Can. J. Math., Vol. XXVI, No. 3, 1974, pp. 513–531

HALL HIGMAN TYPE THEOREMS, I

T. R. BERGER

Suppose Q is a q-group for a prime q and $C \leqq \mathrm{Aut}(Q)$ is cyclic of order p^e for a prime $p \neq q$. Let k be a splitting field for CQ, the semidirect product of C by Q, of characteristic $r \neq q$. Let V be a faithful irreducible $k[CQ]$-module. The $k[CQ]$-module V has been widely studied. When $r = p$ the situation outlined above is similar to the situation occurring in the proof of Theorem B of Hall and Higman [**3**]. When $r \neq p$ it is similar to the corresponding theorem of Shult [**5**]. In all but restricted cases $V|C$ has a regular $k[C]$-direct summand.

It is the object of this sequence of papers to study a related situation. Let G be a group and $A \leqq \mathrm{Aut}(G)$ a nilpotent group of order prime to $|G|$. Assume k is a field. Suppose U is a faithful irreducible $k[AG]$-module. What can be said about $U|A$? In a certain sense this is the general problem. With $C = A$, $Q = G$, $V = U$ we see this as a generalization of the Hall-Higman configuration. In that case $V|C$ "almost always" has a regular direct summand. We then are looking for similar answers when we look at $U|A$. We will not always require that $(|A|, |G|) = 1$; and we will not always find "$U|A$ contains a regular direct summand" is the correct answer. But the analogy with the situation in Theorem B is very good, especially when we start deciding how we might prove some possible theorem.

The path to and the form of answers to the general question are complex. Therefore we have separated the proofs into several parts. The first two major subdivisions are in direct analogy with the proof of Theorem B. In the final steps of that proof the structure of Q is studied closely. Two cases must be considered. In the first case Q is elementary abelian and minimal normal in CQ. For this structure it is observed that C is semiregular on the elements of $Q^\# = Q - 1$. The presence of all regular orbits on $Q^\#$ then is the key to seeing that $V|C$ contains a regular direct summand. In the more general setting we worry about the existence of regular A-orbits on sections of G. To be much more specific, the following question is posed.

(1) If $k = \mathrm{GF}(r)$, when does the permutation representation of A on $U^\#$ contain a regular orbit?

In the second case of Theorem B, Q is extra special, $[C, Z(Q)] = 1$, and $Q/Z(Q)$ is minimal normal in $CQ/Z(Q)$. In this situation the representation of C on V is determined and $V|C$ studied directly. In the more general setting we worry about the appearance of extra special subgroups of G normalized by AG. The question becomes:

Received June 19, 1972 and in revised form, October 17, 1973. This research was partially supported by National Science Foundation Grant GP-38879.

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

(2) If $S \Delta AG$, $S \leqq G$ an extra special s-group with $Z(S) \leqq Z(AG)$, $SZ(AG)/Z(AG)$ minimal normal in $AG/Z(AG)$, and A faithful on S, then when does $U|A$ contain a regular direct summand?

Answers to these two questions are then used to provide answers to the general question. It should be remarked here that no completely general answers are given here. In fact, some of the machinery is developed in a more general fashion than it is used. Hopefully this will avoid future duplication as the results are extended.

Let us look at a special case of (1) and (2). If no Sylow t-subgroup of A involves $\mathbf{Z}_t \wr \mathbf{Z}_t$ then in answer to (1) for $(|A|, r) = 1$, A always has a regular orbit on the elements of $U^{\#}$. For (2) under the same hypothesis it turns out that $U|A$ contains a regular direct summand unless the embedding of S in G is very uncomplicated and certain equations involving primes are satisfied as in Theorem B.

Certain general rules can be laid down about answers like the one above. For a given set of hypotheses the answers to (1) and (2) will be similar. In (1) the words "regular orbit" appear and in (2) these words will be changed to "regular direct summand". Answers to (2) will have more exceptions than (1). If there are prime exceptions in both cases, it will probably be true that changing the signs for case (1) exceptions will lead to case (2) exceptions. There are very good reasons for these similarities. For example, proofs for the two answers given above are very similar. In (1) we argue on additive module structure and in (2) we argue on product module structure. The proofs are by induction. The induction steps are similar for (1) and (2) and will be discussed elsewhere. It is in the discussion of minimal cases that (1) and (2) differ.

The foregoing discussion tells approximately how these papers will be organized. Minimal cases will be discussed separately from the induction steps. Finally answers to (1) and (2) will be given before the general question is tackled. In all papers, all groups will be solvable.

1. Remarks and notation. In this paper we concentrate upon consideration of some minimal cases that might occur in answer to (1). Thus we are looking at the following:

(a) A group $G = AB$ with normal cyclic subgroup B and nilpotent complement A where $A \cap B = 1$;

(b) a field $k = \mathrm{GF}(r)$ for a prime r; and

(c) a $k[G]$-module V which is faithful and irreducible.

Further $V|N$ is homogeneous whenever $N \Delta G$.

Under these conditions, A has a regular orbit on $V^{\#}$ unless G is a group of a very special type. The exceptional groups are all tabulated in (4.2). Most notation is self-explanatory and standard.

This theorem has an almost purely combinatorial proof and was first proved that way. A proof can be based upon ideas in Section 3 of [**1**]. To enhance readability, a group theoretic proof is given here. First G is embedded in the

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

semidirect product of a Galois group by a multiplicative group of a field. Then conditions are found for the existence of regular A-orbits. These conditions limit the order of B. Once B is pinned down, the order of the Galois group is ascertained. Finally, in Section 3 the exceptions are itemized. Three, rather than two or one, regular orbits are given because of later induction steps.

We will need the following lemma.

(1.1) [**2**, Theorem 5.4.9] *If P is a p-group and every characteristic abelian subgroup of P is cyclic, then*

(i) *p is odd and P is the central product of an extra special p-group of exponent p with a cyclic p-group, or*

(ii) *$p = 2$ and $P = E \dot{\times} C$ is the central product of an extra special 2-group E with a group C which is cyclic, dihedral of order $|C| \geqq 16$, semidihedral, or generalized quaternion.*

2. A minimal case: group theoretic arguments. We fix the following assumptions throughout the rest of the paper.

(2.1) (1) *$G = AB$ is a group with normal cyclic subgroup B and nilpotent complement A where $A \cap B = 1$.*

(2) *$k = GF(r)$ for a prime r.*

(3) *V is a faithful irreducible $k[G]$-module such that $V|L$ is homogeneous for all $L \Delta G$.*

Let $\tilde{k} \geqq \hat{k} \geqq k$ be finite extensions of k. Suppose $\mathscr{G} = \operatorname{Aut}(\tilde{k}/\hat{k})$ is the Galois group of $\tilde{k}$ over $\hat{k}$. Let $\mathscr{T} = \mathscr{T}(\tilde{k}/\hat{k}) = \mathscr{G}\tilde{k}^{\times}$ be the semidirect product of $\mathscr{G}$ with the multiplicative group $\tilde{k}^{\times}$ of $\tilde{k}$. When $\tilde{k}$ and $\hat{k}$ are understood we will just denote this group as $\mathscr{T}$. Now for $\sigma\mu \in \mathscr{T}$; $\sigma \in \mathscr{G}$, $\mu \in \tilde{k}^{\times}$, we have the action

$$\sigma\mu \cdot v = \sigma(\mu v)$$

upon $\tilde{k}^{+}$. So $\tilde{k}^{+}$ is a faithful irreducible $\mathscr{T}$-module.

In this section we show that G may be identified with a subgroup of $\mathscr{T}$ and V with $\tilde{k}^{+}$ for some choice of $\tilde{k}$ and $\hat{k}$. Further, we investigate a few properties which G must possess as a subgroup of $\mathscr{T}$. Finally, we state conditions that are necessary and sufficient for finding regular orbits in the action of A upon V.

The following lemma is slightly useful here and appears in later papers of this sequence.

(2.2) *Let P be a p-group. Suppose $P_0 \Delta P$ and every subgroup N of P_0, which is abelian and normal in P, is cyclic. Then*

(a) *if p is odd, P_0 is cyclic;*

(b) *if $p = 2$ then P_0 is cyclic or P_0 contains a cyclic self centralizing subgroup C_0 of index two in P_0 and normal in P.*

Let N be a characteristic abelian subgroup of P_0. Then $N \Delta P$ so N is cyclic. So by (1.1) P_0 is the central product of an extra special group with a cyclic

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

group or $p = 2$ and P_0 is the central product of an extra special group with a group which is semidihedral, generalized quaternion, or dihedral of order $\geqq 16$.

In the above group types, $P_0' = [P_0, P_0] = D$ is cyclic. Now $C_{P_0}(D) = E$ is characteristic in P_0 so it is normal in P. It contains the extra special "part" of P_0 and is the central product of a cyclic group with an extra special group. We show that P normalizes a maximal abelian subgroup of E.

