Ricerche di Matematica (2019) 68:415–420
https://doi.org/10.1007/s11587-018-0413-9

The rank of the automorphism group of a finite group

B. A. F. Wehrfritz[1]

Received: 5 April 2018 / Published online: 9 July 2018

Abstract
Let G be a finite group whose order is divisible by e primes (counting repetitions). Then the automorphism group of G has Prüfer rank at most e^2, meaning that each subgroup of the automorphism group of G can be generated by at most e^2 elements.

Keywords Finite group · Automorphism group · Prüfer rank

Mathematics Subject Classification 20D45

1 Introduction

If G is a finite group, then $d(G)$ denotes its minimal number of generators, $e(G)$ the number of prime divisors (counting repetitions) of its order $|G|$ and $rk(G)$ its rank; that is, the maximum of the $d(X)$ as X ranges over the subgroups of G. Clearly $d(G) \leq rk(G) \leq e(G)$. Also [r] denotes the largest integer not exceeding the real number r.

Theorem 1 *If G is a finite group, then always $rk(Aut(G)) \leq e(G) + [e(G)^2/2] \leq e(G)^2$.*

I mention and use $rk(Aut(G)) \leq e(G)^2$ in [12] as if it is well-known. It seems this is not the case and I have failed to find any proof or indeed any mention of it in the literature. Thus I feel now the need to publish a proof. My proof is in the main elementary. The only really non-elementary facts I use are that if S is a finite perfect simple group, then $d(S) = 2, rk(Out(S)) \leq 5$, $|S|$ is divisible by 4 and $e(S) \geq 4$ (even 5 unless $S = Alt(5)$). I also use results from [5,8], see below for details, although these can be avoided at the expense of substantially lengthening the proof by using Theorem 2 below to reduce to the soluble case.

Communicated by F. de Giovanni.

✉ B. A. F. Wehrfritz
b.a.f.wehrfritz@qmul.ac.uk

[1] Queen Mary University of London, London E1 4NS, England, UK

Clearly $rk(G) \leq e(G)$ and it is easy to prove that $|Aut(G)| \leq |G|^{d(G)} \leq |G|^{e(G)}$, but these easy facts seem to be of no help in proving the theorem. Note also that $rk(Aut(G))$ need not be bounded by $(rk(G))^2$, though in significant special cases (e.g. G elementary abelian) it is. As an obvious counter example, the cyclic group G of order 8 has $rk(G) = 1$ and $rk(Aut(G)) = 2$. More generally it is easy to see that if G is the direct product of r cyclic groups of order 2^f for $f \geq 3$ and $r \geq 1$, then $Aut(G)$ contains an elementary abelian subgroup of rank $r^2 + r$. Hence here $rk(G) = r$ while $rk(Aut(G)) \geq r^2 + r > r^2$. (Also $e(G)^2/2 = (fr)^2/2 > r^2 + r$ of course.)

Our second theorem below we originally used in the proof of Theorem 1 essentially to reduce to the soluble case, but thanks to [5,8], which only very recently were brought to my attention, we no longer need to do this (At the end of this paper we sketch this alternative approach to Theorem 1). However, I think Theorem 2 is of independent interest.

Theorem 2 *Let G be a finite subgroup of $GL(n, F)$, where n is a positive integer and F is a field of positive characteristic p. Suppose G has a soluble normal subgroup S such that G/S is a direct product of r perfect simple groups. Then $r \leq [n/2]$.*

Clearly this bound is attained for all n and all F with $|F| > 3$; recall $GL(2, 2)$ and $GL(2, 3)$ are soluble.

2 Proof of the results

By a theorem of Guralnick and Lucchini (independently), see [5,8], the rank of a finite group is bounded by one more than the maximum of the ranks of its Sylow subgroups. The following lemma is the analogue of Theorems 1 and 2 for the symmetric groups.

