A question of Babai on groups

J.L. Hickman and B.H. Neumann

László Babai raised the question whether every infinite group G contains a set B of elements, of cardinal equal to the order of G, such that for elements a, b, c of B the equation $a = bc^{-1}b$ implies a = c. We show that the answer is affirmative for certain classes of groups, including the soluble groups and the countable groups, if the Axiom of Choice is assumed, but negative, even for abelian groups, if a different axiom, compatible with Zermelo-Fraenkel set theory but incompatible with the Axiom of Choice, is assumed.

1. Introduction

László Babai [2] has asked whether every infinite group G must contain a set B of elements, of cardinal equal to the order of G, such that

(1.1) if
$$a, b, c \in B$$
 and $a = bc^{-1}b$ then $a = c$.

This arose from a problem on graphs and their automorphism groups which Babai can now solve by other means. We understand that he has also answered the above question affirmatively for some classes of groups [2], but by methods different from ours. In this paper we shall show that the answer depends on the underlying set theory: with the Axiom of Choice the answer is affirmative for countable groups and for soluble groups, and may indeed be affirmative for all infinite groups - our methods do not suffice to answer the question - but without the Axiom of Choice the answer can be negative even for some abelian groups.

Received 15 August 1975. The second author is grateful to Dr L.G. Kovács and Dr J.S. Wilson for helpful conversations.

2. Conventions

Script letters, like G, are used for groups, and the corresponding italic letter G denotes the set of elements, or carrier, of G. If B is a set, it is convenient to think of its cardinal, denoted by |B|, though it only occurs in equalities and inequalities. If G is a group, |G| is its order. The group G will usually be understood, and we then call the set B large if |B| = |G|, that is if there is a bijection from B to G, and small if |B| < |G|, that is if there is an injection but no bijection from B to G. A subset B of G, the carrier of G, will be called a Babai set if it satisfies (1.1). The group G is good if G contains a large Babai subset, and Bad otherwise.

If G is a group and H a subgroup or factor group or section, that is a factor group of a subgroup, of G, then H is called large or small according as H, its carrier, is large or small.

We assume Zermelo-Fraenkel set theory (ZF) with an additional axiom for most of the argument. This will be the Axiom of Choice (AC) at first, but a different axiom later, when also the relevant further notation will be introduced. It is well known that if ZF is consistent, then so is ZFC, that is Zermelo-Fraenkel set theory with the addition of the Axiom of Choice; see Gödel [3].

3. Elementary results

For our first results, AC is not needed.

LEMMA 3.1. The whole carrier G of the group G is a Babai set if, and only if, G has exponent 2, that is to say all squares equal the unit element.

Proof. It is well known, and indeed elementary, that groups of exponent 2 are abelian. Thus if G is of exponent 2 and a, b, c are elements of G, then

$$a = be^{-1}b$$
 implies $a = b^2e^{-1} = e^{-1} = e$.

Thus G is a Babai set. Conversely, if G is a Babai set and $g \in G$ an arbitrary element, we put a = 1 (the unit element), b = g, $c = g^2$ in (1.1), and find that c = 1: as g was arbitrary, G has exponent 2,

as claimed.

COROLLARY 3.2. All groups of exponent 2 are good. No finite group other than one of exponent 2 is good.

In the absence of AC, "finite" can be given different meanings, a point we return to later: for the present we leave the term vague, or intuitive.

LEMMA 3.3. If G contains a large good subgroup, then G is itself good.

This is obvious, as a large Babai subset of the carrier of the subgroup is also a large Babai subset of ${\it G}$.

For the next lemma and its corollary we use AC. We do not know whether they remain true without AC.

LEMMA 3.4. If G has a large good factor group, then G is itself good.

