HALF-TRANSITIVE AUTOMORPHISM GROUPS

I. M. ISAACS AND D. S. PASSMAN

Let G be a finite group and A a group of automorphisms of G. Clearly A acts as a permutation group on $G^\#$, the set of non-identity elements of G. We assume that this permutation representation is half transitive, that is all the orbits have the same size. A special case of this occurs when A acts fixed point free on G. In this paper we study the remaining or non-fixed point free cases. We show first that G must be an elementary abelian q-group for some prime q and that A acts irreducibly on G. Then we classify all such occurrences in which A is a p-group.

THEOREM I. *Let A be a group of automorphisms of G which acts half transitively as a permutation group on $G^\#$. If $|A| > 1$, then either A acts fixed point free on G or G is an elementary abelian q-group for some prime q and A acts irreducibly.*

COROLLARY. *If a finite group G admits a non-trivial half-transitive group of automorphisms, then it is nilpotent.*

Proof. We assume that A does not act fixed point free. Let k denote the common size of all the orbits of $G^\#$ under the action of A. Given $x \in G^\#$, let A_x denote the subgroup of A fixing x so that $[A : A_x] = k$. Let P_x be the centralizer of A_x in G, that is

$$P_x = \{g \in G \mid \forall\, \alpha \in A_x,\ \alpha(g) = g\}.$$

If z is a non-identity element of G contained in both P_x and P_y, then A_x and A_y centralize z so that $A_z \supseteq \langle A_x, A_y\rangle$. Since $[A : A_x] = [A : A_y] = [A : A_z]$, we see that $A_x = A_y$ and $P_x = P_y$. Finally $x \in P_x$ and therefore the set of subgroups $\{P_x\}$ forms a partition of G. We mean by this that these subgroups have pairwise trivial intersections and that their set-theoretic union is G. We study this partition.

We show first that each P_x is a normal subgroup of G. Let $L = G \times_\sigma A$, the semidirect product of G by A. We compute the size of x^L. Let x have h conjugates in G. Then for all $\alpha \in A$, $\alpha(x)$ also has h conjugates in G. Hence x^L is a join of conjugacy classes in G of size h and therefore h divides $|x^L|$. On the other hand x^L is the join of orbits under the action of A. Since each of these has size k, k also divides $|x^L|$. Now k divides $|G| - 1$ and h divides $|G|$. Thus h and k are relatively prime and therefore hk divides $|x^L|$. This implies that x^L is the join of at least k conjugacy classes in G.

Since A is a group of automorphisms of G, A permutes the non-identity conjugacy classes of G. Let $A_{\mathrm{cl}\,x}$ be the subgroup of A fixing the class of x

Received September 20, 1965. The work of the second author was supported in part by NSF Grant GP-3933 at the University of California, Los Angeles.

https://doi.org/10.4153/CJM-1966-122-5 Published online by Cambridge University Press

under this action. The above argument shows that all orbits have size at least k. Now let x and y be non-identity conjugates in G. Then clearly $A_{\mathrm{cl}\,x} \supseteq A_x$ and $A_{\mathrm{cl}\,x} \supseteq A_y$. Also

$$[A : A_{\mathrm{cl}\,x}] \geqslant k, \qquad [A : A_x] = [A : A_y] = k.$$

This yields $A_x = A_{\mathrm{cl}\,x} = A_y$ and hence $P_x = P_y$. Therefore the partitioning subgroups are all normal in G.

If there is only one partitioning subgroup, then for all $x \in G^\#$, $P_x = G$. This means that A_x centralizes G and since A is a group of automorphisms, this yields $A_x = \{1\}$ and A acts fixed point free, a contradiction. Thus there are at least two distinct partitioning subgroups and we show that this implies that each of the groups P_x has period q for the same prime q. If not, we can find distinct partitioning subgroups P_x and P_y with elements $x_1 \in P_x^\#$, $y_1 \in P_y^\#$ having different orders. We can, of course, assume that $x = x_1$ and $y = y_1$. Let x have order m, y have order n, and $m < n$. Since P_x and P_y are disjoint normal subgroups, they commute elementwise and thus x and y commute. Set $z = y^m = (xy)^m$. Then clearly $A_z \supseteq A_y$ and $A_z \supseteq A_{xy}$ so that $A_z = A_y = A_{xy}$. Therefore $xy \in P_y$ and $y \in P_y$. Hence $x \in P_y$, a contradiction. Thus G is a q-group of period q.