Lemma 1 *For each positive integer n we have $rk(Sym(n)) \leq 1 + [n/2]$. Further $rk(Sym(n))$ is 0 if $n = 1$ and 1 if $n = 2$. If G is a subgroup of $Sym(n)$ with a soluble normal subgroup S such that G/S is the direct product of s perfect simple groups, then $s \leq [n/4]$.*

Proof The rank of a Sylow p-subgroup of $Sym(n)$ is $[n/p]$ for any prime p, see the Proposition of [10]. Thus the first claim follows from this and Guralnick and Lucchini's theorem. Clearly G/S involves an elementary abelian 2-group of rank $2s$ and by the Proposition of [10] again a Sylow 2-subgroup of $Sym(n)$ has rank $[n/2]$. Therefore $s \leq [n/4]$ (A very simple proof by induction on n shows that at least $rk(Sym(n)) \leq [n^2/4]$, which would actually suffice for our purposes). □

Note that Guralnick and Lucchini's theorem together with bounds in [10] yield that in Theorem 2 we have $r \leq 3n/4$ if $p > 2$ and $r \leq 2n$ if $p = 2$. These are weaker than the claims of Theorem 2; also they do not seem to help with its proof.

Proof of Theorem 2 If $n = 1$ we have $r = 0$. Suppose $n = 2$. If G is metabelian then $r = 0$. If not then G is absolutely irreducible and hence is isomorphic to a subgroup of $GL(2, p^f)$ for some f (e.g. [2] 29.21). Thus from Dickson's list of the subgroups

of $PSL(2, p^f)$, see [6] II.8.27, we have $r \leq 1$. Let G be a counter example to the theorem with n minimal. Then $n \geq 3$ and $r \geq 2$. Hence $G = G_1 G_2 \ldots G_r$, where the G_i are normal subgroups of G, the G_i/S_i are perfect simple for $S_i = G_i \cap S$ and G/S is the direct product of the $G_i S/S$. We break the proof into a number of sublemmas.

(a) If N is a normal subgroup of G, then G/N and N have the same structure as G. Specifically NS/N is soluble and G/NS is the direct product of the $G_i NS/NS$ (each being isomorphic to $G_i S/S$ or $\langle 1 \rangle$). Also $N \cap S$ is soluble, $N/(N \cap S) \simeq NS/S$ and the latter is the direct product of the $(NS \cap G_i S)/S$ (again each of which is isomorphic to $G_i S/S$ or $\langle 1 \rangle$).

(b) We may assume that $(G_i)' = G_i$ for each i.
Now G_i is soluble-by-simple. Let H_i be the soluble residual of G_i, so $(H_i)' = H_i$ and $G_i = H_i S_i$. Also $T_i = H_i \cap S$ is the soluble radical of H_i and $H_i/T_i \simeq G_i/S_i$. Thus if $H = H_1 H_2 \ldots H_t$ and $T = H \cap S$, then

$$H/T = H_1 T/T \times \cdots \times H_r T/T \simeq H_1/T_1 \times \cdots \times H_r/T_r.$$

Thus we may replace G by H. Equivalently we may assume that $(G_i)' = G_i$ for each i.

(c) We may assume F is algebraically closed. Then G is absolutely irreducible.
The first claim is obvious. Let $V = F^{(n)}$ taken as a right $GL(n, F)$-module in the obvious way and let W be an FG-submodule of V with $\{0\} < W < V$. If G is a subgroup of $C_G(W)S \cap C_G(V/W)S$, then G acts as a soluble group on both W and V/W and hence acts as a soluble group on V. But G_i is not soluble. Thus each G_i/S_i is avoided by at least one of $C_G(W)$ and $C_G(V/W)$ and then by the minimal choice of n we have

$$r \leq (dim_F W)/2 + (dim_F(V/W))/2 = n/2.$$

This contradiction shows that G is irreducible.

(d) G is primitive.
Suppose $V = V_1 \oplus \cdots \oplus V_t$ is a system of imprimitivity of G with $t \geq 2$. Set $N = \bigcap_j N_G(V_j)$. Then G permutes the V_i transitively and G/N embeds into $Sym(t)$. Hence G/N involves at most $[t/4]$ of the G_i/S_i by Lemma 1 and thus N must involve the remaining G_i/S_i, of which there are say $r_1 \geq r - [t/4]$. Let I denote the set of all such i. Then $N/(N \cap S)$ is the direct product over I of the $(G_i S \cap N)/(N \cap S)$. For each i in I the group $G_i S \cap N$ cannot act as a soluble group on all the V_i and hence there exists j with $G_i S \cap N$ not contained in $C_N(V_i)(N \cap S)$. Now the G_i are normal in G and G permutes the V_i transitively. Thus $G_i S \cap N$ is not contained in $C_N(V_1)(N \cap S)$ for each i in I and therefore $r_1 = |I| \leq (dim_F(V_1))/2$. Now $t \geq 2$ and $n = t.dim_F V_1$, so

$$r \leq r_1 + [t/4] \leq (dim_F V_1)/2 + t/4 \leq n/2.$$

This final contradiction yields that G is primitive.

