Submitted exclusively to the London Mathematical Society
DOI: 10.1112/S0000000000000000

ON THE ORDERS OF AUTOMORPHISM GROUPS OF FINITE GROUPS

JOHN N. BRAY and ROBERT A. WILSON

Abstract

In the Kourovka Notebook, Deaconescu asks if $|\mathrm{Aut}\, G| \geqslant \phi(|G|)$ for all finite groups G, where ϕ denotes the Euler totient function; and whether G is cyclic whenever $|\mathrm{Aut}\, G| = \phi(|G|)$. We answer both questions in the negative. Moreover we show that $|\mathrm{Aut}\, G|/\phi(|G|)$ can be made arbitrarily small.

1. *The question, and some answers*

Conventions. Throughout this paper, we shall only consider finite groups. The notation for group structures is based on that used in the Atlas [**2**]. The notation $\mathrm{O}_2(G)$, $\mathrm{O}_{2'}(G)$ and $\mathrm{Aut}\, G$ is standard.

Let ϕ denote the Euler totient function, so that $\phi(n)$ is the number of integers m with $1 \leqslant m \leqslant n$ such that m and n are coprime, and

$$\frac{\phi(n)}{n} = \prod_{i=1}^{r} \frac{p_i - 1}{p_i},$$

where $p_1 < p_2 < \ldots < p_r$ are the prime factors of n. It is easy to see that for finite abelian groups G, we have $|\mathrm{Aut}\, G| \geqslant \phi(|G|)$, with equality if and only if G is cyclic. In Problem 15.43 of the Kourovka Notebook [**3**], Deaconescu asks if the same is true for arbitrary finite groups G. More specifically:

> Let G be a finite group of order n.
> a) Is it true that $|\mathrm{Aut}\, G| \geqslant \phi(n)$ where ϕ is Euler's function?
> b) Is it true that G is cyclic if $|\mathrm{Aut}\, G| = \phi(n)$?

In this note we show that the answer to both questions is no. Indeed, we shall prove:

Main Theorem. *For all $\varepsilon > 0$ there exists a group G such that $|\mathrm{Aut}\, G| < \varepsilon.\phi(|G|)$.*

In the course of this paper, it will transpire that there are infinitely many groups G satisfying $|\mathrm{Aut}\, G| < \phi(|G|)$, and infinitely many non-cyclic groups G which satisfy $|\mathrm{Aut}\, G| = \phi(|G|)$.

2000 *Mathematics Subject Classification* 20E36 (primary), 20F28 (secondary).

Part (a)

Examining some quasisimple groups, we quickly found that the perfect groups $G \cong (3 \times 4 \times 2)^{\cdot}\mathrm{L}_3(4)$, $12^{\cdot}\mathrm{M}_{22}$ and $(3^2 \times 4)^{\cdot}\mathrm{U}_4(3)$ satisfy $|\mathrm{Aut}\, G| < \phi(|G|)$, answering this part of the question in the negative. More precisely:

group G	primes dividing $\|G\|$	$\mathrm{Aut}\, G$	$\frac{\|\mathrm{Aut}\, G\|}{\|G\|}$	$\frac{\phi(\|G\|)}{\|G\|}$
$(3 \times 4 \times 2)^{\cdot}\mathrm{L}_3(4)$	$2, 3, 5, 7$	$\mathrm{L}_3(4){:}2^2$	$\frac{1}{6}$	$\frac{8}{35}$
$12^{\cdot}\mathrm{M}_{22}$	$2, 3, 5, 7, 11$	$\mathrm{M}_{22}{:}2$	$\frac{1}{6}$	$\frac{16}{77}$
$(3^2 \times 4)^{\cdot}\mathrm{U}_4(3)$	$2, 3, 5, 7$	$\mathrm{U}_4(3){:}\mathrm{D}_8$	$\frac{2}{9}$	$\frac{8}{35}$

Part (b)

