J. Austral. Math. Soc. (*Series A*) **67** (1999), 356–379

SOME QUESTIONS ABOUT p-GROUPS

AVINOAM MANN

Dedicated to Mike (M. F.) Newman on the occasion of his 65th birthday

(Received 8 February 1999; revised 25 May 1999)

Communicated by E. A. O'Brien

Abstract

We present some questions that we feel are important and interesting for the theory of finite p-groups, and survey known results regarding these questions.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 20D15.

Mike, the other year you asked me how I saw the future of p-group theory. All I can offer in answer are more questions.

1. Enumeration

Most of the effort of finite group theory in the second half of this century was directed at the investigation of simple (non-Abelian) groups, and there are still many outstanding problems in that area. In the present paper I want to concentrate on groups that may be considered as the farthest removed from the simple ones, namely nilpotent groups, or, since a finite nilpotent group is the direct product of its Sylow subgroups, p-groups. Why consider these groups? Personally I find them fascinating, but that opinion is not shared by everyone. I have seen people, particularly ones concerned with simple groups, say that p-groups should be avoided. I think that this attitude is based on a misunderstanding. The kind of problems about p-groups that one may encounter during the investigation of finite simple groups would call for an exact determination,

An extended and thoroughly revised edition of a talk given on June 30th in the 4th Amitsur Memorial Symposium, Bar-Ilan University, June 29 – July 1st, 1998.

up to isomorphism, of a p-group satisfying certain properties. Such problems may be extremely hard, and I do not consider them typical of p-group theory. As we see below, there is a vast number of p-groups, and a complete classification of them does not seem feasible. But we still would like to put some order into this seeming chaos, and recent progress, much of it due to ideas of Mike Newman, indicates that this is possible.

Passing now to mathematical, not personal, reasons, one is that, as Sylow's theorem shows, p-groups are involved in all finite groups. Another reason may be the following conjecture formulated in [P2] (where a related conjecture of Erdös is reported), that I would rather pose as my first question.

QUESTION 1. Is it true that most finite groups are nilpotent?

If that is true, it follows that most finite groups are in fact 2-groups.

In precise terms, the conjecture is that if $g(n)$ is the number of all (isomorphism types of) groups of order at most n, and $g_{nil}(n)$ is the number of nilpotent groups of the same orders, then $\lim_{n\to\infty} g_{nil}(n)/g(n) = 1$. This conjecture is a sharpening of the following theorem of Pyber [P1].

THEOREM 1 (Pyber). $\lim_{n\to\infty} \log g_{nil}(n)/\log g(n) = 1$.

Thus attention is directed to the number of nilpotent groups, or better, to the number of p-groups. Denoting by $f(n)$ the number of groups of order n, we have the following result of Higman [H1] and Sims [Si].

THEOREM 2 (Higman and Sims). $f(p^k) = p^{(2/27)k^3+o(k^3)}$.

(The term $o(k^3)$ depends only on k, not on p.) As usual, I denote by $o(f(k))$ and $O(f(k))$, a function $g(k)$ such that $g(k)/f(k)$ tends to 0, or is bounded in absolute value, respectively, as $k \to \infty$. The constants involved, or the rapidity of the convergence, may be absolute or depend on some parameters of the situation, for example on p.

QUESTION 2. Why?

Of course, there is a proof, and once we go through it (not easy but certainly feasible) we see that even the constant 2/27 is not all that mysterious. Still one would like another, more conceptual, proof. Let me suggest two possible directions that such a proof might take. First, Higman, in [H1], derives lower bounds for $f(p^k)$ by showing that the number of p-groups of class 2 (more precisely, Frattini class 2, that is the Frattini subgroup is central and elementary) is given by the same formula as in Theorem 2. This leads to the problem.

QUESTION 3. Is it true that most p-groups are of class 2? Or, at least, that a positive proportion of all p-groups are of class 2?

A direct positive answer to this question would provide one of these 'better' proofs of Theorem 2, because the calculation of the number of groups of class 2 is not only easier, it is also conceptually clearer than the similar calculation for all p-groups. But why should we assume that a positive answer exists, apart from the fact that we know that it holds 'logarithmically'? Well, the structure of a p-group is determined to a large extent by its commutator function, that is the function associating to each pair of elements x, y their commutator $[x, y]$. For groups of class 2, this is an alternate bilinear function from one Abelian group to another. There is a lot of freedom in choosing such a function. But once the group has class at least 3, we have another severe restriction in the form of the Jacobi identity (called, in the group version, the Witt-Hall identity), and it would not be surprising if this reduces the number of possible groups considerably. Indeed to prove Theorem 2 we do not need such a sharp reduction as is indicated by Question 3. Proving the logarithmic analogue of a positive answer to Question 3 suffices.

In a subsequent paper [H2] Higman turned to the question how $f(p^k)$ depends on p, for a fixed k. Here recall that for $k \leq 4$ the number is independent of p (except that for $k = 4$ there are 15 groups for odd p and for $p = 2$ only 14), but starting with $k = 5$ the number tends to infinity with p. Also, the number of Abelian groups of order p^k is the number of partitions of k, and thus independent of k. Recently Blackburn [Bs] has shown that the number of p-groups G of order p^k satisfying $|G'| = p$ is also independent of p (but is considerably bigger than the number of Abelian groups of the same order). In [H2] it is shown that the number of groups of Frattini class 2, for a fixed k, is given by a particularly nice function, one that Higman calls PORC, standing for *Polynomial On Residue Classes*, that is one that takes on a value given by one of finitely many polynomials, the choice of the polynomial being determined by the residue of p to some modulus (such functions are also called quasi-polynomials). This raises another question of great interest:

QUESTION 4 (Higman). Is $f(p^k)$, for a fixed k, a PORC function?

In the few cases in which we know exactly the number of p-groups of a certain type (for example of orders up to p^6, and also of order p^7 and exponent p, see [Nw]), not only is the answer positive, but the finitely many polynomials involved differ from each other only in their constant terms. But I consider this evidence as being as yet too slim to base any conjectures on it.

The commutator function of a p-group gives rise to a nilpotent Lie ring, of the same size and class as the group, and variations on the construction yield Lie algebras over the field of p elements. A result similar to Theorem 2 holds for such algebras. But here there is an additional aspect. The Lie algebra structure on a vector space can be given by first choosing a basis in the space, then defining multiplication by specifying structure constants, and, finally, imposing on these constants equations ensuring that we indeed have a Lie algebra. If the dimension of the vector space is k, these equations define an algebraic variety in k^3-space. Now the analogue of Theorem 2 is the fact that the dimension of this variety is $(2/27)k^3 + o(k^3)$. This is true over any field [Nr]. It is an intriguing fact that the same asymptotic result holds for the dimension of the variety describing commutative associative algebras, while for associative algebras the coefficient becomes 4/27. It would be nice to be able to pass from the result on Lie algebras to the number of groups. This is the second possible proof of Theorem 2 that I alluded to above. The algebraic geometry approach raises immediately other highly interesting questions, such are what are the irreducible components of the variety of Lie algebras. There is some information about these questions in [KN] and [Nr], but I do not know of any attempt to translate them to group theory. The results of [H2] about PORC functions apply also to algebras.

QUESTION 5. How far can we improve the error term $o(k^3)$ in Theorem 2?

The aforementioned lower bound of Higman for groups of Frattini class two has the error term $-(4/9)k^2$, while Sims' proof establishes an upper bound with an error term $O(k^{8/3})$ (as $k \to \infty$), and this was improved to $O(k^{5/2})$ by Newman and Seeley (unpublished). It was pointed out by Shalev that if one can get $o(k^2)$ in the upper bound, or even $O(k^2)$ with the implied constant small enough, then Question 1 has an affirmative answer (oral communication; see also [Sh2, Proposition 2.1]).

We can enumerate groups in which some other invariant is constrained, not necessarily the class. Let $f(n, d)$ be the number of groups of order n and d generators. By results of McIver and Neumann and the author [MN, Mn1], we have.

