FINITE 3-GROUPS OF CLASS 3 WHOSE ELEMENTS COMMUTE WITH THEIR AUTOMORPHIC IMAGES

A. ABDOLLAHI, A. FAGHIHI, S.A. LINTON, AND E.A. O'BRIEN

Abstract. A group G is an A-group if $x^\alpha x = xx^\alpha$ for all $x \in G$ and all automorphisms α of G. Such groups have nilpotency class at most 3; we construct the first example having class precisely 3.

1. Introduction

A group G is an E-group (respectively A-group) if $x^\phi x = xx^\phi$ for all $x \in G$ and all endomorphisms (respectively automorphisms) ϕ of G. Clearly every E-group is an A-group.

Taking ϕ to be the inner automorphism induced by an arbitrary $g \in G$ shows that $[x^g, x] = 1$ or equivalently $[g, x, x] = 1$ for all $x \in G$. Hence every A-group is a 2-Engel group and so is nilpotent of class at most 3 [15, Theorem 12.3.6]. The first non-abelian E-groups were constructed by Faudree [7]. All known E- and A-groups (see for example [2] and [14]) have class at most 2.

A p-group which is an E-group (A-group) is a pE-group (pA-group). Since 2-Engel groups with no elements of order 3 are nilpotent of class at most 2, a finite pA-group of class 3 must be a 3-group. Caranti [10, Problem 11.46] asked if there exists a finite pE- or pA-group having class 3.

A necessary condition for a finite p-group to be an E-group was given by Malone [11, Theorem 1] in 1969.

Theorem 1.1. *Let P be a finite pE-group. If its derived quotient P/P' has exponent p^r, then all elements of P having order dividing p^r are central.*

Motivated by this property, a class of finite p-groups was introduced in [2]: P is a $p\mathcal{E}$-group if P is a 2-Engel group and there exists a positive integer r such that $\Omega_r(P) \le Z(P)$ and $\exp(P/P') = p^r$. A finite pE-group is a $p\mathcal{E}$-group, but the converse is false in general [2, Remark 2.2]. If $d \le 3$, then every d-generator $p\mathcal{E}$-group has class at most 2.

2000 *Mathematics Subject Classification.* 20D45; 20E36.

Key words and phrases. Automorphisms of groups; endomorphisms of groups; A-groups; E-groups; 2-Engel groups; 3-groups.

We thank Max Neunhöffer for helpful discussions. The work of Abdollahi was partially supported by the Center of Excellence for Mathematics, University of Isfahan. The work of O'Brien was partially supported by the Marsden Fund of New Zealand via grant UOA721.

In [1, Remark 2.1] a finite $3\mathcal{E}$-group of class 3 is constructed as follows. Consider the largest 2-Engel group P of exponent 27 with defining generators $x_1, \dots, x_9$ satisfying the following relations:

$$x_1^3 = [x_2, x_3][x_4, x_5][x_6, x_7][x_8, x_9], \;\; x_2^3 = [x_1, x_3][x_4, x_6][x_5, x_8][x_7, x_9],$$
$$x_3^3 = [x_1, x_2][x_4, x_7][x_5, x_9][x_6, x_8], \;\; x_4^3 = [x_1, x_5][x_2, x_6][x_3, x_9][x_7, x_8],$$
$$x_5^3 = [x_1, x_4][x_2, x_8][x_3, x_7][x_6, x_9], \;\; x_6^3 = [x_1, x_7][x_2, x_9][x_3, x_5][x_4, x_8],$$
$$x_7^3 = [x_1, x_8][x_4, x_9][x_3, x_6][x_2, x_5], \;\; x_8^3 = [x_1, x_9][x_3, x_4][x_2, x_7][x_5, x_6],$$
$$x_9^3 = [x_1, x_6][x_3, x_8][x_2, x_4][x_5, x_7].$$

We used the ANU Nilpotent Quotient package of Nickel [13], available in GAP [8] or Magma [3], to construct a power-conjugate presentation (see §2.1) for P.