We complete the proof with a somewhat different argument. The group $L = G \times_\sigma A$ acts as a permutation group on the elements of G (not $G^\#$) by $x^{g\alpha} = \alpha(xg)$. L is transitive since clearly G is. Now A is easily seen to be L_1, the subgroup fixing the identity, and this acts half transitively on $G - \{1\}$. Hence L acts 3/2 transitively. By (**5**, Theorem 10.4), L is either primitive or Frobenius. In the latter case, $L_1 = A$ would act fixed point free on the regular normal subgroup G. Since this is not the case, L is primitive. Let H be an A-admissible subgroup of G. Then the set of right cosets of H yields a set of L blocks. By primitivity these blocks are trivial, so $H = \{1\}$ or G. Since G is a q-group having only trivial A-admissible subgroups, it must be elementary abelian with A acting irreducibly. Thus the theorem follows.

The corollary follows immediately from Theorem I and the theorem of Thompson (**3** and **4**) which states that a group admitting a non-trivial fixed point free automorphism group must be nilpotent.

THEOREM II. *Let A be a non-trivial p-group of automorphisms of G which acts half transitively as a permutation group on $G^\#$. If $p > 2$, then A acts fixed point free. If $p = 2$, then A also acts fixed point free except for the cases tabulated below. In any case $|A_x| \leqslant 2$ for all non-identity x in G.*

(*i*) *$q = 2^n - 1$ is a Mersenne prime, G is abelian of type (q, q), and A is either*

$$gp\langle x, y \mid x^{2^n} = 1, y^2 = 1, y^{-1}xy = x^{-1}\rangle,$$

the dihedral group of order 2^{n+1}, or

$$gp\langle x, y \mid x^{2^{n+1}} = 1, y^2 = 1, y^{-1}xy = x^{-1+2^n}\rangle,$$

the semidihedral group of order 2^{n+2}.

https://doi.org/10.4153/CJM-1966-122-5 Published online by Cambridge University Press

(ii) $q = 2^n + 1$ *is a Fermat prime*, G *is abelian of type* (q, q), *and* A *is the group*

$gp\langle x, y, z | x^{2n} = 1, y^2 = 1, z^2 = 1, y^{-1}xy = x, z^{-1}yz = yx^{2^{n-1}}, z^{-1}xz = x^{-1}\rangle$.

(iii) $q = 3$, G *is abelian of type* $(3, 3, 3, 3)$, *and* A *is either*

$$gp\langle x, y, z | x^8 = 1, y^2 = 1, z^2 = 1, y^{-1}xy = x, z^{-1}yz = yx^4, z^{-1}xz = x^{-1}\rangle$$

or a central product of the dihedral and quaternion groups of order 8.

Proof. By Theorem I, if A does not act fixed point free, then $G = Q$ is an elementary abelian q-group ($q \neq p$) and A acts irreducibly on Q.

LEMMA 1 (Roquette). *Let P be a p-group with the property that every normal abelian subgroup is cyclic. Then P is one of the following:*
(i) *if p is odd, then P is cyclic,*
(ii) *if $p = 2$, P is cyclic, dihedral, semidihedral, or quaternion.*

LEMMA 2 (Roquette). *Let the p-group P act irreducibly and faithfully on the vector space V. Suppose P has a normal, non-cyclic, abelian subgroup D. Then P has a subgroup H, normal of index p, with $H \supseteq D$ and such that the representation restricted to H splits into p inequivalent conjugates.*

Both results are proved in **(2)**. However the second lemma is given in a slightly different form, so we offer another proof of this below.