One non-cyclic group G satisfying $|\mathrm{Aut}\, G| = \phi(|G|)$ is $G \cong 2 \times 3 \times 5 \times 11 \times \mathrm{M}_{11}$. Each of the five direct factors of G is characteristic, and we obtain

$$\mathrm{Aut}\, G \cong \mathrm{Aut}\, 2 \times \mathrm{Aut}\, 3 \times \mathrm{Aut}\, 5 \times \mathrm{Aut}\, 11 \times \mathrm{Aut}\, \mathrm{M}_{11} \cong 1 \times 2 \times 4 \times 10 \times \mathrm{M}_{11},$$

a group of order $\phi(|G|)$. More generally, if $2.3.5.11 = 330 \mid m$, then the non-cyclic group $G \cong \mathrm{C}_m \times \mathrm{M}_{11}$ has automorphism group $\mathrm{Aut}\, G \cong (\mathrm{Aut}\, \mathrm{C}_m) \times \mathrm{M}_{11}$, and is thus a group of order $\phi(|G|)$.

The smallest non-cyclic group G we know of that satisfies $|\mathrm{Aut}\, G| = \phi(|G|)$ is a group of order 56448, namely the group $G \cong 2^4{:}\mathrm{L}_3(2) \times 3 \times 7$, where the $2^4{:}\mathrm{L}_3(2)$ is isomorphic to the centraliser of an involution in M_{23}. In the direct factor $2^4{:}\mathrm{L}_3(2)$, when we consider the normal 2^4 as an $\mathbb{F}_2$-module for a complementary $\mathrm{L}_3(2)$, it is uniserial with a single non-zero proper submodule; this submodule has dimension 1. We have $\mathrm{Aut}\, G \cong 2^3{:}\mathrm{L}_3(2) \times 2 \times 6$. We may take G to be the group $\langle g_1, g_2, g_3 \rangle$ where:

$$\begin{aligned} g_1 &= (1,3)(2,4)(5,15,6,16)(7,9)(8,10)(11,13,12,14), \\ g_2 &= (1,3,5)(2,4,6)(7,15,11)(8,16,12), \\ g_3 &= (17,18,19)(20,21,22,23,24,25,26). \end{aligned}$$

In fact, this group G is a special case of the groups we construct in the next section.

2. *Proof of the Main Theorem*

Let P be a non-empty finite set of primes such that $p \equiv 7 \pmod 8$ for all $p \in P$. We shall consider groups of the form

$$G = C \times \prod_{p \in P} M_p,$$

where C is a cyclic subgroup of odd order and M_p is a perfect group of shape $2^{f(p)}{:}\mathrm{L}_2(p)$. (We shall define the groups M_p below.)

Lemma 1. *For all $p \in P$, the subgroups C and M_p are characteristic in G. Thus*

$$\mathrm{Aut}\, G \cong \mathrm{Aut}\, C \times \prod_{p \in P} \mathrm{Aut}\, M_p.$$

Proof. First, note that $C = \mathrm{O}_{2'}(G)$, so is characteristic in G. Let $N = \mathrm{F}(G)$, the Fitting subgroup of G, so that N is also characteristic in G. Now $G/N \cong \prod_{p\in P} \mathrm{L}_2(p)$ is a direct product of non-isomorphic simple groups. For each $p \in P$, G/N has a unique normal subgroup N_p/N such that $N_p/N \cong \mathrm{L}_2(p)$. Thus N_p/N is characteristic in G/N, and since N is characteristic in G, we get (for each $p \in P$) that N_p is a characteristic subgroup of G. In fact, $N_p = \langle N, M_p\rangle$, and we have

$$N_p = C \times M_p \times \prod_{q\in P\setminus\{p\}} \mathrm{O}_2(M_q).$$

Since C and $\mathrm{O}_2(M_q)$ are abelian and M_p is perfect, we obtain $N_p' = M_p$, and thus M_p is also a characteristic subgroup of G. □

Since C is cyclic, $\mathrm{Aut}\, C$ is an abelian group of order $\phi(|C|)$. We now concentrate on the groups M_p (where we may now fix $p \equiv 7 \pmod 8$). The order of $\mathrm{Aut}\, M_p$ depends crucially on the structure of $\mathrm{O}_2(M_p)$ as an $\mathbb{F}_2\mathrm{L}_2(p)$-module. We aim to construct a uniserial module with composition factors of dimensions 1 and $\frac{1}{2}(p-1)$, so that M_p has centre of order 2, in such a way that M_p has trivial outer automorphism group. It will then follow that $|\mathrm{Aut}\, M_p| = \frac{1}{2}|M_p|$. In what follows, we shall use $V_1 \cdot V_2$ to denote a non-split extension of modules V_1 by V_2 where V_1 is the submodule and V_2 is the quotient.