Let B be an abelian subgroup of E maximal with respect to being normalized by P. Assume B is not maximal abelian in E. Then $C_E(B) > B$ and is normalized by P. Since P is a p-group there is an $x \in C_E(B) - B$ so that $[x, P] \subseteq B$. Let $B_1 = \langle x, B\rangle$. Now $[x, B] = 1$ so $B_1 > B$ is abelian and $B_1 \Delta P$. This violates the maximality of B. So B is a maximal abelian subgroup of E.

So $B \Delta P$, being abelian and in P_0, must be cyclic. If $|Z(E)| \neq p$ then $\exp Z(E) = \exp E$ so $B \geqq Z(E)$ implies $B = Z(E)$. But this implies that $B = E$ is cyclic. If p is odd, $E = P_0$ and so P_0 is cyclic. If $p = 2$, $[P_0:E] = 2$ or 1 and we are done.

Therefore we may assume $|Z(E)| = p$. Therefore $E = P_0$ and P_0 is extra special or cyclic. If P_0 is cyclic we are done. If P_0 is extra special then $p = 2$ and $[P_0:B] = 2$ completing the proof.

(2.3) *Assume that* ((2.1)1) *holds. Suppose that every normal abelian subgroup of G is cyclic. Then G contains a cyclic self-centralizing subgroup $M \geqq B$. Further,*

(a) $C_G(B) = (A \cap C_G(B)) \times B$;

(b) $(|A \cap C_G(B)|, |B|) = 1$;

(c) $M = C_G(B)$ or $[C_G(B):M] = 2$ *and an S_2-subgroup of $C_G(B)$ is quaternion, generalized quaternion, dihedral, or semidihedral.*

In particular, this lemma applies when (2.1) *holds.*

Among all normal abelian subgroups containing B, choose M maximal. M is cyclic. Now $M \geqq B$ so G/M is nilpotent. Suppose $C_G(M) > M$. Choose $D/M \leqq C_G(M)/M \cap Z(G/M)$ of prime order. Thus $D \Delta G$, $D > M$, and D is abelian. This violates the maximality of M. So $C_G(M) = M$.

Let $C = C_G(B)$. The subgroup $B \Delta G$ and $AB = G$ so $C = (A \cap C)B$. However, $A \cap C$ centralizes B and $A \cap C \cap B \leqq A \cap B = 1$ by (2.1)1) so that $C = (A \cap C) \times B$. We conclude that $Z(A \cap C)B \lhd G$ and is cyclic. Then $(|Z(A \cap C)|, |B|) = 1$. But the same primes divide $A \cap C$ and $Z(A \cap C)$. Therefore (b) holds.

Assume $C > M$. Let P_0 be a nonabelian S_p-subgroup of C so that $P_0 \leqq A \cap C$. Let P be an S_p-subgroup of A (hence also of G) containing P_0. Let N be an abelian subgroup of P_0 which is normal in P. Since B and the p'-part of A centralize P_0, $N \Delta G$. Thus N is cyclic. By (2.2), $p = 2$ and P_0 contains a cyclic self centralizing subgroup C_0 of index 2 which is normal in P. That is, $C_0 \Delta G$. Putting C_0 together with the $2'$-part of C we get a cyclic subgroup M_0 of index 2 in C which is normal in G. But then $C_G(M_0) \leqq C_G(B) = C$. Therefore $C_G(M_0) = C_G(M_0) = M_0$. We also know that $M \leqq C_G(B)$. Since

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

$[C_G(B):M_0] = 2$ we conclude that $M_0 = M$ or $M_0M = C_G(B)$. In any case, maximality of M forces $|M_0| = |M|$ so $[C_G(B):M] = 2$.

Every characteristic abelian subgroup of P_0 (for $p = 2$) is normal in G so is cyclic. Further, P_0 has a cyclic subgroup $M \cap P_0$ of index 2. By (1.1) then P_0 is quaternion, generalized quaternion, dihedral, or semidihedral.

This completes the proof of (2.3).

Note. For the rest of this section we assume $M \neq G$.

At this point we prove that G can be viewed as a subgroup of $\mathscr{T}$ and V as $\tilde{k}^+$. First we need a result on splitting fields for G on V. This result depends only upon the fact that $C_G(M) = M$.

(2.4) *The characteristic of k does not divide $|M|$. If $\tilde{k}$ is an extension of k by a primitive $|M|$*th *root of unity, then $\tilde{k} \otimes V$ splits. An absolutely irreducible summand has dimension $[G:M]$*,

Observe that $V|M$ is homogeneous and faithful. So M is faithful on each irreducible component. We infer that $O_r(M) = 1$. Since M is cyclic, M is an r'-group.

Now $\tilde{k}$ is a splitting field for M and $\tilde{k} \otimes_k V = \tilde{V}$ is completely reducible. Let U be an irreducible summand. Actually U is a faithful, absolutely irreducible $\tilde{k}[G]$-module. To see this, observe that $U|M$ is faithful and completely reducible. Let W be an irreducible $\tilde{k}[M]$-summand. Let λ be the character of W. Since M splits over $\tilde{k}$, $\lambda(1) = 1$. So W is absolutely irreducible. If $x \in G$ and $\lambda^x = \lambda$ then $x \in C_G(M)$ since W is faithful. Thus M is the stabilizer in G of W. We infer that $W|G$ is an absolutely irreducible $\tilde{k}[G]$-module isomorphic to a submodule of the irreducible module U. Thus $W|G \simeq U$ is absolutely irreducible. This proves (2.4).

(2.5) *Assume* (2.1)(1)(2) *hold. Suppose that V is a faithful irreducible $k[G]$-module such that $V|M$ is homogeneous, where M is a cyclic self-centralizing normal subgroup of G.*

*Let $\tilde{k}$ be an extension of k by a primitive $|M|$*th *root of unity. Then there is a subfield $\hat{k}$ of $\tilde{k}$ and monomorphisms*

$$\phi: G \to \mathscr{T}\ (\tilde{k}/\hat{k})$$
$$\Phi: V \to \tilde{k}^+ \ \textit{(an isomorphism)}$$

so that

(a) $\phi(x)\Phi(v) = \Phi(xv)$; $x \in G, v \in V$;
(b) $\phi(M) = \langle \omega \rangle$ *and* $\tilde{k} = k(\omega)$;
(c) $\phi(G)\tilde{k}^\times = \mathscr{T}\ (\tilde{k}/\hat{k})$; *and*
(d) $\phi(G) \cap \tilde{k}^\times = \phi(M)$.

Let $\mathbf{A} = k[G]/\mathbf{J}(k[G])$ where $\mathbf{J}(k[G])$ is the Jacobson radical of $k[G]$. Since the radical anihilates V, V is an $\mathbf{A}$-module. Because V is irreducible, there is a

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

unique primitive central idempotent $e \in \mathbf{A}$ with $eV \neq (0)$. Further,

$$e\mathbf{A} \simeq \mathrm{Hom}_{\mathbf{F}}(V, V)$$

where $\mathbf{F} = \mathrm{Hom}_{\mathbf{F}[G]}(V, V)$ is a division ring. The field k is finite, so by Wedderburn's Theorem on finite division rings, $\mathbf{F} \geqq k$ is a finite extension field of k. Note that we may identify $Z(eA)$ with $\mathbf{F}$, and $e\mathbf{A}$ is absolutely irreducible over $\mathbf{F}$ but not over any subfield. Since $\mathbf{F}$ is a normal extension of k we conclude that any splitting field for G on V contains a copy of $\mathbf{F}$. So we may assume:

(1) $\tilde{k} \geqq \hat{k} \simeq \mathbf{F}$.

Suppose $[eA:\mathbf{F}] = m^2$. Then by (2.4):

(2) $\dim_k V = m[\hat{k}:k]$, $m = [G:M]$.

Let $\mathbf{B}$ be the image in $e\mathbf{A}$ of $k[M]$. Since $V|M$ is homogeneous, $\mathbf{B}$ is isomorphic to a single simple faithful summand of $k[M]$, But such a summand is just an extension of k by a primitive $|M|$th root of unity. So $\mathbf{B} \simeq \tilde{k}$. Suppose $V|M$ has t irreducible summands. Then as a $\mathbf{B}$-module, V has dimension t. Therefore

(3) $\dim_k V = t[\tilde{k}:k]$.

If $x \in G$, let $\bar{x}$ denote its image in $e\mathbf{A}$. Let $\psi_x(y) = \bar{x}y\bar{x}^{-1}$ for $y \in e\mathbf{A}$. Since conjugation by x fixes $k[M]$ it fixes $\mathbf{B}$. Thus ψ_x is an automorphism of $\mathbf{B}$. The map $x \to \psi_x$ is a homomorphism of G onto a subgroup G_1 of $\mathrm{Aut}(\mathbf{B})$. The kernel is $C_G(M) = M$. So $G_1 \cong G/M$, is cyclic of order m. Choose $x \in G$ so that $\langle\psi_x\rangle = G_1$. Since $x^m \in M$, $\bar{x}^m \in \mathbf{B}$. Further, $\bar{x}$ and $\mathbf{B}$ together generate $e\mathbf{A}$, a simple algebra. But $\bar{x}$ acts upon $\mathbf{B}$ as ψ_x, a generator of G_1. Thus $e\mathbf{A}$ is isomorphic to the crossed product of $G_1 \cong \mathrm{Aut}(\mathbf{B})$ by the field $\mathbf{B}$. So $Z(e\mathbf{A}) = \mathbf{F}$ is the fixed field of G_1 in $\mathbf{B}$. That is, $\mathbf{F} \leqq \mathbf{B}$, and

(4) $[G:M] = [\tilde{k}:\hat{k}] = [\mathbf{B}:\mathbf{F}]$.

