

MSC: 05B25 20F16

On the base size of a finite group in its action on the lattice of subgroups

Jia-Li Du^{a,b,1}, Joy Morris^{c,*,2} and Pablo Spiga^d

^a*School of Mathematical Sciences, Nanjing Normal University, Nanjing, 210023, P.R. China*

^b*Ministry of Education Key Laboratory of NSLSCS, Nanjing, 210023, P.R. China*

^c*Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB, T1K 3M4, Canada*

^d*Dipartimento di Matematica e Applicazioni, University of Milano-Bicocca, Via Cozzi 55, 20125, Milano, Italy*

ARTICLE INFO

Keywords:

automorphism group

base size

Baer norm

power automorphism

subgroup lattice

ABSTRACT

Given a finite group R , we investigate the base size of the action of the automorphism group of R on the lattice of subgroups of R . Our main result shows that this base size is at most 1 if and only if R is cyclic. Our motivation arises from a conjecture of Babai on the problem of representing groups as automorphism groups of lattices with a bounded number of orbits.

1. Introduction

Let R be a finite group, let $\text{Aut}(R)$ denote the automorphism group of R and let $\text{Sub}(R)$ be the collection of all subgroups of R . The group $\text{Aut}(R)$ has a natural action on $\text{Sub}(R)$, where given $H \in \text{Sub}(R)$ and $\alpha \in \text{Aut}(R)$, H^α is the image of H under α . In this paper, we are interested in the permutation group induced by the action of $\text{Aut}(R)$ on $\text{Sub}(R)$, which, for lack of a better name, we denote by $A(R)$.

We recall that $\alpha \in \text{Aut}(R)$ is said to be a **power automorphism** if, for every $x \in R$, there exists $n_x \in \mathbb{Z}$ such that $x^\alpha = x^{n_x}$. The set of power automorphisms of R forms a subgroup $\text{PAut}(R)$ of $\text{Aut}(R)$.

In general, the action of $\text{Aut}(R)$ on $\text{Sub}(R)$ is not faithful. Clearly, every power automorphism fixes setwise every subgroup of R , and hence $\text{PAut}(R)$ is contained in the kernel of the action of $\text{Aut}(R)$ on $\text{Sub}(R)$. Conversely, if $\alpha \in \text{Aut}(R)$ acts trivially on the set $\text{Sub}(R)$, then α fixes setwise each cyclic subgroup $\langle x \rangle$ of R , and hence $x^\alpha \in \langle x \rangle$ for every $x \in R$, that is, α is a power automorphism. Summing up, $\text{PAut}(R)$ is the kernel of the action of $\text{Aut}(R)$ on $\text{Sub}(R)$ and hence

$$A(R) \cong \frac{\text{Aut}(R)}{\text{PAut}(R)}.$$

We recall that a **base** for a permutation group G is a sequence $\omega_1, \dots, \omega_\ell$ of elements in the domain of G , where ℓ is a nonnegative integer, whose pointwise stabilizer in G is the identity. When $\ell = 0$, this is the empty sequence. The minimal cardinality of a base is called the **base size**. In particular, a permutation group has base size 0 if and only if it is the identity group.

We are interested in the base size of the action of $\text{Aut}(R)$ on $\text{Sub}(R)$; that is, in the base size of $A(R)$. We determine the finite groups R such that this base size is at most 1. When R is cyclic, every automorphism of R is a power automorphism, and hence $A(R) = 1$. Therefore, $A(R)$ has base size 0, with the empty sequence as a base. Our main result shows the converse.

Theorem 1.1. *Let R be a finite group. The base size of $A(R)$ is at most 1 if and only if R is cyclic.*

*Corresponding author

 <https://orcid.org/0000-0001-5000-1000> (J. Du); joy.morris@uleth.ca (J. Morris); pablo.spiga@unimib.it (P. Spiga)

ORCID(s):

¹This author was supported by the National Natural Science Foundation of China (12571370, 12371025) and National Key R&D Program of China (211070B62501).

²This author was supported by the Natural Science and Engineering Research Council of Canada (grant RGPIN-2024-04013).

We find this result quite unexpected, because it shows that the base size of $A(R)$ is never 1: it is 0 when R is cyclic and at least 2 otherwise. Therefore we have the following corollary.

Corollary 1.2. *Let R be a finite group. In the action of $A(R)$ on $\text{Sub}(R)$ there exists a regular orbit (that is, an orbit on which the permutation group $A(R)$ acts regularly) if and only if R is cyclic.*

2. Our motivation

Our motivation for this investigation arises from an apparently different question. Since the early 1900s, there has been considerable interest in determining, for a given class of combinatorial objects, whether every finite group R can be realized as the automorphism group of some object in that class. Perhaps the most famous example is the theorem of Frucht [10], which shows that, for every finite group R , there exists a graph Γ such that $R \cong \text{Aut}(\Gamma)$. The analogous result for lattices is essentially due to Birkhoff [6]: for every finite group R , there exists a lattice L such that $R \cong \text{Aut}(L)$. Similar results hold for other classes of combinatorial objects.

Once such representation results are established, it is natural to refine the constructions in order to control additional combinatorial properties of the objects involved. The aim is not only to realize a given abstract group as an automorphism group, but also to ensure that the object has a “small” or simple structure, so that the group reflects more closely the combinatorial nature of the object.