Lemma 2. *Let H denote the simple group $\mathrm{L}_2(p)$, where $p \equiv 7 \pmod 8$, and let V denote the permutation module over $\mathbb{F}_2$ of H on the $p+1$ cosets of the Borel subgroup. Then V is isomorphic to the trivial PIM (projective indecomposable module) for H, and has structure $1 \cdot (U_1 \oplus U_2) \cdot 1$, where U_1 and U_2 are absolutely irreducible.*

Proof. First we need some notation for some elements of H. We use t to denote any element of order p; all elements of order p in H are conjugate to t or t^{-1}. The other elements of H have order dividing $\frac{1}{2}(p-1)$ or $\frac{1}{2}(p+1)$; all such non-identity elements can be notated by x, y or z where:

$x \neq 1$ has order dividing $\frac{1}{2}(p-1)$.
$y \neq 1$ has order dividing $\frac{1}{4}(p+1)$.
$z \neq 1$ has order dividing $\frac{1}{2}(p+1)$, but does not have order dividing $\frac{1}{4}(p+1)$.

Four ordinary irreducible characters of $\mathrm{L}_2(p)$ are

Element	1	x	y	z	t	t^{-1}
χ_0	1	1	1	1	1	1
χ_1	$\frac{1}{2}(p-1)$	0	-1	1	β	γ
χ_2	$\frac{1}{2}(p-1)$	0	-1	1	γ	β
χ_3	p	1	-1	-1	0	0

where β and γ denote the irrationalities $\frac{1}{2}(-1 \pm \sqrt{-p})$; thus β and γ have minimal polynomial $X^2+X+\frac{1}{4}(p+1)$. Since χ_0, χ_1 and χ_2 remain irreducible on restriction to the Borel subgroup of shape $p{:}(\frac{p-1}{2})$ (which has odd order because $p \equiv 3 \pmod 4$), they remain irreducible on reduction modulo 2. Moreover, since $p \equiv 7 \pmod 8$, $X^2 + X + \frac{1}{4}(p+1)$ reduces modulo 2 to $X^2 + X$, which has roots in $\mathbb{F}_2$, so the corresponding representations can be written over $\mathbb{F}_2$. For $i \in \{0,1,2\}$ let φ_i denote the 2-modular Brauer character which is the restriction of χ_i to 2-regular classes, and let U_i be a module affording the character φ_i.

Now let P(1) denote the PIM of the trivial representation in characteristic 2, and let $\mathrm{Perm}(p+1)$ denote the characteristic 2 permutation module of $\mathrm{L}_2(p)$, of degree $p+1$, on the cosets of the Borel subgroup $p{:}(\frac{p-1}{2})$. Since $p{:}(\frac{p-1}{2})$ has odd order, $\mathrm{Perm}(p+1)$ is projective, and thus, since it contains a trivial submodule, contains a copy of P(1). Since the corresponding characteristic 0 permutation module of degree $p+1$ has character $\chi_0 + \chi_3$ and any element z is necessarily 2-singular, we see that $\mathrm{Perm}(p+1)$ has Brauer character $2\varphi_0 + \varphi_1 + \varphi_2$, and thus composition factors U_0, U_0, U_1, U_2.