Proof. Let $\eta:G \to G_1$ be an epimorphism, with G_1 large and good. We denote by η also the corresponding surjection $\eta:G \to G_1$ of the carriers. Let B_1 be a large Babai subset of G_1 , and let $\tau:G_1 \to G$ be a left inverse (or transversal map) of η , that is an injection of G_1 to G such that $\tau\eta$ is the identity map of G_1 . Such a τ exists because we have now assumed AC. Now $B=B_1\tau$ is a large Babai subset of G: it is obviously large, and if $a,b,c\in B$, then $a=a_1\tau$, $b=b_1\tau$, $c=c_1\tau$ with $a_1,b_1,c_1\in B_1$. If, moreover, $a=bc^{-1}b$, then $a\eta=b\eta(c\eta)^{-1}b\eta$, that is $a_1=b_1c_1^{-1}b_1$, hence $a_1=c_1$ and a=c.

COROLLARY 3.5. If G is a bad group, then every large section of G is bad.

4. Bad groups

We still assume AC. Let G be a bad infinite group. The following technical lemma will, with Corollary 3.5, allow us to make other bad

groups, and to show that abelian groups are good.1

LEMMA 4.1. Let the group G be infinite and bad and let L be a large subset of G. Then L contains two distinct elements l, m and a large subset X such that all $x \in X$ satisfy the equation

$$(4.11) l = xm^{-1}x.$$

Proof. As AC is assumed, we can use Zorn's Lemma to establish the existence of a maximal Babai subset, say B, of L. This is trivially non-empty but small, as G is bad. If y is an arbitrary element of L-B, then $B\cup\{y\}$ is no longer a Babai set. Thus there must be elements $g,\ h\in B$ such that

(4.12)
$$y = gh^{-1}g \text{ and } y \neq h \text{, or}$$

$$(4.13) h = gy^{-1}g and y \neq h , or$$

$$(4.14)$$
 $g = yh^{-1}y$ and $g \neq h$.

We note in passing that (4.12) and (4.13) are equivalent, and that $y \neq h$ is guaranteed anyway by h being in B and y not. The set of y that satisfy (4.12) (and (4.13)) is small, as the set of pairs (g, h) with $g, h \in B$ is small - note that G is assumed to be infinite. Thus the set of y that satisfy (4.14) for some $g, h \in B$ must be large, and again because only a small set of pairs (g, h) is available, there must be at least one such pair, say (l, m) with $l \neq m$, for which the set

$$X = \{x \in L \mid l = xm^{-1}x\}$$

is large. The lemma follows.

COROLLARY 4.2. Let the group G be infinite and bad, and let L be a large subset of G. Then G contains a large subset R - contained, in fact, in a translate $m^{-1}L$ of L, where $m \in L$ - such that all elements of R have the same square, and this is not the unit element.

We use the notation of Lemma 4.1 and put $R=m^{-1}X$. If $r\in R$, then $r=m^{-1}x$ with $x\in X$, hence

(4.21)
$$r^2 = m^{-1}xm^{-1}x = m^{-1}l \neq 1 ,$$

See note added in proof at end.

and $m^{-1}l$ is independent of x and r.

An incidental consequence of this corollary is that all infinite groups of exponent 2 are good, as (4.21) can never be satisfied in them: but we know this to be the case even without AC, and for finite as well as infinite groups - see Lemma 3.2.

THEOREM 4.3. Under assumption of the Axiom of Choice, all infinite abelian groups are good.

Proof. Let A be an infinite abelian group and R a large subset of its carrier A as in Corollary 4.2, that is to say such that for all $r, s \in R$,

$$r^2 = s^2 \neq 1$$
.

Choose a fixed element, say r , in R and consider the set

$$Q = r^{-1}R = \{r^{-1}s \mid s \in R\}$$
.

Clearly Q is large, and if $q \in Q$ then $q^2 = 1$. Thus Q generates a large subgroup of A of exponent 2. This subgroup is good, by Lemma 3.2, and hence A itself is good, by Lemma 3.3. The theorem follows.

COROLLARY 4.4. All infinite soluble groups are good.

Of the factors in the derived series, at least one must be large: thus the group has a large good section.

