BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 15, Number 1, July 1986

ALMOST ALL p-GROUPS HAVE AUTOMORPHISM GROUP A p-GROUP

URSULA MARTIN

1. Introduction. Groups of prime-power order are tantalizing objects. On one hand they have a delicate and sophisticated combinatorial structure related to representations of $\mathrm{GL}(n,p)$ in characteristic p; on the other there are so many of them and their structure is so varied that any kind of classification seems hopeless and powerful general theorems are rare.

This paper is concerned with the proof that a random group of prime-power order has no automorphisms of order coprime to p. Although in the course of the proof we establish several new combinatorial results about finite p-groups, the result gives further evidence of the apparent structurelessness of groups of prime-power order. The result may not seem entirely plausible at first sight, since most groups of prime-power order with which we are familiar arise as subgroups of Chevalley groups or simple groups and admit automorphisms of order coprime to p. Indeed, apart from the dihedral group of order eight, the known examples of such groups are given by complicated and unnatural-looking constructions. Intuitively, what our result is saying is that most p-groups are complicated and unnatural-looking, and that the familiar examples are far from typical.

At the heart of our proof lies the combinatorics which links finite p-groups and representations of the general linear group $\mathrm{GL}(n,p)$. Isomorphism classes of abelian groups of order p^n correspond to partitions of n and Hall [**Ha**] showed that questions about these groups could be answered in terms of polynomials which form an algebra which can be identified with the algebra of symmetric functions. An account is given in [**Mac**]. Hall's polynomials can be used to give exact formulae for the number of subgroups of an abelian p-group and were used by Green [**Gr**] to determine the characters of the general linear group. In this work we extend Hall's results to give upper bounds for the number of normal subgroups of a nonabelian p-group, and use similar techniques to estimate the number of subspaces of a $\mathrm{GL}(n,p)$ module in characteristic p which are left invariant by no non-identity element of the group.

2. Statement of results. To state our results precisely we introduce some notation. For any prime p and group H the Frattini series is defined as

$$H_1 = H$$

and

$$H_{i+1} = H_i^p[H, H_i] \quad \text{for } i \geq 1.$$

Received by the editors October 11, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20E36, 20D15; Secondary 05A20, 20G40.

A p-group G is said to have Frattini length n if G_n is the last nonidentity term of its Frattini series. Then $G_2 = \Phi(G)$ is the Frattini subgroup of G, and G/G_2 is an elementary abelian p-group of rank d, the minimum number of generators of G. Any automorphism of G induces an automorphism of G/G_2, so we have an exact sequence

$$1 \to K(G) \to \operatorname{Aut} G \to A(G) \to 1,$$

where $K(G)$ is the subgroup of $\operatorname{Aut} G$ which induces the identity on G/G_2 and $A(G)$ is the group of automorphisms induced by $\operatorname{Aut}(G)$ on G/G_2. Then $K(G)$ has order a power of p, and $A(G)$ is a subgroup of $\operatorname{Aut}(G/G_2)$, which is isomorphic to $\mathrm{GL}(d,p)$. Thus if $A(G) = 1$, G has no automorphisms of order coprime to p. Our result is

THEOREM 1. *Let p be a prime, let $a_{d,n}$ be the number of d-generator p-groups of Frattini class n, and $e_{d,n}$ the number of these satisfying $A(G) = 1$. Then*

$$\lim_{d\to\infty} \frac{a_{d,n}}{e_{d,n}} = 1.$$

While our result shows that $A(G)$ is usually the identity, there is little restriction on what other values it can have. Bryant and Kovacs [**BK**] proved that if K is a subgroup of $\mathrm{GL}(d,p)$ for any $d > 1$ then there is a finite d-generator p-group G such that $A(G)$ is isomorphic to K and acts on G/G_2 as K. Even when a p-group is restricted to being of nilpotency class two, we have little control over its automorphism group. Webb [**We**] showed that if M is any finite graph satisfying a very weak technical condition then there is a finite p-group G of nilpotency class two with $A(G)$ isomorphic to $\operatorname{Aut} M$, which means that any finite group can occur as $A(G)$ in this case.

3. Description of proof. Our proof is based on an analysis of the structure of the quotients of the free group F on d generators by factors of its Frattini series. For any $n \geq 1$ the automorphism group of $H = F/F_{n+1}$ is an extension of a p-group by $A(H)$ which is isomorphic to $\mathrm{GL}(d,p)$: each factor $H_j/H_{j+1} \cong F_j/F_{j+1}$ becomes a $\mathrm{GL}(d,p)$ module in a natural way. For $j < p$ the module structure was described by Higman [**Hi**], but for $i \geq p$ the structure is not known in general. For example, F_2/F_3 is isomorphic to the direct sum of F/F_2 and its exterior square for odd p, and to a nonsplit extension of the exterior square by F/F_2 when p is 2.

Our theorem follows from the three results stated below. In Theorem 2 we establish a correspondence between d-generator p-groups of class n and orbits of normal subgroups of H under $\operatorname{Aut} H$. Theorem 3 shows that almost all these groups correspond to orbits under the action of $\mathrm{GL}(d,p)$ of subspaces of H_n. In Theorem 4 we show that almost all such orbits are regular ones, so that they correspond to d-generator p-groups with $A(G) = 1$. Taken together, these results prove Theorem 1.

To state the theorems precisely we introduce the following notation.

$A_{d,n}$:= the set of isomorphism classes of d-generator p-groups of Frattini class n;

$B_{d,n}$:= the subset of $A_{d,n}$ corresponding to subgroups of H which lie in H_n;

$b^*_{d,n}$:= the number of subspaces of H_n;

$C_{d,n}$:= the subset of $B_{d,n}$ consisting of groups with $A(G) = 1$;

s_d := the order of $\mathrm{GL}(d,p)$;

d_n := the Witt number $(1/n)\sum_{t|n} d^t\mu(n/t)$.