We illustrate this with two classical examples. In the case of graphs, one may ask, given a finite group R , to find a graph Γ such that $R \cong \text{Aut}(\Gamma)$ and such that the number of vertex-orbits of $\text{Aut}(\Gamma)$ is as small as possible. (The construction of Frucht depends on the number of generators of R .) In this context, the notion of a **graphical regular representation** arises: this is a graph Γ such that $R \cong \text{Aut}(\Gamma)$ and $\text{Aut}(\Gamma)$ acts regularly on the vertex set.

A related line of investigation considers representations of finite groups via automorphism groups of graphs Γ such that $\text{Aut}(\Gamma)$ has a bounded number of edge-orbits. This problem was motivated by a conjecture of Babai. (Again, Frucht’s construction, via suitable modifications of Cayley graphs, produces graphs whose automorphism groups have a number of edge-orbits bounded above by the number of generators of the group.) Somewhat surprisingly, the answer to this question is negative, as shown by Goodman [11]: for every positive integer ℓ , there exists a finite group R_ℓ such that, if $R_\ell \cong \text{Aut}(\Gamma)$ for some finite graph Γ , then $\text{Aut}(\Gamma)$ has at least ℓ edge-orbits. The methods developed in obtaining this result (see, for instance, [4]) are of independent interest.

In this line of research, a major open problem concerns the analogous question for lattices. This problem was posed by Babai in several places; see, for example, [1, see abstract], [2, Problem 5.27], [3, Conjecture 4.13] and [4, see page 8]. The question is the following:

Is there an absolute constant c such that, for every finite group R , there exists a lattice L with $R \cong \text{Aut}(L)$ and such that $\text{Aut}(L)$ has at most c orbits?

Babai conjectured that the answer is affirmative. To date, there has been almost no progress on this conjecture, and there are good reasons for this. Indeed, given a finite group R , Birkhoff’s construction of a lattice L proceeds via a graph, that is, the lattice L is built from a graph. Through this standard construction, finite groups that can be realized as automorphism groups of graphs with a bounded number of edge-orbits yield lattices whose automorphism groups have a bounded number of orbits. However, as noted above, there exist groups that require arbitrarily many edge-orbits in any such graph representation. Therefore, this natural strategy for approaching Babai’s conjecture appears to lead to a dead end.

The work presented in this paper is inspired by the comments and questions in [4, Section 8]. These problems are twofold in nature. On the one hand, they ask for the minimal number of subgroups required so that the identity is the only automorphism fixing these subgroups setwise. On the other hand, they consider the analogous question when one is allowed to choose a bounded number of subgroups together with a bounded number of group elements, and again ask whether the identity is the only automorphism fixing them.

The scope of these questions is at least threefold: first, to improve the results obtained in [4]; second, to characterize, in purely algebraic terms, the groups admitting a graphical representation with a bounded

number of edge-orbits; and third, to develop ideas that may have further applications, particularly in the context of lattices.

Roughly speaking, some of the questions in [4, Section 8] can be interpreted in terms of the base size of $\text{Aut}(R)$ in its natural action on $\text{Sub}(R)$, that is, the base size of $A(R)$. It is through the study of [4], and in connection with attempts to approach Babai's conjecture on lattices, that we arrived at the result stated in Theorem 1.1.

Although Theorem 1.1 does not appear to have direct applications to Babai's conjecture on lattices, in the course of our exploration of this problem we have also developed methods (not included in this paper) that allow us to extend some of the results in [4], especially in the case of groups of odd order.

3. Preliminaries

The power automorphisms and their collection $\text{PAut}(R)$ are related to the concept of the **Baer norm**. We refer to [5] for the basic properties of the Baer norm. The Baer norm of R is the subgroup

$$N(R) = \bigcap_{H \leq R} \mathbf{N}_R(H);$$

thus, $N(R)$ is the set of elements of R that normalize every subgroup of R .

For $x \in R$, let $\text{Inn}(x)$ be the automorphism of R given by conjugation by x , and, for $X \leq R$, let

$$\text{Inn}(X) = \{\text{Inn}(x) \mid x \in X\}.$$

An inner automorphism $\text{Inn}(x)$ is a power automorphism if and only if it fixes setwise every subgroup of R . This occurs if and only if x normalizes every subgroup of R , that is, if and only if $x \in N(R)$. Therefore,

$$\text{Inn}(R) \cap \text{PAut}(R) = \text{Inn}(N(R)). \quad (1)$$

The structure of the Baer norm $N(R)$ of R is rather restricted. Recall that a group is said to be a **Dedekind group** if all of its subgroups are normal. Since the elements of $N(R)$ normalize each subgroup of R , every subgroup of $N(R)$ is normal in $N(R)$, and hence $N(R)$ is a Dedekind group. Dedekind [9] has shown that a Dedekind group is either abelian, or of the form $Q_8 \times E \times O$, where Q_8 is the quaternion group of order 8, E is an elementary abelian 2-group, and O is an abelian group of odd order.