COROLLARY 4.5. All free groups are good.

They have large abelian sections.

5. Consequences

We still assume AC and restrict our attention to infinite groups. If G is a bad infinite group then the subgroup generated by the large subset R of G of Corollary 4.2 is also bad, and so is the factor group, say H, obtained modulo the common square of the elements of R. Thus we have a bad group H generated by a large set S, say, of involutions. It is convenient to work with S and H rather than the original G. Another technical lemma is required for our main result.

LEMMA 5.1. Let H be an infinite bad group generated by a large set

S of involutions. Then there is an infinite sequence $\Sigma = (s_0, s_1, s_2, \ldots) \text{ of distinct elements of S such that}$

(5.11) if
$$i < j < k$$
 then $s_j s_i s_j = s_k s_i s_k$.

Proof. We proceed by induction. Take Σ_0 and Σ_0' as the empty sequence and put S_0 = S . Assume we have sequences

$$\Sigma_n = (s_0, s_1, \ldots, s_{n-1}), \quad \Sigma_n' = (s_0', s_1', \ldots, s_{n-1}')$$

and a large subset S_n of S with the properties

(5.2n) if
$$i < j \le n$$
—1 then $s_j s_i s_j = s'_i \ne s_i$,

(5.3n) if
$$i \leq n-1$$
 and $s \in S_n$ then

$$ss_is = s_i^i$$
.

Note that (5.20) and (5.30) are vacuously satisfied. Now apply Lemma 4.1 with S_n in place of L and H in place of G, to find two distinct elements l, m of S_n and a large subset X of S_n such that for all $x \in X$,

$$l = xm^{-1}x = xmx .$$

as m is an involution. Put

$$s_n = l$$
 , $s'_n = m$, $S_{n+1} = X$.

Then (5.2(n+1)) and (5.3(n+1)) are easily verified. Finally form the union $\Sigma = (s_0, s_1, s_2, \ldots)$ of all the sequences Σ_n so constructed: then (5.11) is satisfied. Note that if i < j, then s_i and s_j do not commute, hence are distinct. The lemma follows.

COROLLARY 5.4. With the same notation, if i < j < k , then s_i commutes with $s_j s_k$.

Observe that, as we are dealing with involutions,

$$s_i s_i s_j = s_k s_i s_k$$

implies

$$(s_j s_k)^{-1} s_i s_j s_k = s_k s_j s_i s_j s_k = s_i$$
.

LEMMA 5.5. Let H be a group whose carrier H contains a sequence

$$\Sigma = (s_0, s_1, s_2, \ldots)$$

of distinct involutions with the property

(5.11)
$$if i < j < k \text{ then } s_j s_i s_j = s_k s_i s_j.$$

Then H contains an infinite abelian subgroup.

Proof. Choose a sequence

$$i(0) < i(1) < i(2) < \dots$$

of non-negative integers so that for all m < n,

$$(5.51) t_m = s_{i(2m)} s_{i(2m+1)} \neq s_{i(2n)} s_{i(2n+1)} = t_n.$$

Thus, for example, we may take i(0) = 0, i(1) = 1, i(2) = 2, and i(3) = 3 or i(3) = 4, according as

$$s_0 s_1 \neq s_2 s_3$$
 or $s_0 s_1 = s_2 s_3$.

(One can always choose i(2n) = i(2n-1) + 1 , and i(2n+1) in the range

$$i(2n) < i(2n+1) \le i(2n) + n$$
.

Then Corollary 5.4, which only relies on the existence of the sequence Σ of involutions subject to (5.11), will guarantee that for all m, n the elements t_m and t_n commute. As by construction they are distinct, the abelian group they generate is infinite, and the lemma follows.

We are now ready to prove our main result.

THEOREM 5.6. Under assumption of the Axiom of Choice, all countably infinite groups are good.

