N}_H(P_0)] < [H:P_0] \leqq 2^a = p + 1$. By Sylow's theorem then, $P_0 \triangle H$.

Suppose $x \neq 1$ is a real element of G. Then $\mathfrak{N}_G(\langle x\rangle) < G$ has even order and since the only 2-elements are involutions, the order of x^2 is a power of p and x^2 is a real element. If G has no nonidentity real p-elements then for every real $x \in G$, $x^2 = 1$. Since the product of two involutions is real, the set $\{x \mid x^2 = 1\}$ is a normal subgroup of G. Therefore there exists $y \neq 1$, a real p-element. Since y is transformed into its inverse by an element of $\mathfrak{N}_G(\langle y\rangle)$, y is not central in that group and thus $\mathfrak{N}_G(\langle y\rangle)$ does not have a normal S_2. It therefore has a normal S_p which is a full S_p subgroup, P of G and thus $\mathfrak{N}_G(P)$ has even order. It follows that $\mathfrak{N}(P) = PS$ where S is contained in an S_2 T of G and P is the unique S_p of G containing y.

If no involution centralizes any nonidentity p-element then S acts in a Frobenius manner on P and being abelian, it must be cyclic and thus have order 2. If $t \in T$ is an involution then $\mathfrak{C}_G(t) = T$ and in the terminology of Lemma 1, $m = |G|/2^a$ and $u = 2^a - 1$. If $1 \neq s \in S$ then s inverts every element of P. Therefore each nonidentity element of P is real and thus is contained in a unique S_p and hence P is a $T.\ I.$ set. Thus if any two elements of P are conjugate in G they are conjugate in $\mathfrak{N}_G(P)$ and thus are inverses and the nonidentity elements of P span $(|P| - 1)/2$ classes of G. These are the only real classes other than $\{1\}$ and the class of involutions and thus in Lemma 1, $r = (|P| - 1)/2$. If $x \neq 1, x \in P$ then $\mathfrak{C}_G(x) = \mathfrak{C}_{PS}(x) = P$ and the set of involutions transforming x to x^{-1} is the coset Ps. Therefore in Lemma 1, $v_i = |P|$ and $|K_i| = [G:P]$ for each i. The lemma yields

$$m^2 = m(2^a - 1) + \frac{|P| - 1}{2}|P|[G:P]\,.$$

Since $|P|\,|\,m$ and $2^a - 1 = p$, $p|P|$ divides the left side and the first term on the right side but not the remainder of the right side of the above equation and thus we have a contradiction. Therefore an involution centralizes some element of order p.

Now let $C = \mathfrak{C}_G(T)$ and suppose $C > T$. Then $C = T \times P_1$ where $P_1 > 1$ is a p-subgroup of G. Set $A = \mathfrak{C}_G(P_1) \supseteqq C$. Either $T \triangle A$ or an S_p subgroup P^* of A (which is a full S_p of G) is normal. If $P^* \triangle A$ then since $|A| = |P|\,|T| \geqq |\mathfrak{N}_G(P)|$, $A = \mathfrak{N}_G(P^*)$ and

$$1 \neq P_1 \subseteqq P^* \cap \mathfrak{Z}(\mathfrak{N}_G(P^*))$$

and this is impossible in a simple group by 13.5.5 of [5]. Thus $T \triangle A$. Let $s \in S$, $s \neq 1$ and let $B = \mathfrak{C}_G(s)$. If P_2 is an S_p of B then $s \in \mathfrak{N}_B(P_2)$ and thus $[B:\mathfrak{N}_B(P_2)] < p + 1$ and $P_2 \triangle B$. Since $P_1 \subseteqq B$ we have $P_1 \subseteqq P_2$ and thus $P_2 \subseteqq A$ and thus P_2 normalizes T. Since $T \subseteqq B$, T normalizes P_2 and thus P_2 centralizes T and $P_2 \subseteqq P_1$. Now

$$\mathfrak{C}_P(s) = P \cap B = P \cap P_2 \subseteqq P \cap P_1 \subseteqq P \cap \mathfrak{Z}(\mathfrak{N}_G(P)) = 1$$

and therefore S acts without nontrivial fixed points on P and every p-element of G is real. In particular $x \in P_1$, $x \neq 1$ is real. However, we have $\mathfrak{N}_G(\langle x \rangle) \supseteqq A$ and since $|A| = |P|\,|T|$, we have equality and x is central in $\mathfrak{N}_G(\langle x \rangle)$ and this is a contradiction. We have shown that $C = \mathfrak{C}_G(T) = T$.

