Groups of Exponent Dividing Seventy

M. F. Newman

The Australian National University, Canberra, A.C.T., Australia

(Received: 11 September 1978)

This essay is dedicated to Bernhard Neumann on the seventieth anniversary of his birth with gratitude for initiating me into the fascinating world of groups.

The Hungarian Mathematical Journal for Secondary Schools runs what it calls a pool in which a winning combination is a good set of answers to some multiple-choice questions rather than a good set of predictions of football results. The questions are designed to stimulate interest in matters mathematical well beyond the high school curriculum. One recent question on adaptation to the Australian context might become:

Which of these four statements is correct?

(A) The Burnside Conjecture is an unsolved problem in set theory.

(B) The Burnside Conjecture was recently settled by the well-known Australian mathematician B. H. Neumann.

(C) There are several Burnside Conjectures, the best known being one settled over ten years ago by Feit and Thompson.

(D) There is no Burnside Conjecture: we just made it up to fool you.

Hopefully this essay will make choosing an answer a somewhat less random task than it might otherwise be.

It had better be said right at the outset that two questions raised by Burnside have been outstandingly influential on the development of the theory of groups. For instance both rate a mention in a recent (1978) survey of present trends in pure mathematics by Dieudonné (Section 10). Here the concern will be with the one raised by Burnside in a paper of 1902. Recall that a set $S$ of elements of a group generates the group if every element of the group can be written as a product of elements and inverses of elements of $S$. A group has exponent dividing a non-negative integer $n$ if the order of every element divides $n$. Burnside asked whether a group is necessarily finite when it can be generated by a finite set of elements and has positive exponent.

This question and aspects of its many ramifications have attracted the attention of numerous algebraists including, in particular, B. H. Neumann. This note presents a brief account of some of the results and problems which have arisen in connection with Burnside’s question; it is biased towards B. H. Neumann’s interests and involvements and to exponent dividing 70 to help bound the discussion. There is a useful survey

† I am indebted to L. G. Kovács for drawing my attention to this question and providing a translation. The original occurs as Question 7 of Köz. Mat. Lapok (NS) 56 (1978), 99.
account of work on Burnside's and related questions by M. Hall (1964). Another account can be found in his monograph on the theory of groups (1959) and also one in the monograph of Magnus, Karrass and Solitar on combinatorial group theory (1966). These books should also be able to supply those definitions which have been omitted here.

It is one of the notable achievements of the theory of groups that the question itself has been answered, in the negative, by the combined efforts of Novikov, who made a first announcement in 1959, and Adian, who has written a definitive monograph (1975) on their work. The result can be stated: there is a two-generator infinite group of exponent dividing $n$ for every $n$ which has an odd divisor greater than or equal to 665. The proof is a long and delicate nested induction of a highly combinatorial and ingenious nature. As is to be expected the method yields other interesting results. There are, as I write, informal reports of lectures (at Warwick, June 1978) in which E. Rips is making preliminary announcement of another construction of infinite finitely generated groups of positive exponent. His construction is apparently quite different. It is based on a generalization of small cancellation arguments. The exponents for which the construction is claimed to work are much larger than those achieved by Adian. On the other hand it leads to some other surprising groups. A most intriguing feature of the result of Novikov and Adian, and apparently also of Rips, is the need for the exponent to have a sufficiently large odd divisor. This leaves unsettled the question of whether there is an infinite finitely generated group of two-power exponent. Opinion is divided on the answer, with the majority favouring the existence of such a group.

