ISRAEL JOURNAL OF MATHEMATICS, Vol. 55, No. 1, 1986

SOLVABLE GROUPS CONTAIN LARGE CENTRALIZERS†

BY
I. M. ISAACS
Mathematics Department, University of Wisconsin, Madison, WI 53706, USA

ABSTRACT
It is proved that every nonabelian solvable group contains a noncentral element whose centralizer has order exceeding its index.

1. Introduction

If G is a finite group of even order >2 with center of odd order, then there exists an element $x \in G - Z(G)$ with $|C_G(x)| > |G|^{1/3}$. This result of R. Brauer and K. A. Fowler [3] has motivated E. A. Bertram [1] to ask for nonabelian solvable groups G, whether or not there necessarily exists $x \in G - Z(G)$ with $|C_G(x)| > |G|^{1/2}$.

In [1], Bertram answered this affirmatively for groups G with order involving at most two primes. In [2], Bertram and M. Herzog provide further conditions sufficient to guarantee an affirmative answer to Bertram's question. For example, they show that if $G = MN$ with M and N nilpotent or if $|G|$ is not divisible by the fifth power of any prime, then "large" centralizers necessarily exist.

In this paper, we show that no special hypotheses are needed.

THEOREM. *Let G be finite, nonabelian and solvable. Then there exists $x \in G - Z(G)$ with $|C_G(x)| > |G|^{1/2}$.*

We remark that for every prime power $p^a > 2$, there exists a Frobenius group of order $p^a(p^a - 1)$ in which the largest centralizer for any nonidentity element has order p^a. This shows that the exponent $\frac{1}{2}$ in the theorem cannot be replaced by any larger number. Also, some solvability hypothesis is certainly needed since, for instance, the largest centralizer in A_5 has order $5 < 60^{1/2}$.

†Research partially supported by a grant from the National Science Foundation.
Received September 8, 1985

2. Preliminaries

In this section, we prove a few lemmas.

LEMMA 1. *Let $N \lhd G$ and $g \in G$ and suppose g centralizes at least n elements of N with orders coprime to $o(g)$. Then*

$$|C_G(g)| \geqq n\,|C_{\bar{G}}(\bar{g})|$$

where $\bar{G} = G/N$ and $\bar{g} = Ng \in \bar{G}$.

PROOF. Write $\bar{H} = C_{\bar{G}}(\bar{g})$ with $H \supseteq N$ and note that $C_G(g) \subseteq H$. Let K be the conjugacy class of g in H and observe that since $\bar{g} \in Z(\bar{H})$, we have $\bar{K} = \{\bar{g}\}$ and $K \subseteq Ng$.

Now let v be the maximal divisor of $|N|$ which is coprime to $o(g)$ and choose integer m with $m \equiv 1 \bmod o(g)$ and $m \equiv 0 \bmod v$. Since $o(\bar{g})$ divides $o(g)$, we have $\bar{g}^m = \bar{g}$ and so we have a map $\varphi : Ng \rightarrow Ng$ defined by $\varphi(x) = x^m$.

If $y \in K$, there are n elements $z \in N$ with $z^v = 1$ which commute with y. For any of these z, we have $\varphi(zy) = y$ and so $|\varphi^{-1}[\{y\}]| \geqq n$ for all $y \in K$. It follows that

$$|N| = |Ng| \geqq n\,|K|.$$

Therefore,

$$|C_G(g)| = \frac{|H|}{|K|} \geqq n\frac{|H|}{|N|} = n\,|\bar{H}| = n\,|C_{\bar{G}}(\bar{g})|. \qquad \blacksquare$$

LEMMA 2. *Let V be an FG-module for some field F. Let $C \lhd G$ be cyclic with $C = C_G(C)$ and assume $C_V(c) = 0$ whenever $1 \neq c \in C$. If $H \subseteq G$ with $C \cap H = 1$, then $C_V(H) > 0$.*

PROOF. It is no loss to assume F is algebraically closed since if $E \supseteq F$, we could replace V by $V \otimes_F E$ without affecting either the hypothesis or the conclusion. Write $V = V_1 \dotplus \cdots \dotplus V_t$ where the V_i are the homogeneous components of V as an FC-module. (Note that char(F) cannot divide $|C|$ and so V is completely reducible as an FC-module.)

