Math. Proc. Camb. Phil. Soc. (1980), **87**, 393
Printed in Great Britain

The Hughes problem for exponent nine

By THOMAS J. LAFFEY
University College, Dublin

(*Received* 5 *December* 1978)

Let G be a finite group and n a natural number. Set $H_n(G) = \langle g \in G | g^n \neq 1 \rangle$. The aim of this paper is to prove the following result.

THEOREM. *Let G be a finite group which is not a 3-group. Then $|G/H_9(G)| = 1, 3, 9$ or 27. All alternatives can arise.*

This result is related to results on the Hughes problem. When $n = p$ is prime, Hughes and Thompson (2), have shown that if G is not a p-group, $|G/H_p(G)| = 1$ or p. For $p = 3$, Straus and Szekeres (8), have shown that for all G, $H_3(G) \neq 1$ implies $|G/H_3(G)| = 1$ or 3. (A stronger result for $p = 3$ is obtained by the author in (4)). When $n = 4$ and G is not a 2-group, we have shown (5) that $|G/H_4(G)| = 1, 2, 4$ or 8. When $n = 5$, Wall (10), has constructed a 5-group with $|G/H_5(G)| = 25$.

The proof here involves an analysis of the fixed points of elements of order 3 and 9 acting on a finite vector space. Though some of the arguments can easily be extended to elements of order p or p^2 (p an arbitrary prime), there are a few places in the proof where the smallness of 3 or 9 is crucial. We feel that an extension of the theorem to the case of $H_{p2}(G)$, $p > 3$ requires new methods. The notation is standard (cf. (1), (3)). We recall for convenience the following results.

LEMMA 1 ((1), (3·3·3)). *Let P be an elementary abelian p-group acting faithfully on an elementary abelian q-group ($q \neq p$) where p, q are primes. Then*

$$Q = \Sigma \oplus \{C_Q(B) \,|\, \text{all subgroups } B \text{ of } P \text{ with } P/B \text{ of order } p\}.$$

LEMMA 2 ((3), III (6·5), (6·6)). *Let H be a group of exponent 3. Then $[x, y, y] = 1$ for all $x, y \in H$. If H is 2-generated, then $H' \leqslant Z(H)$. In any case, H has class at most 3.*

LEMMA 3 ((3), III (6·9)). *Let G be a group such that $[x, y, y, z] = [x, y, z, z] = 1$ for all $x, y, z \in G$. Then G has class at most 3.*

LEMMA 4 (4). *Let H be a finite group such that $|\{h \in H | h^3 = 1\}| > 7/9|H|$. Then $h^3 = 1$ for all $h \in H$.*

We now prove

LEMMA 5. *Let G be a finite 3-group of linear transformations of a finite dimensional vector space V over a field F. Let $x, y \in G$ be such that (i) $x^3 = y^3 = 1$ and (ii) neither x nor y has 1 as an eigenvalue on V. Then $xy = yx$.*

Proof. We note that the characteristic of F does not divide the order of G. Hence there exists a finite extension K of the prime subfield of F such that K is a splitting

https://doi.org/10.1017/S0305004100056826 Published online by Cambridge University Press

field for G and all its subgroups. We may regard G as a group of matrices with entries in F and hence, by a suitable transformation, we may assume that the elements of G have entries in K. Let X be the algebra generated over K by $G_0 = \langle x, y\rangle$. By Maschke's theorem, X is semisimple and by our choice of K, K splits X. Hence X is a direct sum of a finite number of matrix algebras over K. Assume, for the sake of contradiction, that $xy \neq yx$.