THEOREM 3. $p^{c_0(d)k^2} \leq f(p^k, d) \leq p^{(1/2)dk^2+o(k^2)}$, *for some positive constant* $c_0(d)$.

Thus the following seems reasonable:

QUESTION 6. Is there a constant $c(d)$ such that $f(p^k, d) = p^{c(d)k^2+o(k^2)}$, and what is the value of this constant?

Failing an answer to that, or if the answer is negative, one would like at least to give good estimates for $c_0(d)$.

Combining Theorem 2 and Theorem 3 implies that for most groups G of order p^k the minimal number $d(G)$ of generators is at least $(4/27)k$. This suggests the following

QUESTION 7. Consider the set of groups G of order p^k as a probability space (with uniform distribution) and $d(G)/k$ as a random variable on this space. Does the distribution function of this variable have a limit as $k \to \infty$, and what is this limit distribution? In particular, what is the average (in the limit) of d/k?

Next, let $g(n, r)$ be the number of groups of order n that can be defined by r relations. Let also $r(G)$ be the minimal number of relations needed to define G. For any finite group G we have $r(G) \geq d(G)$, and if G is nilpotent, the Golod-Shafarevich inequality (Theorem 10 below) states that $r(G) > d(G)^2/4$. Therefore, Theorem 3 and its analogues for more general groups [Mn1], imply also upper bounds for $g(n, r)$, in particular we have $g(p^k, r) \leq p^{\sqrt{r}k^2}$. However, the following sharper result can be proved by applying simple probabilistic arguments regarding the Haar measure of free pro-p groups [Mn7]. (For more connections between group theory and probability, see for example [Sh3].)

THEOREM 4. *$g(p^k, r) = o(p^{kr})$, as $k \to \infty$.*

This shows that most groups of order p^k require at least $(2/27)k^2$ relations. Compare that with the Golod-Shafarevich inequality. As in the inequality, we can replace r in Theorem 4 by $r_p(G)$ (defined following Question 18), which is possibly smaller. It is likely that the methods of [Mn1] can establish also a lower bound $p^{c_1(r)kr}$ for $g(p^k, r)$. Of course, one can formulate questions analogous to Question 6 and Question 7 about $g(p^k, r)$ and about the ratio r/k.

Results similar to Theorem 4 hold for nilpotent groups (see [Mn7]).

In contrast to the situation when we count all p-groups, the number of p-groups of order p^k with a given class and a given number of generators is (at most) polynomial in the order, so we cannot have most, or even a significant fraction, of all groups with a bounded number of generators also with bounded class. But the number of groups of bounded number of generators and class is also interesting. Let $f(n, d, c)$ be the number of groups of order n, class at most c, and at most d generators. DuSautoy [dS] considered the generating function $\zeta_{c,d,p}(s) = \sum_k f(p^k, d, c)p^{-ks}$. This Dirichlet series defines an analytic function of s in some right half plane. But it can also be considered as a power series in $X = p^{-s}$. DuSautoy proved

THEOREM 5 (duSautoy). *$\zeta_{c,d,p}$ is, for fixed p, d, c, a rational function of p^{-s}.*

This is equivalent to the following.

THEOREM 5′. *The numbers $f(p^k, d, c)$ satisfy, for fixed p, d, c, and large k, a linear recurrence relation with constant coefficients.*

With some extra work Theorem 5 also implies.

COROLLARY 1 (duSautoy). *Fix p, d, c. There exist a a rational number α, a non-negative integer β, and a positive number γ, such that*

$$f(p^k, d, c) \sim \gamma p^{\alpha k} k^{\beta}.$$

Similar results are also proved for the number of nilpotent groups of bounded order, number of generators, and class.

Note that $f(p^k) = f(p^k, k, k-1)$. Thus the PORC conjecture is a requirement that these functions, regarded as a function of p for a fixed k, exhibit a certain type of uniform behaviour. In that direction the following is proved in [dS].

THEOREM 6 (duSautoy). *Given k, there exist finitely many polynomials $P_i(X)$ with integer coefficients, and systems $\mathbf{S}_i$ of polynomial equalities and inequalities with integer coefficients, such that for all but finitely many primes p:*

$$f(p^k) = \sum e_{k,p,i} P_i(p),$$

where $e_{k,p,i}$ is the number of solutions of $\mathbf{S}_i \pmod p$.

The proofs of these results apply, besides complex analysis, tools from model theory and algebraic geometry. Similar results were obtained earlier for a simpler generating functions, ones that count not groups of a given order, but rather subgroups, or normal subgroups, of certain infinite pro-p groups. The link between the present and the earlier results is that the p-groups with d generators and class at most c are exactly the finite factor group of the free pro-p group of class c and rank d. Such a generating function occurs also naturally in the proof of Theorem 4, though that proof is of a very different nature (and much easier) than the proofs of [dS].

Another natural question is: how many p-groups can be faithfully represented as permutation groups of degree n? In other words, how many p-subgroups does S_n contain, up to isomorphism? It is easy to see that the order of a Sylow p-subgroup of S_n is at most $p^{(n-1)/p}$, and it follows immediately that the number of subgroups of such a Sylow subgroup is at most $p^{(n-1)^2/p^2}$. On the other hand, it is shown in [PyS] that if $n = p^e$ is itself a prime power, then S_n contains at least $c^{n^2/\log n}$ pairwise non-isomorphic transitive p-subgroups. This still leaves a small gap between lower and upper bounds, and it will be of interest to fill this gap, and also to answer

QUESTION 8. How many p-groups does $GL(n, p)$ (or $GL(n, q)$, for q a power of p), contain, up to isomorphism?

2. Automorphisms

Let us return to Question 1. What reason is there to assume that the answer is yes, besides the numerical evidence provided by Theorem 1 and similar results? Much of the complexity of a finite group is provided by the interaction of p-subgroups, for different primes p, inside the group, while in a nilpotent group any such interaction is trivial. A non-trivial interaction means that a q-group acts non-trivially on some p-group G, where the primes p and q are distinct. This implies that the order of the automorphism group of G is divisible by q. Now a 'reason' for a positive answer to Question 1 is provided by the following result of Martin [Mr].

THEOREM 7 (Martin). *The automorphism group of 'most' p-groups is a p-group.*

It is unfortunate that the full proof of Theorem 7 was never published. Moreover, I have put 'most' in inverted commas, because this notion has a different meaning in [Mr] than we have given it in the previous section. Martin considers p-groups with a fixed number of generators and Frattini class, and 'most' for her, is inside this class. Thus the following is still open, where 'most' is interpreted, as in the previous section, in the class of all groups of a given order.

QUESTION 9. Is it true that for most p-groups the automorphism group is a p-group?

Martin's theorem at least provides lots of groups with this property. Using it, the following partial answer to Question 1 was given in [HP].

THEOREM 8 (Henn and Priddy). *'Most' p-groups P have the property, that if P is a Sylow subgroup of a finite group H, then H has a normal p-complement.*

Here 'most' has the same meaning as in Theorem 7.

The simplest way to produce automorphisms of any group is to consider inner automorphisms. For many groups, for example the symmetric groups, these are the only ones. But for our situation we have the following beautiful result [Ga].

THEOREM 9 (Gaschütz). *All p-groups have outer automorphisms.*

Moreover, except for the group of order p, the outer automorphism can be chosen to have order a power of p.

Various refinements of that result are known. In [Wb], in which Martin provides a particularly simple proof of Theorem 9, she shows that the outer automorphism in question can be chosen to act trivially on the centre. In [Sch] Schmid shows that usually the group of outer automorphisms contains a non-trivial normal p-subgroup. This shows that not all finite groups can occur as such an outer automorphism group. On the other hand Heineken and Liebeck have shown that, apart from a normal p-subgroup, the structure is arbitrary (see below).