From this presentation, we learn that $|P| = 3^{84}$ and compute readily that $|P'| = 3^{75}$, $|Z(P)| = 3^{39}$, $\exp(P/P') = 3$, $P' = Z_2(P) \cong C_9^{36} \times C_3^3$ and $\Omega_1(P') = \gamma_3(P) = Z(P) \cong C_3^{39}$. Since every commutator $[x_i, x_j]$ appears only once in the defining relations, it follows that

$$\langle x_1^3, \dots, x_9^3 \rangle = \langle x_1^3 \rangle \times \dots \times \langle x_9^3 \rangle.$$

Therefore $|P^3| = |\langle x_1^3, x_2^3, \dots, x_9^3 \rangle (P')^3| = 3^{45}$, so by regularity $|\Omega_1(P)| = |P : P^3| = 3^{39}$. Hence $\Omega_1(P) = \gamma_3(P) = Z(P)$ and P is a $3\mathcal{E}$-group of class 3.

Let $\mathrm{Aut}_c(G)$ denote the group of central automorphisms of a group G: namely those automorphisms of G which multiply each element of G by an element of its centre. Our principal result, answering one of Caranti's questions, is the following.

Theorem 1.2. $\mathrm{Aut}(P) = \mathrm{Aut}_c(P)\mathrm{Inn}(P)$. *In particular, P is an A-group.*

Motivated in part by a search for such groups, Traustason [16] developed a general theory of symplectic alternating algebras, and constructed a related family of finite 2-Engel 3-groups of class 3.

In Section 3 we establish this theorem by constructing the automorphism group of P. We do this using a refinement of the algorithm of Eick, Leedham-Green and O'Brien [6] which we now review. Implementations are available in both GAP and Magma and these play an important role in our proof, as do computations in both systems.

2. An automorphism group algorithm

The algorithm of [6] proceeds by induction down the lower exponent-p central series of a finite p-group P; namely, it successively computes $\mathrm{Aut}(P_i)$ for the quotients $P_i = P/\mathcal{P}_i(P)$, where $(\mathcal{P}_i(P))$ is the descending sequence of subgroups defined recursively by $\mathcal{P}_0(P) = P$ and $\mathcal{P}_i(P) = [\mathcal{P}_{i-1}(P), P]\mathcal{P}_{i-1}(P)^p$ for $i \geq 1$.

2.1. **Power-commutator presentations.** Let G be a soluble group with composition series $G = C_1 \rhd C_2 \rhd \cdots \rhd C_n \rhd C_{n+1} = 1$. Each factor C_i/C_{i+1} is cyclic of prime order p_i. If we choose $g_i \in C_i \setminus C_{i+1}$, then we obtain a *polycyclic generating sequence* $(g_1, \ldots, g_n)$ of G. Each $g \in G$ can be written uniquely as $g_1^{\epsilon_1} \ldots g_n^{\epsilon_n}$ for $0 \leq \epsilon_i < p_i$. Such descriptions underpin most efficient algorithms for soluble groups; see [9, Chapter 8] for more details. A polycyclic generating sequence for a p-group G determines a *consistent power-commutator presentation* for G whose defining relations are of the form $g_i^p = g_{i+1}^{\beta(i,i,i+1)} \cdots g_n^{\beta(i,i,n)}$ and $[g_j, g_i] = g_{j+1}^{\beta(i,j,j+1)} \cdots g_n^{\beta(i,j,n)}$ for $1 \leq i < j \leq n$ where $\beta(i,j,k) \in \{0, \ldots, p-1\}$.

2.2. **The p-covering group of a p-group.** The *p-covering group* P^* of a p-group P is the largest elementary abelian, central Frattini extension of P. Thus, if $\psi : P^* \to P$ is the natural homomorphism of the extension and $M = \ker(\psi)$, then M is an elementary abelian p-group which is central in P^* and $M \leq \Phi(P^*)$. The kernel M is the *p-multiplicator* of P. If P is described by a consistent power-commutator presentation, then we use the algorithm of [12] to compute efficiently a power-commutator presentation for P^* and an explicit homomorphism $\psi : P^* \to P$.

