J. Austral. Math. Soc. (*Series A*) **46** (1989), 281–288

ODD ORDER GROUPS WITH AN AUTOMORPHISM CUBING MANY ELEMENTS

MARIAN DEACONESCU and DESMOND MacHALE

(Received 3 July 1987; revised 27 January 1988)

Communicated by H. Lausch

Abstract

We determine the structure of a nonabelian group G of odd order such that some automorphism of G sends exactly $(1/p)|G|$ elements to their cubes, where p is the smallest prime dividing $|G|$. These groups are close to being abelian in the sense that they either have nilpotency class 2 or have an abelian subgroup of index p.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 20 E 36.

1. Introduction

Let G be a group and let n be a fixed non-zero integer. An n-automorphism of G is an automorphism which sends every element of G to its nth power. If G has an n-automorphism for $n = -1, 2$ or 3, it is well known that G is abelian. On the other hand, Miller [8] has shown that for every other value of $n \neq 1$ there exists a non-abelian group admitting a non-trivial n-automorphism.

For a finite non-abelian group G and for $n = -1, 2$ and 3, there remains the problem of determining how large a proportion of the elements of G can be sent to their nth powers by an automorphism, and also of determining the structure of the groups for which these maximal proportions are achieved. For $n = -1$ and 2, these problems were solved by Manning [7], Liebeck and MacHale [2], and Liebeck [4]. (See also MacHale [5], and [3].) Concerning $n = 3$, the following results are proved in MacHale [6].

(i) No automorphism of G can send more than $(3/4)|G|$ elements to their cubes.

(ii) G has an automorphism cubing exactly $(3/4)|G|$ elements if and only if $|G : Z(G)| = 4$ and $Z(G)$ has no elements of order 3, where $Z(G)$ is the centre of G.

(iii) If $|G|$ is odd and p is the least prime dividing $|G|$, then no automorphism of G can send more than $(1/p)|G|$ elements to their cubes.

In this paper we settle the outstanding case arising from (iii) above by classifying all non-abelian groups G of odd order with an automorphism α which sends exactly $(1/p)|G|$ elements to their cubes, where p is the least prime dividing $|G|$.

Let $T = T_\alpha = \{x \in G | x\alpha = x^3)\}$ and $F = F_\alpha = \{x \in G | x\alpha = x\}$. The classification theorem depends on whether F is trivial or not.

THEOREM. (i) *If* $|F| = 1$, *then* G *is nilpotent of class* 2, $|G'| = p$, $G^p \cap G' = 1$ *and* $p \geq 5$.

(ii) *If* $|F| \neq 1$, *then* T *is an abelian subgroup of index* p *in* G *and there exists* $f \in F$, $f \notin T$, *such that* f *has order* p. *Moreover* $(|T|, 3) = 1$.

These conditions are necessary and sufficient. Thus, as in the cases $n = -1$ and 2, the groups in question are close to being abelian in that they either have small nilpotency class or an abelian subgroup of small index.

2. Notation

Throughout, G will denote a finite group of odd order. Any notation not explicitly defined is standard and conforms to that of [1].

$\mathscr{G}_p$ the set of all finite groups with order divisible by the prime p but by no smaller prime.

α an automorphism of G,

$T_\alpha = T$, the set $\{x \in G | x\alpha = x^3\}$,

$F_\alpha = F$, the subgroup $\{x \in G | x\alpha = x\}$,

G^p the subgroup generated by the pth powers of elements of G,

$|x|$ the order of the element $x \in G$,

x^G the conjugacy class of G containing x,

$Z(G) = Z$, the centre of G.

3. Preliminary results

The following remarks are at once obvious.

(i) $T \cap F = 1$, since $|G|$ is odd.
(ii) $(T)\alpha = T$.
(iii) No element of T has order divisible by 3.
(iv) If A is a subgroup of G, maximal in T, then $(A)\alpha = A$ and A is abelian, since the resctriction of α to A is a 3-automorphism of A.

LEMMA 3.1. *If $G \in \mathscr{G}_p$ and $H \triangleleft G$ with $|H| = p$, then $H \subset Z(G)$.*

PROOF. Let $H = \langle h \rangle$. Now all the conjugates of h lie in H and their number, being a divisor of $|G|$, is either 1 or p. Since the identity is not conjugate to h, h has exactly one conjugate. Thus h is central and the result follows.