Before going further into the world of groups it may be worthwhile to take a step in the other direction and view this question of Burnside in a slightly wider context. The conscious beginnings of a theory of groups are found in Galois’ work on the famous question of finding formulas for roots or solutions of polynomial equations in terms of the coefficients, the (rational) operations of addition, subtraction, multiplication and division, and $r$th root extraction. The groups involved are groups of permutations of the roots of a polynomial and therefore finite. Infinite groups arose somewhat later, initially as (multiplicative) groups of linear substitutions (or transformations); concretely as groups of matrices. Because a theory of finite groups was already available, it was reasonable (at least in retrospect) to seek sufficient conditions for a group to be finite. The first recorded question of this kind, as far as I am aware, was posed by Loewy in 1900. He asked whether a group of matrices is finite if (a) all of the characteristic roots of the matrices lie in a finite set, and if (b) all of its elements have order at most $n$. He was able to prove that the group is finite under the additional condition (c) at least one matrix has distinct characteristic roots. Burnside’s contribution was to ask the question in more abstract form. This turned out to be significant because it is the abstract formulation which attracted the attention of and provided the intellectual challenge to later workers. Burnside (1905) himself made a contribution in the matrix context by proving that a group of matrices with complex entries is finite whenever all its elements have order at most $n$. Notice that there is a shift here from finite exponent to bounded orders and that finite generation is not assumed. The first is only a shift of emphasis—the corresponding result for finite exponent is an immediate consequence. The second is a bonus which is easily seen to be unavailable in more abstract situations; consider the additive group of an infinite field of positive
characteristic. It is also needed, as the group of all complex two-power roots of unity shows, when the first condition is weakened to read merely that all the elements of the group have finite order. Schur, B. H. Neumann’s first ‘doctor father’, proved (1911) that every finitely generated group of complex matrices is finite if all its elements have finite order.

In his original paper of 1902 Burnside drew attention to the group generated by \( m \) elements which is defined by the system of relations that the \( n \)th power of every element is the identity. This group is the freest \( m \)-generator group of exponent dividing \( n \); freest in the sense that every \( m \)-generator group of exponent dividing \( n \) is a homomorphic image of it. This group is nowadays called a Burnside group—here it will be denoted \( B(m, n) \). Specifically Burnside asked: is \( B(m, n) \) finite and if so what is its order? Burnside pointed out that \( B(m, 2) \) is finite of order \( 2^m \). The key to proof of this is the ubiquitous exercise of showing that, if \( a, b \) are elements of order \( 2 \) of a group whose product \( ab \) also has order \( 2 \), then they commute; it follows that \( B(m, 2) \) may be regarded as a linear (or vector) space of dimension \( m \) over the field of two elements. Burnside also claimed that \( B(m, 3) \) is finite of order \( 3^{2^{m-1}} \) and \( B(2, 4) \) is finite of order \( 2^{15} \). He thus became the first, though by no means the last as Novikov’s original claim that \( B(2, 72) \) is infinite shows, to make an unsubstantiated claim in relation to the question. His finiteness claims were justified; however, he only proved that the numbers above are upper bounds for the orders—already de Séguier ((1904), pp. 72–74) seems to have been aware of this. Burnside also showed that for every prime \( p \) there is a two-generator group of exponent \( p \) whose order is \( p^{2^{p-3}} \).

Just a little jump ahead in the story brings us to B. H. Neumann’s first brush with the Burnside question. It was a light brush though not without incident. G. A. Miller ((1933), p. 1057) had said in effect: the finite groups of exponent \( 3 \) have not yet been completely determined. What he had in mind was, presumably, a way of describing these groups which would classify them up to isomorphism. B. H. Neumann in a review of the paper in the Jahrbuch über die Fortschritte der Mathematik (59, p. 149) said that Miller was clearly unaware of the work of Levi and van der Waerden (1932). They described \( B(m, 3) \) in considerable detail; in particular, they showed that its order is \( 3^k \) with \( k = (\binom{m}{1}) + (\binom{m}{2}) + (\binom{m}{3}) \) and that its nilpotency class is \( 3 \). The review drew a retort from Brahana ((1935), p. 186). He naturally argued that every \( m \)-generator group of exponent \( 3 \) is a homomorphic image of \( B(m, 3) \) but went on: ‘This solves the problem about as adequately as it is solved by remarking that every group of order \( p^m \) is simply isomorphic with some subgroup of the symmetric group on \( p^m \) letters. If the problem is not to be ignored, it is necessary to determine the invariant subgroups of Levi and van der Waerden’s group, and in the writer’s opinion this is not feasible.’ The feasibility must be viewed as a question of practicality because (a) there are only finitely many normal (invariant) subgroups in \( B(m, 3) \) and (b) testing the isomorphism of a pair of homomorphic images of \( B(m, 3) \) is a finite task.