Theorem 2.1. *Let P be a p-group, let $P_i = P/\mathcal{P}_i(P)$ have minimal generating set $g_1, \ldots, g_d$, and let P_i^* be the p-covering group of P_i. Consider the natural epimorphisms $\psi : P_i^* \to P_i$ and $\gamma : P_{i+1} \to P_i$. Let g_j^* and $\overline{g_j}$ be arbitrary preimages of g_j under ψ and γ, respectively. Then $\epsilon : P_i^* \to P_{i+1} : g_j^* \mapsto \overline{g_j}$ defines an epimorphism.*

Since $M \leq \Phi(P_i^*)$ it follows that $P_i^* = \langle g_1^*, \ldots, g_d^* \rangle$. If we have polycyclic generating sequences for P_i^* and P_{i+1}, we can readily determine $U := \ker(\epsilon)$. By construction $U \leq M$.

2.3. **The basic algorithm.** Recall that the algorithm proceeds by induction down the lower exponent-p central series of P. Since $P_1 = P/\mathcal{P}_1(P)$ is elementary abelian, $\mathrm{Aut}(P_1) \cong \mathrm{GL}(d,p)$. Now we assume by induction that we know $\mathrm{Aut}(P_i)$ for some $i \geq 1$ and we seek a generating set of $\mathrm{Aut}(P_{i+1})$. Let P_i^* be the p-covering group of P_i and M the corresponding p-multiplicator.

Theorem 2.2. *Each automorphism α of P_i extends to an automorphism α^* of P_i^* via the natural homomorphism $P_i^* \to P_i$. Moreover, α^* leaves M invariant and α induces an automorphism α_M of M, which depends only on α.*

We describe the explicit construction for the action on M. Let $m \in M$. Since $M \leq \Phi(P_i^*)$, we can write $m = w(g_1^*, \ldots, g_d^*)$ for some word w in the generating set $g_1^*, \ldots, g_d^*$ of P_i^*. Let $h_i = (g_i^*)^{\psi\alpha} \in P_i$ and choose a preimage h_i^* in P_i^* under the natural epimorphism $\psi : P_i^* \longmapsto P_i$. We define $m^{\alpha_M} = w(h_1^*, \ldots, h_d^*)$.

Theorem 2.1 provides an epimorphism $\epsilon : P_i^* \to P_{i+1}$ with kernel $U \leq M$. Using the action of $\mathrm{Aut}(P_i)$ on M, we define the stabiliser $S := \mathrm{Stab}_{\mathrm{Aut}(P_i)}(U)$. The extensions of the inner automorphisms of P_i act trivially on the p-multiplicator of P_i and so stabilise U.

Let T be the group of automorphisms of P_{i+1} which centralise $P_{i+1}/\mathcal{P}_i(P_{i+1})$.

Theorem 2.3. *Let $\nu : \mathrm{Aut}(P_{i+1}) \to \mathrm{Aut}(P_i)$ be the natural homomorphism where $T = \ker(\nu)$ and $S = \mathrm{im}(\nu)$. Then $\mathrm{Aut}(P_{i+1}) = TR$, where R is an arbitrary preimage of S under ν.*

It is straight-forward to construct M, U, and the action of $\mathrm{Aut}(P_i)$ on M. To determine $\mathrm{Aut}(P_{i+1})$, we must determine each of S and T. A generating set for T is readily constructed using the following lemma.

Lemma 2.4. *Let P be a p-group with $\mathcal{P}_{c+1}(P) = 1$ and $c \geq 2$. Let $g_1, \dots, g_d$ and $x_1, \dots, x_l$ be minimal generating sets for P and $\mathcal{P}_c(P)$, respectively. Define*

$$\beta_{i,j} : P \to P : \begin{cases} g_i \mapsto g_i x_j \\ g_k \mapsto g_k \text{ for } k \neq i. \end{cases}$$

Then $\{\beta_{i,j} \mid 1 \leq i \leq d \text{ and } 1 \leq j \leq l\}$ is a polycyclic generating sequence for the elementary abelian p-group of automorphisms of P centralising $P/\mathcal{P}_c(P)$.