Combining (2), (3), and (4) we must have

(5) $t = 1$.

Thus $\mathbf{B}$ is a simple subalgebra and V is irreducible as a $\mathbf{B}$-module. So

$$V = \mathbf{B}v$$

for $v \in V$. Let $x \in G$. Then

$$x(bv) = \bar{x}b\bar{x}^{-1}b_1v = \psi_x(b)b_1v$$

where $\bar{x}v = b_1v$ for $b_1, b \in B$. Let

$$\Phi(bv) = b$$

and

$$\phi(x) = \psi_x b_2$$

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

where $xv = \psi_x(b_2)v$. Since $\mathbf{B} \simeq \tilde{k}$ an easy calculation establishes the condition (a). The conditions (b), (c), (d) are straightforward from the preceding. That ϕ and Φ are monomorphisms follows by computation.

We may now consider $V = \tilde{k}^+$ and $G \leqq \mathscr{T}$ such that $G \cap \tilde{k}^\times = M$ and $G\tilde{k}^\times = \mathscr{T}$.

(2.6) *Consider $\mathscr{T}$ as a permutation group on $\Omega = \tilde{k}^+ \backslash \{0\}$. The representation is isomorphic to $1_{\mathscr{G}}|^{\mathscr{T}}$. Thus A acts upon Ω as $\sum 1_{\mathscr{G}^{x^{-1}} \cap A}|^A$ where the sum is over double cosets $Ax\mathscr{G}$ in $\mathscr{T}$.*

Let $1 \in \Omega$. $\mathscr{T}$ is transitive on Ω since $\tilde{k}^\times$ is. The stabilizer of 1 in $\mathscr{T}$ is $\mathscr{G}$. Thus the representation is $1_{\mathscr{G}}|^{\mathscr{T}}$. The second part follows from Mackey's subgroup theorem.

From the preceding argument, it follows that we obtain a regular orbit whenever $x \in \mathscr{T}$ and $\mathscr{G}^x \cap A = 1$. If we have several such x's belonging to distinct double cosets, we get distinct regular orbits. We wish to d termine all $\mathscr{T}$ and G such that no more than two such x's exist. Since $\mathscr{G}\tilde{k}^\times = \mathscr{T}$ we may choose the x's from $\tilde{k}^\times$.

At this point we prove an enlargement lemma. We would like A to split over $A \cap \tilde{k}^\times = A \cap M = A_0$.

(2.7) *Let π be the set of primes dividing $|A_0|$. Then there exists a π-subgroup $\tilde{A}_0 \supseteqq A_0$ of $\tilde{k}^\times$ with $\tilde{A} = A\tilde{A}_0$ and $\tilde{G} = \tilde{A}B$ so that $\tilde{G}$ satisfies* (2.1) *and $\tilde{A}$ is a split extension of $\tilde{A} \cap \tilde{k}^\times = \tilde{A}_0$.*

Let Q be an S_q-subgroup of A. If Q splits over $Q \cap \tilde{k}^\times = Q \cap A_0$ for every prime q, then A, being nilpotent, splits over $A_0 = A \cap \tilde{k}^\times$. In this case $\tilde{G} = G$ works.

Suppose that $Q_0 = Q \cap A_0 \neq 1$. Let Q_1 be the q-Sylow subgroup of $\tilde{k}^\times$. Since $Q_0 \neq 1$ and A acts as $\mathscr{G}$ by conjugation upon Q_1 we conclude that every q'-automorphism of $\mathscr{G}$ centralizes Q_0 hence Q_1. Thus $QQ_1 \cap \tilde{k}^\times = Q_1$ and $[QQ_1 \colon Q_1] = |\mathscr{G}|_q$. Thus QQ_1 is a q-Sylow subgroup of $\mathscr{T}$ so is split. Further AQ_1 is nilpotent. For each nonsplit Sylow subgroup of A we take Q_1 as above. We let A_1 be the subgroup generated by these Q_1's. Since $A_1 \leqq \tilde{k}^\times$ it is normal in $\mathscr{T}$. We set $\tilde{A}_0 = A_0A_1$. Then $\tilde{A} = A\tilde{A}_0$ is nilpotent and has split Sylow subgroups. Setting $\tilde{G} = \tilde{A}B$ we may easily verify (2.1). The proof is complete.

From here on we consider cases where $A = CA_0$ is split with $C \cap A_0 = 1$.

(2.8) *If $A = CA_0$ is a split extension of A_0 by C then there is an $\omega \in \tilde{k}^\times$ so that $\omega C\omega^{-1} = \mathscr{G}$.*

Choose $\sigma\mu$, $\sigma \in \mathscr{G}$, $\mu \in \tilde{k}^\times$, as a generator of C. If σ has order n then so does $\sigma\mu$. Therefore $(\sigma\mu)^n = 1(\mu) \cdot \sigma(\mu) \cdot \ldots \cdot \sigma^{n-1}(\mu) = 1$. Let $N = N_{\tilde{k}\to\hat{k}}$ be the norm map. Then $N(\mu) = 1$. By Hilbert's Theorem 90 there is an $\omega \in \tilde{k}^\times$ such that $\sigma^{-1}(\omega^{-1})\omega = \mu$. So

$$\omega\sigma\mu\omega^{-1} = \sigma[\sigma^{-1}(\omega)]\omega^{-1}\mu = \sigma\mu^{-1}\mu = \sigma,$$

and $\omega C\omega^{-1} = \langle\sigma\rangle = \mathscr{G}$.

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

Altering G by a $\mathcal{T}$-conjugate does not change the orbit structure on $\tilde{k}^\times$. So in the split case we assume $G = \mathcal{G}M$ and $A = \mathcal{G}A_0$. Further, when G is "nonsplit", by (2.7) we may assume G is a subgroup of $\tilde{G} = \mathcal{G}\tilde{M}$, $\tilde{A} = \mathcal{G}\tilde{A}_0$.

(2.9) *Suppose $A = \mathcal{G}A_0$. For each prime $p||\mathcal{G}|$ let $\sigma_p \in \mathcal{G}$ have order p. Let J_p be the subgroup of all $\omega \in \tilde{k}^\times$ such that $\sigma_p^{-1}(\omega)\omega^{-1} \in A_0$. Fix $x \in \tilde{k}^\times$. Then $\mathcal{G}^x \cap A = 1$ if and only if $x \notin J_p$ for any $p||\mathcal{G}|$.*

Assume $x \in J_p$. Then $\sigma_p^{-1}(x^{-1})x = \mu \in A_0$. But $x^{-1}\sigma_p x = \sigma_p[\sigma_p^{-1}(x^{-1})]x = \sigma_p\mu \in \mathcal{G}A_0 = A$. Thus $\sigma_p\mu \in \mathcal{G}^x \cap A$.

Suppose $\mathcal{G}^x \cap A \neq 1$. Let $\sigma_p\mu$, $\mu \in \tilde{k}^\times$, be of order p in $\mathcal{G}^x \cap A$. Now $x^{-1}\sigma_p x = \sigma_p\mu$ so $\mu = \sigma_p^{-1}(x^{-1})x$. Because $\sigma_p \in A = \mathcal{G}A_0$, $\mu \in A_0$. Therefore $x \in J_p$.

(2.10) *Suppose $A = \mathcal{G}A_0$. Let ω, $\nu \in \tilde{k}^\times$. Then $A\omega\mathcal{G} = A\nu\mathcal{G}$ if and only i $\sigma(\omega)A_0 = \nu A_0$ for some $\sigma \in \mathcal{G}$.*

Suppose $\omega = (\sigma\mu)\nu\tau = \sigma\tau[\tau^{-1}(\mu\nu)]$ for $\mu \in A_0$; $\sigma, \tau \in \mathcal{G}$. Then $\tau^{-1} = \sigma$ and $\omega = \sigma(\nu)\sigma(\mu) \in \sigma(\nu)A_0$. So $\sigma(\nu)A_0 = \omega A_0$.

Assume $\sigma(\omega)A_0 = \nu A_0$. Then $\nu = \sigma(\omega)\mu = \sigma[\sigma^{-1}(\mu)]\omega\sigma^{-1} \in A\omega\mathcal{G}$. Thus $A\nu\mathcal{G} = A\omega\mathcal{G}$.

We know that $(|A_0|, |B|) = 1$ by (2.3). Further, if π is the set of primes dividing $|A_0|$ then increasing the size of B to a Hall π'-subgroup of $\tilde{k}^\times$ does not affect (2.1). We now make the following assumptions explicit.