Proof. We use Clifford's theorem **(1**, §49**)**. The representation restricted to D breaks up into conjugate irreducible representations under the action of G. If $\mathfrak{R}$ is one such representation, let $T = \{x \in G | \mathfrak{R}^x = \mathfrak{R}\}$ be its inertial group. Then D has $t = [P : T]$ distinct irreducible constituents in its representation. If $t = 1$, then all constituents are equivalent and thus $\mathfrak{R}$ is faithful. Since D is abelian, it must be cyclic, a contradiction. Thus $t > 1$ and we can choose H to be a maximal subgroup of P containing T. Since $[P : H] = p$, the representation restricted to H either decomposes into the direct sum of p distinct conjugates or all irreducible constituents are equivalent. We show that the latter possibility cannot occur.

Suppose to the contrary that all the irreducible constituents of H are equivalent. Choose one such $\mathfrak{S}$ so that $\mathfrak{R}$ is a constituent of $\mathfrak{S}|D$. Since all the irreducible constituents of H are equivalent, this implies that $\mathfrak{R}$ has only t/p distinct conjugates, a contradiction.

LEMMA 3. *Let $p > 2$. Then A is cyclic and acts fixed point free on Q.*

Proof. If A is not cyclic, then by Lemmas 1 and 2 we can choose a subgroup B of A of index p on which the representation splits. Then

$$Q = \sum_1^p Q_i,$$

each Q_i is a B-subspace, and if $g \in A - B$, then g permutes the Q_i cyclically.

https://doi.org/10.4153/CJM-1966-122-5 Published online by Cambridge University Press

Choose $x \in Q_1^\#$, $y \in Q_2^\#$. Clearly (using the fact that we have at least three terms in the direct sum) $A_x \subseteq B$, $A_y \subseteq B$, $A_{xy} \subseteq B$. Thus also $A_x \supseteq A_{xy}$, $A_y \supseteq A_{xy}$. Since these centralizers all have the same orders, this yields $A_x = A_{xy} = A_y$.

Let y vary over $Q_2^\#$. Then we see that A_x centralizes Q_2 and hence all Q_i $(i \neq 1)$. But by the same argument A_y centralizes Q_1. Since $A_x = A_y$, A_x centralizes Q. Since the representation is faithful, $A_x = \{1\}$. Finally since A is half transitive, it acts fixed point free. Since $p > 2$, it follows that A is cyclic. On the other hand if A is cyclic, then it has a minimum subgroup and so it acts fixed point free. This proves the result.

This lemma proves the theorem in case $p > 2$. For convenience we define the following groups:

$C_n \; = gp\langle x | x^{2^n} = 1\rangle$, the cyclic group of order 2^n,

$D_n \; = gp\langle x, y | x^{2^n} = 1, y^2 = 1, y^{-1}xy = x^{-1}\rangle$, the dihedral group of order 2^{n+1},

$S_n \; = gp\langle x, y | x^{2^{n+1}} = 1, y^2 = 1, y^{-1}xy = x^{-1+2^n}\rangle$, the semidihedral group of order 2^{n+2},

$Qu_n = gp\langle x, y | x^{2^n} = 1, y^2 = x^{2^{n-1}}, y^{-1}xy = x^{-1}\rangle$, the quaternion group of order 2^{n+1}.

LEMMA 4. *If $2^n = q^r + 1$, then $r = 1$ and $q = 2^n - 1$ is a Mersenne prime. If $2^r = q^s - 1$, then we have either*

(i) *$s = 1$ and $q = 2^r + 1$ is a Fermat prime or*

(ii) *$q = 3$, $s = 2$, $r = 3$.*

Proof. Let $2^n = q^r + 1$. If r is even, then $q^r \equiv 1 \pmod 4$ and hence $2^n \equiv 2 \pmod 4$. Thus $2^n = 2$ and $q^r = 1$, a contradiction. Thus r is odd and $2^n = (q+1)(q^{r-1} - q^{r-2} + \ldots + 1)$. Now the second factor contains an odd number of terms and hence is odd. On the other hand it divides 2^n and so must equal 1. Thus $r = 1$ and the first result follows.