Proof. If G is an infinite bad group, then it has, as we have seen, a bad section H generated by a large set of involutions; by Lemma 5.5 then H contains an infinite abelian subgroup. This can not be large, as otherwise it would, by Theorem 4.3 and Lemma 3.3, make H, and thus G, a good group. Hence |G| is uncountable, and the theorem follows.

It may be remarked that the somewhat indirect proof is in the nature of things, as there exist infinite groups without infinite abelian subgroups; see Adyan [1].

6. More definitions

We now jettison the Axiom of Choice; this allows us to consider different notions of finiteness and infinity. We use standard notation. In particular the natural number n is the set of its predecessors, $n = \{0, 1, \ldots, n-1\}$, and ω stands for the set of natural numbers. A set is *finite* if its cardinal is a natural number, and *infinite* otherwise. Then the set X is infinite if, and only if, for every natural number n there is an injection $\omega: n \rightarrowtail X$.

The set X is called medial if it is infinite but there is no injection $\varphi:\omega\rightarrowtail X$. Every medial set is Dedekind-finite, which is defined to mean that it has no proper subset of its own cardinality. Thus X is Dedekind-finite if $Y\subseteq X$ and |Y|=|X| together imply Y=X. Conversely every infinite Dedekind-finite set is medial. In the parlance introduced (for groups) in §2, the infinite set X is medial if it has only one large subset, namely itself. A set X is Dedekind-infinite if there is an injection $\varphi:\omega\rightarrowtail X$.

We shall say that the set X is quasi-minimal if, whenever it is partitioned into two sets:

$$X = Y \cup Z$$
, $Y \cap Z = \emptyset$,

one and only one of the parts Y, Z is infinite.

It is not difficult to see that every quasi-minimal set is medial; the converse is not true (except if neither quasi-minimal nor medial sets exist, as for example in ZFC). If ZF is consistent, then so is ZFQ obtained by postulating the existence of a quasi-minimal set. This is proved in [4] and also, independently by different methods, by Monro [5]. A discussion of the properties of quasi-minimal and medial sets can also be found in [4] and in Monro [6]. The only result from this theory that we need is stated and proved in the next section.

If X and Y are sets, we write Y^X for the set of functions $f:X \to Y$. In particular if Y=n is a natural number, we define the support of $f \in n^X$ as $\{x \in X \mid xf \neq 0\}$ — note that we use algebraic notation for functions. We further denote by $n^{(X)}$ the set of those functions $f:X \to n$ whose support is finite. This notion and notation

stem from corresponding ones for groups, to be described in §8.

7. A set-theoretic result

The main result of this section is a slight generalization of one in [4]; we present the proof in some detail, to make the present paper self-contained and because [4] is not readily accessible.

THEOREM 7.1. If X is a quasi-minimal set and n a natural number then n^X is Dedekind-finite.

The proof occupies the rest of this section. As $|0^X| = 0$ and $|1^X| = 1$, the first interesting case is n = 2. This is the case treated in [4] (with 2^X replaced by the power set of X, which has the same cardinal).

We start with the obvious remark that if an infinite set X is partitioned into a finite set of subsets, say

$$X = Y_0 \cup Y_1 \cup \ldots \cup Y_{n-1}$$
, $Y_i \cap Y_j = \emptyset$ if $i \neq j$,

then at least one of the parts is infinite; and if X is quasi-minimal then precisely one of the parts is infinite. Now let $f:X\to n$ be an element of n^X and for $i\in n$ put

$$if^{-1} = \{x \in X \mid xf = i\}$$
.

Then, if X is infinite, at least one of $0f^{-1}$, $1f^{-1}$, ..., $(n-1)f^{-1}$ is infinite, and if X is quasi-minimal, then precisely one of these parts is infinite.

LEMMA 7.2. If the set X is quasi-minimal, then n^X is medial if, and (trivially) only if, $n^{(X)}$ is medial.

Proof. Define sets T_{i} , for i \in n , by

$$T_i = \{ f \in n^X \mid if^{-1} \text{ is infinite} \}$$
.