Thus, X has a matrix algebra $M_r(K)$ (some $r \geqslant 2$) as a direct summand. Hence $M_r(K)$ is generated by a pair of elements $\bar{x}, \bar{y}$ (the components of x, y in this direct summand, respectively). So $\bar{x}\bar{y} \neq \bar{y}\bar{x}$. Since x, y have no eigenvalue 1 and $x^3 = y^3 = 1$, $\bar{x}, \bar{y}$ both have minimal polynomial $\lambda^2 + \lambda + 1$. But then $r = 2$ ((6), Remark 1). If K has characteristic zero, we have an immediate contradiction, since G_0 cannot have an irreducible 2-dimensional representation. Suppose that K has characteristic $q > 0$. Then $K = GF(q^n)$, some $n \geqslant 1$ and $\langle \bar{x}, \bar{y}\rangle$ is isomorphic to a non-abelian 3-subgroup of $GL(2, q^n)$. However, $\bar{x}, \bar{y}$ are both similar to the companion matrix of $\lambda^2 + \lambda + 1$ and hence they have determinant 1. Hence $\langle \bar{x}, \bar{y}\rangle$ is isomorphic to a subgroup of a Sylow 3-subgroup S of $SL(2, q^n)$. However, by (3) II(8·3), S is cyclic. This is a final contradiction.

We now prove a result on secretive 3-groups of exponent 9.

LEMMA 6. *Let P be a finite 3-group with $Z(P)$ cyclic and $g^3 \in \Omega_1(Z(P)) - \{1\}$ for all $g \in P - \phi(P)$. Then $|P/\phi(P)| \leqslant 27$ and P has class at most 3.*

Proof. Suppose that $|P/\phi(P)| \geqslant 9$. Then since

$$|P - \phi(P)| \geqslant 8/9|P| > 7/9|P|,$$

Lemma 4 implies that $P/\Omega_1(Z(P))$ has exponent 3. Also if $g \in P - \phi(P)$, $g^3 = z$ for some $1 \neq z \in \Omega_1(Z(P))$ and thus if $|Z(P)| > 3$, $(gw)^3 = 1$ where $w \in Z(P)$ is such that $w^3 = z^{-1}$. Hence $|Z(P)| = 3$.

Since $P/Z(P)$ has exponent 3, Lemma 2 implies that $[x, y, y] \in Z(P)$ for all $x, y \in P$ and that $P/Z(P)$ has class at most 3. Let $P_1 = P, P_2, \ldots$ be the lower central series of P. Note that $P_5 = 1$. If $h, k \in P$, then we have

$$1 = [h, k^3] = [h, k]^3 [h, k, k]^3 [h, k, k, k].$$

Since $[h, k, k] \in Z(P)$, we conclude that

$$1 = [h, k]^3.$$

Let $x \in P - \phi(P)$ and let $u \in P_2$. Then

$$\begin{aligned}(xu)^3 &= x^3[x, [x, u^{-1}]^{-1}] [x, u^{-1}]^3 [x, u^{-1}, u^{-1}] u^3. \\ &= x^3[x, [x, u^{-1}]^{-1}] u^3.\end{aligned}$$

If further $u = [h, k]$ is a simple commutator, we conclude that

$$(xu)^3 = x^3[x, [x, u^{-1}]^{-1}].$$

Hence, if $\alpha = [x, [x, u^{-1}]] \neq 1$, then, since both it and x^3 lie in $Z(P)$, one of the elements $x^3, (xu)^3, (xu^2)^3$ is 1. Since x, xu, xu^2 all lie in $P - \phi(P)$, this is a contradiction. Hence $\alpha = 1$. That is

$$[x, [x, u^{-1}]^{-1}] = 1$$

https://doi.org/10.1017/S0305004100056826 Published online by Cambridge University Press

for all $x \in P - \phi(P)$ and all simple commutators u.

Suppose $x \in \phi(P) = P'$. Then $[x, [x, u^{-1}]^{-1}] \in P_6 = 1$. Hence we have

$$[x, [x, u]] = 1$$

for all $x \in P$ and all simple commutators u. This together with the fact that $[x, y, y, z] = 1$ for all $x, y, z \in P$ implies that P satisfies the hypotheses of Lemma 3. Hence, by that result, P has class at most 3.