Let $2^r = q^s - 1$. If s is odd, then $2^r = (q-1)(q^{s-1} + \ldots + 1)$. Again the second factor is an odd divisor of 2^r and therefore it is equal to 1. This yields (i). Finally let $s = 2m$ be even. Then $2^r = (q^m - 1)(q^m + 1)$ so that $q^m - 1 = 2^u$, $q^m - 1 = 2^v$. Thus $2^v - 2^u = 2$ and therefore $2^v = 4$, $2^u = 2$, and $q^m = 3$. This yields (ii) and the result follows.

LEMMA 5. *Let the 2-group P act transitively on $Q - \{1\}$. Then we have either*

(i) *$P = C_n$, $|Q| = q = 2^n + 1$ so that q is a Fermat prime or*

(ii) *$q = 3$, $|Q| = 9$, $P = S_2$, C_3, or Qu_2.*

Proof. Let P_x fix $x \in Q^\#$. By transitivity, $2^r = [P: P_x] = q^s - 1 = |Q^\#|$. By Lemma 4, the only solutions are then (i′) $s = 1$, $q = 2^r + 1$ or (ii′) $q = 3$, $s = 2$, $r = 3$. In the first case, Q is cyclic of prime order, so P is cyclic. Hence $P_x = \{1\}$, $r = n$, and (i) follows. In the second case $|Q| = 9$ and P is a subgroup of S_2, the Sylow 2-subgroup of GL(2, 3). Note that $|S_2| = 16$ and

https://doi.org/10.4153/CJM-1966-122-5 Published online by Cambridge University Press

$[P: P_x] = 8$. If $|P_x| > 1$, then $|P| \geqslant 16$ so $P = S_2$. If $|P_x| = 1$, then $|P| = 8$ and P acts fixed point free. Thus $P = C_3$ or Qu_2.

LEMMA 6. *Suppose that for all $x \in Q^{\#}$, $|A_x| = 2$. Then $|Q| = q^{2r}$ and $q^r + 1$ is equal to the number of non-central involutions of A.*

Proof. The central involution acts like (-1) and acts fixed point free. Let I denote the set of non-central involutions. Since for $x \in Q^{\#}$, $|A_x| = 2$, we see that $x \in \mathfrak{C}_Q(A_x) = \mathfrak{C}_Q(g)$ where $g \in I$. Thus $Q = \cup_{g \in I} \mathfrak{C}_Q(g)$. If $|I| \leqslant 2$, then Q is the union of two proper subspaces, a contradiction. Hence $|I| \geqslant 3$. Note also that the spaces $\mathfrak{C}_Q(g)$ have pairwise trivial intersection.

Let $g \in I$ and choose $h \in I$ with $h \neq g, -g$. Such a choice is possible since $|I| \geqslant 3$. Then

$$Q = \mathfrak{C}(g) \dotplus \mathfrak{C}(-g) = \mathfrak{C}(h) \dotplus \mathfrak{C}(-h).$$

We assume for convenience that $|\mathfrak{C}(h)| \geqslant |\mathfrak{C}(-h)|$. Now $\mathfrak{C}(g) \cap \mathfrak{C}(h) = \{1\}$ and $\mathfrak{C}(-g) \cap \mathfrak{C}(h) = \{1\}$. These imply that $|\mathfrak{C}(g)| = |\mathfrak{C}(-g)| = |Q|^{1/2}$. Say $|Q| = q^{2r}$. Then $|\mathfrak{C}(g)| = q^r$ and from the disjoint union we conclude that

$$|I|(q^r - 1) = (q^{2r} - 1)$$

or $|I| = q^r + 1$ and the result follows.