Another question is how big is $\mathrm{Aut}(G)$, for G a p-group. It is known, for all finite groups, that $|\mathrm{Aut}(G)|$ tends to infinity with $|G|$. But how fast? In [Hy] it is shown that if $|G|$ is divisible by p^k (G need not be a p-group), then $|\operatorname{Aut}(G)|$ is divisible by, roughly, $p^{\sqrt{k}}$. It is even conjectured that if G is a non-cyclic p-group (not of order p^2) we have $|G| \mid |\operatorname{Aut}(G)|$. It is one of these conjectures that I do not know whether one should believe in or not. On the one hand I see no particular reason for belief, except that it holds in certain cases, and a counter example has not (yet?) been found, even though infinitely many p-groups are known for which $|\operatorname{Aut}(G)| = |G|$ ([NO1]; the examples there are for $p = 2$). On the other hand, I would not be surprised if it were proved even that $|\operatorname{Aut}(G)|$ is usually much bigger than $|G|$. Let me mention that for p-groups there is another standard way of constructing automorphisms. If ϕ is a homomorphism of any finite group G into $Z(G)$, whose square is 0, then $1 + \phi$ is an automorphism of G. Such an automorphism is termed *central*. A p-group always has non-trivial central automorphisms. Using variations of this construction it was shown, for example, that the above divisibility conjecture holds for groups of class 2 [Fa], or for groups satisfying the law $(xy)^p = x^p y^p$. This includes groups of exponent p [Dv]. On the other hand, Heineken and Liebeck showed that it is possible for all automorphisms of G to be central [HL]. More, the set of all central automorphisms is a normal p-subgroup of $\operatorname{Aut}(G)$, and it is shown in [HL] that the factor group over this subgroup may be assigned arbitrarily. Taking this factor group to be itself a p-group (for example trivial), we have many specific instances of Theorem 9, that is of groups with $\operatorname{Aut}(G)$ a p-group (the first such example occurs in [Mi], answering a question from [Hi, page 233]; the question was probably suggested by Burnside). These groups are of class 2. Elaborating these techniques, Heineken [He] constructed p-groups with all normal subgroups characteristic. So these groups behave as if they have only inner automorphisms. A striking construction was given by Bryant and Kovács [BK]. The Frattini factor group of a p-group can be considered as a vector space over the field of p elements. Then $\operatorname{Aut}(G)$ induces a certain linear group on this space. It is shown in [BK] that this group can be assigned arbitrarily, even as a linear group.

In addition to the question of how fast $\operatorname{Aut}(G)$ grows, let me mention some other questions, just to illustrate our state of ignorance about automorphisms. (I have no idea how difficult these questions are.) It is possible for a p-group to have outer automorphisms that preserve all conjugacy classes (which is the same as preserving all irreducible characters) [Sah]. Such automorphisms have a p-power order.

QUESTION 10. Do all p-groups have automorphisms that are not class preserving? If the answer is no, which are the groups that have only class preserving automorphisms?

QUESTION 11. The dihedral group of order 8 is isomorphic to its automorphism group. Are there other p-groups with this property?

More generally, let us consider the *automorphism tower* of a group G, that is the sequence G_i, where $G_1 = G$ and $G_{i+1} = \mathrm{Aut}(G_i)$, together with the homomorphisms mapping each group in the series into the next one, by mapping each element to the inner automorphism that it induces. What is the limit of this tower? In the example above, where G is dihedral of order 8, the limit is of order 2. If at some stage we reach a centreless group, a famous theorem of Wielandt guarantees that the series will become stationary after finitely many more steps, and then the limit is a finite group. But perhaps we should expect that 'generally' the limit is infinite?

QUESTION 12 (Berkovich). Can the non-inner automorphism in Theorem 9 be chosen to have order p?

3. Structural questions

One of the most significant achievements of p-groups theory in recent years was the formulation and subsequent proof of the *coclass conjectures*. These conjectures were formulated by Newman and Leedham-Green [LGN], who based them to some extent on the theory of groups of maximal class (developed by Blackburn [Bn] and continued by Shepherd [Sp], and Leedham-Green and McKay (see [LGM])), and proved by the joint efforts of several people, of whom Leedham-Green was the most prominent [LG]. Another proof was given by Shalev [Sh1]. The strongest of these conjectures states a paradox: if a p-group is of large class, it is virtually of small class. More precisely, if G has order p^n and class c, then G contains a subgroup H of class 2 (Abelian if $p = 2$) such that $|G : H|$ is bounded by some function of p and of the *coclass* $n - c$ (groups of coclass 1 are the same as groups of maximal class). To explain this paradox, consider a very simple example: the dihedral group of order 2^n is a 2-group of maximal class. But this group contains a cyclic subgroup of index 2. It is easy to construct also for odd primes p-groups of maximal class which contain Abelian subgroups of index p. More generally, using so-called *p-adic crystallographic groups*, we can construct groups of small coclass containing big Abelian subgroups. Thus these groups are very close to being Abelian. The intuition behind the coclass conjectures is that these examples are typical. As I said, the conjectures are theorems now, and the proof by Shalev even gives explicit bounds for the index of the class two subgroup. Both proofs provide more information on the structure of groups of small coclass. Such groups have a small normal subgroup such that the factor group over it is obtained by 'twisting' an extension of an Abelian group by another small group. Thus these groups have a reasonable theory, and the work on elaborating this theory is continuing. In this theory, all p-groups of a given coclass are considered as the vertices of a directed graph, and there is an arrow from H to G if $cl(G) = c$ and $G/\gamma_c(G) \cong H$. The theory shows that this graph is the union of finitely many trees, so most groups belong to infinite trees. In such an infinite tree there is a unique infinite 'trunk', from each of whose vertices finitely many finite branches can still grow. There are some results, and some highly intriguing conjectures, on the nature of these finite branches (see [Nw, NO2]). One of these conjectures was recently proved by duSautoy [dS]. His theorem states that for $p = 2$, the trees are ultimately periodic. More generally, for any p, if we trim the trees, that is cut the branches at some (fixed but arbitrary) distance from the trunk, the resulting tree is (ultimately) periodic. For $p = 2$ all the branches have a bounded length to begin with, so the trimming is unnecessary, but this is not the case for the odd primes. Other conjectures estimate how far we have to go up (or down—these trees are often drawn as growing downwards—Mike claims that this is a peculiarity of the northern hemisphere), the trunk to find the periodic behaviour, and how big are the period and the branches. The proofs of [dS] employ again, as in his enumeration results mentioned in Section 1, generating functions.

Let us pass to other questions. You have noticed that the coclass theory relates groups of large class with ones of small class. But it is possible that most difficulties arise with groups of middle class (as I have said elsewhere, this is not (or not necessarily) a sociological statement). I will present several problems about more general groups. Note that if G has small coclass, most of its central factors G_i/G_{i+1}, or more generally factors $N/[N, G]$, where N is any normal subgroup, have order p.

QUESTION 13 (Leedham-Green). Study groups in which most central factors have small order.

Such groups are said to have *small width*, see [KLGP].

While the class (or coclass) of a p-group is probably its most important commutativity invariant, its derived length $\mathrm{dl}(G)$ is also interesting. So let me state.

QUESTION 14 (Burnside and Hall). What is the minimal order of a p-group of derived length k?

Hall showed that if $|G| = p^n$, $\mathrm{dl}(G) > k$, then $n \geq 2^k + k$, and this can be improved slightly to $n \geq 2^k + 2k - 2$ [Mn4]. On the other hand, Hall gave examples showing that n can be as small as $2^{k+1} - 1$, and this was recently improved to $2^{k+1} - 2$ [ERNS], so you see that closing the still remaining gap is not easy. For low values of k, we know that the minimal order is p^3 for $k = 2$ (this is probably due to Hölder [Ho]), p^6 for $k = 3$ and $p \geq 5$, p^7 for $k = 3$ and $p = 2, 3$ [Bn], and for $k = 4$ the minimum order is p^{14} for $p \geq 5$, and either p^{13}, p^{14} or p^{15} for $p = 2, 3$ (see the theses of Blackburn and Evans-Riley; the remaining ambiguity for $p = 2, 3$ will probably be settled by a computer calculation.)