One of the main results concerning the Baer norm is a result of Schenkman [13]. To state this result we need some basic definitions. We let $\mathbf{Z}(R)$ denote the **center** of R . This definition allows us to define an ascending series of subgroups of R , namely, given $n \in \mathbb{N}$, let $\mathbf{Z}_0(R) = 1$, $\mathbf{Z}_1(R) = \mathbf{Z}(R)$ and, for $n \geq 2$, let $\mathbf{Z}_n(R)$ be the subgroup of R such that $\mathbf{Z}(R/\mathbf{Z}_{n-1}(R)) = \mathbf{Z}_n(R)/\mathbf{Z}_{n-1}(R)$. Moreover, the **derived subgroup** R' of R is the subgroup of R generated by the **commutators** of R , that is, by the expressions $[x, y] = x^{-1}y^{-1}xy$, for $x, y \in R$. Finally, for a subgroup H of R , $\mathbf{C}_R(H)$ is the centralizer of H in R .

Theorem 3.1 (Schenkman [13, Theorem]). *We have $R' \leq \mathbf{C}_R(N(R))$ and $N(R) \leq \mathbf{Z}_2(R)$.*

When $\text{Aut}(R) = \text{PAut}(R)$ then $A(R) = 1$, so clearly the base size of $A(R)$ is 0. Therefore it is relevant to observe the following.

Lemma 3.2. *We have $\text{Aut}(R) = \text{PAut}(R)$ if and only if R is cyclic.*

We postpone the proof of Lemma 3.2 because we first prove an auxiliary result (needed in the proof of Lemma 3.2) that will be useful also later.

Lemma 3.3. *Let R be a Dedekind group. If R is not cyclic, then for every subgroup H of R there exists a non-power automorphism of R fixing H setwise.*

Proof. We use the classification of Dedekind [9] for Dedekind groups. Suppose first that $R = Q_8 \times E \times O$, where Q_8 is the quaternion group of order 8, E is an elementary abelian 2-group and O is an abelian group of odd order. Let H be a subgroup of R . Then, replacing H by a suitable $\text{Aut}(R)$ -conjugate, we have $H = H_1 \times H_2 \times H_3$, where $H_1 \leq Q_8$, $H_2 \leq E$ and $H_3 \leq O$. We let $i, j, k, -i, -j, -k, -1, 1$ denote

the elements of Q_8 . Representatives for the $\text{Aut}(Q_8)$ -classes of subgroups of Q_8 are $1, \langle -1 \rangle, \langle i \rangle$ and Q_8 . Therefore, replacing H_1 by a suitable $\text{Aut}(Q_8)$ -conjugate, we may suppose that H_1 is one of these four subgroups. Now, Q_8 admits an automorphism φ with $i^\varphi = i, j^\varphi = k$ and $k^\varphi = -j$. Clearly, φ is not a power automorphism (because $k = j^\varphi \notin \langle j \rangle$) and it fixes setwise $1, \langle -1 \rangle, \langle i \rangle$ and Q_8 . This automorphism φ extends to an automorphism of $R = Q_8 \times E \times O$ fixing H setwise.

Assume then that R is abelian and non-cyclic. Let H be a subgroup of R . For each prime p , let R_p be the Sylow p -subgroup of R . Thus $R = \prod_p R_p$ and $H = \prod_p (H \cap R_p)$. In particular, there exists a prime p such that R_p is not cyclic. Using the structure theorem of finitely generated abelian groups, we may write

$$R_p = \langle a_1 \rangle \times \cdots \times \langle a_\ell \rangle, \\ H \cap R_p = \langle a_1^{p^{f_1}} \rangle \times \cdots \times \langle a_\ell^{p^{f_\ell}} \rangle,$$

where $\ell \geq 2$, and taking e_i to be the nonnegative integer such that $\mathbf{o}(a_i) = p^{e_i}$, we have $e_i \geq f_i \geq 0$ and $e_i \geq 1$ for every $i \in \{1, \dots, \ell\}$.

If $H \cap R_p \neq R_p$ then there is some i such that $f_i > 0$ and some $1 \leq j \leq \ell$ with $j \neq i$; fix such an i and j . Otherwise, take $i = 1$ and $j = 2$. Let φ be the homomorphism of R_p into itself mapping a_k to a_k when $k \neq i$ and mapping a_i to $a_i a_j^{p^{e_j-1}}$. Clearly, φ is an automorphism of R_p because it is a surjective homomorphism. Moreover, φ fixes $H \cap R_p$ setwise: if $H \cap R_p = R_p$ then this is obvious; otherwise since $f_i \geq 1$,

$$(a_i^\varphi)^{p^{f_i}} = a_i^{p^{f_i}} a_j^{p^{e_j-1+f_i}} = a_i^{p^{f_i}} \in H \cap R_p.$$

Furthermore, φ is a non-power automorphism of R_p because $a_i^{-1} a_i^\varphi = a_j^{p^{e_j-1}} \notin \langle a_i \rangle$.

