On a theorem of Ledermann and Neumann

Benjamin Sambale*

September 29, 2019

Abstract

We give a short and self-contained proof of a theorem of Ledermann and Neumann stating that there are only finitely many finite groups with a given number of automorphisms. We also discuss the history of related conjectures.

Keywords: finite groups, automorphisms
AMS classification: 20D45

1 Introduction

Obviously, every finite group G has only finitely many automorphisms. In fact,

$$|\mathrm{Aut}(G)| \le (|G| - 1)! \tag{1.1}$$

as every automorphism permutes the non-trivial elements of G (an optimal bound will be given at the end of the paper).

It is far less obvious, if conversely the order of G is bounded by a function depending only on $|\mathrm{Aut}(G)|$. Ledermann and Neumann [11, Theorem 6.6] affirmatively answered this question in 1956 by constructing an explicit (but crude) bound. Unfortunately, their proof is rather long and complicated. In a second paper [12, Theorem 8.6] the authors provided a local version by bounding the p-part $|G|_p$ in terms of $|\mathrm{Aut}(G)|_p$ where p is a prime (this resolved a conjecture of Scott [24] and is now presented in the recent book [18, Chapter 3]). Ledermann and Neumann's original theorem was rediscovered by Nagrebeckiĭ [14] in 1970 and (presumably) independently by Iyer [8, Theorem 3.1] in 1979. The former proof is somewhat opaque and the latter implicitly relies on [12] via the PhD thesis of Hyde [7]. However, Nagrebeckiĭ [16, Theorem 4] gave a more transparent second proof within a generalized framework dealing with infinite groups. It seems that his work was not widely recognized (the English translation is not mentioned on MathSciNet for instance). The purpose of the present paper is to give a self-contained proof of the following version of the Ledermann–Neumann theorem based on some ideas from [16].

Theorem A. *For every integer n there exist only finitely many finite groups with at most n automorphisms.*

Our proof of Theorem A uses only first principles of elementary group theory, which are summarized in the next section. In the final section we discuss some related conjectures. The reader interested in infinite groups can find several generalizations of Theorem A in [1, 15, 17, 19, 20, 21].

*Institut für Mathematik, Friedrich-Schiller-Universität Jena, 07737 Jena, Germany, benjamin.sambale@uni-jena.de

2 Preliminaries

All groups considered in this paper are finite. Every element g of a group G induces an *inner* automorphism f_g of G by sending x to gxg^{-1}. The map $G \to \mathrm{Aut}(G)$, $g \mapsto f_g$ is a homomorphism whose kernel is the *center* $\mathrm{Z}(G) = \{g \in G : gx = xg \, \forall x \in G\}$ of G. In particular,

$$|G/\mathrm{Z}(G)| \le |\mathrm{Aut}(G)| \tag{2.1}$$

by the first isomorphism theorem.

For $x, y \in G$ we define the *commutator* $[x, y] := xyx^{-1}y^{-1} \in G$. A direct computation reveals

$$g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}], \quad [x, y^2] = [x,y]y[x,y]y^{-1} = [x,y][yxy^{-1}, y] \tag{2.2}$$

for $g \in G$. The commutators of G generate the *commutator subgroup* G' of G. By (2.2), G' is normal in G and G/G' is abelian.

The *exponent* $\exp(G)$ of G is the smallest positive integer e such that $g^e = 1$ for all $g \in G$. Clearly, the exponent of every subgroup or quotient of G divides $\exp(G)$. The smallest integer d such that G can be generated by d elements is denoted by $d(G)$.