QUESTION 15. What is the structure of the minimal groups of the previous question? Do they have a nice theory, like the ones of maximal class have?

I want next to discuss extensions. Hall proposed constructing p-groups recursively, obtaining G as a central extension of $G/Z(G)$. Thus he termed a group *capable*, if it can be the central factor group of some group. Capable groups are exactly the ones that can occur as the group of inner automorphisms of some group. The capability of a given group can be determined by looking at its covering groups. Recall that H is a *covering group* of G (also called a *representation group*), if $G \cong H/N$, where $N \leq H' \cap Z(H)$, and H has maximal order among such extensions. Covering groups exist. They need not be unique, but the kernel N is uniquely determined, and is called the *Schur multiplier* of G, denoted $M(G)$. It can also be characterised homologically. The group G is capable if and only if, given any covering group H of G, the equality $Z(H) = M(G)$ holds.

I consider it useful to widen the notion of capability. Let us call a group G *adequate*, if there exists a group H such that $G \cong H/N, N \leq Z(H)$, and $\mathrm{cl}(H) > \mathrm{cl}(G)$. Capable groups are adequate, but there are others. For example any non-cyclic Abelian p-group is adequate, but not all of them are capable. Again adequacy can be determined by means of covering groups: G is adequate if and only if its covering groups have class $\mathrm{cl}(G) + 1$. Another way is by means of the *unicentre*. If H is a covering group of G, identify G with $H/M(G)$, and write $U(G) = Z(H)/M(G)$. I call $U(G)$ the *unicentre* of G (it has also been denoted $Z^*(G)$, and called the *epicentre*). Then G is capable if and only if $U(G) = 1$, and it is adequate if and only if $\gamma_c(G) \not\leq U(G)$, where $c = \mathrm{cl}(G)$ (so $\gamma_c(G)$ is the last non-trivial term of the lower central series of G).

Adequacy appears to be a much less demanding requirement than capability, and I expect that most p-groups enjoy this property. It is desirable to investigate further this notion, as well as obtain more information on capable groups and related concepts. Some results appear in [LMMW] (where non-adequate groups are called *absolutely nilpotent*), for example the central product of a non-Abelian p-group by itself is not adequate. Also, if G and G/N have the same class, and G is not adequate, neither is G/N. A two generated p-group of class two that is not metacyclic is adequate.

QUESTION 16. Give non-trivial criteria for a p-group to be adequate. In particular, elaborate and prove the claim about 'most' groups above.

Let me mention a couple of related notions. They relate to a possible isomorphism $G \cong H/\gamma_c(H)$. A group G is *terminal*, if such an isomorphism is possible only if $\gamma_c(H) = 1$. The non-terminal groups are adequate. In the language of trees that was used above for the coclass theory, the terminal groups are the extreme points ('leaves') of the tree. Further, G is *settled*, if the isomorphism above implies that G and H have the same coclass. An important result in the coclass theory is that groups of a given coclass and large enough order are settled. It is desirable to investigate all these concepts, and relations between them, further.

Having mentioned the Schur multiplier, the following famous problem is still wide open.

QUESTION 17. Which p-groups have trivial Schur multiplier?

As is well known, this is related to problems about defining relations. Recall that $d(G)$ denotes the minimal number of generators of G, and that $r(G)$ is the minimal number of its defining relations. Then $d(M(G)) \leq r(G) - d(G)$.

QUESTION 18. Is this inequality an equality?

Another way of putting this question is to consider $r_p(G)$, the minimal number of defining relations needed if we are also given the information that G is a p-group. (In other words, $r_p(G)$ is the number of relations needed to define G in the variety of pro-p groups.) Then Question 18 is equivalent to the following

QUESTION 18′. Is $r(G) = r_p(G)$?

A famous result about defining relations is the following (see [DDMS, interlude D]).

THEOREM 10 (Golod and Shafarevich). *Let G be a finite p-group. Then*

$$r_p(G) > d(G)^2/4.$$

This implies that a p-group with a trivial Schur multiplier has at most three generators.

QUESTION 19. What is the minimum of $r(G)$, or of $r_p(G)$, for a given $d = d(G)$? In particular, is the Golod–Shafarevich inequality the best possible?

The Golod–Shafarevich inequality has been shown to be the best possible for $d \leq 6$ [NSW]. Moreover, the minimum of $r_p(G)$ is at most $d^2/4 + d/2 - (7 + (-1)^d)/8$, [Ws, Sa]. There are similar results for Lie algebras, but a strange situation described in [NSW] for $d = 5$ suggests that surprises are possible here.

In a completely different direction, let me say a few words on Abelian subgroups. Since the structure of finite Abelian groups is known and simple, it is desirable to, first obtain information on Abelian subgroups of a p-group, and second, to exploit this information to study the ambient group. Considerable progress was achieved recently by Alperin and Glauberman ([Gl2, AG]). Some of their results are summarised below.

THEOREM 11 (Alperin and Glauberman). *Let the p-group G contain an elementary Abelian subgroup of order p^n. Then G contains a normal elementary Abelian subgroup of the same order under any one of the following assumptions*:

(i) *p is odd and $p > 4n - 7$;*
(ii) $\mathrm{cl}(G) \leq p$;
(iii) $\exp(G) = p$ *and* $\mathrm{cl}(G) \leq p + 1$.

Moreover, assuming only $p \geq 5$, G contains an elementary Abelian subgroup of order p^n which is 2-subnormal.

In [Gl2] a certain partial order is defined on subgroups of a p-group G. Let $\{Z_i\}$ be any central series of G. Then the subgroup A precedes B under that partial order if and only if $|A \cap Z_i| \leq |B \cap Z_i|$ for each i.

THEOREM 12 (Glauberman). *Let G be a p-group, and among the Abelian subgroups of G of maximal order consider the ones that are maximal under the partial order just described. If $p \geq 5$, then any two such subgroups normalise each other. In particular, they are 2-subnormal.*

The last claim has the following corollary.

COROLLARY 2. *Let a p-group G, $p \geq 5$, have an Abelian subgroup of index p^n. Then* $\mathrm{dl}(G) \leq 2 \log n$.

An interesting special case was recently noted by Sanders and Wilde ([Sn, SW]; another proof was given by Berkovich [private communication]): If a p-group G, p odd, contains a cyclic subgroup of index p^n, then $\mathrm{cl}(G) \leq 2n$. The upper bound can often be reduced to n, which, if it holds generally, would be the best possible. It was remarked by Shalev that if we replace 'cyclic' by 'Abelian of rank $p - 2$ at most' we still get a bound on the class in terms of n and p. Indeed in both cases we get more: the index of the centre is bounded. The groups of maximal class show that we cannot allow rank $p - 1$.

The paper [Gl2] provides further ways in which these remarkable subgroups occurring in Theorem 12 are close to being normal, some of them requiring only that p be odd, and derives applications for general finite groups. These applications employ a certain characteristic subgroup of G, which is generated by some of the maximal Abelian subgroups just discussed. This subgroup is similar to previous ones that were also defined by Glauberman, such as $J(G)$, generated by all Abelian subgroups of the maximal order, and so on. It is an intriguing question whether these subgroups can also be employed to study the p-groups themselves, not just their embedding in larger finite groups. Also the dependence of these subgroups on the particular central series chosen to define the partial order should be considered. Another natural problem, less vague, is:

QUESTION 20. Extend the above results to small primes.

A noteworthy feature of [Gl2] and [AG] is their use of the results of Lazard on the equivalence of p-groups of small class and Lie algebras of the same class [L]. Much earlier, using elementary counting techniques, Konvisser and Jonah [KJ] showed that if a p-group, p odd, contains an Abelian, or elementary Abelian, subgroup of order at most p^5, it contains a normal Abelian, or elementary Abelian, subgroup of the same order. Berkovich [B1] has given examples showing that this is no longer true for order p^7; I am not sure what happens at order p^6. Gillam [Gi] showed that if a metabelian p-group contains any Abelian subgroup, it has a normal Abelian subgroup of the same order. [KJ] also includes another proof of an earlier result from [Al], that if a p-group, p odd, contains an Abelian subgroup of index p^3, it contains a normal Abelian subgroup of the same index (the case of index p^2, which holds also for $p = 2$, is easy). The examples of Berkovich just mentioned have index p^4. But in these examples $p = 5$. So we can still ask

QUESTION 21. Are there results analogous to Theorem 11 where the restrictions are not on the order, but rather on the index of Abelian subgroups?