(e) $E(G)$, the subgroup of G generated by the subnormal quasi-simple subgroups of G is non-trivial.
For suppose $E(G) = \langle 1 \rangle$. Set $N = Fitt(G)$, the Fitting subgroup of G. Now every abelian normal subgroup of G lies in $Z = \mathrm{F}^*1_n \cap G$ by c), d) and [9] 1.13. (F^* denotes the multiplicative group of F.) Also $N \geq Z = C_G(N)$ (e.g. see [11] 6.2 or [1] 31.13). Suppose N is nilpotent of class $c \geq 3$. Then, with $\{\gamma^i(N)\}$ denoting the lower central series of N, $(\gamma^{c-1}(N))' \leq \gamma^{2c-2}(N) = \langle 1 \rangle$, so $\gamma^{c-1}(N) \leq Z$ and N is not nilpotent of class C.
Consequently $c \leq 2$. In fact $c = 2$, since if N is abelian, then $N = Z = C_G(N) = G$ and $r = 0 \leq [n/2]$. If q is some prime and if x and y are elements of N of order q^2 modulo Z, then $[x^q, y^q] = [x, y^{q \cdot q}] = 1$. Hence $\langle x^q : x \in N, |xZ| = q^2 \rangle$ is abelian and therefore lies in Z. Consequently every Sylow subgroup of N/Z is elementary abelian.
Since G is primitive, N is homogeneous ([9] 1.7). Therefore $(N : Z) = (n')^2$ for some divisor n' of n, see [9] 3.2. Suppose $n' = p_1^{e(1)} p_2^{e(2)} \dots p_t^{e(t)}$, where the p_i are distinct primes. Set $K = C_G(N/Z)$. Then $K' \leq C_G(N) = Z$ and so K is soluble. Also G/K embeds into the direct product of the t-groups $GL(2e(i), p_i)$. Now $GL(2, 2)$ is soluble and $GL(4, 2) \simeq Alt(8)$. Neither involves the direct product of 2 perfect simple groups ($|Alt(8)| = 2.60.168$ and is not divisible by 5^2) and trivially $1 \leq [n/2]$. Then $n' \neq 2$ or 4 and so $\sum_i 2.e(i) < n$ and $r \leq \sum_i e(i) < n/2$. This final contradiction yields that $E(G) \neq \langle 1 \rangle$.

(f) $E(G).S \neq G$.
If $E(G).S = G$, then $E(G) = E_1 E_2 \dots E_t = E$ say, where the E_i are the subnormal quasi-simple subgroups of G. Thus we can work with E instead of G. If $r = 0$ trivially $r \leq [n/2]$. If $r = 1$ clearly $n \geq 2$ and again $r \leq [n/2]$. Thus $r \geq 2$. If E is reducible, then $r \leq [n/2]$, cf. c) above. Therefore E is irreducible. Set $E_0 = E_1 E_2 \dots E_{r-1}$ and consider an irreducible FE_0-submodule U of V. Now $[E_0, E_r] = \langle 1 \rangle$, see [1,11] again, so $Ux \simeq U$ as FE_0-module for all $x \in E_r$ and clearly $UE_r = UE = V$. Thus E_0 is homogeneous and therefore E_0 acts faithfully on U.
Suppose $dim_F(V/U) \geq 2$. By the minimal choice of n we have $r - 1 \leq (n-2)/2$ and hence $r \leq [n/2]$. Consequently $dim_F(V/U) \leq 1$. If $dim_F(V/U) = 1$, then since E_0 is homogeneous and U is irreducible we have $dim_F U = 1$. But then E_0 is diagonalizable and so abelian, which is false since $r > 1$. Hence $U = V$. But then $E_r \leq C_E(E_0) \leq F^*1_n$ (Schur's Lemma) and yet E_r is not abelian. This final contradiction completes the proof of f).