It remains to bound $|P/\phi(P)|$. Suppose, for the sake of contradiction, that

$$|P/\phi(P)| \geqslant 3^4$$

and let u, v, w, y be elements of $P - \phi(P)$ independent mod $\phi(P)$. Using the fact that P has class 3, we find that

$$\begin{aligned}(u^i v^j w^k y^l)^3 = {} & u^{3i} v^{3j} w^{3k} y^3 [u, v, v]^{ij^2} \quad [v, u, u]^{i^2 j} [u, w, w]^{ik^2} \\ & \times [v, w, w]^{jk^2} [w, u, u]^{ki^2} [w, v, v]^{kj^2} \quad [w, u, v]^{ijk} [w, v, u]^{ijk} [u, y, y]^{il^2} \\ & \times [v, y, y]^{jl^2} [w, y, y]^{kl^2} [y, u, \bar{y}]^{i^2 l} \quad [y, v, v]^{j^2 l} [y, w, w]^{k^2 l} [y, u, v]^{ijl} \\ & \times [y, u, w]^{ikl} [y, v, u]^{ijl} [y, v, w]^{jil} \quad [y, v, w]^{jkl} \quad [y, w, u]^{ikl} [y, w, v]^{jkl}.\end{aligned}$$

Each of the triple commutators is an element of $Z(P)$ and hence can be written as z^a for some $a \in GF(3)$ where z generates $Z(P)$. We can also regard i, j, k, l as elements of $GF(3)$. Hence we can write

$$(u^i v^j w^k y^l)^3 = z^{f(i,j,k,l)},$$

where f is a polynomial of total degree 3 with coefficients in $GF(3)$. Also $f(0, 0, 0, 0) = 0$. By Chevalley's theorem ((7), p. 37), f has a nontrivial zero on $GF(3)$. But this implies that some element of $P - \phi(P)$ has order 3, giving a contradiction. Note that since $P/Z(P)$ is 3-generated of exponent 3, $|P/Z(P)| \leqslant 3^7$ ((3), III(6·6)), so $|P| \leqslant 3^8$.

Remark 1. In (9), Wall has constructed, *inter alia*, a 3-group of rank 3 satisfying the hypotheses of Lemma 6; so the bound in the Lemma can be attained.

We now begin the proof of the theorem. Assume the result is false, and let G be a minimal counterexample. We first show:

(I) $G = VP$, where V is a minimal normal subgroup of G and P is a Sylow 3-subgroup of G. V is a q-group for some prime $q \neq 3$ and P acts faithfully on V.

The proof of (I) is essentially the same as the reduction on the first paragraph of § 2 of (2). We include it here for the sake of completeness.

Let $H = H_9(G)$, $q \neq 3$ a prime divisor of $|H|$ and V a Sylow q-subgroup of H. Let P be a Sylow 3-subgroup of G and let $P_0 = P \cap H$. By the Frattini argument,

$$G = HN_G(V).$$

Let $N = N_G(V)$. Suppose $N \neq G$. Since N is not a 3-group, $|N/H_9(N)| \leqslant 27$, by the minimality of N. However $|G/H| = |HN/H| = |N/N \cap H|$. But $N \cap H \geqslant H_9(N)$. This implies that $|G/H| \leqslant 27$, a contradiction. Hence $N = G$. Again, if $PV \neq G$, $|PV/H_9(PV)| \leqslant 27$. However, $H_9(PV) \leqslant H \cap PV$ and $P \cap H_9(PV) \leqslant P_0 \cap PV$, so

https://doi.org/10.1017/S0305004100056826 Published online by Cambridge University Press

$|PV/H_9(PV)| \geqslant |P/P_0|$. Since $|G/H| = |P/P_0|$, we again get a contradiction. So $G = PV$. Let $1 \neq V_0 \leqslant V$ with $V_0 \lhd G$. If G/V_0 is not a 3-group, then by minimality of G,

$$|G/V_0 : H_9(G/V_0)| \leqslant 27$$

and since

$$H_9(G/V_0) \leqslant H/V_0$$

we have a contradiction. Hence G/V_0 is a 3-group and $V_0 = V$. Also $C_P(V) \lhd \langle P, V\rangle = G$, so $C_P(V) \leqslant O_3(G)$. Hence $P/O_3(G)$ acts faithfully and irreducibly on V.