Now, φ extends to a group automorphism ϕ of R by fixing R_q element-wise, for every $q \neq p$. Hence, ϕ is a non-power automorphism fixing H setwise. $\square$

Proof of Lemma 3.2. Clearly, if R is cyclic, then $\text{Aut}(R) = \text{PAut}(R)$. Conversely, suppose $\text{Aut}(R) = \text{PAut}(R)$. In particular, $\text{Inn}(R) \leq \text{PAut}(R)$, so by (1), we have $\text{Inn}(N(R)) = \text{Inn}(R) \cap \text{PAut}(R) = \text{Inn}(R)$. Let $x \in R$ be arbitrary. Then this says that $\text{Inn}(x) = \text{Inn}(y)$ for some $y \in N(R)$. By definition of $N(R)$, the element y normalizes every subgroup of R . Since $\text{Inn}(x) = \text{Inn}(y)$, conjugation by x and conjugation by y coincide, and hence x also normalizes every subgroup of R . Thus $x \in N(R)$. Since x was arbitrary, we have $R = N(R)$. In particular, R is a Dedekind group. Now the proof follows from Lemma 3.3. $\square$

4. Proof of Theorem 1.1

The rest of the paper is devoted to the proof of Theorem 1.1. Since Lemma 3.2 shows one implication, we may assume that the base size of the action of $\text{Aut}(R)$ on $\text{Sub}(R)$ is 1 and we need to prove that R is cyclic. Since the base size is 1, there exists a subgroup H of R such that

$$\mathbf{N}_{\text{Aut}(R)}(H) = \text{PAut}(R). \quad (2)$$

Now, by definition of $N(R)$, $N(R) \leq \mathbf{N}_R(H)$, so (1) and (2) imply

$$N(R) = \mathbf{N}_R(H). \quad (3)$$

We single out the first step of the proof in a separate result, because we believe it is of independent interest.

Lemma 4.1. *Let R be a finite group and let H be a subgroup of R such that $N(R) = \mathbf{N}_R(H)$. Then R is nilpotent of nilpotency class at most 3.*

Proof. From Theorem 3.1, the hypothesis $N(R) = \mathbf{N}_R(H)$, and the fact that $H \leq \mathbf{N}_R(H)$, we deduce the series of inequalities

$$R' \leq \mathbf{C}_R(N(R)) = \mathbf{C}_R(\mathbf{N}_R(H)) \leq \mathbf{C}_R(H) \leq \mathbf{N}_R(H) = N(R) \leq \mathbf{Z}_2(R).$$

This shows that $[R, R, R] = [R', R] \leq [\mathbf{Z}_2(R), R] \leq \mathbf{Z}(R)$ and hence

$$[R, R, R, R] \leq [\mathbf{Z}(R), R] = 1.$$

Thus the lower central series of R terminates at its fourth term. Therefore, R is nilpotent and has nilpotency class at most 3. $\square$

We now continue with the proof of Theorem 1.1. From (3) and Lemma 4.1, we deduce that R is nilpotent of class at most 3. Therefore,

$$R = \prod_p R_p,$$

where R_p is the Sylow p -subgroup of R and R_p has nilpotency class at most 3. Since each R_p is characteristic, we have

$$\begin{aligned} \text{Aut}(R) &= \text{Aut}\left(\prod_p R_p\right) = \prod_p \text{Aut}(R_p), \\ \text{PAut}(R) &= \text{PAut}\left(\prod_p R_p\right) = \prod_p \text{PAut}(R_p). \end{aligned}$$

In particular, (1) implies $\text{PAut}(R_p) = \mathbf{N}_{\text{Aut}(R_p)}(H \cap R_p)$ for every prime p , and hence for the rest of the proof we may assume, without loss of generality, that R itself is a p -group for some prime p . Moreover, we may suppose that R has nilpotency class at most 3.

We argue now by contradiction and suppose that R is not cyclic.

We claim that

$$N(R) < R. \quad (4)$$

If $R = N(R)$, then R is a Dedekind group, and hence we obtain a contradiction from Lemma 3.3. This establishes (4).

The following two technical lemmas will be used repeatedly during the remainder of our proof.

Lemma 4.2. *Suppose $A \leq K \leq R$ and $A \leq \mathbf{Z}(R)$. Let $\chi : R \rightarrow A$ be a homomorphism with kernel K , and define $\phi_\chi : R \rightarrow R$ by $x^{\phi_\chi} = x\chi(x)$ for every $x \in R$. Then ϕ_χ is a group automorphism. Furthermore, if $H \leq K$ then ϕ_χ is a power automorphism.*

Proof. Since $\chi(x) \in A \leq \mathbf{Z}(R)$, we have

$$x^{\phi_\chi} y^{\phi_\chi} = x\chi(x)y\chi(y) = xy\chi(x)\chi(y) = xy\chi(xy) = (xy)^{\phi_\chi}$$

for every $x, y \in R$, so ϕ_χ is a homomorphism. Let $x \in \text{Ker}(\phi_\chi)$. Then $1 = x^{\phi_\chi} = x\chi(x)$ and hence $x^{-1} = \chi(x) \in A$. Since $A \leq K = \text{Ker}(\chi)$, we have $\chi(x) = 1$, forcing $x = 1$. Therefore $\text{Ker}(\phi_\chi) = 1$, so ϕ_χ is a group automorphism as claimed.

If $H \leq K$ then ϕ_χ fixes each element of H and hence fixes H setwise. By our choice of H , this means ϕ_χ is a power automorphism. $\square$

Lemma 4.3. *Suppose $y \in \mathbf{Z}_2(R) \setminus \mathbf{Z}(R)$ and $|[R, y]| = p$ is prime. If p is odd, further suppose $\mathbf{o}(y) = p$, while if $p = 2$, suppose that $y^2 = z$, where z is the nonidentity element of $[R, y]$.*

Fix $t \in R \setminus \mathbf{C}_R(y)$, and for every $c \in \mathbf{C}_R(y)$ and $x \in R$, if $x = t^i c$ with $0 \leq i \leq p-1$ then define $\phi(t^i c) = (yt)^i c$. Then ϕ is an automorphism of R .