(2.11) *Assume $G \leqq \mathcal{T}$, $G \cap \tilde{k}^\times = M$, $M \neq G$, $A_0 = A \cap M$, $M = A_0 \times B$, and $A = \mathcal{G}A_0$ satisfy* (2.1). *If π is the set of primes dividing $|A_0|$ then suppose B is a Hall π'-subgroup of $\tilde{k}^\times$.*

(a) *For all $p||\mathcal{G}|$, $J_p \neq \tilde{k}^\times$.*

(b) *$C_G(B) = M$.*

(2.12) *Assume G satisfies* (2.11) *except that* (a) *or* (b) *fails. Then*

(a) *$\tilde{k} = GF(r^2)$,*

(b) *$r \equiv -1 \pmod 4$,*

(c) *$2^t = r + 1$,*

(d) *$B \leqq GF(r)$.*

By (2.3), $[C_G(B):M] = 1, 2$. We show first that if (2.11) (a) fails then (2.11) (b) also fails. So we assume $J_p = \tilde{k}^\times$ for some prime p. Let $\sigma \in \mathcal{G}$ have order p. Then $(\sigma - 1)\tilde{k}^\times \leqq A_0$. Therefore, $(\sigma - 1)B \leqq A_0 \cap B = 1$. We conclude that $\sigma \in C_G(B)$ and $C_G(B) > M$.

We assume (2.11) (b) fails. Hence $[C_G(B):M] = 2$. Choose $\sigma \in \mathcal{G}$ of order 2. Then $\sigma \in C_G(B)$. Set $\tilde{k} = \mathrm{GF}(r^{2m})$ and let $\tilde{\mathcal{G}}$ be the Galois group of $\tilde{k}$ over k. By (2.3) the S_2-subgroup of $C_G(B)$ is dihedral or semidihedral. This can only occur if σ is not a square in $\tilde{\mathcal{G}}$ and $r \equiv -1 \pmod 4$; so m is odd. Suppose $2^t||r^m + 1$. Then $2^t||r + 1$. Let $s|r^m + 1$ be an odd prime. We may choose $\sigma: x \rightarrow x^{r^m}$. Take ω of order s in $\tilde{k}^\times$. Then $\sigma(\omega) = \omega^{-1}$. So $\langle\sigma, \omega\rangle$ is dihedral of

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

order $2s$ and $s \nmid |A_0|$. Since B is a Hall π'-subgroup, it follows that $s||B|$ and $\omega \in B \leqq C_G(\sigma)$. Therefore $r^m + 1 = 2^t = r + 1$ is divisible by no odd primes and $m = 1$. Finally, $(|B|, |A_0|) = 1$ means $|B|$ is odd and $B \leqq GF(r)$.

We now assume (2.11) holds. If we let ω be a generator of $\tilde{k}^\times$, then $\omega \notin J_p$ for any p. Let $\mathscr{B}$ be the set of generators of $\tilde{k}^\times/A_0$. Suppose $\sigma \in \mathscr{G}$ has prime order q and fixes $\nu A_0 \in \mathscr{B}$. This means that $\sigma(\nu)\nu^{-1} = \mu \in A_0$. We may choose ν so that it also generates $\tilde{k}^\times$. Therefore $\sigma(\nu)\nu^{-1} \notin A_0$. We conclude that:

(2.13) *If* (2.11) *holds, then* $\mathscr{G}$ *is semiregular on the generators of* $\tilde{k}^\times/A_0$.

We now restrict the structure of $\tilde{k}^\times/A_0$.

(2.14) *Assume* (2.11) *and suppose* A *does not have* 3 *regular orbits in its action upon* $\tilde{k}^+$. *Then one of the following cases holds:*

(a) $|B| = pq$ *for odd primes* p, q; $|\mathscr{G}| = (p-1)(q-1)/2$, $(p-1, q-1) = 2$; *and* $[\tilde{k}^\times : BA_0] = 1, 2$.

(b) $|B| = 2p$ *for an odd prime* p; $|\mathscr{G}| = (p-1)/2$ *is odd; and* $[\tilde{k}^\times : BA_0] = 1$.

(c) $|B| = p$ *for an odd prime* p; $|\mathscr{G}| = (p-1)/\delta$ *where values for* $[\tilde{k}^\times : BA_0]$ *and* δ *are tabulated below.*

$[\tilde{k}^\times : BA_0]$	δ
1	1,2
2	1,2
4	1

By (2.6), (2.9), and (2.10) we may assume $\mathscr{G}$ has fewer than three regular orbits in its action upon $\tilde{k}^\times/A_0$. Set $\bar{B} = BA_0/A_0$. Since $\bar{B} \cong B$ is a Hall-group, we may write $\tilde{k}^\times/A_0 = \bar{C} \times \bar{B}$. We may view $\mathscr{G} \leqq \operatorname{Aut}(\bar{B})$ since $C_G(B) = M$ and $(|A_0|, |B|) = 1$. Thus $\mathscr{G}$ is semiregular upon the generators of $\bar{B}$. The number of regular orbits on the generators of $\bar{C} \times \bar{B}$ is (where $c = |C|$ and $b = |B|$)

$$\phi(c) \cdot (\phi(b)/|\mathscr{G}|) \leqq 2$$

where ϕ is the Euler function. In other words, $[\operatorname{Aut}(B) : \mathscr{G}] \leqq 2$. Now $\mathscr{G}$ is cyclic so that $\operatorname{Aut}(\bar{B})$ is cyclic or $\operatorname{Aut}(\bar{B}) \cong \mathbf{Z}_2 \times \mathscr{G}$. By properties of Euler's function we may now state:

(i) If $\operatorname{Aut}(\bar{B})$ is cyclic then $|B| = p^e$, $2p^e$, or 4 for an odd prime p.

(ii) If $\operatorname{Aut}(\bar{B}) \cong \mathbf{Z}_2 \times \mathscr{G}$ where $|\mathscr{G}|$ is even then $|B| = 2^t$ $(t > 2)$, $4p^e$, $p^e q^f$, or $2p^e q^f$ for odd primes p, q.

Since $|\mathscr{G}| > 1$ and $[\operatorname{Aut}(B) : \mathscr{G}] \leqq 2$ we may also state conditions when $2||\mathscr{G}|$.

(iii) We always have $2||\mathscr{G}|$ unless $\operatorname{Aut}(\bar{B})$ is cyclic; $|B| = p^e$ or $2p^e$ for an odd prime $p \equiv -1 \pmod 4$; and $[\operatorname{Aut}(\bar{B}) : \mathscr{G}] = 2$.

(iv) If $2||\mathscr{G}|$ and $2||B|$ then $8||B|$.

Assume that $\tilde{k} = \mathrm{GF}(r^m)$. Assume that 2 divides both $|B|$ and $|\mathscr{G}|$. Then $2|m$. Now r must be odd so that $8|r^m - 1$. Since B is a Hall-subgroup of $\tilde{k}^\times$, $8||B|$.

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

Observe that (iii) and (iv) eliminate the values $|B| = 4$, $4p^e$, and $2p^eq^f$. Further, if $|B| = 2p^e$ then $p = -1 \pmod 4$ and $[\mathrm{Aut}(\bar{B}):\mathscr{G}] = 2$.

(v) If $\mathscr{G} = \mathrm{Aut}(\bar{B})$ then $|\bar{B}| = p^e$. If $|\mathrm{Aut}(\bar{B}):\mathscr{G}| = 2$ then $|\bar{B}| = p^e$, $2p^e(p \equiv -1 \pmod 4))$, $2^t(t > 2)$, or p^eq^f.

(vi) If $p^e||B|$ for an odd prime p then $e = 1$.

Suppose $e > 1$. Then $p^{e-1}||\mathscr{G}|$. Choose $\sigma \in \mathscr{G}$ of order p. If q is a prime dividing $|B|$, $q \neq p$, then $\mathscr{G}$ contains a subgroup which is the direct product of two cyclic groups, one of order $p^{e-1}(p-1)/2$ and one of order $q - 1$. But $\mathscr{G}$ is cyclic. So $(p, q-1) = 1$. We conclude that σ centralizes the S_q-subgroups of $\bar{B}$ for all odd $q \neq p$. Further σ centralizes A_0 since A is nilpotent and $(|B|, |A_0|) = 1$. Therefore, $\langle \sigma, P \rangle$ is normal in G where P is an S_p-subgroup of G. Since σ has order p, $P_0 = \langle \sigma, \mho_1(P) \rangle$ is abelian. Certainly $\mathscr{G}$ normalizes this group. If μ is any p'-element of $\tilde{k}^\times$ then $[P_0, \mu] \leqq \langle \mu \rangle \cap P = 1$. So $\tilde{k}^\times$ normalizes P_0. Therefore $P_0 \lhd G$. But then P_0 is cyclic. Thus $\mho_1(P) = 1$. This contradicts $e > 1$. So (vi) holds.

We work case by case now. Observe that $\phi(c) = 1, 2$ so that $c = 1, 2, 3, 4, 6$.