Then we have

THEOREM 2. 1. *$A_{d,n}$ bijects with the set of orbits of* $\mathrm{Aut}\, H$ *on normal subgroups of H which lie in H_2.*

2. *$C_{d,n}$ bijects with the set of regular orbits of* $\mathrm{GL}(d,p)$ *on subspaces of H_n.*

THEOREM 3. *Let $n \geq 2$ and*

$$w = -d_n^2 + d_{n-1} - d_n/2(n-1) + d_2/4.$$

Then

$$0 \leq \frac{|A_{d,n}|}{|B_{d,n}|} - 1 \leq O(p^w).$$

THEOREM 4. 1. *Let*

$$x = d^2 - d_n/2 \quad \text{if } n \geq 3$$

and

$$x = -d \quad \text{if } n = 2.$$

Then

$$1 \leq s_d \frac{|B_{d,n}|}{b^*_{d,n}} \leq 1 + O(p^x).$$

2. *Let*

$$y = d^2 - d_n^2/4 \quad \text{if } n \geq 3$$

and

$$y = -d \quad \text{if } n = 2.$$

Then

$$1 \leq \frac{|B_{d,n}|}{|C_{d,n}|} \leq 1 + O(p^y).$$

4. Proof of Theorems 3 and 4. We prove Theorem 3 by estimating the number of normal subgroups of H. To do this we first estimate in Theorem 5 the number of normal subgroups of fixed type of an arbitrary p-group, generalizing an old result about abelian p-groups. Our estimate depends on certain parameters which are difficult to work out in general, but are calculated for factors of the Frattini series of free groups in Theorem 6.

So let H be a finite p-group of Frattini class n. If U is a normal subgroup of H, let

$$U_i = U \cap H_i / U \cap H_{i+1} \cong (U \cap H_i)H_{i+1}/H_{i+1}$$

and let

$$A(\mathbf{u}) = \{U \lhd H \mid r(U_i) = u_i\},$$

where $\mathbf{u} = (u_1, \ldots, u_n)$ and the integers u_i satisfy

$$0 \leq u_i \leq d_i = r(H_i/H_{i+1}) \quad \text{for each } 1 \leq i \leq n.$$

The vector $\mathbf{u}$ is called the type of the subgroup U.

We have

THEOREM 5. *Suppose that for each* $U \in A(\mathbf{u})$

$$r(\Phi(U) \cap H_i/\Phi(U) \cap H_{i+1}) \geq v_i$$

and

$$r(U^p[H,U] \cap H_i/U^p[H,U] \cap H_{i+1}) \geq w_i.$$

Then

$$|A(\mathbf{u})| \leq \begin{bmatrix} d_1 \\ u_1 \end{bmatrix}_p \begin{bmatrix} d_2 - w_2 \\ u_2 - w_2 \end{bmatrix}_p \cdots \begin{bmatrix} d_n - w_n \\ u_n - w_n \end{bmatrix}_p p^x,$$

where

$$x = (u_1 - v_1)(d_2 - u_2) + \cdots + (u_1 + \cdots + u_{n-1} - (v_1 + \cdots + v_{n-1}))(d_n - u_n),$$

and

$$\begin{bmatrix} r \\ s \end{bmatrix}_q = \frac{(q^r - 1)\cdots(q^r - q^{s-1})}{(q^s - 1)\cdots(q^s - q^{s-1})}$$

denotes the number of s-dimensional subspaces of a vector space of dimension r over the field of q elements.

When H is a quotient of a free group F by F_n we obtain estimates for v_i and w_i in terms of the Witt numbers, and some further delicate combinatorial estimates give us Theorem 3.

The proof of Theorem 4 depends upon estimating the number of orbits of subspaces of $J_n = H_n/H_{n+1}$ under the action of $\mathrm{GL}(d,p)$, using the Cauchy-Frobenius lemma which states that if a group acts on a set the number of orbits is equal to the average number of elements left fixed by an element of the group. We do this by obtaining an upper bound for the number of subspaces of J_n normalized by an element of $\mathrm{GL}(d,p)$.

THEOREM 6. *Let $G = \langle g \rangle$ be a cyclic group and V a vector space of dimension n over the field of p elements on which G acts. Let m be the number of G-invariant subspaces of V. If g does not act on V as scalar multiplication then*

$$\log_p m \leq n^2/4 - n/2 + 6.$$

The number m is largest when g has order a power of p, and the theorem is proved by calculating m exactly in this case, by a method similar to that of Theorem 3.

REFERENCES

[**BK**] R. Bryant and L. Kovacs, *Lie representations and groups of prime power order*, J. London Math. Soc. **17** (1978), 415–421.

[**Gr**] J. A. Green, *The characters of the finite general linear groups*, Trans. Amer. Math. Soc. **80** (1955), 402–477.

[**Ha**] P. Hall, *The algebra of partitions*, Proc. Fourth Canadian Math. Congress (Banff, 1957), 147–149.

[**Hi**] G. Higman, *Enumerating p-groups.* I, *Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30.

[**Mac**] I. G. Macdonald, *Symmetric functions and Hall polynomials*, Oxford Mathematical Monographs, Oxford, 1979.

[**We**] U. H. M. Webb, *The occurrence of groups as automorphisms of nilpotent p-groups*, Arch. Math. (Basel) **37** (1981), 481–498.

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MANCHESTER, MANCHESTER M13 9PL, ENGLAND