Proof. Define $\varphi : R \rightarrow R$ by $x^\varphi = [x, y]$ for every $x \in R$, and observe that φ is a homomorphism whose image is $[R, y]$ and whose kernel is $\mathbf{C}_R(y)$. Thus $R/\mathbf{C}_R(y) \cong [R, y]$ is cyclic of order p , so every element of R can be written uniquely as $t^i c$ for some $0 \leq i \leq p-1$ and some $c \in \mathbf{C}_R(y)$.

Arguing inductively on i , using the fact that y commutes with every element of $\mathbf{C}_R(y)$ and that $c \in \mathbf{C}_R(y)$ implies $c^{t^i} \in \mathbf{C}_R(y)$ since $R/\mathbf{C}_R(y)$ is cyclic, we get

$$c^{t^i} = c^{(yt)^i}.$$

We can now show that ϕ is a homomorphism. Let $c_1, c_2 \in \mathbf{C}_R(y)$ and $0 \leq i_1, i_2 < p$ and suppose $i_1 + i_2 < p$. Then

$$\begin{aligned} (t^{i_1} c_1 \cdot t^{i_2} c_2)^\phi &= (t^{i_1+i_2} c_1^{t^{i_2}} c_2)^\phi = (yt)^{i_1+i_2} c_1^{t^{i_2}} c_2 \\ &= (yt)^{i_1+i_2} c_1^{(yt)^{i_2}} c_2 = (yt)^{i_1} c_1 (yt)^{i_2} c_2 = (t^{i_1} c_1)^\phi (t^{i_2} c_2)^\phi. \end{aligned}$$

In order to deal with the case $i_1 + i_2 \geq p$ we need an additional observation. Standard commutator computations give

$$(yt)^p = y^p t^p [t, y]^{\binom{p}{2}}.$$

If p is odd then by hypothesis $y^p = 1$; also p divides $\binom{p}{2}$ and since $[t, y] \in [R, y]$ which has order p , this is t^p . If $p = 2$ then this is $y^2 [t, y] t^p$ and by hypothesis $[t, y] = y^2 = z$ which has order 2, so again we have t^p .

Now assume $i_1 + i_2 \geq p$, say $i_1 + i_2 = p + i_3$ where $0 \leq i_3 < p$. Then using our new observation together with calculations similar to the previous case, we have

$$\begin{aligned} (t^{i_1} c_1 \cdot t^{i_2} c_2)^\phi &= (t^{i_1+i_2} c_1^{t^{i_2}} c_2)^\phi = (t^{i_3} t^p c_1^{t^{i_2}} c_2)^\phi \\ &= (yt)^{i_3} t^p c_1^{t^{i_2}} c_2 = (yt)^{i_3} (yt)^p c_1^{t^{i_2}} c_2 \\ &= (yt)^{i_1+i_2} c_1^{(yt)^{i_2}} c_2 = (yt)^{i_1} c_1 (yt)^{i_2} c_2 = (t^{i_1} c_1)^\phi (t^{i_2} c_2)^\phi. \end{aligned}$$

Since $t^i c$ and $(yt)^i c$ lie in the same coset of $\mathbf{C}_R(y)$, it is clear that the kernel of ϕ is trivial, so ϕ is an automorphism. $\square$

Let A be a subgroup of $\mathbf{Z}(R)$ and let K be a subgroup of R with $|R : K| = |A| = p$ and $AH \leq K$ (since R is not cyclic we cannot have $H = R$, so finding such a pair (A, K) is possible). Let $\chi : R \rightarrow A$ be any surjective group homomorphism with kernel K : the existence of χ is clear because $R/K \cong A$; thus we have $p - 1$ choices for an isomorphism from R/K to A , and each such isomorphism can be lifted to a homomorphism χ from R to A with kernel K . By Lemma 4.2, the map ϕ_χ defined by $x^{\phi_\chi} = x\chi(x)$ for every $x \in R$ is a power automorphism.

Assume now that $\mathbf{Z}(R)$ admits two distinct subgroups A_1, A_2 and that R admits a subgroup K with $|R : K| = |A_1| = |A_2| = p$ and $A_1 A_2 H \leq K$. By Lemma 4.2, ϕ_{χ_1} and ϕ_{χ_2} are both power automorphisms of R . Let $x \in R \setminus K$. Then $x\chi_i(x) = x^{\phi_{\chi_i}} \in \langle x \rangle$, and hence $\chi_i(x) \in \langle x \rangle$. As x is an arbitrary element outside $\text{Ker}(\chi_i)$ and $\chi_i : R \rightarrow A_i$, we deduce $A_i \leq \langle x \rangle$ and hence $A_1 A_2 \leq \langle x \rangle$, which is a contradiction because $\langle x \rangle$ is cyclic whereas $A_1 A_2$ is not. This contradiction arises from assuming the existence of A_1, A_2 and K as above. Therefore, there are two alternatives: either $\mathbf{Z}(R)$ is cyclic (which excludes the existence of two distinct subgroups of order p in $\mathbf{Z}(R)$), or $\mathbf{Z}(R)H = R$. In the latter case, $R = \mathbf{N}_R(H) = N(R)$ and we contradict (4). We have shown that