The sentiment expressed by Brahana has been shared over the years by most workers in the field. One way of giving more substance to the feeling is to provide measures of the complexity of the family of finite groups of exponent \( 3 \). For instance, a slight modification of a lovely argument of Higman ((1960), p. 26) yields that there are at least \( 3^{3m(m-5)/16} \) isomorphically distinct \( m \)-generator groups of exponent \( 3 \). A less direct indication of the complexity can be given by going over to the family of all groups of
exponent 3 and using a criterion of which B. H. Neumann was an early proponent (1937a), p. 126). There are uncountably many different countable groups of exponent 3. This is true even when one restricts to the apparently much smaller subfamily consisting of groups whose commutator subgroup has order 9.

B. H. Neumann's (second) doctoral dissertation, Cambridge 1935, is motivated by the Burnside question. He saw the exponent condition as an example of an identical relation. To say that a group $G$ has exponent dividing $n$ is equivalent to saying that it satisfies the identical relation: $x^n = e$ (the identity element) for all $x$ in $G$. He used this to initiate a more general study of identical relations in groups and through them of varieties of groups. One of his most direct contributions to the Burnside question was made not long after. He studied finitely generated groups in which each element has order at most 3. He obtained (1937b) a classification up to isomorphism for those groups of this kind which contain an element of order 2—the remaining groups have exponent 3. In a recent paper Bolker (1972) observed that one can remove the restriction of finite generation and still obtain a complete classification of the groups in question.

I will take this discussion a little further: in part because the groups in question can be realized in a pleasant way—as groups of affine transformations; and in part because a similar situation arises later in the story.

Let $U$ be a linear space with scalars from a field $K$. (The scalar action will be written on the right.) Let $(k, u)$ denote the affine transformation of $U$ which maps $v$ to $vk + u$. The set of all such transformations with $k \neq 0$ forms a group under the usual multiplication for

$$v((k, u)(k', u')) = (vk + u)(kk' + u')$$

$$= vkk' + ukk' + u'$$

$$= v(kk', uk' + u');$$

this group will be denoted $\mathcal{L}(K, U)$. If $K$ is the field of either 3 or 4 elements, then every element of $\mathcal{L}(K, U)$ has order 1, 2 or 3 and (unless $U$ is zero-dimensional) elements of all these orders occur. Two of these groups are isomorphic if and only if the underlying fields are isomorphic and the underlying linear spaces are isomorphic. The arguments of B. H. Neumann and Bolker show that every group which has elements of orders 1, 2 and 3 and of these orders alone is isomorphic to one of the above groups.

It is time to begin applying the restriction to exponent dividing 70. Before proceeding I should make explicit that in discussing 'exponent' I have been thinking in terms of the non-negative integers endowed with their divisibility order. In this every group has exponent dividing 0; moreover, for every group $G$ there is a unique smallest element in the set of those integers $n$ for which $G$ has exponent dividing $n$, namely the least common multiple of the orders of its elements; this non-negative integer is the exponent of $G$.