LEMMA 3.2. *If $t \in T$, $C_G(t) = C_G(t^3)$.*

PROOF. If $tg = gt$ then $t^3g = gt^3$. Conversely, if $t^3g = gt^3$ then applying the automorphism α^{-1}, $t(g\alpha^{-1}) = (g\alpha^{-1})t$. Since the correspondence $g \leftrightarrow g(\alpha^{-1})$ is one-to-one, the result follows.

LEMMA 3.3. *If α is fixed-point-free, then any conjugacy class of G contains at most one element of T.*

PROOF. For $g \in G$, $t \in T$, suppose that $g^{-1}tg \in T$. Then $(g^{-1}tg)\alpha = (g^{-1}tg)^3$, whence $[g(g\alpha)^{-1}, t^3] = 1$. By Lemma 3.2, $[g(g\alpha)^{-1}, t] = 1$, and since α is fixed-point-free, this implies $[g, t] = 1$, as claimed.

LEMMA 3.4. *If $G \in \mathscr{G}_p$ has k conjugacy classes, then*

$$\frac{k}{|G|} \leq \frac{1}{p^2}\left[1 + \frac{p^2 - 1}{|G'|}\right].$$

PROOF. G has $|G : G'|$ irreducible representations of degree 1 and all other ones have degrees at least p. The degree equation, $|G| = \sum_{i=1}^{k} d_i^2$, now gives $|G| \geq |G : G'| + (k - |G : G'|)p^2$, from which the result follows.

LEMMA 3.5. *If $G \in \mathscr{G}_p$ and $|F| > 1$, then $Tf_1 = Tf_2$ implies $f_1 = f_2$, for $f_1, f_2 \in F$. In this case $G = TF = FT$ and $|F| = p$.*

PROOF. Suppose $f_1 = tf_2$, for $t \in T$. Applying α, we have $f_1 = t^3 f_2 = t^2 f_1$. Since $|G|$ is odd, $t = 1$ and $f_1 = f_2$. Now any $f \in F, f \neq 1$, has order at least p so $G = T \cup Tf \cup \cdots \cup Tf^{p-1}$. Thus $G = TF$ and $|F| = p$. Similarly, $G = FT$. We assume from now on that G is a non-abelian group in $\mathscr{G}_p$ $(p > 2)$ and some automorphism α of G satisfies $p|T_\alpha| = p|T| = |G|$.

4. Case where $|F| = 1$

We assume throughout this section that α is fixed-point-free. In this case we claim that T cannot be a subgroup, so suppose otherwise. Then $|G:T| = p$, $T \lhd G$ and so T consists of complete conjugacy classes in G. Then, by Lemma 3.3, $T \subset Z(G)$, $G/Z(G)$ is cyclic and G is abelian, a contradiction.

Suppose that G has k conjugacy classes. Then, by Lemma 3.3, $k \geq |T|$, so $k/|G| \geq |T|/|G| = 1/p$. By Lemma 3.4

$$\frac{1}{p^2}\left[1 + \frac{p^2-1}{|G'|}\right] \geq \frac{1}{p}$$

whence $|G'| \leq p+1$. Since $G \in \mathscr{G}_p$ and p is odd, $|G'| = p$. By Lemma 3.1, $G' \subset Z(G)$, so G is nilpotent of class 2.

Next, we show $p \neq 3$, so suppose $p = 3$. Let $a, b \in T$ be such that $[a,b] \neq 1$. Such a pair of elements exists since otherwise T is a subgroup, a contradiction. Since G' is characteristic in G and α is fixed-point-free, $[a,b]^2 = [a,b]\alpha = [a^3, b^3] = [a,b]^9$. Thus $[a,b]^7 = 1$ and so $[a,b] = 1$, a contradiction. Thus $p \geq 5$.

We now claim that $Z = Z(G) \not\subset T$, so suppose otherwise. Since then $G' \subset Z \subset T$, $G' \subset T$. If $a, b \in T, [a,b] \neq 1$ then

$$[a,b]\alpha = [a,b]^3 = [a^3, b^3] = [a,b]^9.$$

Thus $[a,b]^6 = 1$, which forces $[a,b] = 1$, since $|G|$ is odd and T has no elements of order 3. This contradiction shows $Z \not\subset T$.

Let $Z^* = Z \cap T$. Then Z^* is a subgroup of Z with $|Z : Z^*| = p$. To see this, consider $Zt \cap T$ for any $t \in T$. Let $z \in Z$. Now $zt \in T \Leftrightarrow (zt)^3 = z\alpha t^3 \Leftrightarrow z\alpha = z^3 \Leftrightarrow z \in Z^*$. Thus $Zt \cap T = Z^*t$. If $|Z : Z^*| > p$, then $|T| < (1/p)|G|$, a contradiction. For $a, b \in T$, if $1 \neq [a,b] = c$ then c generates G', and $c \notin Z^*$, since then $c^3 = c\alpha = [a^3, b^3] = c^9$ and $c = 1$. Thus, $Z = Z^* \times G'$.