Finally,

$$H_9(G/O_3(G)) \leqslant H/O_3(G)$$

(note that $O_3(G) \leqslant H$), so if $O_3(G) \neq 1$, minimality of G forces

$$|G/O_3(G) : H_9(G/O_3(G))| \leqslant 27$$

and this forces $|G/H| \leqslant 27$, which is a contradiction. This proves (I).

(II) $P_0 = P \cap H \neq 1$.

Note that by the definition of H each element of $P - P_0$ has order dividing 9. Also by the definition, each element of $P - P_0$ acts fixed-point-freely on V. If $P_0 = 1$, we thus conclude that P is cyclic giving a contradiction.

(III) If $y \in P - P_0$ then y^3 has no fixed point on V. In particular, each element of $P - P_0$ has order 9. (By a *fixed point* we mean a fixed point $v \neq 1$).

Let $y \in P - P_0$. Suppose that y^3 has a fixed point on V. Let z be an element of order 3 in $Z(P)$. Note that since P has a faithful irreducible $GF(q)$-module, $Z(P)$ is cyclic. Also z has no fixed point on V. Hence $\langle y^3\rangle \neq \langle z\rangle$. Then $C_V(y^3)$ is $\langle y, z\rangle$-invariant and thus $C_V(y^3)$ is invariant under the *elementary abelian* group $\langle y, z\rangle/\langle y^3\rangle$.

But now Lemma 1 implies $C_V(y^3) = C_V(y)\, C_V(yz)\, C_V(yz^2)$ (using the fact that $C_V(z) = 1$).

Note that $1 \neq P_0 \lhd P$, so $P_0 \cap Z(P) \neq 1$, so $z \in P_0$. But then y, yz and yz^2 are all elements of $P - P_0$ and none of them have a fixed point on V. This implies $C_V(y^3) = 1$, giving a contradiction.

We now prove:

(IV) Let $A = \langle y^3 | y \in P - P_0\rangle$. Then A is an elementary abelian normal subgroup of P, P/A has exponent 3, $[x, y, y] \in A$ for all $x, y \in P$ and $[A, w, w] = 1$ for all $w \in P - P_0$.

For let $y \in P - P_0$. By (III), y^3 has no fixed points on V. By Lemma 5, A is therefore abelian. Since $P_0 \lhd P$, $A \lhd P$. Also, by (III), $A \leqslant P_0$, since each nontrivial element of A has order 3. Now $k^3 = 1$ for all

$$k \in P/A - P_0/A,$$

and since

$$|P/A - P_0/A| > \tfrac{7}{9}|P/A|,$$

Lemma 4 implies that P/A has exponent 3. So $[u, v, v] \in A$ for all $u, v \in P$.

Now let $u, a \in P$. Then

$$(ua)^3 = u^3[u, [u, a^{-1}]^{-1}]\,[u, a^{-1}]^3\,[u, a^{-1}, a^{-1}]\,a^3. \qquad (*)$$

https://doi.org/10.1017/S0305004100056826 Published online by Cambridge University Press

Let $u \in P - P_0$, $a \in A$. Then

$$(ua)^3 = u^3[u, [u, a^{-1}]^{-1}],$$

using the fact that $A \lhd P$ and is elementary abelian.

Let $\alpha = [u, [u, a^{-1}]^{-1}]$. Note that

$$\alpha^2 = [u, [u, a^{-1}]^{-1}]^2 = [u, [u, a^{-2}]^{-1}].$$

Suppose now that $\alpha \neq 1$. Suppose first that $\langle \alpha \rangle = \langle u^3 \rangle$. Then either $(ua)^3 = 1$ or $(ua^2)^3 = 1$. However, since $A \leqslant P_0$, $ua, ua^2 \in P - P_0$. This contradicts (III). Hence $\langle \alpha \rangle \neq \langle u^3 \rangle$. So $B = \langle \alpha, u^3 \rangle$ is elementary abelian of order 9 and applying Lemma 1, we see that one of the elements u^3, αu^3, $\alpha^2 u^3$ has a fixed point on V. This again contradicts (III). Hence we must have $\alpha = 1$. This implies that $[a, u, u] = 1$ for all $a \in A$ and $u \in P - P_0$, and the proof of (IV) is complete.