The known negative answers to the Burnside question, which have been described above, say nothing for exponent 70. The discussion in a lecture by Adian (1974) shows that he expects a negative answer even for exponent 35. Let me begin the more detailed discussion with groups whose exponents are prime divisors of 70. As already remarked the exponent 2 case is easy. Burnside's question remains unanswered for groups of exponent 5 and 7. However, this is not the end of the story for these exponents because a
restricted version of Burnside's question came into circulation some time in the 1930s. Before going into that let me flash forward to bring B. H. Neumann back into the story again for a moment. In a survey of results and questions about varieties of groups delivered to a meeting of the American Mathematical Society (1967), he asked what he called an extended Burnside problem (p. 608). A special case which fits the present context is: is a group of exponent 5 in which every two-generator subgroup is finite itself necessarily finite?

The restricted Burnside question is usually stated: is there among the finite $m$-generator groups of exponent dividing $n$ a largest one? It is convenient to take a different point of view. A group is residually finite if the intersection of its normal subgroups of finite index is the identity. Every group has a largest residually finite quotient, namely the quotient to the intersection of all its normal subgroups of finite index. Let $B(m, n)$ denote the largest residually finite quotient of $B(m, n)$, then the restricted Burnside question is equivalent to the question: is $B(m, n)$ finite and if so what is its order? The exponent 5 case has turned out to play a prominent role in connection with this question especially by providing a benchmark against which to test progress. One important development has been the creation of Lie ring methods (by Magnus and others; see, for example, Magnus (1950)). By the early 1950s it was possible to exhibit a two-generator group of exponent 5 with order $5^{22}$ (see Lyndon (1955)). Then Kostrikin (1955) made a significant break-through by showing quite directly that $B(2, 5)$ has order at most $5^{36}$ and nilpotency class at most 12. A little later (without knowledge of Kostrikin's work) Higman (1956) showed that $B(m, 5)$ is finite for all $m$. His methods were rather different. In particular they were more qualitative; however they were still direct and could yield upper bounds for the orders. Over the next few years Kostrikin pushed ahead dramatically. He first obtained lower bounds for the orders and classes of the restricted Burnside groups $B(2, p)$ ((1957a), Theorem 7)—for instance he showed that $B(2, 5)$ has order divisible by $5^{31}$ and class at least 10 ((1957a), Theorem 6), and $B(2, 7)$ has order divisible by $7^{1075}$ ((1957b), p. 192) and class at least 17 ((1957a), p. 170). Next he showed that the restricted Burnside question has a positive solution for exponents 5 and 7 ((1957b), Theorem 1). He went on to obtain a positive answer to the restricted Burnside question for all prime exponents (1958), (1959). The methods were very different. In particular they made essential use of argument by contradiction and so showed that $B(m, p)$ is finite without yielding an upper bound for its order. Even now no upper bound is known for the order of $B(2, 7)$. The gap between the upper and lower bounds for the order of $B(2, 5)$ was closed only recently by Havas, Wall and Wamsley (1974); they showed, using computers, that $B(2, 5)$ has order $5^{34}$—and class 12. In the paper of Higman mentioned earlier he raised the question of whether the nilpotency class of $B(m, 5)$ increases with $m$. In a different context Macdonald and B. H. Neumann (1967) made a conjecture whose correctness would imply an affirmative answer to Higman's question. An affirmative answer was provided by Bachmuth, Mochizuki and Walkup (1970)—and in 1971 the correctness of the Macdonald–Neumann conjecture was established by Bachmuth and Mochizuki. Razmyslov, also in 1971, obtained the stronger result that $B(m, p)$ has class at least $2m - 1$. Kostrikin (1974), p. 411) has conjectured that the nilpotency class of $B(2, p)$ is quadratic in $p$. Of course the remarks made earlier about the classification problem for groups of exponent 3 apply, with even more force, for larger prime exponents.
The next case to consider under the restriction to exponent dividing 70 is that of exponent dividing 10. In light of what has been said already one can not at present hope for an answer to the original Burnside question in this case. The restricted Burnside question has an affirmative answer. This follows via reduction theorems of P. Hall and Higgins (1956), Section 4) from the exponent 2 and exponent 5 cases. This reduction theory is a major contribution to the solution of the restricted Burnside question. As a result in order to obtain a solution for exponent \( n \) it remains to obtain one for the prime-power divisors of \( n \) together with answers to two questions about non-abelian simple groups of exponent dividing \( n \). When only two distinct primes divide \( n \) the well-known Burnside solubility theorem (Theorem 16.8.7 of M. Hall’s book) applies to complete the reduction to the prime-power exponent case. When \( n \) is square-free the reduction theory combined with the result of Kostrikin (1959) already mentioned, with Walter’s (1969) theorem on simple groups with abelian Sylow subgroups and with some detailed structural information about ‘known’ simple groups yields that \( B(m, n) \) is finite. In particular \( B(m, 70) \) is finite. Moreover the reduction theory gives a formula for the order of \( B(m, 70) \) in terms of those for \( B(m_1, 2) \), \( B(m_2, 5) \) and \( B(m_3, 7) \) where \( m_1 \), \( m_2 \), \( m_3 \) are calculable functions of \( m \) (see Hall and Higgins (1956), Theorem 4.3.2).