Now assume that G is abelian. Then clearly

$$|G| \le \exp(G)^{d(G)}. \tag{2.3}$$

By the main theorem of finite abelian groups there exists a decomposition

$$G = \langle x_1 \rangle \times \ldots \times \langle x_k \rangle \tag{2.4}$$

such that the order of x_i is a prime power for $i = 1, \ldots, k$. This yields a factorization into *primary components* $G = G_{p_1} \times \ldots \times G_{p_n}$ where $p_1, \ldots, p_n$ are the prime divisors of $|G|$ and G_{p_i} is the set of p_i-elements of G for $i = 1, \ldots, n$. Suppose that x_1 in (2.4) is a p-element and $r \in \mathbb{Z}$ is a primitive root modulo p. Then the map $x_1 \mapsto x_1^r$ defines an automorphism α of $\langle x_1 \rangle$ whose order is divisible by $p - 1$. Since α extends to G, we obtain

$$p - 1 \le |\mathrm{Aut}(G)| \tag{2.5}$$

whenever p divides $|G|$.

Finally we need a rather special case of the famous Schur–Zassenhaus theorem, which is at the same time a special case of Burnside's transfer theorem.

Proposition 1. *Let p be a prime such that $|G|_p = |\mathrm{Z}(G)|_p$. Then $G = \mathrm{Z}(G)_p \times Q$ for some $Q \le G$.*

Proof. See [10, Theorem 3.3.1 or Theorem 7.2.1]. $\qquad\qquad\square$

3 Proof of Theorem A

In the following let G be a finite group and $n := |\mathrm{Aut}(G)|$. We prove Theorem A by bounding $|G|$ in terms of n. This is done in a series of lemmas.

Lemma 2 (Schur [23]). $|G'| \le n^{2n^3}$.

Proof (Rosenlicht [22]). Let $g_1, \ldots, g_m \in G$ be representatives for the cosets of $G/\mathrm{Z}(G)$. Then $m = |G/\mathrm{Z}(G)| \leq n$ by (2.1). Arbitrary elements $g, h \in G$ can be written as $g = g_i z$ and $h = g_j w$ with $z, w \in \mathrm{Z}(G)$. It follows that $[g, h] = [g_i, g_j]$. Hence, the set of commutators

$$\Gamma := \big\{ [g, h] : g, h \in G \big\} = \big\{ [g_i, g_j] : 1 \leq i, j \leq m \big\}$$

has at most m^2 elements. It suffices therefore to show that every element $g \in G'$ is a product of at most m^3 commutators. Let $g = \gamma_1 \ldots \gamma_s$ such that $\gamma_1, \ldots, \gamma_s \in \Gamma$ and s is as small as possible. By way of contradiction suppose that $s > m^3$. Then some commutator $\gamma = [x, y]$ appears more than m times among the γ_i. Since $\gamma_i \gamma_{i+1} = \gamma_{i+1} \delta$ where $\delta := \gamma_{i+1}^{-1} \gamma_i \gamma_{i+1} \in \Gamma$ by (2.2), we may assume that $\gamma = \gamma_1 = \ldots = \gamma_{m+1}$. Since $\gamma^m = \gamma^{|G/\mathrm{Z}(G)|} \in \mathrm{Z}(G)$, we have

$$\gamma^{m+1} = \gamma \gamma^m = \gamma y \gamma^m y^{-1} = \gamma (y \gamma y^{-1})^m = \gamma y \gamma y^{-1} \cdot (y \gamma y^{-1})^{m-1} = [x, y^2][y x y^{-1}, y]^{m-1}$$

according to (2.2). But now $g = \gamma^{m+1} \gamma_{m+2} \ldots \gamma_s$ is a product of $s-1$ commutators. Contradiction. □

Lemma 2 shifts the focus to the abelian group G/G'. It is however not clear if and how automorphisms of G/G' lift to G.

Lemma 3. *Every prime divisor p of $|G|$ is at most $n + 1$.*

Proof. If $|G/\mathrm{Z}(G)|_p \neq 1$, then $p \leq n$ by (2.1). Otherwise, $|\mathrm{Z}(G)|_p = |G|_p$ and $G = \mathrm{Z}(G)_p \times Q$ by Proposition 1. Since every automorphism of $\mathrm{Z}(G)_p$ extends to G, we obtain $p - 1 \leq n$ by (2.5). □

A careful analysis of the proof shows that $p^2 \mid |G|$ implies $p \mid n$. This observation of Herstein–Adney [6] is however not needed below.