(A) $|B| = 2^t(t > 2)$. This case does not occur. Here $c = 1$ since $\phi(c) = 1$ and $(|\bar{B}|, |\bar{C}|) = 1$. Now $|\mathscr{G}| = 2^{t-2}$. Let σ generate $\mathscr{G}$. We must have $(2, |A_0|) = (|B|, |Ap|) = 1$. Therefore σ centralizes A_0. But then $G = A_0 \times \langle \sigma, B \rangle$. Every normal abelian subgroup of $\langle \sigma, B \rangle$ is cyclic by (2.1). So $\langle \sigma, B \rangle$ being an S_2-subgroup of $\mathscr{T}$, must be semidihedral. Thus $|\mathscr{G}| = 2$ and $t = 3$. It follows that $|B| = 8$. Here $\tilde{k} = \mathrm{GF}(r^{2n})$, $A_0 \leqq \mathrm{GF}(r^n)$, and $\mathrm{GF}(r^n)^\times B = \tilde{k}^\times$. From this we find that $r^n + 1$ divides 4. Therefore $r^n = 3$, $A_0 = 1$, and $\tilde{k}^+ = \mathrm{GF}(9)$ is the regular $A = \langle \sigma \rangle$-module. So A has $(9\text{-}3)/2 = 3$ regular orbits upon $\tilde{k}^+$.

(B) $|B| = 2p^e$. By (vi), $e = 1$. By (v), $p \equiv -1 \pmod 4$. Since $e = 1, 2$ and $|B|$ is even we must have $[\tilde{k}^\times:BA_0] = 1$. This proves (b).

(C) $|B| = p^eq^f$. By (vi), $e = f = 1$. Since $|\mathrm{Aut}(\bar{B}):\mathscr{G}| = 2$, we must have $(p-1, q-1) = 2$. Finally $[\tilde{k}^\times:BA_0] = c = 1, 2$. This proves (a).

(D) $|B| = p^e$. By (vi), $e = 1$. Here $[\tilde{k}^\times:BA_0] = c = 1, 2, 3, 4, 6$. Also $|\mathscr{G}| = (p-1)/\delta$ where $\delta = 1, 2$. If $\delta = 2$ then $c = 1, 2$. The proof of (c) will be complete if we can show that $3 \nmid c$.

Suppose that $3|c$. Choose σ a generator of $\mathscr{G}$. Let $\bar{D}$ be an S_3-subgroup of $\bar{C}$. Then $|\bar{D}| = 3$. Therefore $3||A_0|$. The automorphism σ acts as an element of $\mathrm{Aut}(\bar{D})$, so it is trivial or of order 2 upon $\bar{D}$. It cannot be of order 2 since $3||A_0|$ and the S_3-subgroup of $\tilde{k}^\times$ is cyclic (recall that A is nilpotent). Thus σ is trivial upon $\bar{D}$. Let C be the inverse image in $\tilde{k}^\times$ of $\bar{C}$. Then $J_s \geqq C$ for every prime $s||\mathscr{G}|$. The group B has order p and σ is regular upon the generators of B. Let ωA_0 be such a generator. Then J_s does not contain ω for any prime $s||\mathscr{G}|$. Let μ, ν be representatives from the two non-identity cosets of $\bar{D}$. Thus $\mu\omega A_0$, $\nu\omega A_0$, and ωA_0 are not in any J_s/A_0. They clearly belong to distinct $\mathscr{G}$-orbits since σ fixes μA_0 and νA_0. All three orbits are regular $\mathscr{G}$-orbits. So by (2.6), (2.9), and (2.10) $3 \nmid c$. This proves (c).

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

The structure of B is fairly clear now. The object is to determine $|\mathscr{G}|$ more closely. All the arguments are essentially the same. Suppose H/K is a section of $\mathscr{G}$ of prime order s. Let $\mathbf{H}$ and $\mathbf{K}$ be respectively the fixed fields of H and K. Then $|\mathbf{H}| = x$, some power of r, and $[\mathbf{K}^\times : \mathbf{H}^\times] = (x^s - 1)/(x - 1)$. We compute this index a second way and compare the answers. That is the essence of the arguments.

(2.15) *Assume* (2.11) *and suppose A has at most two regular orbits upon $\tilde{k}^+$, Let $\sigma \in \mathscr{G}$ have order s^t for a prime s. Let* $\mathbf{F}$ *be the fixed field of σ.*

(a) *If s is odd then $t < 2$.*

(b) *If $s = 2$ then $t < 3$.*

(c) *If $s = 2$ and $t = 2$ then $4 \nmid |F^\times|$, or $|B| = pq$ and σ is fixed point free upon B.*

We proceed in steps.

(i) $[\tilde{k}^\times : \mathbf{F}^\times]$ divides $s^e p$ for some e and some odd $p|\ |B|$ unless σ is fixed point free upon B, $s = 2$, and $|B| = pq$.

Let π be the set of primes dividing $|A_0|$. Then B is a Hall π'-subgroup of $\tilde{k}^\times$. Since $A = \mathscr{G}A_0$ is nilpotent and $\tilde{k}^\times/B$ is a cyclic π-group, we conclude that $\mathscr{G}\tilde{k}^\times/B$ is nilpotent. So the set of fixed elements of σ in $\tilde{k}^\times/B$ must be of index a power of s. Therefore $[\tilde{k}^\times : \mathbf{F}^\times]$ divides $s^e|B|$ for some e.

We turn now to the cases of (2.14). In case (2.14)(c) we have $|B| = p$ and our assertion is immediate. In case (2.14)(b), $|B| = 2p$ and $2\|\ |\tilde{k}^\times|$. So $-1 \in B \cap \mathbf{F}$. Thus $[\tilde{k}^\times : \mathbf{F}^\times]$ divides $s^e|B|/2 = s^e p$. Finally, we have case (2.14)(a) where $|B| = pq$. Since $(p - 1, q - 1) = 2$, for some ordering of p and q, $s^t|p - 1$. If s is odd then $s \nmid q - 1$ so the S_q-subgroup of B is fixed by σ. In this case $[\tilde{k}^\times : \mathbf{F}^\times]$ divides $s^e|B|/q = s^e p$. The same argument holds for $s = 2$ unless σ is fixed point free upon B.

(ii) If $s = 2$, σ is fixed point free upon B, and $|B| = pq$ then $[\tilde{k}^\times : \mathbf{F}^\times]$ divides $2^e pq$ and $[\tilde{k}^\times : \mathbf{F}_1^\times]$ divides $2^e p$ where F_1 is the fixed field of σ^2 and $t > 1$.

We continue our argument from above. Now σ^2 will fix an S_q-subgroup of B. So our argument from above may be applied to the element σ^2 in place of σ.

Let $\sigma^{s^i} = \sigma_i$. Let $\mathbf{F}_i$ be the fixed field of σ_i so that $\mathbf{F}_0 = \mathbf{F}$. If $i < t$ then σ_i is fixed point free upon the S_p-subgroup of B. Thus $p|[\tilde{k}^\times : \mathbf{F}_i]$ for all $i < t$.

(iii) In case (i), $[\mathbf{F}_{i+1}{}^\times : \mathbf{F}_i{}^\times]$ is a power of s for all $0 \leqq i < t - 1$.

(iv) In case (ii), $[\mathbf{F}_{i+1}{}^\times : \mathbf{F}_i{}^\times]$ is a power of 2 for all $1 \leqq i < t - 1$.

These statements follow from (i) and (ii) and our observations above.

Let x be a power of the prime r. Suppose $(x^s - 1)/(x - 1) = s^e$. This equality will hold if and only if $s = 2$, $2|x - 1$, and $x + 1 = 2^e$. To have this occur, $x = r^n$ where n is odd and $r = -1 \pmod 4$.

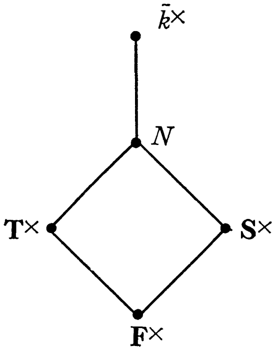
Suppose that $[\mathbf{F}_{i+1}{}^\times : \mathbf{F}_i{}^\times] = s^e$ for some i. Let $|\mathbf{F}_i| = x$, a power of r. From our remarks above, we must have $s = 2$ and $x = r^n$ for an odd n. In particular, $i = 0$. From (iii) we conclude that $t < 2$ if s is odd. If $s = 2$ then $t < 3$; and if $t = 2$ then $2\|\ |\mathbf{F}^\times|$. From (iv) we conclude that $t < 3$. So (2.15) holds.

This lemma bounds the exponent of primes in $|\mathscr{G}|$. Next we bound the number of primes in $|\mathscr{G}|$. The proof here is similar.

(2.16) *Assume* (2.11) *and suppose A has at most two regular orbits upon $\tilde{k}^+$. Let $p| \; |B|$ be odd, and B_0 an S_p-subgroup of B. Let $\mathscr{G}^*$ be the automorphism group of B_0 given by restricting $\mathscr{G}$ to B_0. Then $|\mathscr{G}^*|$ is a prime power.*

Suppose $t > s$ are two primes dividing $|\mathscr{G}^*|$. Since t is odd we may choose $\tau \in \mathscr{G}$ of order t so that in $\mathscr{G}^*$ τ has order t. We may choose $\sigma \in \mathscr{G}$ of order s^e so that σ has order s in $\mathscr{G}^*$.