This is a suitable moment to mention the remaining affirmative answers to the (unrestricted) Burnside question. With the aid of some of the information on \( B(m, 6) \) which was obtained by P. Hall and Higgins, M. Hall (1958) was able to show \( B(m, 6) \) is finite—so it coincides with \( B(m, 6) \). Earlier Sanov (1940) had shown \( B(m, 4) \) is finite. However, the order of \( B(m, 4) \) is not explicitly known (for \( m \) exceeding 4).

The work of Hall and Higgins is an excellent example within the theory of groups of the value of fundamental research. It was inspired by and contributed to the restricted Burnside question. Its key technical result, about \( p \)-soluble linear groups over fields of characteristic \( p \) and universally referred to as Theorem B, now plays a vital role in the work on the classification of finite simple groups.

The work of B. H. Neumann on groups whose elements have order at most 3 suggested to Higgins the study of finite groups in which every element has prime-power order. He was able to get (1957b) quite detailed information about the structure of such groups. He proved that such a group has at most one insoluble composition factor. This result was rounded off by Suzuki when he showed (1962, Theorem 16) that there are precisely eight non-abelian simple groups all of whose elements have prime-power order. Higgins also proved that, if such a group is soluble, then its order is divisible by at most two primes; and if there are two prime divisors, \( p \), \( q \), of the order, then the soluble length is bounded above in terms of \( p \) and \( q \) only. This latter depends on a result of Higgins about groups admitting a fixed-point-free automorphism of prime order (1957a). The case when the prime is 2 or 3 had been settled earlier by B. H. Neumann (1940), (1956). This is already enough to yield that every finite group of exponent (exactly) 10 all of whose elements have prime order is metabelian. Indeed, combined with B. H. Neumann’s 1937 argument it suffices to complete the classification of this family of groups. The groups are again groups of affine transformations; with one more ingredient—a subgroup \( A \) of the multiplicative group of the field \( K \). Let \( \mathcal{L}(A, K, U) \) be the subgroup of \( \mathcal{L}(K, U) \) consisting of the transformations \((a, u)\) with \( u \) in \( A \). If \( K \) is the field of either 5 or 16 elements and \( A \) is correspondingly the subgroup of order 2 or 5, then \( \mathcal{L}(A, K, U) \) has exponent 10 and no elements of order 10. Two such groups are
isomorphic only if the fields, the spaces and the multiplicative groups are. If \( U \) has finite dimension, \( \mathcal{L}(A, K, U) \) is finite.