Lemma 4. *The exponent $\exp(G)$ is bounded in terms of n.*

Proof. By Lemma 2 it suffices to show that $\exp(G/G')$ is bounded in terms of n. By (2.4) we may write $G/G' = H/G' \times \langle g G' \rangle$ with $g \in G$ and $H \trianglelefteq G$. Then $G = H \langle g \rangle$ and $H \cap \langle g \rangle \leq G'$. Note that

$$N := |G/\mathrm{Z}(G)| \cdot |G'| \cdot \prod_{p \,\mid\, |G|} p \leq n \cdot n^{2n^3} \cdot (n+1)!$$

by (2.5), Lemma 2 and Lemma 3. Let $h_1, h_2 \in H$ and $i, j \in \mathbb{Z}$ such that $h_1 g^i = h_2 g^j$. Then $h_2^{-1} h_1 = g^{j-i} \in H \cap \langle g \rangle \leq G'$. Since $|G'|$ divides N we conclude that $h_2^{-1} h_1 = (g^{j-i})^{1+N}$. Therefore the map

$$\alpha : G \to G, \quad h g^i \mapsto h g^{i(1+N)} \quad (h \in H,\ i \in \mathbb{Z})$$

is well-defined. Since $g^N \in \langle g^{|G/\mathrm{Z}(G)|} \rangle \subseteq \mathrm{Z}(G)$, we obtain

$$\alpha(h_1 g^i h_2 g^j) = \alpha(h_1 (g^i h_2 g^{-i}) g^{i+j}) = h_1 (g^i h_2 g^{-i}) g^{(i+j)(1+N)} = h_1 g^i h_2 g^{-i+i(1+N)} g^{j(1+N)}$$
$$= h_1 g^{i+iN} h_2 g^{j(1+N)} = \alpha(h_1 g^i) \alpha(h_2 g^j)$$

for all $h_1, h_2 \in H$ and $i, j \in \mathbb{Z}$. Hence, α is a homomorphism. Every prime divisor of $|\langle g \rangle|$ divides $|G|$ and is therefore coprime to $1 + N$. Consequently, $\langle g^{1+N} \rangle = \langle g \rangle$ and α is surjective. Now $\alpha \in \mathrm{Aut}(G)$, since G is finite. In particular, $g = \alpha^n(g) = g^{(1+N)^n}$. Since $\langle g G' \rangle$ was an arbitrary direct factor of G/G', it follows that

$$\exp(G/G') \leq (1+N)^n - 1.$$
□

Lemma 5. *Let A be an abelian group and $a \in A$ of prime order p. Then there exists a decomposition $A = B \times C$ such that B is cyclic and $a \in B$.*

Proof. By (2.4) we may assume that $A = A_p$. Let $A = B \times C$ such that $a \in B$ and $|B|$ is as small as possible ($B = A$ may do). Let

$$B = \langle x_1 \rangle \times \ldots \times \langle x_n \rangle$$

such that $|\langle x_i \rangle| = p^{\alpha_i}$ and $\alpha_1 \geq \ldots \geq \alpha_n$. The choice of B implies that $a = x_1^{\beta_1 p^{\alpha_1 - 1}} \ldots x_n^{\beta_n p^{\alpha_n - 1}}$ where $\beta_i \not\equiv 0 \pmod{p}$ for $i = 1, \ldots, n$. We define

$$b := x_1^{\beta_1 p^{\alpha_1 - \alpha_n}} x_2^{\beta_2 p^{\alpha_2 - \alpha_n}} \ldots x_n^{\beta_n}.$$

Then $a = b^{p^{\alpha_n - 1}} \in \langle b \rangle$ and $B = \langle x_1 \rangle \times \ldots \times \langle x_{n-1} \rangle \times \langle b \rangle$. Now the minimality of B yields $B = \langle b \rangle$ as desired. $\qquad \square$

Lemma 6. *Let $B \leq A$ be abelian groups. Then there exists a decomposition $A = C \times D$ such that $B \leq C$ and $d(C) \leq |B|$.*