Let $\mathbf{S}$ be the fixed field of σ and $\mathbf{T}$ that of τ. So $\mathbf{F} = \mathbf{S} \cap \mathbf{T}$ is the fixed field of $\sigma\tau$. Set $N = \mathbf{S}^\times\mathbf{T}^\times$.



Arguing as before, the index $[\tilde{k}^\times:\mathbf{T}^\times] = t^f p$, and $[\tilde{k}^\times:\mathbf{S}^\times] = s^g p\delta$ where $\delta = 1$ or q. Since $p|| \; |\tilde{k}^\times|$ we conclude that p divides $[\tilde{k}^\times:N]$. So $[N:\mathbf{T}^\times] = [\mathbf{S}^\times:\mathbf{F}^\times] = t^h$. Let $|\mathbf{F}| = x$, a power of r. Then $[\mathbf{S}^\times:\mathbf{F}^\times] = (x^t - 1)/(x - 1) = t^h$. Since x is a power of r and t is odd there is no solution to $(x^t - 1)/(x - 1) = t^h$. This contradiction proves the lemma.

We now apply (2.14), (2.15), and (2.16) to obtain some values.

(2.17) *Assume* (2.11) *and suppose A has at most two regular orbits in its action upon $\tilde{k}^+$. Then we have the following possibilities for $|B|$ where s is an odd prime:*

	$\lvert B\rvert$	$(p - 1)$	$(q - 1)/2$	$\lvert\mathscr{G}\rvert$
(1)	3,6	2		2
(2)	5,10	4		2,4
(3)	$2s + 1, 4s + 2$	$2s$		s
(4)	$3(2s + 1)$	2	s	$2s$
(5)	$5(2s + 1)$	4	s	$4s$
(6)	$3 \cdot 5$	4	1	4.

By (2.14) we know the structure of B.

(A) $|B| = p, 2p$: Since $\mathscr{G}$ is faithful upon B, it is faithful upon an S_p-subgroup of B. So by (2.16) $|\mathscr{G}|$ is a prime power. Then by (2.15) $|\mathscr{G}| = 2^t$ for $t < 3$ or $|\mathscr{G}| = s$ an odd prime. By (2.14) we have $p - 1 = |\mathscr{G}|$ or $2|\mathscr{G}|$. Suppose $|\mathscr{G}| = 2^t \leqq 4$. Then $p - 1 \leqq 8$ so that $p = 3, 5$. If $p = 3$ then $|\mathscr{G}| = 2$. If $p = 5$ then $|\mathscr{G}| = 2, 4$. This settles entries (1) and (2). Suppose $|\mathscr{G}| = s$. Then $p - 1 = 2s$ or $p = 2s + 1$. This settles entry (3).

(B) $|B| = pq$: By (2.14) we may arrange p and q so that $2||q - 1$. Then $(p - 1, (q - 1)/2) = 1$. Let $\mathscr{G}^*$ be the restriction of $\mathscr{G}$ to an S_p-subgroup and $\mathscr{G}^{**}$ the restriction of $\mathscr{G}$ to an S_q-subgroup of B. Then $\mathscr{G}$ is a subdirect product of $\mathscr{G}^* \times \mathscr{G}^{**}$. By (2.16) these two groups are of prime power order. One of $\mathscr{G}^*$ or $\mathscr{G}^{**}$ has even order. We may arrange p and q so that it is $\mathscr{G}^*$. Thus $p - 1 = 2^t$. By (2.15) we have $t < 3$ and $q - 1 = 2s$ where $s = 1$ or s is an odd prime. For $t = 1$ we have $p = 3$, $q = 2s + 1$ for s a prime, and $|\mathscr{G}| = 2s$. This gives entry (4). For $t = 2$ we have $p = 5$, and $q = 2s + 1$. Also $|\mathscr{G}| = 2s$. If s is a prime we get entry (5). If $s = 1$ we get entry (6).

(2.18) *In* (2.17), $|B| \neq pq$.

Consider first the cases (4) and (5).

Let σ have order s in $\mathscr{G}$ and τ have order 2. Let $\mathbf{S}$ be the fixed field of σ and $\mathbf{T}$ the fixed field of τ. Set $\mathbf{F} = \mathbf{S} \cap \mathbf{T}$, the fixed field of $\sigma\tau$. Now look at the figure above. We have $|\mathbf{F}| = x$, a power of r. So $[\tilde{k}^\times:\mathbf{S}^\times] = (x^{2s} - 1)/(x^2 - 1) = s^e p$ and $[\tilde{k}^\times:\mathbf{T}^\times] = (x^{2s} - 1)/(x^s - 1) = 2^f q$. These two indices are relatively prime so that $N = \mathbf{S}^\times\mathbf{T}^\times = \tilde{k}^\times$. Thus

$$(x^{2s} - 1)/(x^s - 1) = [N:\mathbf{S}^\times] = (\mathbf{T}^\times:\mathbf{F}^\times] = (x^2 - 1)/(x - 1).$$

But $(x^{2s} - 1)/(x^s - 1) > (x^2 - 1)/(x - 1)$.

We finally consider the case (6). Here there are several routes. We choose the following one. Let $\sigma \in \mathscr{G}$ generate $\mathscr{G}$. Let $\mathbf{S}$ be the fixed field of σ and $\mathbf{F}$ the fixed field of σ^2. There are two possibilities. First, σ may fix an S_q-subgroup of B. In that case $p|[\tilde{k}^\times:\mathbf{F}^\times]$ so that $[\mathbf{F}^\times:\mathbf{S}^\times]$ is a power of 2 where $p = 5$ and $q = 3$. In the other case σ will be fixed point free upon an S_q-subgroup of B. Putting this with the above fact we have:

(i) $[\tilde{k}^\times:\mathbf{F}^\times] = 2^e 5$ and $[\mathbf{F}^\times:\mathbf{S}^\times] = 2^f q$ where $q = 1, 3$.

Let $|S| = x$, a power of r. Then

(ii) $(x^4 - 1)/(x^2 - 1) = x^2 + 1 = 2^e 5$ and $(x^2 - 1)/(x - 1) = (x + 1) = 2^f q$. If $f > 0$ then $e = 1$. So $x = 3$ and $q = 1$. If $f = 0$ then $x = 2$ and $e = 0$.

(iii) $x = 3$ and $q = 1$, or $z = 2$ and $q = 3$.

If $x = 3$ then $|\tilde{k}^\times| = 3^4 - 1 = 80$ which is not divisible by $|B| = 15$. Assume $x = 2$. Then $B = \tilde{k}^\times$ so that $A = \mathscr{G}$. Now $\tilde{k}^+$ is the regular A-module. So A has exactly 3 regular orbits in its action upon $\tilde{k}^+$.

(2.19) *Assume* (2.11) *and suppose A has at most two regular orbits upon $\tilde{k}^+$.*

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

Then one of the following holds:

	$\|\mathscr{G}\|$	$\|\tilde{k}\|$	$\|B\|$	
(1)	4	3	5	
(2)	3	4	7	
(3)	3	2	7	
(4)	2	$2^a \cdot 5 - 1$	5	$a \geqq 1$
(5)	2	$2^a \cdot 3 - 1$	3	$a \geqq 1$
(6)	2	4	5	
(7)	2	2	3.	

Assume first that $x > 1$ and $y > 2$ are prime powers. Then $(x^y - 1)/(x - 1) > 2y^2 + y$ unless

x	y
2	3, 4, 5
3	3
4	3.

Also $(x^y - 1)/(x - 1) > 2y + 1$ unless $x = 2$ and $y = 3$.

Suppose $|\mathscr{G}| = s$ is an odd prime. Let $|\hat{k}| = x$, a power of r. Choose $\sigma \in \mathscr{G}$ of order s. Then $\hat{k}$ is the fixed field of σ. Therefore $[\tilde{k}^\times : \hat{k}^\times] = s^e p$. Thus $(x^s - 1)/(x - 1) = s^e p = s^e(2s + 1)$. It is easy to see that $e = 0$ unless $s | x - 1$ and then $e = 1$. Assume $e = 1$ so that $(x^s - 1)/(x - 1) = 2s^2 + s$. Here $s | x - 1$. With $y = s$, the above table yields $x = 4$, $y = 3$ as the only solution. We conclude that $|\hat{k}| = 4$ and $s = |\mathscr{G}| = 3$. Now $|B| = 2(2 \cdot 3 + 1) = 14$ only if $2 \| \, |\tilde{k}^\times|$. This is obviously not the case, so $|B| = 2 \cdot 3 + 1 = 7$. We now have entry (2).

Continuing, we can have $(x^s - 1)/(x - 1) = 2s + 1$ when $s \nmid (x - 1)$. The only solution is $x = 2$ and $s = 3$. Again $2 \nmid 2^3 - 1$ so that $|B| = 2 \cdot 3 + 1 = 7$. Here $|\hat{k}| = 2$ and $s = |\mathscr{G}| = 3$ yielding (3).