The major task is to construct a generating set for S. The standard technique to construct the stabiliser S of a subspace U is to list the orbit of U and, concurrently with its construction, calculate Schreier generators for S; see for example [9, Chapter 4]. If the orbit is small, this approach is very efficient. In [6] various refinements were introduced to break up a difficult stabiliser computation into smaller pieces; these extend significantly the range of application of the automorphism group algorithm. We identify those key refinements needed to establish Theorem 1.2.

(1) Exploit the internal structure of the p-multiplicator M of P_i. Since M is elementary abelian, it is an $\mathrm{Aut}(P_i)$-module. Use its submodule structure to minimise the lengths of the orbits constructed.
(2) Observe, from Lemma 2.4, that the acting group $A := \mathrm{Aut}(P_i)$ has a normal p-subgroup N, namely the centraliser in A of $V \cong P/\mathcal{P}_1(P)$, and A/N is a subgroup of $\mathrm{GL}(V)$. In particular, the action of N on M is as a *unipotent* subgroup of $\mathrm{GL}(M)$. Costi [5] (see also [6, §5.2]) describes an algorithm UnipotentStabiliser to construct a canonical representative $\overline{U}$ of the N-orbit of a subspace U of M. Simultaneously, it constructs a generating set for the stabiliser in N of $\overline{U}$ and $t \in N$ such that $U^t = \overline{U}$. Use this algorithm to construct the stabiliser of U in N *without* explicitly constructing its orbit.
(3) If possible, replace the acting group A by a proper subgroup which contains the stabiliser of U.
(4) If the acting group A is soluble then ascend a composition series for A, determining orbits under successive terms of the series. At each step, use the property that an orbit under a normal subgroup is a block of a permutation action.

3. The automorphism group of P

Recall that P has order 3^{84} and class 3. Its lower exponent-p central series and lower central series coincide; hence $P_1 := P/\mathcal{P}_1(P)$ has order 3^9, and $P_2 := P/\mathcal{P}_2(P)$ has order 3^{45} and a centre of order 3^{36}. In Table 1, we record $\log_3(|P_i|)$, the rank of the p-multiplicator M of P_i and the rank of the kernel U of the homomorphism from P_i^* to P_{i+1}. We identify U with a subspace of the corresponding vector space.

i	P_i	M	U
1	9	45	9
2	45	204	165
3	84		

Table 1. Data for P

Lemma 3.1. $\mathrm{Aut}(P_2) = \mathrm{Aut}_c(P_2)$.

Proof. Let $A := \mathrm{Aut}(P_1)$ and observe that $A \cong \mathrm{GL}(9,3)$. The 45-dimensional A-module M has a direct sum decomposition into irreducibles submodules $M_1 \oplus M_2$, where M_1 has dimension 36 and M_2 has dimension 9. The action of A on M_1 is the alternating square representation $\Lambda^2(V)$ for $V = \mathrm{GF}(3)^9$ and its action on M_2 is as $\mathrm{GL}(V)$. The stabiliser in A of the 18-dimensional space $U + M_2$ contains the stabiliser of U, and is also the stabiliser of the 9-dimensional space $W := (U + M_2)/M_2$. We restrict the A-module action from M to the composition factor M/M_2 of dimension 36.

Thus our task is to construct the stabiliser of W under $\Lambda^2(V)$. Since the action of A on M_1 is as the alternating square representation $\Lambda^2(V)$, each of the 19682 non-zero vectors in W determines an anti-symmetric bilinear 9×9 form, where the 36 entries in the vector define the above-diagonal entries in the matrix of the form. Precisely four of these forms have rank 4, 956 have rank 6, and 18722 have rank 8. The four forms of rank 4 occur as two pairs, $\{\gamma, -\gamma\}$ and $\{\zeta, -\zeta\}$. It is easy to write down the stabiliser of γ as a subgroup of $\mathrm{GL}(V)$ since it has known shape $3^{20}.(\mathrm{GL}(5,3) \times \mathrm{Sp}(4,3))$. This we also do for ζ. The intersection C of these two groups has order $2^{11} \times 3^{23}$ and fixes both γ and ζ. Its normaliser $N := N_{\mathrm{GL}(9,3)}(C)$ has order $2^{14} \times 3^{23}$ and contains the stabiliser of U under A. Since the action of N on M is highly reducible, it is reasonably routine using the refinements of [6] to establish that the stabiliser of U in N is trivial. Theorem 2.3 now implies that $\mathrm{Aut}(P_2) = T$, the group defined in Lemma 2.4. □