Finally, we show that $G^p \cap G' = 1$. Now, since G has class 2, for all $t \in T$, $x \in G$, $[t^p, x] = [t,x]^p = 1$, so $t^p \in Z \cap T = Z^*$. Thus, for all $a, b \in T$, $(ab)^p = a^p b^p [b,a]^{p(p-1)/2} = a^p b^p$, since p is odd. Thus $G^p \subset Z^*$, so $G^p \cap G' = 1$.

We can now state a structure theorem in the case $F = 1$.

THEOREM 4.1. *Necessary and sufficient conditions that a non-abelian group $G \in \mathscr{G}_p$ $(p > 2)$ have an automorphism α such that $|F_\alpha| = 1$ and $p|T_\alpha| = G$ are*

(i) *G is nilpotent of class 2 with $|G'| = p$,*

(ii) $G^p \cap G' = 1$

and

(iii) $p \geq 5$.

PROOF. We have already established the necessity of these conditions. Suppose that G is a group which satisfies (i)–(iii). Then G/Z is an elementary

https://doi.org/10.1017/S1446788700030743 Published online by Cambridge University Press

abelian p-group and $Z = Z^* \times G'$, where $G^p \subset Z^* \subset G$. Thus $G/Z = \langle Za_1, \dots, Za_k, Zx_1, \dots, Zx_k \rangle$, where $[x_i, x_j] = [a_i, a_j] = 1$ for all $i, j = 1, \dots, k$; $[a_i, x_j] = 1$ $(i \neq j)$; $[a_i, x_i] = c$ $(i = 1, \dots, k)$, where $\langle c \rangle = G'$. Put $A = \langle a_1, \dots, a_k, Z^* \rangle$. Then every element $g \in G$ is uniquely expressible as $g = ac^s x_1^{q_1} \cdots x_k^{q_k}$, where $a \in A$, $0 \leq s \leq p-1$, $0 \leq q_i < p$ $(i = 1, \dots, k)$. The map α defined by

$$g\alpha = (ac^s x_1^{q_1} \cdots x_k^{q_k})\alpha = a^3 c^{9s} x_1^{3q_1} \cdots x_k^{3q_k}$$

defines an automorphism of G. Moreover, $p|T_\alpha| = G$ because, given any $a \in A$ and integers $q_1, \dots, q_k$, there is exactly one s, $0 \leq s < p$, such that $g\alpha = g^3$. Finally, we note that $|G_\alpha| = 1$ since $p \geq 5$.

5. Groups in which $p|T| = |G|$ and $|F| \neq 1$

The analysis in this section resembles section $4B$ of Liebeck [4]. However, it differs in detail and the outcome is different.

Up to the end of this section we shall assume the following conditions: $G \in \mathscr{G}_p$ $(p > 2)$ is a non-abelian group, $\alpha \in \operatorname{Aut}(G)$ with $p|T| = p|T_\alpha| = |G|$ and $F = F_\alpha \neq 1$.

By Lemma 3.5, $|F| = p$, so if $F = \langle f \rangle$ we have the disjoint union

$$G = T \cup Tf \cup \cdots \cup Tf^{p-1} = T \cup fT \cup \cdots \cup f^{p-1}T. \tag{0}$$

LEMMA 5.2. *The conjugacy class containing f has no elements in T.*

PROOF. Suppose there exists $g \in G$ such that $g^{-1}fg \in T$. By (0), $g = tf^r$, for $t \in T$ and some integer r. Thus $(f^{-r}t^{-1}ftf^r)\alpha = (f^{-r}t^{-1}ftf^r)^3$, whence $t^{-2}ft^2 = f^3$. Applying α, we have $t^{-6}ft^6 = f^3$, from which $f = t^{-4}ft^4$, and so $t^{-1}ft = f$, since $|G|$ is odd. Finally, $t^{-2}ft^2 = f = f^3$, so $f = 1$, a contradiction.