Next suppose $|\mathscr{G}| = 4$. Let $\mathbf{F}$ be the fixed field of σ^2 where σ has order 4 in $\mathscr{G}$. Then $[\tilde{k}^\times : \mathbf{F}^\times] = (x^4 - 1)/(x^2 - 1) = 2^e \cdot 5$. Here we must have $e = 0, 1$. If $e = 0$ we get $(x^4 - 1)/(x^2 - 1) = 5$ and $x = 2$. So $|\hat{k}| = 2$ and $|B| = 5$. But $\tilde{k}^\times$ contains an element of order $(2^2 - 1)/(2 - 1) = 3$ not fixed by σ. So 3 can divide neither $|B|$ nor $|A_0|$. Therefore $3 \nmid |\tilde{k}^\times|$. This case cannot occur. If $e = 1$ we obtain $(x^4 - 1)/(x^2 - 1) = 10$ so that $x = 3$. Since $4 | 3^4 - 1$, $|B| = 5$. Thus $|\mathscr{G}| = 4$, $|\hat{k}| = 3$, and $|B| = 5$ giving (1).

Finally, assume $|\mathscr{G}| = 2$. Then if $\sigma \in \mathscr{G}$ has order 2 we get $[\tilde{k}^\times : \hat{k}^\times] = (x^2 - 1)/(x - 1) = x + 1 = 2^e \cdot 3$ or $2^e \cdot 5$. Since $4 | x^2 - 1$, $|B| = 3, 5$ whenever $e \geqq 1$. If $e = 0$ then $2 \nmid x^2 - 1$ and hence $|B| = 3, 5$.

The values given here complete cases (4)–(7).

(2.20) *In* (4), (5) *of* (2.19), $|\hat{k}| = r$ *is a prime unless* $|\hat{k}| = 9$ *and we are in case* (4) *with* $a = 1$.

Let $\delta = 3, 5$ and assume $r^m = 2^a\delta - 1$ where $m > 1$ so that $r^m + 1 = 2^a\delta$. If $a > 1$ then $r^m \equiv -1 \pmod 4$ and m is odd. So $2^a | r + 1$. Therefore $2^a = r + 1$. We obtain $(r^m + 1)/(r + 1) = \delta$. The latter equation has no solution in integers since r is odd. Thus $a > 1$ implies $m = 1$ and $|\hat{k}| = r$ is a prime.

When $r^m + 1 = 2\delta$ we observe that $5 + 1 = 6$ and again $r^m = 5 = |\hat{k}|$ is a prime, and $9 + 1 = 10$ so $r^m = 3^2 = 9 = |\hat{k}|$.

3. A minimal case: itemization of possibilities.

We continue the considerations of the previous section. We now itemize all possibilities for G. Recall that $G \leqq \mathscr{T} = \mathscr{T}(\tilde{k}/\hat{k})$ and $G \cap \tilde{k}^\times = M = A_0 \times B$ is a maximal cyclic self-centralizing normal subgroup of G. Further, $k(M) = \tilde{k} = \mathrm{GF}(r^m)$. Let $|\mathscr{G}| = g$, $|\hat{k}| = r^n$.

(I) $M = G$. Here the number of regular orbits of A upon $\tilde{k}^+$ is just $[\tilde{k}^\times : A] = (r^m - 1)/|A| \geqq 3$ unless $(r^m - 1)/|A| = 1, 2$. But $|B| = 1$ unless $(r^m - 1)/|A| = 2$ and $2 || (r^m - 1)$. In that case, $|B| = 1, 2$. We may list these values as

r	g	n	$\lvert A_0\rvert$	$\lvert B\rvert$	reg	other
r	1	n	$r^n - 1$	1	1	0
r	1	n	$(\mathrm{r}^n - 1)/2$	1,2	2	0

where $|B| = 1$ unless $(|A|, |B|) = 1$. The entry "reg" gives the number of regular orbits and "other" gives the remaining orbits upon $\tilde{k}^+ \backslash \{0\}$.

(II) $M < G$, *$\mathscr{T}$ is nilpotent.* Here $C_G(B) = G > M$. So for "maximal" G, that is, $A = \mathscr{G}A_0$, (2.12) applies. Thus $\hat{k} = k$ and $\tilde{k} = \mathrm{GF}(r^2)$ where $r \equiv -1 \pmod 4$, and $r = 2^a - 1$. In this case $\mathscr{T} = \mathscr{T}(\tilde{k}/k)$ is nilpotent with semidihedral S_2-subgroup. Let T be an S_2-subgroup of $\tilde{k}^\times$. Under these circumstances $[\tilde{k}^\times : T] = (r - 1)/2$. Further, $\mathscr{G}T$ permutes the elements of $\tilde{k}^+ \backslash \{0\}$ in exactly $(r - 1)/2$ orbits each of length $|T| = 2(r + 1) = 2^{a+1}$. Each orbit is induced from $\mathscr{G}$ in $\mathscr{G}T$. Let $T_1 = \mathscr{G}T$.

Next suppose that $T_2 = \mathscr{G}T^2$ is the maximal dihedral subgroup of T_1. Now T_1 has 2 non-conjugate classes of orbits on $\tilde{k}^+ \backslash \{0\}$. Each class has orbits of length $|T|/2$. There are $(r - 1)/2$ orbits in each class. If α, β are two non-conjugate elements of order 2 in $T_2 \backslash T^2$ then the identity induced from $\langle \alpha \rangle$ or $\langle \beta \rangle$ gives these representations.

Suppose $T_3 < T_2$ is a maximal dihedral subgroup. Then T_3 has $(r - 1)/2$ regular orbits, and $(r - 1)/2$ in each of two classes. Each class has orbit length $|T|/4$.

Suppose $T_4 < T_1$ is a maximal generalized quaternion or quaternion subgroup. Then T_4 has $(r - 1)/2$ regular orbits on $\tilde{k}^+ \backslash \{0\}$.

Suppose $T_5 < T_4$ is a maximal quaternion or generalized quaternion subgroup of T_4. Then T has $(r - 1)$ regular orbits upon $\tilde{k}^{+}\backslash\{0\}$. If $|T_1| = 16$, then T_5 will not exist. We take T_5 cyclic then.

Let C be an odd order subgroup of $\tilde{k}^{\times}$. Then $|C| = (r - 1)/2\mu$ for an odd μ. We list below the orbit structures.

group	reg	other
T_1C	0	$(2^{a+1}\|C\|)^{\mu}$
T_2C	0	$(2^{a}\|C\|)^{2\mu}$
T_3C	μ	$(2^{a+1}\|C\|)^{2\mu}$
T_4C	μ	0
T_5C	2μ	0

It should be remarked that $(x)^y$ means y orbits each of length x.

All other subgroups with non-abelian S_2-groups have at least three regular orbits. Since a dihedral group of order 8 has a normal non-cyclic abelian subgroup, by (2.1) we must avoid this possibility. We obtain the following table of exceptions.

r	g	n	$\|A_0\|$	$\|B\|$	reg	other	
$2^a - 1$	2	1	$2^a(r - 1)/\mu$	b	0	$(\|A_0\|)^{\mu}$	split
$2^a - 1$	2	1	$2^{a-1}(r - 1)/\mu\ (a > 2)$	b	0	$(\|A_0\|)^{2\mu}$	split
$2^a - 1$	2	1	$2^{a-2}(r - 1)\ (a > 3)$	1	1	$(\|A_0\|)^{2}$	split
$2^a - 1$	2	1	$2^{a-1}(r - 1)$	1	1	0	non
$2^a - 1$	2	1	$2^{a-2}(r - 1)\ (a > 2)$	1	2	0	non

Here $(|A|, b) = 1$ and $b|\mu$ where μ is odd. The last column tells whether A splits over A_0.

(III) $\mathscr{T}$ *is not nilpotent.*

We first examine those cases where A is split and B is maximal. By (2.12) we know that G satisfies (2.11) unless there are three regular A-orbits. Suppose there are at most 2. This case is fully tabulated in (2.19) and (2.20). Actually these tables completely determine G. We need only check subgroups which satisfy (2.1). We itemize the cases of (2.19).

(1) $|\mathscr{G}| = 4$, $|\hat{k}| = 3$, $|B| = 5$.

Let T be the S_2-subgroup of $\tilde{k}^{\times}$. Here T has order 16. The S_2-subgroup $\mathscr{G}T$ is the split extension of T by $\mathscr{G}$. The orbit structure of $\mathscr{G}T$ upon $\tilde{k}^{+}\backslash\{0\}$ consists of one regular orbit and one orbit of length $16 = |T|$ induced from $\mathscr{G}$. By looking at a subgroup $\mathscr{G}T^2$ we obtain 2 regular orbits and 2 non-regular orbits of length 8.

Let $\mathscr{G} = \langle\sigma\rangle$ and $\langle x\rangle = T$. Then $\langle\sigma x, x^2\rangle$ has 2 regular orbits and one of length 16.

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press

Because $|B| = 1$ violates (2.1) we have:

r	g	n	$\|A_0\|$	$\|B\|$	reg	other
3	4	1	16	5	1	(16)
3	4	1	8	5	2	$(8)^2$
3	4	1	8	5	2	(16)

(2) $|\mathscr{G}| = 3$, $|\hat{k}| = 4$, $|B| = 7$.