Subgroups of class two have also found their uses, see for example [Gl1, Bi]. Let us define the *rank* $\mathrm{rk}(G)$ of a group G as the maximal value of $d(H)$ for all subgroups H of G. It is known that for odd primes, $\mathrm{rk}(G)$ is realized by a group of class two [Lf]. Following [Ka], let us call G *d-maximal*, if $d(G) > d(H)$ for all proper subgroups H of G. Thus d-maximal p-groups are, for odd p, of class two.

QUESTION 22. What is the structure of d-maximal 2-groups? Do they have bounded derived length?

See [Ka] for some partial results. The following is a special case of a problem raised in [P3].

QUESTION 23 (Pyber). Does there exist an $\epsilon > 0$ such that each p-group G contains a subgroup of class two and order at least $|G|^\epsilon$?

What about subgroups of still higher class? It is easy to see that a non-Abelian p-group contains subgroups of class (exactly) two. It was proved by Macdonald [Mc] that a p-group of class more than two always contains subgroups of class three. In the same paper he constructs, for each prime $p \geq 5$, p-groups of class 6 all of whose proper subgroups are of class at most three. His examples are of order p^{11}, have two generators and derived length 3. He also shows that such examples are impossible for metabelian groups. The situation for the small primes remains unclear.

QUESTION 24. Given $k > 3$, is there a number $n = n(k)$ such that all p-groups of class at least n contain subgroups of class k?

Changing direction again, let me mention *powerful* p-groups, a class of groups that has found many applications in recent years, for example in Shalev's proof of the coclass conjectures; also in the proof of Theorem 13 below. A p-group G is *powerful*, if $G' \leq G^p$ (for $p = 2$, if $G' \leq G^4$) The name *powerful* was chosen to indicate that the groups contain many pth powers. For their theory, see [DDMS]. These groups have many nice properties, and can often be used to replace Abelian subgroups, which are less available. One similarity to Abelian groups is that if G is powerful, and $H \leq G$, then $d(H) \leq d(G)$. Thus $\mathrm{rk}(G) = d(G)$. A sort of converse is the fact that if $\mathrm{rk}(G) = r$, then G contains a characteristic powerful subgroup H satisfying $|G : H| \leq p^{r(\log_2 r+1)}$ (for $p = 2$ the bound is $p^{r(\log_2 r+2)}$).

QUESTION 25. Can we improve the last inequality? Specifically, can we get rid of the $\log r$ factor in the exponent?

It was shown by Lubotzky that every p-group is involved in some powerful p-group, that is it is isomorphic to a factor group of a subgroup of a powerful group ([DDMS, Example 2.16, page 51]). But we still have only partial results on the following.

QUESTION 26. Which p-groups are subgroups of powerful p-groups?

In [PF] it is noted that if $G/Z(G)$ is powerful (for example if $\mathrm{cl}(G) = 2$), then G can be embedded in a powerful p-group H in such a way that $H = GZ(H)$. This applies in particular to p-groups (p odd) with a cyclic derived subgroup.

A class of groups which is, in some sense, 'dual' to powerful groups is the class of *p-central* groups. A p-group G is p-central, if all elements of order p lie in $Z(G)$ (for $p = 2$, all elements of order 2 and 4). These groups have some properties analogous to those of powerful groups, for example a nice power structure, but they have not yet found as many uses as powerful groups have, though it often happens that when we look for powerful subgroups, the ones we find are both powerful and p-central. This is the situation for the characteristic subgroup mentioned just before Question 25. The rank of a p-central group is equal to $d(Z(G))$. The question analogous to Question 26 is to characterise factor groups of p-central groups.

I close this section with a question involving upper central series. A maximal subgroup M of a p-group G is *exceptional at the ith level*, if there exists an index k, such that the inclusion $Z_i(L) \leq Z_k(G)$ holds for all maximal subgroups L of G, except for M, and M is *exceptional*, if it is exceptional at some level. See [Mn3] for the motivation for this definition. Groups of small coclass have exceptional subgroups.

QUESTION 27. Study the p-groups without exceptional maximal subgroups.

(This problem is quoted from [Mn3]. The answer to the extra question formulated there is trivially 'yes'.)

4. Representations and conjugacy classes

It is well known that all irreducible characters of a p-group are monomial, that is, induced from a linear character of some subgroup. However, despite this nice starting point, the representation theory of p-groups was not developed much beyond that. Isaacs and Passman have written an important series of papers on this topic, for example they determined the groups in which all non-linear irreducible characters have the same degree, and discussed groups with bounds on the degrees of their characters (see [I1, Chapter 12], and the further references given there). From time to time other interesting articles appear, but there is no systematic theory. Nor is it easy to point at some specific problems to be answered here. What I would like to see is not only a theory of characters of p-groups, but even more, applications of such a theory. Below I describe some of the results known to me, and formulate some questions.

Conjugacy classes are in some sense dual to characters, and we can formulate for both classes and characters similar questions. It is known that both the set of character degrees of a p-group, and the set of conjugacy class sizes, can be arbitrarily given (except that, trivially, both sets have to include the number 1), even for groups of class two [I3, CH]. But suppose we know either of these sets or even both; what can we say about the groups? On the one hand, there are examples showing that two p-groups can have even the same character table and still be of different derived lengths [Mt]. But some information is available. The character table does determine the class of G. Further, a group having n different character degrees has derived length at most n. If all these degrees are bounded above by p^e, then it is shown in [IP] that G contains an Abelian subgroup of index bounded by p^{4e}, and then the Corollary to Theorem 12 gives a bound for the derived length which is often much better than n.

QUESTION 28. Suppose that the p-group G has n distinct sizes for its conjugacy classes. Can we bound the derived length of G in terms of n?

Should we try to be bolder and bound even the class? I have already pointed out that for each order (and each prime) there exist p-groups of maximal class and an Abelian subgroup of index p. The only character degrees for such a group are 1 and p, the class sizes are 1, p, and $|G'|$, but the class is arbitrary. Thus we usually cannot bound the class in terms of the number of character degrees or of class sizes. However, if G has for its character degrees the numbers 1 and p^k, with $k > 1$, then $\mathrm{cl}(G) \leq p$ [IP]. Presumably there are other sets of powers of p such that, if they are the character degrees of some p-group, the class of that group is bounded. For class sizes, let us write the maximal class size as p^b ($b = b(G)$ is known as the *breadth* of G; more generally, if x has $p^{b(x)}$ conjugates, $b(x)$ is termed the *breadth* of x). Then $\mathrm{cl}(G) \leq (5/3)b+1$ [C]. If we assume only that G is generated by elements of breadth

https://doi.org/10.1017/S1446788700002068 Published online by Cambridge University Press

b, then $\mathrm{cl}(G) \leq b^2 - b + 1$ (for $b > 1$; this is a slight improvement of [VLW]). But the best possible bounds are not yet known.

Returning to Question 28, let us consider the extreme case: what is the structure of p-groups in which all non-central classes have the same size? This question seems to be surprisingly hard. It is known that in such groups $G/Z(G)$ has exponent p ([I5]; see also [Mn5] and [V]), but is the class (or even the derived length) bounded? If the group is metabelian, it has class three at most (Heineken; see [V]); are there similar results for higher derived lengths?

So far I referred mostly to the class and derived length, but another commutativity invariant closely linked to questions about characters and classes is the size of a maximal Abelian section, and there is still enough to be done in clarifying the relationships between the various numerical invariants involved.