We now study the exceptional groups of Lemma 1. If A is cyclic or generalized quaternion, then A acts fixed point free. The others cannot act fixed point free.

LEMMA 7. *If $A = D_n$ or S_n then $q = 2^n - 1$ is a Mersenne prime and $|Q| = q^2$. Conversely, let $q = 2^n - 1$ be a Mersenne prime. Then S_n is a Sylow 2-subgroup of* GL$(2, q)$ *and both S_n and its subgroup of index 2, D_n, act half transitively on $Q - \{1\}$, where Q is abelian of type (q, q).*

Proof. Let $A = D_n$ or S_n. Then A has 2^n non-central involutions and a cyclic subgroup of index 2 acting fixed point free. Since, for all $x \in Q^{\#}$, A_x is disjoint from this cyclic subgroup, we have $|A_x| \leqslant 2$. If A acts half transitively, then since A cannot act fixed point free, we have $|A_x| = 2$. Thus Lemma 6 applies and $|I| = 2^n = q^r + 1$ with $|Q| = q^{2r}$. By Lemma 4, $r = 1$ and $q = 2^n - 1$ is a Mersenne prime. Thus the first result follows.

Let $q = 2^n - 1$ be a Mersenne prime so that a Sylow 2-subgroup of GL$(2, q)$ is isomorphic to S_n. S_n has a subgroup of index 2 isomorphic to D_n. Let A be either of these two groups. Then A has 2^n non-central involutions and a cyclic subgroup of index 2 acting fixed point free. Thus again $|A_x| = 1$ or 2 for each $x \in Q^{\#}$. Now each non-central involution centralizes a proper subspace of Q and hence (since $|Q| = q^2$) fixes precisely $q - 1$ elements of $Q^{\#}$. Thus there are $2^n(q - 1) = (q + 1)(q - 1) = q^2 - 1$ elements x of $Q^{\#}$ with $|A_x| = 2$. Hence A acts half transitively on Q.

We now proceed to prove the theorem. We need only consider the case where $p = 2$ and A does not act fixed point free. Thus A is not cyclic or quaternion.

If $A = S_n$ or D_n, the result follows by the previous lemma. Hence we assume $A \neq C_n$, Qu_n, S_n, or D_n. By Lemmas 1 and 2, A has a subgroup B of index 2 on which the representation splits. Moreover B contains a normal abelian non-cyclic subgroup of A. Then $Q = Q_1 + Q_2$, each Q_i is a B-subspace, and if $g \in A - B$, then g permutes the Q_i.

Let K_i be the kernel of the representation of B and Q_i. Then K_1 and K_2 are conjugate in A, $K_1 \cap K_2 = \{1\}$ and $|K_1| = |K_2|$. Moreover $B/K_1 \simeq B/K_2$. Let $x \in Q_i^{\#}$. Then clearly $B \supseteq A_x \supseteq K_i$. Thus we see that B/K_i acts half transitively on Q_i. Let $x \in Q_1^{\#}$. If A_x centralizes Q_2, then $K_2 \supseteq A_x \supseteq K_1$. Since $K_1 \cap K_2 = \{1\}$, this yields $A_x = \{1\}$ and A acts fixed point free, a contradiction. Thus $\mathfrak{C}_{Q_2}(A_x) = Q'_2$ is a proper subspace of Q_2. Let g be a fixed element of $A - B$. Let $y \in Q_2 - Q'_2$. If $A_{xy} \subseteq B$, then $A_{xy} \subseteq A_x$ and $A_{xy} \subseteq A_y$ so $A_x = A_y$ and A_x centralizes y, a contradiction. Thus $A_{xy} \not\subseteq B$. Let $gb \in A_{xy}$ with $b \in B$. Then $x^{gb} = y$ and y belongs to the orbit of x^g under the action of B/K_2. Thus

$$|(x^g)^{B/K_2}| \geqslant |Q_2 - Q'_2| > \tfrac{1}{2}|Q_2^{\#}|.$$

But B/K_2 acts half transitively on Q_2 so all the orbits have the same size. Hence B/K_2 acts transitively on Q_2 and Lemma 5 applies. There are several possibilities to consider.