By what we have seen, the T_i partition n^X . Moreover they all have the same cardinal, for we can define a bijection from T_i to T_0 by just

exchanging the values i and 0: if $f \in T_i$, we map it to $g \in T_0$, where

$$xg = xf$$
 if $xf \neq 0$ and $xf \neq i$, $xq = i$ if $xf = 0$ and $xq = 0$ if $xf = i$.

Also we note that $T_0 = n^{(X)}$. Now if there is an injection

$$\varphi:\omega \longrightarrow n^X$$

then there is an injection

$$\varphi_i : \omega \rightarrow T_i$$

for at least one $i \in n$, and as we have seen that $|T_i| = |T_0|$, there is then also an injection

$$\psi : \omega \longrightarrow T_0 = n^{(X)}$$
.

Thus if n^X is Dedekind-infinite, that is infinite but not medial, then $n^{(X)}$ is infinite but not medial. The converse is trivial, as is also the case (when n = 0 or 1) that n^X is finite. The lemma follows.

From now on we assume that X is an infinite set and that $n^{(X)}$ is Dedekind-infinite; specifically let

$$\psi : \omega \longrightarrow n^{(X)}$$

be an injection. Thus, for $\textit{m} \in \omega$, the image $\textit{m} \psi$ is a function,

$$m\psi: X \to n$$
,

of finite support. Denote the support of $m\psi$ by $m\sigma$, and define

$$m\tau = 0\sigma \cup 1\sigma \cup \ldots \cup (m-1)\sigma$$
.

Then $m\tau$ is, for every $m \in \omega$, a finite subset of X; moreover

if
$$p \leq q$$
 then $p\tau \subset q\tau$.

On the other hand, as there are only finitely many functions $m\psi: X \to n$ whose support is contained in any particular finite set $p\tau$, the terms of the sequence $0\tau \subseteq 1\tau \subseteq 2\tau \subseteq \ldots$ must properly increase again and again; that is to say there must be an infinite sequence $p_0 < p_1 < p_2 < \ldots$ of

natural numbers such that

$$p_i^{\tau} \neq (p_i^{+1})^{\tau}$$
.

We define a mapping

$$\varphi:\omega\to 2^{(X)}$$

from this sequence by $i\phi = f_i : X \rightarrow 2$, where

$$xf_i = 1$$
 if $x \in (p_i+1)\tau - p_i\tau$,

$$xf_i = 0$$
 otherwise.

It is clear that all $\,f_{i}\,$ have finite support and that these supports are non-empty and disjoint.

Define two subsets Y, Z of X by

$$\mathbf{Y} = \{ y \in \mathbf{X} \mid yf_i = 1 \text{ for some even number } i \}$$
 ,

$$Z = \{z \in X \mid zf_i = 1 \text{ for some odd number } i\}$$
 .

Then it is easy to see that Y and Z are both infinite, and disjoint. Thus Y and X-Y are also both infinite and disjoint, and X can not be quasi-minimal. Thus we have proved:

LEMMA 7.3. If X is a quasi-minimal set and n a natural number, then $n^{(X)}$ is Dedekind-finite.

Now Theorem 7.1 is an immediate consequence of this and Lemma 7.2.

8. Examples of bad groups

We shall call a group Dedekind-finite, medial, quasi-minimal, and so on, if its carrier is Dedekind-finite, medial, quasi-minimal, and so on. We now return to Corollary 3.2 and observe that its real content is the following lemma:

LEMMA 8.1. A Dedekind-finite group is good if, and only if, it is of exponent 2.

Thus to make examples of bad groups, we only need to construct

Dedekind-finite groups that are not of exponent 2; and as finite groups

are uninteresting in this context, we want to construct medial groups that are not of exponent 2. To do this we now work in ZFQ, that is Zermelo-Fraenkel set theory with an additional axiom postulating the existence of a quasi-minimal set; and we denote by X such a set.