I have mentioned that the degrees of the characters, or the class sizes, can be assigned arbitrarily. But this is not so if we also want to specify the number of characters (classes) of each degree. To be specific, let the p-group G have a_i conjugacy classes of size p^i, and b_i irreducible characters of degree p^i. We can ask to characterise the vectors of non-negative integers that can occur as (a_i), or as (b_i), for some non-Abelian p-group, or even characterise the pairs of vectors that can occur as the pair (a_i), (b_i) for some such group. But I am not at all sure that these questions have reasonable answers. Perhaps we should be content just to look for some nice necessary, or sufficient, conditions, that these vectors have to obey. It is known that if a group G has the same character degrees, with the same multiplicities, as a nilpotent group, then G is nilpotent (Isaacs [I2]) and the analogous result for class sizes also holds (Cossey and Hawkes, [CHM]).

Other questions deal with the number of classes, which is also the number of characters. For example, Berkovich has determined the groups with only a few non-linear characters [BZ, 3.50], and, motivated by that, I have considered *minimal* characters, that is non-linear irreducible characters of least degree [Mn2], while minimal classes are discussed in [LMM].

For the number of classes a nice formula was found by Hall. Let $k(G)$ be this number, and write $|G| = p^n$, $n = 2m + e$, $e = 0$ or 1. Then

$$k(G) = 1 + e(p-1) + m(p^2-1) + s(p-1)(p^2-1)$$

for some non-negative integer $s = s(G)$. It is known that if $s = 0$, then G is of maximal class, $n \leq p + 2$, and if $p \geq 11$, then $n \leq p + 1$. These bounds are sharp [FS]. Recently this was extended by Jaikin-Zapirain to all values of s [JZ].

THEOREM 13 (Jaikin-Zapirain). *There are only finitely many p-groups with a given value of $s(G)$.*

https://doi.org/10.1017/S1446788700002068 Published online by Cambridge University Press

Let me remark that assumptions about conjugacy classes do not lend themselves easily to inductive treatment, and this leads to difficulties in handling them.

Character values are of much interest in representation theory. Let G be a p-group, and let F be the field obtained by adjoining to the rational field $\mathbb{Q}$ all values of irreducible characters of G. If $p = 2$, let F contain also $\sqrt{-1}$. Then all irreducible representations of G can be written in F. Moreover $F = \mathbb{Q}(\epsilon)$ where ϵ is a primitive p^r-th root of unity, for some r [Fe, Section 14]. Here p^r is bounded above by the exponent of G, and below by the exponents of $Z(G)$ and of G/G'.

QUESTION 29. Investigate this 'representation exponent' p^r.

Some questions in representation theory are special to the prime 2. For example.

QUESTION 30. What are the 2-groups all of whose characters are rational valued? Or real? Or have Frobenius-Schur indicators equal to 1?

Of course, one answer is that the characters are real if and only if each element is conjugate to its inverse, and they are rational if and only if any two elements generating the same subgroup are conjugate. But is this the most that one can say? Anyway I am not familiar with any answer to the third part of Question 30.

In [T] it is shown that for odd p, the character ring of a p-group is isomorphic to the centre of its group ring (this centre is spanned by the class sums), but this can be false for 2-groups. So for which 2-groups does it hold? The rational ones are one family. As in other contexts, it seems that the difference between 2 and the odd primes arises because the automorphism group of a cyclic 2-group is not cyclic. Another curious question is suggested by [FT], where Frame and Tamaschke have shown that in each finite group the product of the orders of the centralisers of cyclic subgroups, taken one only from each conjugacy class of cyclic subgroups, is either a square or twice a square. In [Dd] an example is provided of a group of order 32 in which the above product is not a square. Can one determine the 2-groups of this type? Again in a rational group the product is a square. Intriguingly, the example in [Dd] is the smallest example occurring in [T].

Some interesting special groups have been investigated. Pálfy and Szalay [PaS] have obtained a lot of information about the character degrees and class sizes (and also about the orders of elements) of P_n, the Sylow subgroup of the symmetric group S_{p^n}. For example they show the existence of two constants $c = c(p) \sim 1 - 2/p$ and γ (independent of p) such that

$$k(P_n) = \lfloor c|P_n|^{\gamma} \rfloor.$$

For the Sylow subgroup $P(n, q)$ of the general linear group $GL(n, q)$, where q is a power of p it has been conjectured that $k(P(n, q))$ is, for a fixed n, a polynomial in q [Kr]. These polynomials have been calculated for $n \leq 8$ by Vera-López [VA] and his colleagues. The character degrees of both P_n and $P(n, q)$ were determined by Huppert [Hu], applying for the latter a result of Isaacs [I4], that the relevant degrees are powers of q. (The analogous result for the Sylow subgroups of other classical groups does not always hold.) Some results on classes and characters of $P(n, q)$ are given in [Kr], which applies methods of algebraic geometry. In particular there is a proof there that $k(P(n, q))$ is a polynomial. However, counter examples to some of the results of [Kr] are given in [IK], so it is not clear if the above proof is valid. I am grateful to A. Melnikov and Thompson who drew my attention to these papers.

In closing this section, I allow myself to deviate from p-groups and pose a question about Lie algebras. It is easy and well known that, in any finite group G, the product $k(G)|G|$ equals the number of commuting ordered pairs of elements in G. (This is a special case of the orbit lemma of permutation group theory.) But this number of commuting pairs can be counted in any algebraic system. In particular, let L be a finite Lie algebra, and let $\mathrm{cm}(L)$ be the number of commuting ordered pairs of elements of L. Unlike the case of groups, the quotient $\mathrm{cm}(L)/|L|$ is usually not an integer, as easy examples show. But in all examples of *nilpotent* Lie algebras that I was able to check (not many) the quotient is an integer. So let me state, as a digression,

QUESTION L. Is it true that in all finite nilpotent Lie algebras the above quotient is an integer?

If the answer is yes, then for this quotient a formula similar to Hall's for $k(G)$ holds. This question was noted also in the Master's Thesis of B. Szegedy, who obtained for it partial results similar to ours, for example the answer is yes if the nilpotency class of L is no bigger than the characteristic.

5. Conclusion

It should be obvious that the above list of results and problems is far from comprehensive (the list in [B2] has hundreds of entries), and reflects my own (necessarily individual) taste, (necessarily limited) knowledge, and (unfortunate) prejudices. I have not mentioned, say, automorphisms with a few fixed points (see [Kh2, Sh2]), nor have I touched on the power structure of p-groups (see [Xu, Mn6, Mn8]), or on cohomology. Originally I was going to have a section on the Burnside Problem, but since this issue has an article by Vaughan-Lee and Zel'manov on that subject, such a section would have been both superfluous and presumptuous. I will just mention that while Zel'manov's celebrated solution of the Restricted Burnside Problem deals with groups of a given exponent, some results can be proved under the slightly weaker assumption that our group has many elements of a given order. For example in [MM1] it is deduced from Zel'manov's theorem that if G (any finite group) has many elements of order dividing n, then G has exponent n; exactly how many is 'many' here depends on both n and the number of generators of G. Other variations state that a p-group G with d generators has its order bounded in terms of p and d, under either of the following assumptions: the Hughes' subgroup $H_p(G)$, generated by all elements of G not of order p, has index at least p^2 (see Khukhro's book [Kh1]), or: more than $1 - 1/(3^p - 1)$ of the elements of G have order p (this follows from the results of [MM2] together with Kostrikin's solution of the Restricted Burnside Problem for prime exponent). In the first case, Khukhro also shows that the exponent of G is bounded in terms of p only, independently of d.

In a similar vein we have the following.

QUESTION 31. Let the p-group G be a transitive subgroup of S_n. Suppose that all fixed-point-free elements of G have order p. Does G have exponent p?

See [MP] and [HKKP] for the origin of this problem and partial results. In the latter paper it is shown that a group satisfying the assumptions of Question 31 has its exponent bounded by a function of p only.

Finally, recall that the original Burnside problem is still open for small exponents, for example we have.