LEMMA 5.3. *The conjugacy class of $t \in T$ either has one element in T when $[t, f] = 1$, or has exactly p elements in T, when $[t, f] \neq 1$. These elements are $f^{-r}tf^r$, $r = 0, 1, \dots, p-1$.*

PROOF. Let $g \in G$ and $t \in T$ with $g^{-1}tg \in T$. Then from $(g^{-1}tg)\alpha = (g^{-1}tg)^3$ we find that $[(g\alpha)g^{-1}, t^3] = 1$, implies $[(g\alpha)g^{-1}, t] = 1$. But $g = t_1 f^r$ for some $t_1 \in T$ and some integer r, so $(t_1f^r)\alpha(t_1f^r)^{-1}t = t(t_1f^r)\alpha(t_1f^r)^{-1}$. This simplifies to $t_1^2 t = tt_1^2$, so $t_1 t = tt_1$ and $g^{-1}tg = f^{-r}tf^r$, which proves the assertion of the lemma.

https://doi.org/10.1017/S1446788700030743 Published online by Cambridge University Press

LEMMA 5.4. *Suppose that T is not a subgroup of G. If x, y and xy all belong to T, then $xy = yx$.*

PROOF. Suppose x, y and xy belong to T. Then since $|xy| = |yx|$, we have $3 \nmid |x||y||xy||yx|$. Applying α, we obtain $(xy)^3 = x^3y^3$, so

$$(1) \qquad (yx)^2 = x^2y^2$$

By (0), $yx = ft$, for some $f \in F$, $t \in T$, and applying α, we get $y^3x^3 = ft^3 = ft.t^2 = yxt^2$. Thus $x^{-1}y^2x^3 = t^2 = x^{-1}(y^2x^2)x$. Now conjugating (1) by y^{-2} gives $(y^3xy^{-2})^2 = y^2x^2$ and substituting gives $t = x^{-1}y^3xy^{-2}x$, since $t^2 = u^2$ implies $t = u$. Hence $yx = ft = fx^{-1}y^3xy^{-2}x$, so

$$(2) \qquad y^3 = fx^{-1}y^2x.$$

Applying α to (2) we get

$$(3) \qquad y^9 = fx^{-3}y^9x^3.$$

Combining (2) and (3) yields $y^6 = x^{-1}y^{-3}x^{-2}y^9x^3 = (yx)^{-1}(y^{-2}x^{-2})y^9x^3 = (yx)^{-3}y^9x^6$ from (1). Thus $(yx)^3 = y^9x^3y^{-6} = y^9x^3y^3y^{-9} = [y^9(xy)y^{-9}]^3$. Since $3 \nmid |xy||yx|$, we conclude that $yx = y^9xyy^{-9}$ so $xy^8 = y^8x$ and $xy = yx$.

LEMMA 5.5. *Suppose that T is not a subgroup of G. Let A be a subgroup of G maximal in T. Then there exists a coset decomposition*

$$G = A \cup Af \cup \cdots \cup Af^{p-1} \cup Ag_1 \cup \cdots \cup Ag_n$$

such that

(i) $Af^j \cap T = \phi$, $j = 1, 2, \ldots, p-1$, *and*
(ii) $|Ag_i \cap T| = |C_A(g_i)| = |A|/p$, $i = 1, 2, \ldots, n$.

PROOF. (i) is a consequence of (0).

(ii) Clearly, exactly $1/p$ of the elements of $A \cup Af \cup \cdots \cup Af^{p-1}$ belong to T. For $t \in T \backslash A$ we have $At \cap T = C_A(t)t$ by Lemma 5.4. Since A is abelian and maximal in T, $C_A(At) = C_A(t)$ is a proper subgroup of A. Consequently $|Ag \cap T| \leq |A|/p$ for all $g \in G \backslash A$. It follows that every coset Ag_i must have exactly $1/p$ of its elements in T, otherwise the condition $p|T| = |G|$ is violated. Hence $|Ag_i \cap T| = |A|/p$ for $i = 1, 2, \ldots, n$.

We now proceed to prove the following result, which, together with the corollary below and Theorem 4.1 establishes the characterisation theorem stated at the outset.

THEOREM 5.6. *If $G \in \mathcal{G}_p$ $(p > 2)$ is non-abelian and has an automorphism α such that $F_\alpha \neq 1$ and $p|T| = |G|$, then T is a subgroup of G.*

PROOF. We proceed by induction on $|G|$. Assume first that $Z^* = Z(G) \cap T \neq 1$. It is clear that Z^* is an α-invariant normal subgroup of G. If $G' \subset Z^*$, then for all $a, b \in T$ by "bilinearity"

$$[a,b]^3 = [a,b]\alpha = [a\alpha, b\alpha] = [a^3, b^3] = [a,b]^9.$$

This implies that $[a,b] = 1$ as $|G|$ is odd and T has no element of order 3. We may infer that T is a subgroup of G.