Now P(1) has a unique simple submodule, and unique simple quotient, and thus (since $4 \mid |\mathrm{L}_2(p)|$) has the form $1 \cdot U \cdot 1$ where U is a non-zero module. Since U_1 and U_2 are conjugate under an outer automorphism of $\mathrm{L}_2(p)$ while $U_0 = 1$ remains invariant, we obtain that $\mathrm{P}(1) \cong \mathrm{Perm}(p+1) \cong 1 \cdot (U_1 \oplus U_2) \cdot 1$. This structure is valid over any field of characteristic 2. □

Since modules with simple socle M embed in the PIM corresponding to M, there are unique $\mathbb{F}_2\mathrm{L}_2(p)$-modules of shapes $1 \cdot U_1$ and $1 \cdot U_2$ while there are no $\mathbb{F}_2\mathrm{L}_2(p)$-modules of shapes $1 \cdot U_1 \cdot 1$ or $1 \cdot U_2 \cdot 1$. We now define $M_p \cong 2^{f(p)}{:}\mathrm{L}_2(p)$ to be the split extension of the $\mathbb{F}_2\mathrm{L}_2(p)$-module $1 \cdot U_1$ by $\mathrm{L}_2(p)$; in particular $f(p) = \frac{1}{2}(p+1)$. It remains to prove:

LEMMA 3. *With this definition, M_p has trivial outer automorphism group.*

Proof. Since $\mathrm{O}_2(M_p)$ is a characteristic subgroup of M_p, any automorphism of M_p permutes the complements to $\mathrm{O}_2(M_p)$ in M_p. Now let S denote a complementary $\mathrm{L}_2(p)$ in M_p. We have ensured that the module $1 \cdot U_1$ has zero 1-cohomology; thus M_p has just one class of complements, so we may assume that our automorphism α of M_p normalises S. Since the module $1 \cdot U_1$ is not invariant under outer automorphisms of S, $\alpha|_S$ must be an inner automorphism of S, and adjusting by an inner automorphism of M_p that is conjugation by an element of S, we may assume that α centralises S. So now α is an $\mathbb{F}_2S$-module automorphism of $1 \cdot U_1$, and thus is a scalar, and therefore trivial. □

It follows that $|\mathrm{Aut}\, M_p| = \frac{1}{2}|M_p|$ and therefore

$$\frac{|\mathrm{Aut}\, G|}{|G|} = \frac{\phi(|C|)}{|C|} \times \frac{1}{2^{|P|}}$$

whence

$$\frac{|\mathrm{Aut}\, G|}{\phi(|G|)} = \frac{\phi(|C|)}{|C|} \times \frac{|G|}{\phi(|G|)} \times \frac{1}{2^{|P|}}.$$

Now if for all $p \in P$ and odd prime divisors q of $p(p+1)(p-1)$ we have that $q \mid |C|$ then it follows that $\phi(|C|)/|C| = 2\phi(|G|)/|G|$, and therefore

$$\frac{|\mathrm{Aut}\, G|}{\phi(|G|)} = \frac{\phi(|C|)}{|C|} \times \frac{|G|}{\phi(|G|)} \times \frac{1}{2^{|P|}} = \frac{1}{2^{|P|-1}}.$$

In particular, this holds if $|C|$ is the product of all the odd primes which divide $p(p+1)(p-1)$ for some $p \in P$. To complete the proof of the Main Theorem, we invoke Dirichlet's Theorem that there are infinitely many primes p such that $p \equiv 7 \pmod 8$ to conclude that $|P|$ can be made arbitrarily large.

3. *Further work*

We have now extended our constructions and have been able to show that the Main Theorem holds when G is restricted to being soluble, and also when G is restricted to being perfect. Moreover, there are infinitely many perfect groups G and infinitely many non-cyclic soluble groups G such that $|\mathrm{Aut}\, G| = \phi(|G|)$. These results are the subject of a forthcoming publication [**1**].

References

1. J. N. Bray and R. A. Wilson. On the orders of automorphism groups of finite groups. II. *In preparation*.

2. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson. An $\mathbb{ATLAS}$ of Finite Groups. *Clarendon Press, Oxford* (1985; reprinted with corrections, 2003).

3. E. I. Khukhro and V. D. Mazurov (Eds). Unsolved problems in group theory. The Kourovka Notebook, no. 15. Novosibirsk, 2002.

John N. Bray and Robert A. Wilson.
School of Mathematics and Statistics,
University of Birmingham,
Edgbaston, Birmingham, B15 2TT.

jnb@maths.bham.ac.uk
R.A.Wilson@bham.ac.uk