If $x \neq 1$ is a p-element centralized by an involution then $\mathfrak{C}_G(x)$ has even order but does not contain a full S_2 of G and thus has a normal S_p which is a full S_p of G. Hence x is contained in a unique S_p of G which is normalized by an involution centralizing x. By taking conjugates we may suppose that $x \in P$ is centralized by $s \in S$. Put $E = \mathfrak{C}_P(s) > 1$. Now $\mathfrak{C}_G(s)$ has the normal S_p $P_0 \supseteqq E$ and since E can meet no S_p of G other than P we see that $P_0 \subseteqq P$ and thus

$P_0 = E$. If $P^* \neq P$ is an S_p of G then $P_0 \cap P^* = 1$ and thus $\mathfrak{C}_{P^*}(s) = 1$.

Choose $t \in S$, $t \neq 1$. Since all involutions of T are conjugate in $\mathfrak{N}(T)$, choose $u \in \mathfrak{N}(T)$ with $s = t^u$. If $P^u \neq P$, then $1 = \mathfrak{C}_{P^u}(s) = \mathfrak{C}_{P^u}(t^u) = \mathfrak{C}_P(t)^u$ and thus $\mathfrak{C}_P(t) = 1$. Otherwise, $P^u = P$ and $u \in \mathfrak{N}(P) = PS$ so that $u = ry$ for some $r \in S$ and $y \in P$. Now S^u normalizes P and $S^u \subseteqq T$ and thus $S^u \subseteqq \mathfrak{N}_T(P) = S$ and therefore $S = S^u = S^y$ and $y \in \mathfrak{N}_P(S)$. This group is normalized and thus centralized by S and $y \in P \cap \mathfrak{Z}(\mathfrak{N}_G(P))$ which as we have seen is trivial. Thus $y = 1$ and $u = r$ and hence $s = t$. We have therefore shown that s is the only involution in S which centralizes any nonidentity element of P.

If $|S| = 2$ then $1 \neq \mathfrak{C}_P(s) \subseteqq P \cap \mathfrak{Z}(\mathfrak{N}_G(P))$ and this is a contradiction. Thus $|S| \geqq 4$ and we may find two involutions t and t' in S, both different from s. Then both t and t' invert every element of P. Therefore tt' centralizes P and hence $tt' = s$ and $\langle s \rangle$ has index 2 in S. We have now $|\mathfrak{N}_G(P)| = |S||P| = 4|P|$ and $|\mathfrak{C}_G(P)| = |\langle P, s \rangle| = 2|P|$. Since we have seen that a nontrivial p-element which is centralized by an involution is in only one S_p, P is a $T.\ I.$ set. If $P^* \neq P$ is an S_p of G then if $\mathfrak{C}(P) \cap \mathfrak{C}(P^*) > 1$ it is not a p-group and thus contains an involution. Because $P \triangle \mathfrak{C}_G(s)$ this is impossible and $\mathfrak{C}_G(P)$ is a $T.\ I.$ set. Furthermore, since $T \subseteqq \mathfrak{C}(s)$, T normalizes P and $T = S$. Therefore $|T| = 4 = p + 1$ and $p = 3$. If $H < G$ has even order then $|H| \mid (|T||P|)$ and the hypotheses of the proposition are satisfied. Since G is simple, we have a contradiction and the theorem is proved.

We note that for $p = 2$ we can get a counterexample to the theorem by taking $G = A_5$ and $q = 3$.

References

1. R. Brauer and K. A. Fowler, *On groups of even order*, Ann. of Math. **62** (1955), 565–583.

2. R. Brauer, M. Suzuki and G. E. Wall, *A characterization of the one-dimensional unimodular projective groups over finite fields*, Illinois. J. Math. **2** (1958), 718–745.

3. C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, New York, 1962.

4. W. Feit, *Characters of finite groups*, Mimeographed notes, Yale University Math. Dept., 1965.

5. W. R. Scott, *Group Theory*, Prentice Hall, Englewood Cliffs, N. J., 1964.

Received August 8, 1966.

UNIVERSITY OF CHICAGO

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced). The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, Richard Arens at the University of California, Los Angeles, California 90024.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is \$8.00; single issues, \$3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$4.00 per volume; single issues \$1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 7-17, Fujimi 2-chome, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Pacific Journal of Mathematics

Vol. 23, No. 2 April, 1967