MATH. SCAND. 7 (1959), 191–201

SOME UNSOLVABLE PROBLEMS ABOUT ELEMENTS AND SUBGROUPS OF GROUPS

GILBERT BAUMSLAG, W. W. BOONE, AND B. H. NEUMANN

1. Introduction. Many algebraic problems have in recent years been shown to have no solution, in the sense that there exists no general and effective method of solving them. One that is typical, and most important, is the word problem, that is the problem whether two words in a given algebraic system represent the same element of the system; and the most interesting and difficult case is that of groups. The word problem in groups was first shown insoluble by Novikov [9] [10]; he exhibits a finitely presented group for which there is no general and effective procedure for determining whether any word in the (given) generators represents the unit element as a consequence of the (given) defining relations. Adyan [1] [2] and Rabin [11] have, independently, used this group to show that for a very extensive class of group theoretic properties there does not exist any general and effective method of deciding whether a given finite group presentation defines a group with the property in question. (For a discussion of the word problem in groups cf. Kuroš [5, p. 271] = [6, vol. 2, p. 75].)

In this note we prove a number of similar insolubility results concerning problems about elements and subgroups of groups. Our results are mostly near-trivial, in the sense that they can be proved in a few lines, using nothing deeper than the free product of groups and its known properties; but they are, af course, based on Novikov's very deep result and make use of his group, or some other group with an undecidable word problem. (Cf. e.g. Boone [3], Britton [4].)

REMARK BY W. W. BOONE. Novikov's proof of the unsolvability of the word problem for groups [9] is based upon Turing's proof of the corresponding result for cancellation semi-groups [Annals of Math. (2) 52 (1950), 491–505, with corrections same journal, 67 (1958), 195–202]. Boone's research showing the unsolvability of the word problem for

Received November 6, 1958.

The second author was supported by the John Simon Guggenheim Memorial Foundation and the Office of Naval Research, U. S. A.

groups [Indagationes Mathematicae 16 (1954), 231–237, 492–497, and 17 (1955), 252–256, 571–577; 19 (1957), 22–27, 227–232], does not use the Turing result and was carried out independently of Novikov's work. J. L. Britton's proof [4] likewise does not depend on the Turing result. (Britton announced a proof of the unsolvability of the word problem for groups at the British Math. Colloquium, Nottingham, September, 1957.) An exceedingly interesting aspect of Britton's group with unsolvable word problem is this: it is the free product—with amalgamations—of groups with *solvable* word problems.

The following theorems are typical of our results.

THEOREM 1. *There is a finitely presented group G_0 such that no effective procedure exists to determine whether a word in given generators of G_0 represents*

1.1 *an element of the centre of G_0;*

1.2 *an element permutable with a given element of G_0;*

1.3 *an n-th power, where $n > 1$ is an integer;*

1.4 *an element whose class of conjugates is finite;*

1.5 *an element of a given subgroup of G_0 (equivalently, what is known as the "Magnus' extended word problem" is insoluble in the group);*

1.6 *a commutator;*

1.7 *an element of finite order > 1.*

The list could be extended, and one is led to suspect that there is no meaningful property of group elements that can be effectively decided. This is, however, not the case; for, by contrast with 1.6 (and also, in a way, 1.5), there is an effective procedure to decide, in every finitely presented group G, whether a word represents an element in the commutator subgroup G'; for one only has to decide whether the corresponding word in G/G' represents the unit element; and in the (finitely presented) abelian group G/G' the word problem can (trivially) be solved.

THEOREM 2. *Let P be an algebraic property of groups (i.e. one that is shared by all isomorphic copies of any group that has it), and assume* (i) *that there is a finitely presented group that has P, and* (ii) *that there is an integer n such that no free group F_r of rank $r \geqq n$ has P; then there is a finitely presented group G_P such that no effective procedure exists to determine whether the elements represented by a finite set of words in given generators of G_P generate a subgroup with P.*

This theorem may be compared with Rabin's main theorems [11, Theorems 1.1 and 2.1]; it is similarly general (and was indeed suggested to us by Rabin's paper), and it allows us to match most of the particular applications that Rabin makes of his theorems. Thus we can deduce the following special cases.

COROLLARY 3. *There are finitely presented groups G (depending on the property considered) such that no effective procedure exists to determine whether the elements represented by a finite set of words generate a subgroup of G that is* (i) *trivial,* (ii) *finite,* (iii) *free,* (iv) *locally infinite,* (v) *cyclic,* (vi) *abelian,* (vii) *nilpotent,* (viii) *soluble,* (ix) *simple,* (x) *directly indecomposable,* (xi) *freely indecomposable,* (xii) *a group with soluble word problem; and so on ad nauseam.*

Note that some of these properties are the non-P of Theorem 2.