Now C acts like scalar multiplication on each V_i and the V_i are permuted by G. We claim that the action of H on $\{V_i \mid 1 \leqq i \leqq t\}$ is semiregular, for suppose $K \subseteq H$ stabilizes V_i. Then the actions of K and C on V_i commute and hence $[C, K]$ acts trivially on V_i. Now $[C, K] \subseteq C$ and $C_V([C, K]) \neq 0$ and so we have $[C, K] = 1$ and $K \subseteq C(C) = C$. Therefore $K \subseteq C \cap H = 1$ and our claim is established.

Now choose $0 \neq v \in V_1$. The vectors vh for $h \in H$ all lie in different V_i and since the sum of these spaces is direct, we have

$$w = \sum_{h \in H} vh \neq 0.$$

It is clear that $w \in C_V(H)$. ∎

LEMMA 3. *Let U and V be FG-modules for some field F. Suppose we have a nonzero bilinear map $\langle \cdot, \cdot \rangle : U \times V \to F$ which is G invariant. (I.e. $\langle ug, vg \rangle = \langle u, v \rangle$ for all $u \in U$, $v \in V$ and $g \in G$.) Let V^* be the FG-module which is the dual of V. Then U and V^* have a common composition factor as FG-modules.*

PROOF. It suffices to construct a nontrivial FG-homomorphism from U to V^*. For $u \in U$, define $u\theta : V \to F$ to be the map $\langle u, \cdot \rangle$ so that $u\theta \in V^*$. The map $\theta : U \to V^*$ is linear since $\langle \cdot, v \rangle$ is linear for each $v \in V$. Now to show that θ respects the G-actions, we need that $ug\theta = u\theta g$. We have

$$(v)(ug\theta) = \langle ug, v \rangle = \langle u, vg^{-1} \rangle = (vg^{-1})(u\theta) = v(u\theta g)$$

as required. Finally, $\theta \neq 0$ since $\langle \cdot, \cdot \rangle$ is not identically zero. ∎

3. Proof of the theorem

Let G be solvable and write $Z = \mathbf{Z}(G)$ and $s = |G|^{1/2}$. We assume that $Z < G$, and working for a contradiction, we assume that $|C_G(g)| \leqq s$ for all $g \in G - Z$. Equivalently, $|\mathrm{cl}(g)| \geqq s$ when $g \in G - Z$.

STEP 1. *Let $N \lhd G$ with $N \not\subseteq Z$. then $|N| > s$ and N is nonabelian.*

PROOF. Let $n \in N - Z$. then

$$|N| > |\mathrm{cl}(n)| \geqq s.$$

If N is abelian, then $N \subseteq \mathbf{C}(n)$ and so $|N| \leqq |\mathbf{C}(n)| \leqq s$, a contradiction. ∎

Now put $F = \mathbf{F}(G)$, the Fitting subgroup.

STEP 2. *We have $Z < F < G$ and if U/Z is a chief factor of G with $U \subseteq F$ and U/Z a p-group, then*
(a) $F \subseteq C_G(U/Z)$,
(b) *$[F, U]$ is a p-group contained in Z.*

PROOF. If G is nilpotent, there exists abelian $A \lhd G$ with $A = \mathbf{C}(A)$. By Step 1, $A \subseteq Z$ and so $G = \mathbf{C}(A) = A$ and G is abelian, a contradiction. Therefore $F < G$ and since $F \supseteq C_G(F)$, this forces $Z < F$.

Statement (a) follows since $1 < U/Z \cap \mathbf{Z}(F/Z) \lhd G/Z$ and so $U/Z \subseteq \mathbf{Z}(F/Z)$. We now have $[F, U] \subseteq Z$ and so if $x \in F$ and $y \in U$, we get $[x, y]^p = [x, y^p] = 1$ since $y^p \in Z$. It follows that $[F, U]$ is a p-group. ■

Now fix a particular U as in Step 2 with U/Z an elementary abelian p-group. Write $\bar{G} = G/F$ and use overbars to denote the natural homomorphism $G \to \bar{G}$. Since $F < G$, we have $\bar{G} > \bar{1}$ and by Step 2a, $\bar{G}$ acts on U/Z and in fact, U/Z is a simple $\mathbb{Z}_p\bar{G}$-module.