Let T be the S_3-subgroup of $\tilde{k}^\times$. Then $\mathscr{G}T$ acts upon $\tilde{k}^+\backslash\{0\}$ with 2 regular orbits and one orbit of length 9. Again $|B| = 1$ violates (2.1).

r	g	n	$\|A_0\|$	$\|B\|$	reg	other
2	3	2	9	7	2	(9)

(3) $|\mathscr{G}| = 3$, $|\hat{k}| = 2$, $|B| = 7$.

Since $|\tilde{k}^\times| = 7 = |B|$, $A_0 = 1$. Then $\mathscr{G}$ acts with 2 regular and one trivial orbit. Again $|B| = 1$ violates (2.1) so we obtain

r	g	n	$\|A_0\|$	$\|B\|$	reg	other
2	3	1	1	7	2	(1)

(4) $|\mathscr{G}| = 2$, $|\hat{k}| = 9 = 2 \cdot 5 - 1$, $|B| = 5$.

The S_2-subgroup of $\mathscr{T}$ acts with 2 regular orbits and one of length 16. This group alone on $\tilde{k}^+$ does not satisfy (2.1) so that $|B| \neq 1$.

r	g	n	$\|A_0\|$	$\|B\|$	reg	other
3	2	2	16	5	2	(16)

(4′) $|\mathscr{G}| = 2$, $|\hat{k}| = r = 2^a \cdot 5 - 1$, $a > 1$, $|B| = 5$.

In this case the S_2-subgroup of $\mathscr{T}$ is semidihedral. It acts with $r - 1$ regular orbits and $(r - 1)/2$ orbits of length 2^{a+1}. This group is irreducible and satisfies (2.1). So $|B| = 1$ is possible.

r	g	n	$\|A_0\|$	$\|B\|$	reg	other	
$5 \cdot 2^a - 1$	2	1	$2^a(r-1)$	1,5	2	$(\|A_0\|)$	$a > 1$

(5) $|\mathscr{G}| = 2$, $|\hat{k}| = r = 5$, $|B| = 3$.

The analysis is the same as in (4). Again $|B| = 1$ is not allowable because of (2.1). Here a subgroup is also possible.

r	g	n	$\|A_0\|$	$\|B\|$	reg	other
5	2	1	8	3	1	(8)
5	2	1	4	3	2	$(4)^2$

(5′) $|\mathscr{G}| = 2$, $|\hat{k}| = r = 2^a \cdot 3 - 1$, $a > 1$, $|B| = 3$.

The analysis is identical to (4′). If $|B| = 1$ then (*) $a > 2$ so that the S_2-subgroup has order >8.

r	g	n	$\|A_0\|$	$\|B\|$	reg	other	
$2^a \cdot 3 - 1$	2	1	$2^a(r-1)$ $(a > 1)$	1,3	1	$(\|A_0\|)$	
$2^a \cdot 3 - 1$	2	1	$2^{a-1}(r-1)$ $(a > 1)$	1,3	2	$(\|A_0\|)^2$	split (*)

(6) $|\mathscr{G}| = 2, |\hat{k}| = 4, |B| = 5.$

(7) $|\mathscr{G}| = 2, |\hat{k}| = 2, |B| = 3.$

r	g	n	$\|A_0\|$	$\|B\|$	reg	other
2	2	2	6	5	2	(3)
2	2	1	1	3	1	(1)

In checking cases, one must recall that (2.1) implies G has only cyclic normal abelian subgroups. If we have one regular orbit for A then any subgroup of index $\geqq 3$ will have at least three. In passing to subgroups we must make certain we cover $A/A_0 \simeq \mathscr{G}$. Also we must check to see we do not pick up extra regular orbits from the "other" orbits of A.

We have itemized all cases. It should be remarked that the referee was most helpful in clearing up several glaring mistakes and "missing" entries in the author's earlier itemizations.

4. Statement of the theorem. We repeat our hypotheses here for convenience.

(4.1) (1) *$G = AB$ is a group with normal cyclic subgroup B and nilpotent complement A where $A \cap B = 1$.*

(2) $\tilde{k}$ = GF(r) *for a prime r.*

(3) *V is a faithful irreducible $k[G]$-module such that $V|L$ is homogeneous for all $L \Delta G$.*

The group G contains a normal cyclic self centralizing subgroup $M \geqq B$. Let $A_0 = A \cap M$. We use the following symbols:

c—G is cyclic.

n—G is nilpotent.

n^*—If $|B| = 1$ then G is nilpotent. All cases not marked with c, n, or n^* are non-nilpotent.

q—If Q is an S_2-subgroup of A then Q is quaternion or generalized quaternion. In all other cases Q splits over $Q \cap A_0$.

μ, b—μ is an odd divisor of $r - 1$. b is a divisor of μ which is relatively prime to $|A_0|$.

reg—number of regular A-orbits upon V.

other—length e and number f of other A-orbits denoted by $(e)^f$.

(4.2) *Assume* (4.1). *Then A has at least* 3 *regular orbits upon V unless one of the following occurs. Let t* = dim $V/[A:A_0]$.

	r	$[A:A_0]$	t	$\|A_0\|$	$\|B\|$	reg	other	notes
(1)	2	2	1	1	3	1	(1)	
(2)	2	2	2	6	5	2	(3)	
(3)	2	3	1	1	7	2	(1)	
(4)	2	3	2	9	7	2	(9)	
(5)	3	2	2	16	5	2	(16)	
(6)	3	4	1	16	5	1	(16)	
(7)	3	4	1	8	5	2	$(8)^2$	
(8)	3	4	1	8	5	2	(16)	
(9)	5	2	1	8	3	1	(8)	
(10)	5	2	1	4	3	2	$(4)^2$	
(11)	r	1	m	$r^m - 1$	1	1	0	c
(12)	r	1	m	$(r^m - 1)/2$	1,2	2	0	c, (*)
(13)	$2^a - 1$	2	1	$2^a(r - 1)/\mu$	b	0	$(\|A_0\|)^\mu$	$n, a > 1$
(14)	$2^2 - 1$	2	1	$2^{a-1}(r - 1)/\mu$	b	0	$(\|A_0\|)^{2\mu}$	$n, a > 2$
(15)	$2^a - 1$	2	1	$2^{a-2}(r - 1)$	1	1	$(\|A_0\|)^2$	$n, a > 3$
(16)	$2^a - 1$	2	1	$2^{a-1}(r - 1)$	1	1	0	n, q
(17)	$2^a - 1$	2	1	$2^{a-2}(r - 1)$	1	2	0	$n, q, a > 2$
(18)	$2^a \cdot 3 - 1$	2	1	$2^a(r - 1)$	1,2	1	$(\|A_0\|)$	$n^*, a > 1$
(19)	$2^a \cdot 3 - 1$	2	1	$2^{a-1}(r - 1)$	1,3	2	$(\|A_0\|)^2$	$n^*, a > 1$, (**)
(20)	$2^a \cdot 5 - 1$	2	1	$2^a(r - 1)$	1,5	2	$(\|A_0\|)$	$n^*, a > 1$

We have used (*) *and* (**) *as described below.*

(*) $|B| = 2$ *is possible only if* $(r^m - 1)/2$ *is odd;*
(**) *if* $|B| = 1$ *then* $a > 2$.

If $AB = G$ is a tabulated exception then we may describe G and its action upon V as follows:

Let $\hat{k} = \mathrm{GF}(r^t)$ and $[\tilde{k}:\hat{k}] = [A:A_0]$. Form the semidirect product $\mathscr{T} = \mathscr{T}(\tilde{k}/\hat{k}) = \mathscr{G}\tilde{k}^\times$ where $\mathscr{G}$ is the Galois group of $\tilde{k}/\hat{k}$. Then $\mathscr{T}$ acts naturally upon $\tilde{k}^+$.

(4.3) *Suppose* G *is an exceptional tabulated group in* (4.2). *Then* V *can be identified with* $\tilde{k}^+$ *and* G *with a subgroup of* $\mathscr{T}$. *Up to a conjugate, the tabulated data uniquely determines* G *as a subgroup of* $\mathscr{T}$ *where* $A_0B = G \cap \tilde{k}^\times$, $k(A_0B) = \tilde{k}$, *and* $A\tilde{k}^\times = \mathscr{T}$.

References

1. T. R. Berger, *Class two p-groups as fixed point free automorphism groups*, Illinois. J. Math. *14* (1970), 121–149.
2. D. Gorenstein, *Finite groups* (Harper and Row, New York, 1968).
3. P. Hall and G. Higman, *On the p-length of p-solvable groups and reduction theorems for Burnside's problem*, Proc. London Math. Soc. *6* (1956), 1–42.
4. D. S. Passman, *Solvable half-transitive automorphism groups*, J. Algebra *6* (1967), 285–304.
5. E. Shult, *On groups admitting fixed point free abelian operator groups*, Illinois J. Math. *9* (1965), 701–720.

Trinity College,
Hartford, Connecticut;
University of Minnesota,
Minneapolis, Minnesota

https://doi.org/10.4153/CJM-1974-048-5 Published online by Cambridge University Press