We can construct C readily using either the faithful representation of $\mathrm{GL}(V)$ as permutations of the non-zero vectors in V, or the algorithm of Brooksbank & O'Brien [4].

Proof of Theorem 1.2. Lemma 3.1 shows that $A := \mathrm{Aut}(P_2)$ is a group of order 3^{224}. It acts on M, the p-multiplicator of P_2, as a unipotent subgroup of $\mathrm{GL}(204, 3)$. We use the UnipotentStabiliser algorithm to construct the stabiliser in A of the kernel U. This stabiliser is the inner automorphism group of P_2. The result now follows from Theorem 2.3. □

References

[1] A. Abdollahi, A. Faghihi and A. Mohammadi Hassanabadi, 3-generator groups whose elements commute with their endomorphic images are abelian, Comm. Algebra **36**, (2008) 3783-3791.

[2] A. Abdollahi, A. Faghihi and A. Mohammadi Hassanabadi, Minimal number of generators and minimum order of a non-abelian group whose elements commute with their endomorphic images, Comm. Algebra **36**, (2008) 1976–1987.

[3] Wieb Bosma, John Cannon and Catherine Playoust, The Magma algebra system I: The user language. J. Symbolic Comput. **24**, (1997) 235–265.

[4] Peter A. Brooksbank and E.A. O'Brien, Constructing the group preserving a system of forms, *Internat. J. Algebra and Comput.* **18**, 227–241, 2008.

[5] Elliot Costi, Constructive membership testing in classical groups, PhD thesis, Queen Mary, University of London, 2009.

[6] Bettina Eick, C.R. Leedham-Green and E.A. O'Brien, Constructing the automorphism group of a p-group, *Comm. Algebra* **30**, (2002) 2271-2295.

[7] R. Faudree, Groups in which each element commutes with its endomorphic images, Proc. Amer. Math. Soc. **27**, (1971) 236-240.

[8] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12; 2008. `www.gap-system.org`.

[9] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien, *Handbook of computational group theory*, Chapman and Hall/CRC, London, 2005.

[10] The Kourovka Notebook, Unsolved problems in group theory, 16th edition, Novosibirsk, 2006.

[11] J.J. Malone, More on groups in which each element commutes with its endomorphic images, Proc. Amer. Math. Soc. **65**, (1977) 209-214.

[12] M.F. Newman and E.A. O'Brien, Application of computers to questions like those of Burnside, II. Internat. J. Algebra Comput. **6**, (1996) 593–605.

[13] Werner Nickel, Computation of nilpotent Engel groups. J. Austral. Math. Soc. Ser. A **67**, (1999) 214–222.

[14] Martin R. Pettet, On automorphisms of A-groups, Arch. Math. (Basel) **91**, (2008) 289-299.

[15] Derek J.S. Robinson, A course in the theory of groups, Second Edition, Springer, New York, 1995.

[16] Gunnar Traustason, Symplectic alternating algebras, Internat. J. Algebra Comput. **18**, (2008) 719–757.

Department of Mathematics, University of Isfahan, Isfahan 81746-73441, Iran
E-mail address: `a.abdollahi@math.ui.ac.ir`

Department of Mathematics, Qom University, Qom, Iran
E-mail address: `saf@sci.ui.ac.ir`

School of Computer Science, University of St. Andrews, North Haugh, St. Andrews, Fife, KY16 9SX, Scotland
E-mail address: `sal@cs.st-andrews.ac.uk`

Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand
E-mail address: `obrien@math.auckland.ac.nz`