Proof. We argue by induction on $|B|$. If $|B| = 1$, then we take $C = 1$ and $D = A$. Now assume that $|B| > 1$ and pick a subgroup $B_0 \leq B$ of prime index p. By induction there exists a decomposition $A = C_0 \times D_0$ such that $B_0 \leq C_0$ and $d(C_0) \leq |B_0|$. Let $b \in B \setminus B_0$ and write $b = cd$ with $c \in C_0$ and $d \in D_0$. Then

$$d^p = b^p c^{-p} \in B_0 C_0 \cap D_0 \leq C_0 \cap D_0 = 1.$$

By Lemma 5 there exists a decomposition $D_0 = D_1 \times D_2$ such that D_1 is cyclic and $d \in D_1$. Now we define $C := C_0 \times D_1$. Then $B = B_0 \langle b \rangle \leq C$, $A = C_0 \times D_0 = C_0 \times D_1 \times D_2 = C \times D_2$ and

$$d(C) \leq d(C_0) + 1 \leq |B_0| + 1 \leq |B|$$

as desired. $\qquad \square$

Proof of Theorem A. By (2.5) it suffices to bound $|Z(G)|$ in terms of n. Let $g_1, \ldots, g_m \in G$ be representatives for the cosets of $G/Z(G)G'$. Let $U := \langle g_1, \ldots, g_m \rangle G'$. Then

$$d(U/G') \leq m = |G : Z(G)G'| \leq |G : Z(G)| \leq n.$$

By Lemma 2 and (2.3),

$$|U| = |U/G'||G'| \leq \exp(U/G')^{d(U/G')} n^{2n^3} \leq \exp(G)^n n^{2n^3}.$$

Hence by Lemma 4, $|U|$ is bounded by a function on n. By Lemma 6 we have $Z(G) = C \times D$ such that $U \cap Z(G) \leq C$ and $d(C) \leq |U \cap Z(G)| \leq |U|$. Now also $|C|$ is bounded and it remains to prove that $|D|$ can be bounded in terms of n. Let $d = uc \in UC \cap D$ with $u \in U$ and $c \in C$. Then $u = dc^{-1} \in U \cap Z(G) \leq C$ and it follows that $d = dc^{-1}c \in D \cap C = 1$. This shows

$$G = UZ(G) = U(C \times D) = UC \times D.$$

Since every automorphism of D extends to G, we may assume that $G = D$ is abelian. By Lemma 3 we may assume that $G = G_p$ is a p-group, say

$$G = \langle x_1 \rangle \times \ldots \times \langle x_k \rangle$$

with $|\langle x_1 \rangle| \geq \ldots \geq |\langle x_k \rangle|$. It is easily checked that the map

$$x_1 \mapsto x_1 x_l, \qquad\qquad x_i \mapsto x_i \qquad (2 \leq i \leq k)$$

defines an automorphism of G whenever $2 \leq l \leq k$. Hence, $k \leq n$ and $|G|$ is bounded in terms of n by Lemma 4. $\qquad \square$

4

4 The reverse bound

As promised at the very beginning, we now give an optimal bound on $|\mathrm{Aut}(G)|$ in terms of $|G|$. Recall that a group G is called *boolean* if $\exp(G) \leq 2$. In this case G is abelian, since $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$ for all $g, h \in G$. The following improves (1.1).

Proposition 7. *For every finite group G we have $d(G) \leq \log_2 |G|$ and*

$$|\mathrm{Aut}(G)| \leq \prod_{k=0}^{d(G)-1} \left(|G| - 2^k\right)$$

with equality if and only if $|G|$ is a prime or G is boolean.