STEP 3. *The $\mathbb{Z}_p\bar{G}$-module U/Z is faithful and $\mathbf{O}_p(\bar{G}) = 1$.*

PROOF. It suffices to prove the first assertion. Let $\bar{K} = \mathbf{C}_{\bar{G}}(U/Z)$. Then $[U, K] \subseteq Z$ and so $[U, K, F] = 1$. Also, $[F, U, K] \subseteq [Z, K] = 1$ by Step 2. By the three subgroups lemma, therefore, we have $[K, F, U] = 1$ and so $U \subseteq \mathbf{C}([K, F])$. Since $U \not\subseteq Z$, we have $|U| > s$ by Step 1, and this forces $[K, F] \subseteq Z$.

Since $Z = \mathbf{Z}(G)$, we see that $F/Z = \mathbf{F}(G/Z)$ and so contains its own centralizer in G/Z. Therefore, $K \subseteq F$ and so $\bar{K} = \bar{1}$ as required. ■

We consider the centralizers in $\bar{G}$ of the nonzero vectors uZ in the module U/Z (where $u \in U - Z$). Fix the notation

$$m = \max\{|\mathbf{C}_{\bar{G}}(uZ)| \mid u \in U - Z\}$$

and let Q be the Sylow p-subgroup of Z.

STEP 4. *We have $|\bar{G}| \cdot |Q| \geqq ms$ with strict inequality if p does not divide $(1/m)|\bar{G}|$.*

PROOF. Choose $u \in U - Z$ such that $|\mathbf{C}_{\bar{G}}(uZ)| = m$ and write $C = \mathbf{C}_G(uZ)$ so that $F \subseteq C$ by Step 2a. We therefore have $|C/F| = m$.

Since $[C, u] \subseteq Z$, we have $[c, u]^p = [c, u^p] = 1$, since $u^p \in Z$ and thus $[C, u]$ is a p-group contained in Q. It follows that $|\mathrm{cl}_C(u)| \leqq |Q|$. We now have

$$s \geqq |\mathbf{C}_G(u)| \geqq |\mathbf{C}_C(u)| = |C|/|\mathrm{cl}_C(u)| \geqq |C|/|Q| = m|F|/|Q|$$

and thus

$$ms = m|G|/s \leqq |G| \cdot |Q|/|F| = |\bar{G}| \cdot |Q|$$

as desired.

If equality holds and p does not divide $(1/m)|\bar{G}|$, then s is an integer with p-part equal to $|Q|$. Equality also implies that $|\mathbf{C}_G(u)| = s$ and thus Q is a full Sylow p-subgroup of $\mathbf{C}_G(u)$. Since $u^p \in Z$, it follows that $u \in QZ = Z$ and this contradiction completes the proof. ■

STEP 5. *Suppose $g \in G - F$ with $o(g)$ not divisible by p and choose V with $Z \subseteq V \subseteq C_U(g)$. Let $T = N_G(V)$. Then*

(a) $|\bar{T} : C_{\bar{T}}(\bar{g})| \geqq m|V:Z|/|\bar{G}:\bar{T}|$

and

(b) $|\bar{G} : C_{\bar{G}}(\bar{g})| \geqq m$.

These inequalities are strict if p does not divide $(1/m)|\bar{G}|$.

PROOF. Note that (b) follows from (a) by taking $V = Z$. We proceed to prove (a). If P is the Sylow p-subgroup of V, then since $p \nmid o(g)$, Lemma 1 yields that

$$s \geqq |C_G(g)| \geqq |C_T(g)| \geqq |P| \cdot |C_{\bar{T}}(\bar{g})|.$$

By Step 4, then,

$$|\bar{G}| \cdot |Q| \geqq ms \geqq m|P| \cdot |C_{\bar{T}}(\bar{g})|.$$

Since $|P:Q| = |V:Z|$, (a) follows.