The next step is one of the major steps of the proof.

(V) Let $x \in P - P_0$. Then $x^3 \in Z(P)$.

First P/P_0 is not cyclic, since otherwise $|P/P_0| \leqslant 9$. So $P/\phi(P)P_0$ is not cyclic. Let $x, y \in P - \phi(P)P_0$ be independent mod $\phi(P)P_0$. Let $P_1 = \langle x, u \rangle$, $A_1 = \langle u^3 | u \in P_1 - P_0 \rangle$. Note that A_1 is an elementary abelian normal subgroup of P_1 and that $A_1 \leqslant A$. Also since

$$|P_1 - P_0| = |P_1| \left(1 - \frac{|P_0 \cap P_1|}{|P_1|}\right) \geqslant \tfrac{8}{9}|P_1|$$

(using the fact that $P_1/P_0 \cap P_1$ is not cyclic) Lemma 4 implies that $w^3 \in A_1$ for all $w \in P_1$. Since P_1 is 2-generated, Lemma 2 implies that $[x, y, w] \in A_1$ for all $w \in P_1$.

Let $w \in P_1 - P_0$. Then

$$[x, y, w^3] = [x, y, w]^3 [x, y, w, w]^3 [x, y, w, w, w].$$

Now $$[x, y, w, w, w] \in [A_1, w, w] \leqslant [A, w, w] = 1,$$

using (IV). Hence $[x, y, w^3] = 1$ for all $w \in P_1 - P_0$. However, $A_1 = \langle w^3 | w \in P_1 - P_0 \rangle$. Hence

$$[x, y, a] = 1 \quad \text{for all} \quad a \in A_1.$$

Next,

$$\begin{aligned}(x[x, y])^3 &= x^3 [x, [x, [x, y]^{-1}]^{-1}] [x, [x, y]^{-1}]^3 [x, [x, y]^{-1}, [x, y]^{-1}] [x, y]^3 \\ &= x^3 [x, [x, [x, y]^{-1}]^{-1}] [x, y]^3,\end{aligned}$$

using the fact that $[x, [x, y]^{-1}] \in A_1$ and hence has order at most 3 and commutes with $[x, y]^{-1}$.

Let $b = [x, [x, [x, y]^{-1}]^{-1}] [x, y]^3$. Suppose that $b \neq 1$. As before, if $\langle b \rangle = \langle x^3 \rangle$ we find that one of x^3, $(x[x, y])^3$, $(x[x, y^2])^3$ is trivial contradicting (III) (since $x, x[x, y]$, $x[x, y^2] \in P - P_0$). On the other hand, if $1 \neq \langle b \rangle \neq \langle x^3 \rangle$, then $\langle b, x^3 \rangle$ is elementary abelian of order 9 and thus using Lemma 1, one of the elements x^3, $x^3 b$, $x^3 b^2$ has a fixed point on V. This again contradicts (III). Hence $b = 1$. But $b^{-1} = [y, x^3]$. Hence we conclude that y commutes with x^3.

https://doi.org/10.1017/S0305004100056826 Published online by Cambridge University Press

Let $w \in P - \phi(P) P_0\langle x\rangle$. Applying the above argument with w in place of y, we find that w commutes with x^3. Hence

$$|C_P(x^3)| > \tfrac{2}{3}|P|$$

and thus $C_P(x^3) = P$. This proves (V).

Since $A = \langle x^3 | x \in P - P_0\rangle$, we thus find that $A = Z(P)$ and thus, by (IV), we have

(VI) $P/Z(P)$ has exponent 3, $Z(P)$ has order 3 and $x^3 \in Z(P) - \{1\}$ for all $x \in P - P_0$.

(VII) P' has exponent 3.

Let $u, v \in P$. Then

$$\begin{aligned} 1 &= [u, v^3] = [u, v]^3 [u, v, v]^3 [u, v, v, v] \\ &= [u, v]^3 \end{aligned}$$

(using the fact that $[u, v, v] \in A = Z(P)$).