Case 1. $B/K_1 \simeq B/K_2 \simeq S_2$, $|Q_1| = |Q_2| = 9$.

We show that this cannot occur. Since S_2 has a cyclic subgroup of index 2 acting fixed point free, we see that $x \in Q_i^{\#}$ implies $[A_x : K_i] = 2$. Let $x \in Q_1^{\#}$, $y \in Q_2^{\#}$. Then $A_{xy} \cap B = A_x \cap A_y$ so that $[A_{xy} : A_x \cap A_y] \leqslant 2$. Since $|A_x| = |A_y| = |A_{xy}|$, this yields $[A_x : A_x \cap A_y] \leqslant 2$, $[A_y : A_x \cap A_y] \leqslant 2$. Thus $[A_x : A_x \cap K_2] \leqslant 4$ and $[A_x : K_1 \cap K_2] \leqslant 8$. Since $K_1 \cap K_2 = \{1\}$, $|A_x| \leqslant 8$ and $|K_1| = |K_2| \leqslant 4$. Let x_i $(i = 1, 2, 3, 4)$ be generators for the four subspaces of Q_1. Then $[K_2 : A_{x_i} \cap K_2] \leqslant [A_y : A_{x_i} \cap A_y] \leqslant 2$. Since $|K_2| \leqslant 4$, K_2 has at most three subgroups of index 2. Thus for, say, x_1 and x_2 we have $[K_2 : K_2 \cap A_{x_1} \cap A_{x_2}] \leqslant 2$. Since $Q_1 = \langle x_1, x_2 \rangle$, $A_{x_1} \cap A_{x_2} = K_1$, so $|K_2| \leqslant 2$ and $|A_y| \leqslant 4$.

Again $[A_y : A_{x_i} \cap A_y] \leqslant 2$ and A_y has at most three subgroups of index 2. Thus for, say, x_1 and x_2 we have

$$[A_y : A_{x_1} \cap A_{x_2} \cap A_y] = [A_y : K_1 \cap A_y] \leqslant 2.$$

Therefore $|K_1| \geqslant |K_1 \cap A_y| \geqslant |A_y|/2 = |K_2| = |K_1|$. Hence $K_1 = K_1 \cap A_y$ and $K_1 \subseteq A_y$. Thus $K = \langle K_1, K_2 \rangle \subseteq A_y$. But $K \lhd A$, so K centralizes the subgroup of Q generated by all y^A. Since A acts irreducibly, K centralizes Q. Hence $K = \{1\}$ and $K_1 = K_2 = \{1\}$. This means that $B \simeq S_2$. Now we have assumed that B contains a non-cyclic normal abelian subgroup. Since S_2 does not contain such a subgroup, we have a contradiction. Thus this case does not occur.

In the remaining cases, B/K_i acts fixed point free. Let $x \in Q_1^{\#}$, $y \in Q_2^{\#}$. Then $A_{xy} \cap B = K_1 \cap K_2 = \{1\}$, so $|A_{xy}| = 2$. Thus Lemma 6 applies and $I \not\subseteq B$. Also $A_x = K_1$ so $|K_1| = |K_2| = 2$.

Case 2. $B/K_1 \simeq B/K_2 \simeq C_n$, $|Q| = q^2$ where $q = 2^n + 1$ is a Fermat prime.