If G is a group, we denote by G^X the cartesian power of G: its elements are the functions

$$f: X \to G$$

and the group operations are component-wise:

$$x(f^{-1}) = (xf)^{-1}, x(fg) = (xf)(xg).$$

The support $f\sigma$ of $f\in G^X$ is

$$f\sigma = \{x \in X \mid xf \neq 1\},\$$

where 1 is the unit element of G. The functions $f \in G^X$ of finite support are the elements of a subgroup of G^X , the *direct power* $G^{(X)}$. This is generated by the elements of the cartesian power whose support is a singleton. (These definitions are standard in group theory, though the nomenclature is a matter of local group-theoretical dialect.)

We note that the carrier of G^X is G^X , and the carrier of $G^{(X)}$ is a natural generalization of $n^{(X)}$ - they coincide if G is of finite order n, the carrier of G is n, and 0 is taken as the unit element.

Thus in particular, if F is a finite group of order $|F| \ge 2$, then F^X and $F^{(X)}$, the cartesian and direct powers, are medial, by Theorem 7.1 and Lemma 7.3, respectively. Thus we have shown:

THEOREM 8.2. Let F be a finite non-trivial group and X a quasiminimal set. Then the cartesian power F^X and the direct power $F^{(X)}$ are medial groups. If F is not of exponent 2, then F^X and $F^{(X)}$ are infinite bad groups. In particular, if F is abelian - say cyclic of order 3 -, then we thus obtain bad infinite abelian groups.

Note added in proof [25 November 1975]. The authors are indebted to Dr Paul C. Eklof, Dr James H. Schmerl, and Dr László Babai for pointing out that Lemma 4.1 and, consequently, Corollary 4.2 tacitly assume the

regularity of the cardinal of G. If G can be written as the union of a small set of small sets, we can not prove the existence of a single pair 1, m such that all elements x of a large set X satisfy (4.11), but only the existence of a small set P of pairs such that all $x \in X$ satisfy (4.11) for some pair $(1, m) \in P$. Similarly, in this case the corollary needs to be modified to say that the set of squares of elements of R is small (not necessarily a singleton, as claimed).

Theorem 4.3 remains true, though the argument proving it has to be trivially modified if the cardinal of G is singular. The authors have been informed by Dr Babai that this theorem was also proved, by similar methods, by R.G. Gurevič (Leningrad).

In $\S 5$ no harm is done by the tacit assumption that the cardinal of G is regular, as the main conclusion is only about countably infinite groups. Dr Vance Faber has a short and elegant proof of Theorem 5.6, using Ramsey's Theorem (oral communication); so has Dr Babai who plans to submit this and further results, for higher cardinals, in a paper entitled "Infinite digraphs with given regular automorphism group" to the J. Combinatorial Theory.

References

- [1] S.I. Adyan, "Periodic groups of odd exponent", Proc. Second Internat. Conf. Theory of Groups, Austral. National Univ. 1973, 8-12 (Lecture Notes in Mathematics, 372. Springer-Verlag, Berlin, Heidelberg, New York, 1974).
- [2] László Babai, in litt.
- [3] Kurt Gödel, The consistency of the axiom of choice and of the generalized continuum-hypothesis with the axioms of set theory (Annals of Mathematics Studies, 3. Princeton University Press, Princeton, New Jersey, 1940; 7th printing, 1966).
- [4] John Llewellyn Hickman, "An investigation of several finiteness criteria relative to Zermelo-Fraenkel set theory" (PhD thesis, Flinders University of South Australia, 1971). See also:

 Abstract, Bull. Austral. Math. Soc. 7 (1972), 300.

- [5] G.P. Monro, "Some independence results for weak axioms of choice" (PhD thesis, University of Bristol, 1971).
- [6] G.P. Monro, "Small sets with large power sets", Bull. Austral. Math. Soc. 8 (1973), 413-421.

Department of Mathematics, Institute of Advanced Studies, Australian National University, Canberra, ACT

and

Division of Mathematics and Statistics, Commonwealth Scientific and Industrial Research Organization, Canberra, ACT.