$$\mathbf{Z}(R) \text{ is cyclic.} \quad (5)$$

We claim that

$$N(R) \text{ is abelian.} \quad (6)$$

Suppose that $N(R)$ is non-abelian. Then, by the theorem of Dedekind, $N(R) = Q \times E$, where $Q \cong Q_8$ and E is an elementary abelian 2-group. Let $\langle z \rangle = \mathbf{Z}(Q)$. Since $\langle z \rangle$ is characteristic in $N(R)$ and $N(R) \triangleleft R$, we have $\langle z \rangle \triangleleft R$. Since $\langle z \rangle$ has order 2, we have $\langle z \rangle \leq \mathbf{Z}(R)$. Moreover,

$$\mathbf{Z}(R) \leq \mathbf{Z}(N(R)) = \langle z \rangle \times E.$$

Since $\mathbf{Z}(R)$ is cyclic and $\langle z \rangle \times E$ is an elementary abelian 2-group, we deduce that $\mathbf{Z}(R) = \langle z \rangle$.

Observe that $H \leq \mathbf{N}_R(H) = N(R)$. Suppose that $\mathbf{Z}(R) \leq H$. For every $x \in R$ and $h \in H$ we have $[h, x] \in \mathbf{Z}(R)$ because $h \in \mathbf{Z}_2(R)$ from Theorem 3.1. Thus $h^x = h[h, x] \in H$ since $h, [h, x] \in H$, so $H \trianglelefteq R$. This implies $N(R) = \mathbf{N}_R(H) = R$, and as usual we contradict (4). So we must have $\mathbf{Z}(R) \not\leq H$ and hence $\mathbf{Z}(R) \cap H = 1$. From the structure of $N(R) = Q \times E$, we deduce that H is an elementary abelian 2-group and $H \leq \mathbf{Z}(N(R))$.

Let $y \in N(R)$ with $\mathbf{o}(y) = 4$. From the structure of $N(R)$, we deduce that $y^2 = z$. We also have $y \in \mathbf{Z}_2(R) \setminus \mathbf{Z}(R)$, so since $[R, y] \leq \mathbf{Z}(R)$ which has order 2, the conditions of Lemma 4.3 are met with $p = 2$, and with $t \in R \setminus \mathbf{C}_R(y)$ fixed, the map $\phi : R \rightarrow R$ defined by $\phi(tc) = ytc$ for every $c \in \mathbf{C}_R(y)$ is a group automorphism. Since $H \leq \mathbf{Z}(N(R))$, we have $H \leq \mathbf{C}_R(y)$ and hence ϕ fixes H pointwise. Thus ϕ is a power automorphism. However, $yt = t^\phi \notin \langle t \rangle$, because t does not commute with y . This contradiction establishes (6).

Since $N(R)$ is abelian by (6), by the structure theorem for finitely generated abelian groups, we may write

$$N(R) = \langle a_1 \rangle \times \cdots \times \langle a_\ell \rangle, \quad (7)$$

where $\mathbf{o}(a_i) = p^{n_i}$, $n_i \geq 1$ and, after relabeling the indices if necessary, we may assume $\mathbf{Z}(R) \leq \langle a_1 \rangle$. If $\ell = 1$, then $N(R)$ is cyclic and hence every subgroup of $N(R)$ is characteristic. As $N(R)$ is characteristic in R , this implies that H is a characteristic subgroup of R . Thus, by (2), we have

$$\text{PAut}(R) = \mathbf{N}_{\text{Aut}(R)}(H) = \text{Aut}(R)$$

and hence R is cyclic by Lemma 3.2, contradicting our hypothesis on R . Therefore,

$$\ell \geq 2. \quad (8)$$

We claim that

$$p = 2. \quad (9)$$

Assume towards a contradiction that p is odd. Set $y = a_\ell^{p^{n_\ell-1}}$. We have $y \in N(R) \leq \mathbf{Z}_2(R)$ and $y \notin \langle a_1 \rangle$, so $y \notin \mathbf{Z}(R)$. For every $x \in R$, since $[x, y] \in \mathbf{Z}(R)$ and $y^p = 1$, we have

$$[x, y]^p = [x, y^p] = [x, 1] = 1.$$

This yields $|[R, y]| \leq p$ and so $|[R, y]| = p$. The conditions of Lemma 4.3 are now satisfied, so with $t \in R \setminus \mathbf{C}_R(y)$ fixed, the map $\phi : R \rightarrow R$ defined by $\phi(t^i c) = (yt)^i c$ for every $c \in \mathbf{C}_R(y)$ and every $0 \leq i < p$ is a group automorphism.

Since $N(R)$ is abelian and $h \in N(R)$, we have $H \leq N(R) \leq \mathbf{C}_R(h)$ and hence ϕ fixes H pointwise. Thus ϕ is a power automorphism. However, $ht = t^\phi \notin \langle t \rangle$, because t does not commute with h . This contradiction establishes (9).