If equality occurs here, it must occur in Step 4 and so p divides $(1/m)|\bar{G}|$. ∎

STEP 6. *For some prime $r \leqq m$, we have $O_r(\bar{G}) > 1$.*

PROOF. Let $\bar{C} = F(\bar{G})$ and assume, by way of contradiction, that every prime divisor of $|\bar{C}|$ exceeds m. By the definition of m, therefore, the action of $\bar{C}$ on U/Z is elementwise fixed point free and so $\bar{C}$ is a nilpotent Frobenius complement.

We claim that $|\bar{C}|$ is cyclic. If this fails, then $\bar{C}$ necessarily has a characteristic subgroup $\bar{X}$ of order 2. Then $2 > m$ and we have $m = 1$ and the action of all of $\bar{G}$ on U/Z is elementwise fixed point free. In this case, $p \nmid |\bar{G}|$. Let $g \in X$ be a 2-element with $\bar{X} = \langle \bar{g} \rangle$. Then $\bar{g} \in Z(\bar{C})$ and this contradicts Step 5b since we must have strict inequality in this case.

Since $\bar{C} = C_{\bar{G}}(\bar{C})$, we can apply Lemma 2 and conclude that if $\bar{H} \subseteq \bar{G}$ with $\bar{H} \cap \bar{C} = \bar{1}$, then $\bar{H}$ has a nontrivial fixed point in U/Z. It follows that $m \geqq |\bar{H}|$. In particular, if we let π be the set of all primes not dividing $|\bar{C}|$, we can take $\bar{H}$ to be a Hall π-subgroup of $\bar{G}$ and we conclude that $|\bar{G}|_\pi \leqq m$.

Now let q be the smallest prime divisor of $|\bar{C}|$ and let $\bar{Y} \subseteq \bar{C}$ have order q. Then $\bar{Y} \lhd \bar{G}$ and so $|\bar{G} : C_{\bar{G}}(\bar{Y})|$ divides $q-1$ and so is a π-number. This yields that

$$|\bar{G} : C_{\bar{G}}(\bar{Y})| \leqq |\bar{G}|_\pi \leqq m.$$

Now $p \nmid |\bar{C}|$ (for instance, by Step 3) and so $p \neq q$ and we can apply Step 5b (with g a q-element such that $\langle \bar{g} \rangle = \bar{Y}$) to conclude the reverse inequality.

Equality therefore occurs in 5b and also, we have $|\bar{G}|_\pi = m$. Therefore, $(1/m)|\bar{G}| = |\bar{G}|_{\pi'}$ and this is not divisible by p since $p \nmid |\bar{C}|$. In this situation, however, the inequality in 5b must be strict, and this is a contradiction. ■

By Step 6, we can choose a chief factor E/F of G such that $\bar{E}$ is an r-group with $r \leqq m$. Fix this choice of E.

STEP 7. *The group $\bar{E}$ is not cyclic.*

PROOF. Otherwise, $|\bar{G} : C_{\bar{G}}(\bar{E})| \leqq r - 1 < m$ and this contradicts Step 5b since $r \neq p$. ■

Since $\bar{E}$ is not cyclic and U/Z is (by Step 3) a faithful, completely reducible $\mathbb{Z}_p\bar{E}$-module, it cannot be that this module is homogeneous. We can therefore write

$$U/Z = U_1/Z \times U_2/Z \times \cdots \times U_t/Z$$

where the U_i/Z are the homogeneous components of U/Z as a $\mathbb{Z}_p\bar{E}$-module and $t > 1$. The subgroups U_i are transitively permuted by the action of $\bar{G}$.

Let $\bar{E}_i = C_{\bar{E}}(U_i/Z)$. Then $\bar{E}/\bar{E}_i$ acts faithfully and homogeneously on U_i/Z and thus it is cyclic and $|\bar{E} : \bar{E}_i| = r$.