If $G/Z^* = (FZ^*/Z^*)(T/Z^*)$ is non-abelian, it satisfies all hypotheses of the theorem, in view of the statement (iii) in the introduction and Lemma 3.5. Thus by induction T/Z^* and hence T are groups. We may therefore assume that $Z^* = 1$.

We claim that there is a $g \in G$ such that $|g^G \cap T| = p$ and $|g^G| < p^2$. Assume the contrary. If $|x^G \cap T| \neq p$ for some $1 \neq x \in G$, then either $x^G \cap T = \varnothing$ or $|x^G \cap T| = 1$ and $|x^G| = |G : C_G(x)| \geq p$, by Lemma 5.3. We know that $Z^* = 1$ and $G \in \mathcal{G}_p$, so from $|G| = p|T|$ (and our assumption) we may conclude that the union of all conjugacy classes of G intersecting T trivially contains at most $p - 1$ elements. Combining Lemmas 5.2 and 3.5 we obtain that $F = Z(G)$ is this union with 1 added.

Since α induces on G/F a 3-automorphism by (0), we get $G' \subseteq F$. Now for all $a, b \in T$, $[a,b] = [a,b]\alpha = [a^3, b^3] = [a,b]^9$, implying that $[a,b] = 1$. It follows that G is abelian, a contradiction.

Hence there is a $g \in G$ such that $|g^G \cap T| = p$ and $|g^G| < p^2$. By Lemma 5.3, $A = C_G(g)$ does not contain F, whence $A \cap F = 1$. In view of Lemma 3.2, A is α-invariant. For any $a \in A$ there exist j such that $af^j \in T$ by (0), so $(af^j)^3 = (af^j)\alpha = a^\alpha f^j$ implies $(f^j a)^2 = a^{-1}a\alpha \in A$. It follows that $f^j a \in A$ and $f^j \in A \cap F = 1$, whence $j = 0$ and $a \in T$. Thus $A \subset T$, so A is abelian. We claim that $A = T$.

Assuming the contrary we have $p < |G : A| < p^2$. Since $G \in \mathcal{G}_p$, $|G : A| = |g^G|$ must be a prime q, say. In particular, A is a maximal subgroup of G. There exists $t \in T \backslash A$. By Lemma 5.5, $|C_A(t)| = |A|/p$. On the other hand, $C_G(C_A(t)) \supseteq \langle A, t \rangle = G$. Since $Z^* = 1$, we obtain $C_A(t) = 1$, $|A| = p$ and $|G| = pq$. But now A and F are conjugate in G (Sylow), contradicting Lemma 5.2. The proof is complete.

From the proof of Theorem 5.6 we have

COROLLARY 5.7. *A non-abelian group $G \in \mathcal{G}_p$ $(p > 2)$ has an automorphism α such that $F \neq 1$ and T is a subgroup of index p in G if and only if G has* *an abelian subgroup A of index p with $(|A|, 3) = 1$ and an element $f \in G \backslash A$ of order p.*

Acknowledgement

We wish to thank Professor T. J. Laffey for his valuable help in the construction of this paper. Thanks are due also to the referee, whose useful remarks led to a shortened version of the proof of Theorem 5.6.

References

[1] D. Gorenstein, *Finite groups* (Harper and Row, New York, 1968).
[2] H. Liebeck and D. MacHale, 'Groups with automorphisms inverting most elements', *Math. Z.* **124** (1972), 51–63.
[3] H. Liebeck and D. MacHale, 'Groups of odd order with automorphisms inverting many elements', *J. London Math. Soc.* **6** (1973), 215–225.
[4] H. Liebeck, 'Groups with an automorphism squaring many elements', *J. Austral. Math. Soc.* **16** (1973), 33–42.
[5] D. MacHale, 'Universal power automorphisms in finite groups', *J. London Math. Soc.* **2** (1975), 366–368.
[6] D. MacHale 'Groups with an automorphism cubing many elements', *J. Austral. Math. Soc.* **2** (1975), 253–256.
[7] W. A. Manning, 'Groups in which a large number of operators may correspond to their inverses', *Trans. Amer. Math. Soc.* **7** (1906), 233–240.
[8] G. A. Miller, 'Possible α-automorphisms of non-Abelian groups', *Proc. Nat. Acad. Sci. U.S.A.* **15** (1929), 89–91.

Department of Mathematics
University of Timisoara
1900–Timisoara
Romania

Department of Mathematics
University College
Cork
Ireland

https://doi.org/10.1017/S1446788700030743 Published online by Cambridge University Press