We claim that

$$|\mathbf{Z}(R)| = 2. \quad (10)$$

We argue by contradiction and suppose that there exists $\bar{c} \in \mathbf{Z}(R)$ with $\mathbf{o}(\bar{c}) = 4$. Now, we mimic previous arguments, with a slight twist. Set $h = a_\ell^{2^{n_\ell-1}}$ and $y = \bar{c}h$. As before (with $\bar{c} \in \mathbf{Z}(R)$ not impacting these matters), h (and therefore y) is not in $\mathbf{Z}(R)$, but is in $\mathbf{Z}_2(R)$. Let $t \in R \setminus \mathbf{C}_R(y)$. As $[t, y] \neq 1$, $|[R, y]| = 2$ and $[R, y] \leq \mathbf{Z}(R)$, we have $[t, y] = z$, where z is the involution in the cyclic group $\mathbf{Z}(R)$. Thus $\bar{c}^2 = z$, so $y^2 = h^2 \bar{c}^2 = z$. So the conditions of Lemma 4.3 are met with $p = 2$, and with $t \in R \setminus \mathbf{C}_R(y)$ fixed, the map $\phi : R \rightarrow R$ defined by $\phi(tc) = ytc$ for every $c \in \mathbf{C}_R(y)$ is a group automorphism. Since $N(R)$ is abelian, we have $H \leq N(R) \leq \mathbf{C}_R(y)$ and hence ϕ fixes H pointwise. Thus ϕ is a power automorphism. However, $yt = t^\phi \notin \langle t \rangle$, because t does not commute with y . This contradiction establishes (10).

We claim that

$$N(R) \text{ is an elementary abelian 2-group.} \quad (11)$$

We use the direct product decomposition in (7). For every $i \in \{2, \dots, \ell\}$, we have $[R, a_i] \leq \mathbf{Z}(R)$, because $a_i \in N(R) \leq \mathbf{Z}_2(R)$ by Theorem 3.1. By (10), for every $x \in R$, we have $1 = [x, a_i]^2 = [x, a_i^2]$ and hence $a_i^2 \in \langle a_i \rangle \cap \mathbf{Z}(R) \leq \langle a_i \rangle \cap \langle a_1 \rangle = 1$. This implies $a_i^2 = 1$ and hence $\mathbf{o}(a_i) = 2$. The same argument applied with $i = 1$ gives $\mathbf{o}(a_1) \leq 4$. Suppose that $\mathbf{o}(a_1) = 4$. Then $|R : \mathbf{C}_R(a_1)| = |[R, a_1]| = 2$ and $a_1^2 = z$ is the involution of $\mathbf{Z}(R)$. Arguing as before, Lemma 4.3 with $y = a_1$ produces a non-power automorphism of R fixing H setwise, which is a contradiction. Therefore $\mathbf{o}(a_1) = 2$ and this establishes (11).

We claim that

$$x^2 \in N(R) \text{ and } \mathbf{o}(x) = 4, \quad \forall x \in R \setminus N(R). \quad (12)$$

From (11), we have $y^2 = 1$ for every $y \in N(R)$. Let $h_1, \dots, h_\kappa$ be generators of H . As $N(R)$ is abelian and $H \leq N(R) = \mathbf{N}_R(H)$, we have

$$\mathbf{N}_R(H) = \mathbf{C}_R(H) = \bigcap_{i=1}^{\kappa} \mathbf{C}_R(h_i).$$

As $[R, h_i] \leq \mathbf{Z}(R)$ (again this follows from Theorem 3.1 and $H \leq N(R)$), we have $|R : \mathbf{C}_R(h_i)| = |[R, h_i]| \leq 2$. Since $R/N(R) = R/\bigcap_i \mathbf{C}_R(h_i)$ embeds into $\prod_i (R/\mathbf{C}_R(h_i))$, we deduce that $R/N(R)$ is an elementary abelian 2-group. Since $N(R)$ is also an elementary abelian 2-group, each element of R has order at most 4.

Assume that there exists $t \in R \setminus N(R)$ with $\mathbf{o}(t) = 2$. Let K be any maximal subgroup of R containing $N(R)$ and with $t \notin K$, and let $\chi : R \rightarrow \mathbf{Z}(R)$ be the surjective homomorphism with kernel K . Then Lemma 4.2 produces a group automorphism $\phi_\chi : R \rightarrow R$, and since $H \leq N(R) \leq K$, ϕ_χ is a power automorphism. However, $t^{\phi_\chi} = tz \notin \langle t \rangle$, as $z \notin \langle t \rangle$, where z is the involution in $\mathbf{Z}(R)$. Since this is a contradiction, we have established (12).

We are finally ready to finish the proof. Let $t \in R \setminus N(R)$. From (12), t has order 4 and $t^2 \in N(R)$. Assume towards a contradiction that $t^2 = z$, where z is the generator of $\mathbf{Z}(R)$. Since $t \notin N(R) = \mathbf{C}_R(H)$, there exists $h \in H$ with $[h, t] = z$. Now, $th \notin N(R)$ and

$$(th)^2 = th \cdot th = t^2 h [h, t] h = z h z h = z^2 h^2 = 1,$$

contradicting that all elements in $R \setminus N(R)$ have order 4. Thus $t^2 \notin \mathbf{Z}(R)$. Now, let K be any maximal subgroup of R with $N(R) \leq K$ and $t \notin K$ and let $\chi : R \rightarrow \mathbf{Z}(R)$ be the surjective group homomorphism with kernel K . Then Lemma 4.2 produces a group automorphism $\phi_\chi : R \rightarrow R$, and since $H \leq N(R) \leq K$, it is a power automorphism. But ϕ_χ is not a power automorphism because $t^{\phi_\chi} = tz \notin \langle t \rangle$, as $z \neq t^2$. This final contradiction concludes the proof.