Now by Lemma 2, $P/Z(P)$ has class at most 3 and hence P' has class at most 2. Since P' is generated by simple commutators, each of which has order at most 3, P' has therefore exponent at most 3.

(VIII) Final contradiction.

Since $\mho_1(P) = Z(P) \leqslant P'$, $\phi(P) = P'$ and hence $\phi(P)$ has exponent 3. By (IV), $\phi(P) \leqslant P_0$. Let $P_2 \geqslant \phi(P)$ be such that

$$P/\phi(P) = P_0/\phi(P) \oplus P_2/\phi(P).$$

Note that $P_2 \cap P_0 = \phi(P)$. Let $G_2 = VP_2$. Note that $H_9(G_2) = V\phi(P)$. If $G_2 \neq G$, then by minimality, $|P_2/\phi(P)| \leqslant 27$. This implies that $|P/P_0| \leqslant 27$, a contradiction. Hence $G_2 = G$ and thus $P_0 = \phi(P)$. But now P satisfies the hypotheses of Lemma 6 and we conclude that $|P/\phi(P)| \leqslant 27$. This is a final contradiction.

Example. Let P be the 3-group of exponent 9 and rank 3 with $|Z(P)| = 3$ and such that $x^3 \in Z(P) - \{1\}$ for all $x \in P - \phi(P)$ constructed by Wall in (9). Let $q \neq 3$ be a prime. Then P has a faithful irreducible representation on a finite dimensional vector space V over $GF(q)$. Let G be the associated semidirect product VP. Then $H_9(G) = V\phi(P)$ has index 27 in G. Examples of groups G_1 with $|G_1/H_9(G_1)| = 9$ or 3 can be obtained by taking a subgroup of G of index 3 or 9, respectively, containing $H_9(G)$.

Frobenius groups with Frobenius complement cyclic of order 3 or 9 provide other examples of groups G_1 with $|G_1/H_9(G_1)| = 3$ or 9, respectively.

In conclusion, we remark that it should be possible to get a result of the form: If G is not a 3-group, then

$$|\{g \in G | g^9 = 1\} < k|G|,$$

where k is a fixed fraction < 1, analogous to the results of (4), (5).

Finally we remark that if p is prime, Wall's work (9) shows as in the example above that there exists a finite group G not a p-group with $|G/H_{p^3}(G)| = p^p$.

https://doi.org/10.1017/S0305004100056826 Published online by Cambridge University Press

REFERENCES

(1) Gorenstein, D. *Finite Groups* (New York, Harper and Row, 1968).
(2) Hughes, D. R. and Thompson, J. G. The H_p-problem and the structure of H_p-groups. *Pacific Journal Math.* **9** (1959), 1097–1101.
(3) Huppert, B. *Endliche Gruppen Bd.* I (Berlin, Heidelberg, New York, Springer-Verlag, 1967).
(4) Laffey, T. J. The number of solutions of $x^3 = 1$ in a 3-group. *Math. Z.* **149** (1976), 43–45.
(5) Laffey, T. J. The number of solutions of $x^4 = 1$ in a finite group. *Proc. Roy. Irish Acad.* **79**, (1979), 29–36.
(6) Laffey, T. J. Algebras generated by two idempotents. *Linear Algebra and Appl.* (in the Press).
(7) Mordell, L. J. *Diophantine equations* (New York, Academic Press, 1969).
(8) Straus, E. G. and Szekeres, G. On a problem of D. R. Hughes. *Proc. Amer. Math. Soc.* **9** (1958), 157–158.
(9) Wall, G. E. Secretive p-groups of large rank. *Bull. Austral. Math. Soc.* **12** (1975), 363–369.
(10) Wall, G. E. On Hughes H_p-problem. Article in *Proc. of the International Conference on the Theory of Groups* (Canberra, 1965). (New York, Gordon and Breach, 1967.)

https://doi.org/10.1017/S0305004100056826 Published online by Cambridge University Press