QUESTION 32. Are all finitely generated groups of exponent 5 finite?

Acknowledgment

I am indebted to many people, in particular to Mike Newman, and also to the referee and the editor, for some very helpful comments on earlier drafts and for communication of results prior to publication. For other collections of problems about p-groups, see [B2] and [Sh2].

References

[Al] J. L. Alperin, 'Large Abelian subgroups of p-groups', *Trans. Amer. Math. Soc.* **117** (1965), 10–20.

[AG] J. L. Alperin and G. Glauberman, 'Limits of Abelian subgroups of finite p-groups', *J. Algebra* **203** (1998), 533–566.

[B1] Ja. G. Berkovich, 'Subgroups and normal structure of a finite p-group', *Soviet Math. Dokl.* **12** (1971), 71–75.

[B2] Y. Berkovich, 'Groups of prime power order', in: *Finite groups* (Y. Berkovich, L. Kazarin and E. Zhmuď) in preparation.

https://doi.org/10.1017/S1446788700002068 Published online by Cambridge University Press

[Bi] A. Bialostocki, 'On the other $p^\alpha q^\beta$ theorem of Burnside', *Proc. Edinburgh Math. Soc.* **30** (1987), 41–49.

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

[Bn] N. Blackburn, 'On a special class of p-groups', *Acta Math.* **100** (1958), 45–92.

[Bs] S. R. Blackburn, 'Groups of prime power order with derived subgroup of prime order', Technical Report.

[BZ] Ya. G. Berkovich and E. M. Zhmuď, *Characters of finite groups 1* (Amer. Math. Soc., Providence, 1997).

[C] M. Cartwright, 'Class and breadth of a finite p-group', *Bull. London Math. Soc.* **19** (1987), 425–430.

[CH] J. Cossey and T. Hawkes, 'Sets of p-powers as conjugacy class sizes', *Proc. Amer. Math. Soc.* to appear.

[CHM] J. Cossey, T. Hawkes and A. Mann, 'A criterion for a group to be nilpotent', *Bull. London Math. Soc.* **24** (1992), 267–270.

[Dd] E. C. Dade, 'Products of orders of centralizers', *Math. Z.* **96** (1967), 223–225.

[Dv] R. M. Davitt, 'The automorphism group of finite p-Abelian p-groups', *Illinois J. Math.* **16** (1972), 76–85.

[DDMS] J. D. Dixon, M. P. F. duSautoy, A. Mann and D. Segal, *Analytic pro-p groups*, 2nd edition (Cambridge University Press), to appear.

[dS] M. P. F. duSautoy, 'Counting p-groups and nilpotent groups', Technical Report.

[ERNS] S. Evans-Riley, M. F. Newman and C. Schneider, 'On the soluble length of groups with prime-power order', *Bull. Austral. Math. Soc.* **59** (1999), 343–346.

[Fa] R. Faudree, 'A note on the automorphism group of a p-group', *Proc. Amer. Math. Soc.* **19** (1968), 1379–1382.

[Fe] W. Feit, *Characters of finite groups* (Benjamin, New York, 1967).

[FS] G. A. Fernández-Alcober and R. T. Shepherd, 'On the order of p-groups of abundance zero', *J. Algebra* **201** (1998), 392–400.

[FT] J. S. Frame and O. Tamaschke, 'Über die Ordnungen der Zentralisatoren der Elemente in endlichen Gruppen', *Math. Z.* **83** (1964), 41–45.

[Ga] W. Gaschütz, 'Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen', *J. Algebra* **4** (1966), 1–2.

[Gi] J. D. Gillam, 'A note on finite metabelian p-groups', *Proc. Amer. Math. Soc.* **25** (1970), 189–190.

[Gl1] G. Glauberman, 'On Burnside's other $p^\alpha q^\beta$ theorem', *Pacific J. Math.* **56** (1975), 469–476.

[Gl2] ———, 'Large Abelian subgroups of finite p-groups', *J. Algebra* **196** (1997), 301–338.

[H1] G. Higman, 'Enumerating p-groups, I. Inequalities', *Proc. London Math. Soc. (3)* **10** (1960), 24–30.

[H2] ———, 'Enumerating p-groups, II. Problems whose solution is PORC', *Proc. London Math. Soc. (3)* **10** (1960), 566–582.

[He] H. Heineken, 'Nilpotente Gruppen, deren sämtliche Normalteiler charakteristish sind', *Arch. Math.* **33** (1979/80), 497–503.

[Hi] H. Hilton, *An introduction to the theory of groups of finite order* (Oxford Press, Oxford, 1908).

[HKKP] A. Hassani, M. Khayaty, E. I. Khukhro and C. E. Praeger, 'Transitive permutation groups with bounded movement and maximal degree', *J. Algebra* **214** (1999), 317–337.

[HL] H. Heineken and H. Liebeck, 'The occurrence of finite groups in the automorphism group of nilpotent groups of class 2', *Arch. Math.* **25** (1974), 8–16.

[Ho] O. Hölder, 'Die Gruppen der Ordnung p^3, pq^2, pqr, p^4', *Math. Ann.* **43** (1893), 301–412.

[HP] H.-W. Henn and S. Priddy, 'p-nilpotence, classifying space indecomposability, and other properties of almost all finite groups', *Comment. Math. Helv.* **69** (1994), 335–350.

[Hu] B. Huppert, 'A remark on the character-degrees of some p-groups', *Arch. Math.* **59** (1992), 313–318.

[Hy] 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.

[I1] I. M. Isaacs, *Character theory of finite groups* (Academic Press, San Diego, 1992).

[I2] ———, 'Recovering information about a group from its complex group algebra', *Arch. Math.* **47** (1986), 293–295.

[I3] ———, 'Sets of p-powers as irreducible character degrees', *Proc. Amer. Math. Soc.* **96** (1986), 551–552.

[I4] ———, 'Characters of groups associated with finite algebras', *J. Algebra* **177** (1995), 708–730.

[I5] ———, 'Groups with many equal classes', *Duke Math. J.* **37** (1970), 501–506.

[IK] I. M. Isaacs and D. Karagueuzia, 'Conjugacy in groups of upper triangular matrices', *J. Algebra* **202** (1998), 704–711.

[IP] I. M. Isaacs and D. S. Passman, 'A characterization of groups in terms of their irreducible character degrees', *Pacific J. Math.* **15** (1965), 899–903.

[JZ] A. Jaikin-Zapirain, 'On the abundance of finite p-groups', Technical Report.

[Ka] B. Kahn, 'A characterisation of powerfully embedded normal subgroups of a p-group', *J. Algebra* **188** (1997), 401–408.

[Kh1] E. I. Khukhro, *Nilpotent groups and their automorphisms* (de Gruyter, Berlin, 1993).

[Kh2] ———, *p-automorphisms of finite p-groups* (Cambridge University Press, Cambridge, 1997).

[KJ] M. Konvisser and D. Jonah, 'Counting Abelian subgroups of p-groups, a projective approach', *J. Algebra* **34** (1975), 309–330.

[KLGP] G. Klaas, C. R. Leedham-Green and W. Plesken, *Linear pro-p groups of finite width*, Lecture Notes in Math. 1674 (Springer, Berlin, 1997).

[KN] A. A. Kirilov and Yu. A. Neretin, 'The variety A_n of n-dimensional Lie algebra structures', *Transl. Amer. Math. Soc. (2)* **137** (1987), 21–30.

[Kr] A. A. Kirilov, 'Variations on the triangular theme', *Transl. Amer. Math. Soc. (2)* **169** (1995), 43–73.

[L] M. Lazard, 'Sur les groupes nilpotents et les anneaux de Lie', *Ann. Sci. Ecole Norm. Sup. (3)* **71** (1954), 101–190.

[Lf] T. J. Laffey, 'The minimum number of generators of a finite p-group', *Bull. London Math. Soc.* **5** (1973), 288–290.

[LG] C. R. Leedham-Green, 'The structure of finite p-groups', *J. London Math. Soc.* **50** (1994), 49–67.