It is natural to ask whether the above \( \mathcal{L}(A, K, U) \)—without the dimension restriction—are the only groups of exponent 10 with no elements of order 10. And natural to try an argument modelled on that of B. H. Neumann (1937b). There are a number of difficulties to be overcome. The first of these is to show that one of these groups which can be generated by an element of order 2 and one of order 5 is finite. It can be done using one of B. H. Neumann’s favourite techniques—coset enumeration. This is—when appropriately formulated—an algorithm (see, for example, Sims (1978), p. 117) which given a finite group presentation can sometimes (surprisingly often) answer the question of whether the group given by the presentation is finite. One of my earliest memories of B. H. Neumann is seeing him do such enumerations by hand. Coset enumerations were mechanized quite early (see J. C. P. Miller (1954), p. 161), though it was some time before machines could match skilled calculators. It is the most frequently implemented group-theoretic algorithm with the Australian National University under B. H. Neumann’s guidance playing a leading role (see for example Coxeter and Moser (1972), p. 16). In the present context the finiteness comes fairly easily using the current Canberra implementation (designed by G. Havas). Consider groups generated by two elements \( a, b \) with \( a^2 = b^5 = e \). If \((ab)^2 = e\), the group is also generated by two elements of order 2 whose product has order 5; so the group is certainly finite. Similarly if \((ab)^3 = e\), \((ab)^2 = e\) or \((ab)^2 = e\). Thus it remains to consider the case \((ab)^3 = (ab)^2 \) \((ab)^5 = (ab)^2 \) \((ab)^5 = e\). The group defined by the above six relations can be shown to be infinite. Considering the possible orders of the element \( ab^{-1} \) is enough to yield the finiteness. If \((abab^{-1})^2 = e\), then a coset enumeration over the subgroup generated by \( b \) yields that the subgroup has index 16—defining only 16 cosets; if \((abab^{-1})^5 = e\), then a similar enumeration yields index 1—though it defines 452 cosets in the process. The other difficulties arise near the end of the proof. At this point the setting is a group \( G \) of exponent 10 with no elements of order 10. Moreover either the elements of order 2 or those of order 5 generate a normal subgroup \( H \) of exponent 2 or 5. So, if \( A \) is a Sylow subgroup for the other prime, then \( G \) is a split extension of \( H \) by \( A \). Moreover the automorphisms of \( H \) induced by conjugation by elements of \( A \) are fixed-point-free and it follows from a result of Burnside ((1911), p. 334) that every finite subgroup of \( A \) is cyclic. This seems a strong additional condition, but in general it is not enough to guarantee finiteness for Adian (see (1975), p. 296) has shown that \( B(2, p) \) has all its finite subgroups cyclic for \( p \) large enough. Of course when \( A \) has exponent 2, it is finite—of order 2—and \( H \) is abelian (B. H. Neumann (1940)) and it follows that \( G \) is isomorphic to an affine group \( \mathcal{L}(A, K, U) \). When \( A \) has exponent 5 no further progress is to be expected at present.

The above discussion applies, mutatis mutandis, to groups of exponent 14 with no elements of order 14; except for two points. Firstly, the classification of finite groups of this type is less pleasant to describe (and therefore omitted) because the cyclotomic polynomial \((x^2 - 1)/(x - 1)\) is reducible over the field of 2 elements to \((x^3 + x + 1)(x^3 + x^2 + 1)\). Secondly, I have not succeeded in showing that such a group which is generated by an element of order 2 and one of order 7 is finite. Perhaps this is not so. Certainly there is a limit to the odd primes for which such groups are finite, for Adian ((1976), Theorem 6) has recently proved a result which implies that for primes
exceeding 665 there is an infinite two-generator group generated by an element of order 2 and one of order $p$ in which every element has order 1, 2 or $p$.

For exponent 35 the classification of finite groups with no elements of order 35 has not been done. It would clearly involve much more work than the corresponding questions discussed so far.

Turning finally to exponent 70 itself, the most natural question to ask, in light of the foregoing, is what can one say about groups of exponent 70 all of whose elements have order less than 10. The work of Higman and Suzuki shows they would have to be infinite. So here there is only the unrestricted question. B. H. Neumann enjoys conjecturing in such situations; I believe he would conjecture that such infinite groups exist; if so I offer this conjecture to him as a seventieth birthday present.

References