Proof. If $G = 1$, then $d(G) = 0$ and equality holds by interpreting the empty product as 1 (note that the trivial group is boolean). Now let $G \neq 1$ with a minimal generating set $g_1, \ldots, g_d \in G$ where $d = d(G)$. For $\alpha \in \mathrm{Aut}(G)$, also $\alpha(g_1), \ldots, \alpha(g_d)$ is a (minimal) generating set and α is uniquely determined by those images. Since $\alpha(g_1) \neq 1$, there are at most $|G| - 1$ choices for $\alpha(g_1)$. Since $\alpha(g_2) \notin \langle \alpha(g_1) \rangle$, there are at most $|G \setminus \langle \alpha(g_1) \rangle| \leq |G| - 2$ possibilities for $\alpha(g_2)$ and so on. This proves $d(G) \leq \log_2 |G|$ and the inequality on $|\mathrm{Aut}(G)|$.

If equality holds, then for every $g \neq 1$ there exists an automorphism mapping g_1 to g. In particular, all non-trivial elements of G have the same order, which necessarily must be a prime p (if not, consider a power of g). If additionally $d = 1$, then $|G| = |\langle g_1 \rangle| = p$. On the other hand, if $d \geq 2$, then there are $|G| - 2 = |G \setminus \langle \alpha(g_1) \rangle|$ choices for $\alpha(g_2)$. Hence $p = |\langle \alpha(g_1) \rangle| = 2$ and G is boolean.

Conversely, every group of prime order p has $p - 1$ automorphisms by (2.5). Moreover, every boolean group G is an $\mathbb{F}_2$-vector space and $\mathrm{Aut}(G) \cong \mathrm{GL}(d, 2)$ where $d = d(G)$. Counting matrices with linearly independent rows yields the well-known formula

$$|\mathrm{GL}(d, 2)| = (2^d - 1)(2^d - 2) \ldots (2^d - 2^{d-1}).$$

Thus, we have shown equality. $\qquad\qquad\square$

The proof above actually shows slightly more: If $|G| = p_1 \ldots p_n$ with primes $p_1 \leq \ldots \leq p_n$, then $d(G) \leq n$ and

$$|\mathrm{Aut}(G)| \leq \prod_{k=0}^{d(G)-1} \left(|G| - p_1 \ldots p_k\right).$$

5 Some related conjectures

A complete classification of all finite groups with less than 48 automorphisms was given by MacHale and Sheehy [13] (see also [25]). They noticed that $\varphi(|G|) \leq |\mathrm{Aut}(G)|$ holds in these small cases where φ is Euler's totient function. In fact, this inequality was conjectured in general by Deaconescu [4] who also conjectured that equality holds if and only if G is cyclic (it is Problem 15.43 in the Kourovka Notebook [9]). If true, this would yield a bound on $|G|$ as well (e.g., $|G| \leq |\mathrm{Aut}(G)|^{1+\epsilon}$ provided $|G|$ is large enough with respect to $\epsilon > 0$). However, Bray and Wilson [2, 3] constructed solvable and nonsolvable counterexamples.

Similarly, the long-standing Problem 12.77 in [9] proposed that $|G|$ divides $|\mathrm{Aut}(G)|$ for every non-abelian p-group G. This was disproved recently by González-Sánchez and Jaikin-Zapirain [5] using pro-p group techniques. In fact, $|\mathrm{Aut}(G)|/|G|$ can be arbitrarily small.

Yet another conjecture, this time from [13], reads $|G| \le |\mathrm{End}(G)|$ where $\mathrm{End}(G)$ is the set of endomorphisms of G. However, the triple cover $G = 3.A_7$ of the alternating group of degree 7 is a counterexample. Since A_7 is a simple group, G has only three normal subgroups: 1, $\mathrm{Z}(G)$ and G. Here, $\mathrm{Z}(G)$ cannot occur as a kernel of an endomorphism, because as a perfect group G does not contain subgroups of index 3. Hence, every nontrivial endomorphism is an automorphism. Moreover, it is known that $\mathrm{Aut}(G)$ acts faithfully on $G/\mathrm{Z}(G) \cong A_7$ (this holds for any quasisimple group). Since $\mathrm{Aut}(A_7)$ is isomorphic to the symmetric group S_7, we finally conclude that

$$|\mathrm{End}(G)| = 1 + |\mathrm{Aut}(G)| \le 1 + |\mathrm{Aut}(G/\mathrm{Z}(G))| = 1 + |S_7| = 1 + 7! < \frac{3}{2}7! = |G|.$$

Acknowledgment

References

[1] J. L. Alperin, *Groups with finitely many automorphisms*, Pacific J. Math. **12** (1962), 1–5.