(g) The completion of the proof of Theorem 2.

Again set $E = E(G)$ and define $K \leq G$ by $S \leq K$ and $G/S = K/S \times ES/S$. By (e) and (f) we have $S < K < G$. Also $[K, E] \leq E \cap S \leq Z = F^*1_n \cap G$ by (d). Then K stabilizes the series $\langle 1 \rangle \leq Z \leq EZ$, so if $C = C_G(E)$, then $K' \leq C$. Hence $G = KEW = K'ES = CES$ and $C/(C \cap S)$ involves G/ES.

Neither E nor C is abelian. Thus if U is an irreducible FE-submodule of V, then V is a direct sum of copies of U by (d), so $1 < m = dim_F(U) < n$ and $n = mk$ for some integer $k < n$. Further, by (c), (d) and [9] 1.15 the group G is isomorphic to a subgroup of $(GL(m, F) \times GL(k, F))/A$, where A is a central subgroup of this direct

product. Since $m < n$ and $k < n$, by the choice of n we have $r \leq m/2 + k/2 \leq n/2$. This final contradiction completes the proof of Theorem 2. □

If S_q is a Sylow q-subgroup $GL(n, p)$, p prime, for some prime q, then rkS, is at most n if $2 < q \neq p$, is at most $[3n/2]$ if $q = 2 \neq p$ and is at most (less than if $n > 2$) $n(n-1)/2$ if $q = p$, see [10]. We define the integer function $s(n, p)$ of the positive integer variables n and p, p prime, as follows. Set $s(1, p) = 1$ and $s(2, 2) = 2$. If $p > 2$ set $s(2, p) = 4$, $s(3, p) = 5$ and $s(4, p) = 7$. For all other values of n and p set $s(n, p) = n(n-1)/2$. Notice that $s(n, p) \leq n + [n^2/2] \leq n^2$ for all n and p and $s(n, p) < [n^2/2]$ if $n > 3$ or if $p = 2 < n$.

Lemma 2 *We have $rk(GL(n, p)) \leq s(n, p)$ for all $n \geq 1$ and primes p.*

Proof Clearly $rk(GL(1, p)) = 1$ and $rk(GL(2, 2)) = rk(Sym(3)) = 2$, while $rk(GL(2, p)) \leq 4$; just check Dickson's list of the subgroups of $PSL(2, p)$, see [6] II.8.27. The theorem from [5,8] together with the results from [10] quoted above yield the lemma. □

It is easy to see that always $rk(GL(n, p)) \geq [n^2/4]$ and that $rk(GL(n, p)) \geq [3n/2]$ if $p > 2$. Lemma 2 is effectively the special case of the theorem where G is elementary abelian.

Proof of Theorem 1 Set $e = e(G)$. We induct on e. If $e \leq 1$ the claim is clear, so assume $e \geq 2$. We have to prove that $rk(Aut(G)) \leq e + [e^2/2]$. Suppose N is a characteristic subgroup of G with $\langle 1 \rangle < N < G$. There is an obvious homomorphism of $Aut(G)$ into the direct product of $Aut(N)$ and $Aut(G/N)$ with say kernel K, where by stability theory K is isomorphic to a section of $N^{e(G/N)}$, e.g. see [7] 1.C.3. Then $e(K) \leq e(N).e(G/N)$ and $e = e(N) + e(G/N)$. Induction on e now yields that

$$\begin{aligned} rk(Aut(G)) &\leq e(N) + [e(N)^2/2] + e(G/N) + [e(G/N)^2/2] \\ &\quad + e(N) \cdot e(G/N) \leq \\ e + (e(N) + e(G/N))^2/2 &= e + e^2/2. \end{aligned}$$

But $rk(Aut(G))$ is an integer, so $rk(Aut(G)) \leq e + e[e^2/2]$.

If no such N exists then either G is elementary abelian of rank e, when $rk(Aut(G)) \leq e + [e^2/2]$ by Lemma 2, or G is a direct sum of say t copies of a perfect simple group S. Assume the latter case. Now $d(S) = 2$, $rk(Out(S)) \leq 5$, $rk(S) \leq e(S)$ and $e(S) \geq 4$. Then $rk(Aut(S)) \leq e(S) + 5 < e(S) + [e(S)^2/2]$. This settes the case $t = 1$.