Now K_1 is central in B (since it is normal in B and has order 2) and B/K_1 is cyclic, so B is abelian. Since B has two disjoint subgroups K_1 and K_2, we see that B is abelian of type $(2, 2^n)$ and $|I \cap B| = 2$. By Lemma 6, $|I| = q + 1 = 2^n + 2$, so $|I - (I \cap B)| = 2^n$. Let g be an element of order 2 not in B and let $b \in B$. Then $(gb)^2 = 1$ if and only if $g^{-1}bg = b^{-1}$. Let $D = \{b \in B | g^{-1} bg = b^{-1}\}$. Since B is abelian, D is a subgroup of B and $|D| = |I - (I \cap B)| = 2^n$. Since K_1 is not a central subgroup of A, $K_1 \cap D = \{1\}$. Thus $B = D + K_1$ and D is cyclic of order 2^n. This yields the groups of type (ii) in the theorem.

We show now that this situation does in fact occur. Let θ be an element of an order 2^n in GF(q) = GF$(1 + 2^n)$. Set

$$x = \begin{bmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{bmatrix}, \qquad y = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad z = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Then $A = \langle x, y, z \rangle$ is the group of type (ii). A trivial argument using Lemma 6 shows that A acts half transitively on Q, a group of type (q, q).

Case 3. $B/K_1 \simeq B/K_2 \simeq C_3$, $|Q| = 3^4$.

The methods of Case 2 yield the result here. We need only show that this situation occurs. Set

$$x = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{bmatrix}, \qquad y = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad z = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Let $A = \langle x, y, z \rangle$. Again trivial verification shows that A acts half transitively on Q, a group of type $(3, 3, 3, 3)$.

Case 4. $B/K_1 \simeq B/K_2 \simeq Qu_2$, $|Q| = 3^4$.

Since B is not abelian, we require an alternative approach here. Let Z be the third subgroup of order 2 of $\langle K_1, K_2 \rangle = K$. Since $B/K_1 \simeq Qu_2$, we have B/K abelian of type $(2, 2)$. Let $x \in B$. If $x \in K$, then $x^2 = 1 \in Z$. If $x \notin K$, then $x^2 \in K$. Now $B/K_i \simeq Qu_2$, so $x^2 \notin K_i$. Hence $x^2 \in Z$. Clearly Z is central in A. Now B contains two non-central involutions of A, so by Lemma 6,

$$|I - (I \cap B)| = 10 - 2 = 8.$$

Let $w \in I - (I \cap B)$. If $(bw)^2 = 1$ with $b \in B$, then $w^{-1}bw = b^{-1}$. Since b has order 2 or 4, we have $b^{-1} = bz$ with $z \in Z$. Let

$$C = \{b \in B | w^{-1}bw = bz \text{ for some } z \in Z\}.$$

Since Z is central, C is a subgroup of B. Now C contains the eight $b \in B$ with $(bw)^2 = 1$ and also $C \supseteq K_1$. Hence $|C| > 8$ and since $|B| = 16$, we have $B = C$. Thus for each $b \in B$, $w^{-1}bw = bf(b)$ with $f(b) \in Z$. The map $b \rightarrow f(b)$ is easily seen to be a homomorphism of B into Z, a group of order 2. Let D be its kernel. Since $D \cap K_1 = \{1\}$, we see that $|D| = 8$ and $D + K_1 = B$. Clearly $D \simeq Qu_2$.

Let $E = \langle Z, K_1, w\rangle$. Clearly E centralizes D and $E \simeq D_2$. Also $E \cap D = Z$, the common centre of both. Hence $A = \langle D, E\rangle$ is the central product of Qu_2 and D_2. Since such a group A has 10 non-central involutions, it is easy to see that this case does occur.

This completes the proof of Theorem II.

The authors wish to thank Professors R. Steinberg and E. Straus for their helpful suggestions.

References

1. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (New York, 1962).
2. P. Roquette, *Realisierung von Darstellungen endlicher nilpotenter Gruppen*, Arch. Math., *9* (1958), 241–250.
3. J. G. Thompson, *Normal* p-*complements for finite groups*, Math. Z., *72* (1960), 332–354.
4. ——— *Normal* p-*complements for finite groups*, J. Alg., *1* (1964), 43–46.
5. H. Wielandt, *Finite permutation groups* (New York, 1964).

University of Chicago and
Yale University