[LGM] C. R. Leedham-Green and S. McKay, 'On the classification of p-groups of maximal class', *Quart. J. Math. Oxford Ser. (2)* **35** (1984), 293–304.

[LGN] C. R. Leedham-Green and M. F. Newman, 'Space groups and groups of prime power order I', *Arch. Math.* **35** (1980), 193–202.

[LMM] P. Longobardi, M. Maj and A. Mann, 'Minimal classes and maximal class in p-groups', *Israel J. Math.* **110** (1999), 93–102.

[LMMW] P. Longobardi, T. MacHenry, M. Maj and J. Wiegold, 'On absolutely-nilpotent of class k groups', *Rend. Mat. Acc. Lincei* **6** (1995), 201–209.

[Mc] I. D. Macdonald, 'Generalizations of a classical theorem about nilpotent groups', *Illinois J. Math.* **8** (1964), 556–570.

[Mi] G. A. Miller, 'A non-Abelian group whose group of isomorphisms is Abelian', *Messenger Math.* **43** (1913), 124–125 (or G. A. Miller, *Collected works*, vol. 5, 415–417).

[MM1] A. Mann and C. Martinez, 'The exponent of finite groups', *Arch. Math.* **67** (1996), 8–10.

[MM2] ———, 'Groups nearly of prime exponent and nearly Engel Lie algebras', *Arch. Math.* **71** (1998), 5–11.

[MN] A. McIver and P. M. Neumann, 'Enumerating finite groups', *Quart. J. Math. Oxford Ser. (2)* **38** (1987), 473–488.

[Mn1] A. Mann, 'Enumerating finite groups and their defining relations', *J. Group Theory* **1** (1998), 59–64.

[Mn2] ———, 'Minimal characters of p-groups', *J. Group Theory* **2** (1999), 225–250.

[Mn3] ———, 'On p-groups whose maximal subgroups are isomorphic', *J. Austral. Math. Soc. (Ser. A)* **59** (1995), 143–147.

[Mn4] ———, 'The derived length of p-groups', *J. Algebra*, to appear.

[Mn5] ———, 'Conjugacy classes in finite groups', *Israel J. Math.* **31** (1978), 78–84.

[Mn6] ———, 'The power structure of p-groups I', *J. Algebra* **42** (1976), 121–135.

[Mn7] ———, 'Enumerating finite groups and their defining relations II', Technical Report.

[Mn8] ———, 'On the power structure of some p-groups', in: *Proceedings of the 2nd International Group Theory Conference, Supp. Rend. Circolo Mat. Palermo (2)*, vol. 23 (1990) pp. 227–235.

[MP] A. Mann and C. E. Praeger, 'Transitive permutation groups of minimal movement', *J. Algebra* **181** (1996), 903–911.

[Mr] U. Martin, 'Almost all p-groups have automorphism group a p-group', *Bull. Amer. Math. Soc.* **15** (1986), 78–82.

[Mt] S. Mattarei, 'On character tables of wreath products', *J. Algebra* **175** (1995), 151–178.

[Nr] Yu. A. Neretin, 'An estimate of the number of parameters defining an n-dimensional algebra', *Math. USSR-Izv.* **30** (1988), 283–294.

[Nw] M. F. Newman, 'Groups of prime-power order', in: *Groups - Canberra 1989* (ed. L. G. Kovács), Lecture Notes in Math. 1456 (Springer, Berlin, 1990) pp. 49–62.

[NO1] M. F. Newman and E. A. O'Brien, 'A CAYLEY library for the groups of order dividing 128', in: *Group Theory, Proceedings of the Singapore conference* (eds. K. N. Cheng and Y. K. Leong) (de Gruyter, Berlin, 1989) pp. 437–442.

[NO2] ———, 'Classifying 2-groups by coclass', *Trans. Amer. Math. Soc.* **351** (1999), 131–169.

[NSW] M. F. Newman, G. Sauerbier and J. Wisliceny, 'Groups of prime-power order with a small number of relations', *Rostock Math. Kolloq.* **49** (1995), 141–154.

[P1] L. Pyber, 'Enumerating finite groups of given order', *Ann. of Math.* **137** (1993), 203–220.

[P2] ———, 'Group enumeration and where it leads us', in: *Proceedings of the European Congress of Mathematics* (Budapest, 1996), to appear.

[P3] ———, 'How Abelian is a finite group?', in: *The Mathematics of Paul Erdös* (eds. R. L. Graham and J. Nesetril) (Springer, Berlin, 1998).

[PaS] P. P. Pálfy and M. Szalay, 'The distribution of the character degrees of the symmetric p-groups', *Acta Math. Hung.* **41** (1983), 137–150.

[PF] F. Posnick (Fradkin), *3-powerful groups and subgroups of powerful groups* (Master's Thesis, Hebrew University, Jerusalem, 1998).

[PyS] L. Pyber and A. Shalev, 'Asymptotic results for primitive permutation groups', *J. Algebra* **188** (1997), 103–124.

[R] R. Ree, 'The existence of outer automorphisms of some groups II', *Proc. Amer. Math. Soc.* **9** (1958), 105–109.

[Sa] G. Sauerbier, 'Zur Darstellung von Pro-2-Gruppen durch Erzeugende und Relationen', *Wiss. Z. Päd. Hochsch. Güstrow (Math. - Nat. Fak.)* **1** (1986), 27–38.

[Sah] C. H. Sah, 'Automorphisms of finite groups', *J. Algebra* **10** (1968), 47–68.

[Sch] P. Schmid, 'Normal p-subgroups in the group of outer automorphisms of a finite p-group', *Math. Z.* **147** (1976), 271–277.

[Sh1] A. Shalev, 'The structure of finite p-groups: effective proof of the coclass conjectures', *Invent. Math.* **115** (1994), 315–345.

[Sh2] ———, 'Finite p-groups', in: *Finite and locally finite groups* (Kluwer Acad. Publ., Dodrecht, 1995) pp. 401–450.

[Sh3] ———, 'Probabilistic group theory', in: *Groups St Andrews 1997 in Bath, II*, London Math. Soc. Lecture Note Ser. 261 (Cambridge University Press, Cambridge, 1999) pp. 648–678.

[Si] C. C. Sims, 'Enumerating p-groups', *Proc. London Math. Soc.* **15** (1965), 151–166.

[Sn] P. J. Sanders, 'The coexponent of a regular p-group', *Comm. Algebra*, to appear.

[Sp] R. T. Shepherd, *p-groups of maximal class* (Ph.D. Thesis, University of Chicago, 1970).

[SW] P. J. Sanders and T. S. Wilde, 'The class and coexponent of a finite p-group', Technical Report.

[T] J. G. Thomoson, 'A non-duality theorem for finite groups', *J. Algebra* **14** (1970), 1–4.

[V] L. Verardi, 'On groups whose non-central elements have the same finite number of conjugates', *Boll. Un. Mat. Ital. (7)* **2-A** (1988), 391–400.

[VA] A. Vera-López and J. M. Arregi, 'Some algorithms for the calculation of conjugacy classes in the Sylow p-subgroups of $GL(n, q)$', *J. Algebra* **177** (1995), 899–925.

[VLW] M. R. Vaughan-Lee and J. Wiegold, 'Generation of p-groups by elements of bounded breadth', *Proc. Royal Soc. Edinburgh* **95A** (1983), 215–221.

[Wb] U. H. M. Webb, 'An elementary proof of Gaschütz' theorem', *Arch. Math.* **35** (1980), 23–26.

[Ws] J. Wisliceny, 'Zur Darstellung von Pro-p-Gruppen und Lieschen Algebren durch Erzeugende und Relationen', *Math. Nachr.* **102** (1981), 57–78.

[Xu] M. Y. Xu, 'Regular p-groups and their generalizations', unpublished book manuscript.

Einstein Institute of Mathematics
Hebrew University
Givat Ram
Jerusalem 91904
Israel
e-mail: mann@vms.huji.ac.il