5. Future directions

A natural next step for this work would be attempting to characterize groups R such that the base size of the action of $\text{Aut}(R)$ on $\text{Sub}(R)$ is 2. We have made a variety of attempts to consider this. Computational results suggest that this family of groups is larger than one might intuitively anticipate, but our algorithms have been unable to consider large enough groups even to suggest a classification that we might then hope to prove. The methods we have used in this paper do have some relevance to the context of base size 2, but it seems that some additional ideas would be required.

If general results on base sizes greater than 1 seem beyond our reach, it would also be of interest to study the question of the base size of this action on some more specific families of groups. We believe that results of Burness and coauthors, for example [7, 8], might be useful for groups close to being simple. For instance, one can easily show that, for every non-abelian simple group R , the base size of $A(R)$ is at most 3. Here we do not use [7, 8]; instead, to make the proof even shorter, we use a result about generation [12]. Indeed, when $R = \text{PSU}_3(3)$ the result follows from a computer computation. Assume then that $R \neq \text{PSU}_3(3)$. By [12, Theorem A], R is generated by three involutions x_1, x_2, x_3 . It is now clear that

$$\mathbf{N}_{\text{Aut}(R)}(\langle x_1 \rangle) \cap \mathbf{N}_{\text{Aut}(R)}(\langle x_2 \rangle) \cap \mathbf{N}_{\text{Aut}(R)}(\langle x_3 \rangle) = \mathbf{C}_{\text{Aut}(R)}(\langle x_1, x_2, x_3 \rangle) = \mathbf{C}_{\text{Aut}(R)}(R) = 1.$$

Hence $A(R)$ has base size at most 3.

In the case of abelian groups, the work of Babai, Goodman, and Lovász can be used to show that the base size is at most 5. Let R be an abelian group. In the notation of [4, Lemma 6.1], let H_1, H_2, H_3, H_4 be the four subgroups constructed there, and let x denote the element called x_1 in their notation. The element x is not assumed to be an involution. By [4, Lemma 6.3], an automorphism of R fixing each H_i setwise and fixing x is the identity. If, instead, an automorphism α fixes each H_i setwise and fixes $\langle x \rangle$ setwise, the same proof shows that α maps every element of R to a power of itself. Therefore,

$$\bigcap_{i=1}^4 \mathbf{N}_{\text{Aut}(R)}(H_i) \cap \mathbf{N}_{\text{Aut}(R)}(\langle x \rangle) = \text{PAut}(R).$$

It follows that $H_1, H_2, H_3, H_4, \langle x \rangle$ form a base for $A(R)$, and hence the base size of $A(R)$ is at most 5.

Of course, Babai's conjecture about lattice representations of groups (our original motivation for this work) remains open and of great interest. As noted previously, we have achieved some extensions of previous work on this (especially on groups of odd order) but the general problem remains challenging, particularly in the context of 2-groups.

References

- [1] L. Babai, Finite digraphs with given regular automorphism groups, *Period. Math. Hungar.* 11 (4) (1980) 257–270.
- [2] L. Babai, On the abstract group of automorphisms, *Combinatorics, Proceedings 8th British Combinatorics Conference, Swansea 1981*, ed. H. N. V. Temperley; London Mathematical Society Lecture Notes 52 (University Press, Cambridge, 1981) 1–40.
- [3] L. Babai, A. J. Goodman, Subdirectly reducible groups and edge-minimal graphs with given automorphism group, *J. London Math. Soc.* 47 (1993) 417–432.
- [4] L. Babai, A. J. Goodman, L. Lovász, Graphs with given automorphism group and few edge orbits, *European J. Combin.* 12 (1991) 185–203.
- [5] R. Baer, Der Kern, eine charakteristische Untergruppe, *Compositio Math.* 1 (1935) 254–283.
- [6] G. Birkhoff, Sobre los grupos de automorfismos, *Rev. Un. Mat. Argentina* 11 (1946) 155–157.
- [7] T. C. Burness, M. Garonzi, A. Lucchini, Finite groups, minimal bases and the intersection number, *Trans. Amer. Math. Soc.* 9 (2022) 20–55.
- [8] T. C. Burness, H. Y. Huang, On the intersection of Sylow subgroups in almost simple groups, *J. Algebra* 690 (2026) 596–631.
- [9] R. Dedekind, Über Gruppen, deren sämtliche Theiler Normaltheiler sind, *Mathematische Annalen* 48 (1897) 548–561.
- [10] R. Frucht, Herstellung von Graphen mit vorgegebener abstrakter Gruppe, *Compositio Math.* 6 (1938) 239–250.
- [11] A. J. Goodman, The edge-orbit conjecture of Babai, *J. Combin. Theory Ser. B* 57 (1993) 26–35.
- [12] G. Malle, T. Weigel, Generation of classical groups, *Geometriae Dedicata* 49 (1995) 85–116.
- [13] E. Schenkman, On the norm of a group, *Illinois J. Math.* 4 (1960) 150–152.