Assume $t \geq 2$. Then $Aut(G)$ is isomorphic to the wreath product of $Aut(S)$ by $Sym(t)$, where $Aut(G)$ permutes transitively the copies of S in the given direct decomposition of G. Therefore Lemma 1 yields that $rk(Aut(G)) \leq (e(S) + 5)t + 1 + [t/2]$. Now $e = e(S)t$, $e(S) \geq 4$, $t \geq 2$ and $e \geq 8$. Hence

$$rk(Aut(G)) \leq e + 5e/4 + e/8 + e/8 \leq 5e/2 \leq 5e^2/16.$$

The theorem follows. □

3 Final remarks

We conclude with a sketch of a proof of Lemma 2 and hence of Theorem 1 that uses Theorem 2 but avoids using [5,8]. Let G be a subgroup of $GL(n, p)$. As in the first sentence of the proof of Lemma 2 above we may assume $n \geq 3$. By results of Roggenkamp, see [3] 7.8, 7.9(i) and 7.20, there exists a Sylow subgroup S of G with $d(G) \leq pr(G) + 1 + rk(S)$, where $pr(G)$ denotes the presentation rank of G. Thus if $pr(G) = 0$ (e.g. if G is soluble, see [3] 6.9), then $d(G)$ is bounded using the bounds for $rk(S)$ in [10].

Let N denote the soluble radical of G. If $pr(G) \neq 0$, then $d(G/N) = d(G)$ by Theorem B(ii) of [4]. Clearly $H = G/N$ has trivial soluble radical. Then there exists a normal subgroup $E(H) = S_1 \times S_2 \times \ldots S_r = E$ say of H with $C_H(E) = \langle 1 \rangle$, where the S_i are perfect simple groups and $1 \leq r \leq n/2$ by Theorem 2. Now H permutes the S_i by conjugation. Applying the arguments from the final two paragraphs of the above proof of Theorem 1, but now to each orbit of H in this action, and using the weak bound $[n^2/4]$ in Lemma 1, whose proof does not use [5,8], we can again bound $d(G)$. Specifically we obtain $d(G) \leq 2t + 5r + [r^2/4]$, where t is the number of such orbits.

Using $1 \leq t \leq r \leq [n/2]$ we obtain $d(G) \leq n + [n^2/2]$ for all $n \geq 3$ except when $n = 4 = 2r$. If $n = 4 = 2r$ we only obtain in this way that $d(G) \leq 15 < n^2$. To obtain the better bound when $n = 4 = 2r$ we need a more delicate study of the simple groups S_1 and S_2. But in this elementary way we have at least bound $rk(GL(n, p))$ independently of [5,8] by n^2 always and by $n + [n^2/2]$ for all $n \neq 4$.

References

1. Aschbacher, M.: Finite Group Theory. Cambridge University Press, Cambridge (1986); re-issued (2008)
2. Curtis, C.W., Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. Wiley, New York (1962)
3. Gruenberg, K.W.: Relation Modules of Finite Groups. Regional Conference Series in Maths, vol. 25. American Mathematical Society, Providence (1976)
4. Gruenberg, K.W.: Groups of non-zero presentation rank. Symp. Math. **17**, 215–224 (1976)
5. Guralnick, R.M.: On the number of generators of a finite group. Arch. Math. (Basel) **53**, 251–253 (1989)
6. Huppert, B.: Endliche Gruppen I. Springer, Berlin (1967)
7. Kegel, O.H., Wehrfritz, B.A.F.: Locally Finite Groups. North-Holland, Amsterdam (1973)
8. Lucchini, A.: A bound on the number of generators of a finite group. Arch. Math. (Basel) **53**, 313–317 (1989)
9. Wehrfritz, B.A.F.: Infinite Linear Groups. Springer, Berlin (1973)
10. Wehrfritz, B.A.F.: The rank of a linear p-group; an apology. J. Lond. Math. Soc. **21**, 237–243 (1980)
11. Wehrfritz, B.A.F.: Finite Groups. World Scientific, Singapore (1999)
12. Wehrfritz, B.A.F.: Variants of theorems of Schur, Baer and Hall, Ricerche Mat, to appear