[2] J. N. Bray and R. A. Wilson, *On the orders of automorphism groups of finite groups*, Bull. London Math. Soc. **37** (2005), 381–385.

[3] J. N. Bray and R. A. Wilson, *On the orders of automorphism groups of finite groups. II*, J. Group Theory **9** (2006), 537–545.

[4] M. Deaconescu, *Krutik groups and a conjecture on automorphisms*, An. Univ. Timişoara Ser. Mat.-Inform. **35** (1997), 209–210.

[5] J. González-Sánchez and A. Jaikin-Zapirain, *Finite p-groups with small automorphism group*, Forum Math. Sigma **3** (2015), e7, 11.

[6] I. N. Herstein and J. E. Adney, *A note on the automorphism group of a finite group*, Amer. Math. Monthly **59** (1952), 309–310.

[7] K. H. Hyde, *On the order of the Sylow subgroups of the automorphism group of a finite group*, Glasgow Math. J. **11** (1970), 88–96.

[8] H. K. Iyer, *On solving the equation* $\mathrm{Aut}(X) = G$, Rocky Mountain J. Math. **9** (1979), 653–670.

[9] E. I. Khukhro and V. D. Mazurov, *The Kourovka notebook. Unsolved problems in group theory*, 18th edition, Russian Academy of Sciences Siberian Division, Institute of Mathematics, Novosibirsk, 2014.

[10] H. Kurzweil and B. Stellmacher, *The theory of finite groups*, Universitext, Springer-Verlag, New York, 2004.

[11] W. Ledermann and B. H. Neumann, *On the order of the automorphism group of a finite group. I*, Proc. Roy. Soc. London. Ser. A. **233** (1956), 494–506.

[12] W. Ledermann and B. H. Neumann, *On the order of the automorphism group of a finite group. II*, Proc. Roy. Soc. London. Ser. A. **235** (1956), 235–246.

[13] D. MacHale and R. Sheehy, *Finite groups with few automorphisms*, Math. Proc. R. Ir. Acad. **104A** (2004), 231–238.

[14] V. T. Nagrebeckiĭ, *On the number of finite groups with a given automorphism group*, Math. USSR, Sb. **12** (1970), 521–524 (translated by D.L. Johnson).

[15] V. T. Nagrebeckiĭ, *Finitely generated groups with a finite number of automorphisms*, Siberian Math. J. **13** (1972), 331–33.

[16] V. T. Nagrebeckiĭ, *On groups with a finite number of automorphisms*, Math. USSR, Sb. **15** (1972), 568–575 (translated by J.C. Lennox).

[17] V. T. Nagrebeckiĭ, *The periodic part of a group with a finite number of automorphisms*, Soviet Math. Dokl. **13** (1972), 953–956.

[18] I. B. S. Passi, M. Singh and M. K. Yadav, *Automorphisms of finite groups*, Springer Monographs in Mathematics, Springer, Singapore, 2018.

[19] D. J. S. Robinson, *A contribution to the theory of groups with finitely many automorphisms*, Proc. London Math. Soc. (3) **35** (1977), 34–54.

[20] D. J. S. Robinson, *Groups with prescribed automorphism group*, Proc. Edinburgh Math. Soc. (2) **25** (1982), 217–227.

[21] D. J. S. Robinson, *A clarification: "Groups with prescribed automorphism group"*, Proc. Edinburgh Math. Soc. (2) **27** (1984), 59–60.

[22] M. Rosenlicht, *On a result of Baer*, Proc. Amer. Math. Soc. **13** (1962), 99–101.

[23] I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math **127** (1904), 20–50.

[24] W. R. Scott, *On the order of the automorphism group of a finite group*, Proc. Amer. Math. Soc. **5** (1954), 23–24.

[25] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences, Sequence A137315*, `https://oeis.org/A137315`.