STEP 8. *We have $t = 2$ and $|\bar{E}| = r^2$.*

PROOF. If $[U_1, U_i] \neq 1$, let $C = [U_1, U_i]$. Then $C \subseteq U' \subseteq [F, U]$ and so is a p-group by Step 2b. Let H be of index p in C and identify C/H with the additive group of $\mathbb{Z}_p$. Then commutation defines a nonzero bilinear map

$$U_1/Z \times U_i/Z \to \mathbb{Z}_p.$$

(Read the commutator mod H.) Since $C \subseteq Z$, this map is $\bar{E}$-invariant and so by Lemma 3, $(U_1/Z)^*$ and U_i/Z have a common composition factor as $\mathbb{Z}_p\bar{E}$-modules. Since $(U_1/Z)^*$ and each U_i/Z is homogeneous, this can happen for at most one value of i (possibly $i = 1$). Thus $[U_1, U_j] = 1$ for $j \neq i$.

We now do some computations. Write $z = |Z|$ and $u = |U_1/Z|$. Then $|U_j/Z| = u$ for all j and

$$\left|\prod_{j \neq i} U_j\right| = zu^{t-1}.$$

This group centralizes $U_1 \not\subseteq Z$ and thus $zu^{t-1} \leqq s$.

If $x \in U_1 - Z$, then all G-conjugates of x lie in the various $U_j - Z$ and so

$$s \leqq |\mathrm{cl}_G(x)| \leqq t(zu - z).$$

Therefore,

$$zu^{t-1} \leqq zt(u-1).$$

This yields $u^{t-1} - 1 < t(u-1)$ and

$$t > 1 + u + u^2 + \cdots + u^{t-2}.$$

If $t \geqq 3$, this gives

$$t > 1 + u + 1 + \cdots + 1 = u + t - 2$$

and $u < 2$, a contradiction. Thus $t \leqq 2$ and since $t > 1$, we have $t = 2$, exactly.

Finally, $\bar{E}_1 \cap \bar{E}_2 = \bar{1}$ since $\bar{E}$ is faithful on $U/Z = U_1/Z \times U_2/Z$. Since $|\bar{E} : \bar{E}_i| = r$, it follows that $|\bar{E}| = r^2$. ■

Step 9. *Our counterexample does not exist.*

Proof. Let $T = N_G(U_1)$ so that $T \supseteq F$ and $|G : T| = 2$ since $\{U_1, U_2\}$ is a conjugacy class of subgroups.

Now $\bar{E}_1 \lhd \bar{T}$ and $|\bar{E}_1| = r$ so that we have

$$|\bar{T} : C_{\bar{T}}(\bar{E}_1)| \leqq r - 1.$$

Let $g \in E_1$ be an r-element with $\langle \bar{g} \rangle = \bar{E}_1$. We wish to apply Step 5a for this g, with U_1 in place of V. To do this, we need to check that $U_1 \subseteq C(g)$. Since $\bar{g} \in \bar{E}_1 = C_{\bar{E}}(U_1/Z)$, we have $[U_1, \langle g \rangle] \subseteq Z$ and thus $[U_1, \langle g \rangle, \langle g \rangle] = 1$.

If P is the Sylow p-subgroup of U_1, then $1 = [P, \langle g \rangle, \langle g \rangle] = [P, \langle g \rangle]$ since $(|P|, |\langle g \rangle|) = 1$. Thus $P \subseteq C(g)$ and since $U_1 = PZ$, we have $U_1 \subseteq C(g)$ as required.

Step 5a now yields that

$$m > r - 1 \geqq |\bar{T} : C_{\bar{T}}(\bar{E}_1)| \geqq m\,|U_1 : Z|/|\bar{G} : \bar{T}|.$$

Therefore, $|U_1 : Z| < |\bar{G} : \bar{T}| = 2$, a contradiction. ■

References

1. E. A. Bertram, *Large centralizers in finite solvable groups*, Israel J. Math. **47** (1984), 335–344.

2. E. A. Bertram and M. Herzog, *Finite groups with large centralizers*, J. Austral. Math. Soc., to appear.

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