These results can be extended and modified in various ways; thus e.g. in place of algebraic properties of groups one can use properties of group presentations; or again, one can consider properties that relate the subgroup to the whole group, such as the properties of being normal, or of having finite index in the whole group. Theorems on such properties will be stated and proved in Section 5. One of the miscellaneous theorems proved in the final section requires a lemma to the effect that a finitely presented group can possess subgroups that are finitely generated but not finitely related. Though this fact is not surprising and almost certainly well known, we know of no published proof and have, therefore, included one in Section 4.

2. Proof of Theorem 1. Let U once and for all be a finitely presented group with unsolvable word problem; to make a definite choice, we may take the group of Boone [3], with two generators u_1, u_2 and with 32 defining relations. There is then no effective procedure to decide, for all words $w(u_1, u_2)$ in the two generators, whether

$$w(u_1, u_2) = 1$$

is a consequence of the 32 defining relations; or, differently put, to every alleged algorithm A that tells whether a word does or does not represent the unit element, there is a word $w_A(u_1, u_2)$ that defeats the algorithm A.

We further provide ourselves with a group S, generated by two elements s, t with the single defining relation

$$t^3 = 1 .$$

This is the free product of the infinite cycle generated by s and the cycle of order 3 generated by t. Finally we put

$$G_0 = S * U ,$$

the free product of S and U.

To prove Theorem 1, we show that an effective procedure that answers one of the questions of the theorem will also solve the word problem in U. More precisely, we specify a word

$$v_1 = v_1(s, t, w(u_1, u_2))$$

in the generators of S and an arbitrary word in the generators of U such that v_1 represents an element of the centre of G_0 if, and only if, $w(u_1, u_2) = 1$ in U: thus an algorithm A that tells whether v_1 is in the centre of G_0 or not, also tells whether $w(u_1, u_2) = 1$ or not, and A is defeated by

$$v_1(s, t, w_A(u_1, u_2)) .$$

We follow the same pattern, *mutatis mutandis*, for the other six properties of an element listed in the theorem.

In fact, one and the same word will serve for the first five properties, namely

$$v_1 = [s, w(u_1, u_2)] ,$$

where brackets denote the commutator:

$$[x, y] = x^{-1}y^{-1}xy ;$$

and for 1.2 we take t as the given element of G_0, for 1.5 we take S as the given subgroup. (These choices are arbitrary; any element $\neq 1$ of S or of U will do for 1.2, and the trivial group, or U, will do equally well for 1.5.) As the centre of a (non-trivial) free product is trivial, v_1 is in the centre of G_0 if, and only if, $v_1 = 1$, and thus if, and only if, $w(u_1, u_2) = 1$. In fact v_1 is permutable with t if, and only if, $v_1 = 1$. Next v_1 is an n-th power, with $n > 1$ if, and only if, $v_1 = 1$; for if $v_1 \neq 1$, then the length of v_1 (as an element of the free product $S * U$) is 4, and thus v_1 could at best be the square of an element of G_0; but one immediately verifies that it is no such square because $s^2 \neq 1$. Next we notice that the infinitely many conjugates $t^{-i}v_1t^i$ are all distinct if $v_1 \neq 1$. Again, as the length of v_1 is 4 unless $v_1 = 1$, it lies in S if, and only if, it is trivial, that is if, and only if, $w(u_1, u_2) = 1$.

For 1.6 we put

$$v_6 = [s, t]\, w(u_1, u_2) .$$

If $w(u_1, u_2) \neq 1$, then this has length 2, and thus cannot be a commutator; if $w(u_1, u_2) = 1$, then v_6 clearly equals a commutator. Hence v_6 represents a commutator in G_0 if, and only if, $w(u_1, u_2) = 1$.

Finally we put

$$v_7 = t \cdot w(u_1, u_2)$$

and remark that this has length 2 and therefore infinite order if $w(u_1, u_2) \neq 1$; but v_7 equals t and thus has order 3 if $w(u_1, u_2) = 1$. Hence v_7 has finite order >1 if, and only if, $w(u_1, u_2) = 1$. This completes the proof of Theorem 1.

3. Proof of Theorem 2. We are given the algebraic property P of groups and a finitely presented group T that has P; and there is an integer n such that the free groups F_r of rank $r \geqq n$ do not have P. We may assume that T is generated by at least n elements, say by $t_1, t_2, \ldots, t_r$ $(r \geqq n)$. Denote by G_P the free product of T and G_0—defined as in Section 2; thus

$$G_P = T * G_0 = T * S * U .$$

We first note the following fact.

LEMMA 4. *If $w = w(u_1, u_2) \neq 1$ in U, then the commutators*

$$(4.1) \qquad v_1 = [s, w], \qquad v_2 = [t, w]$$

are independent, that is to say, they freely generate a free group of rank 2.

This is an immediate consequence of Kuroš's Subgroup Theorem (cf. e.g. [5, p. 212], [6, vol. 2, p. 17]); if the group V generated by v_1, v_2 were not free, it would have to intersect a conjugate of S or of U non-trivially; hence its map under the retractive homomorphism of G_0 onto S or onto U would have to be non-trivial; but this is not so. If the rank of V were only 1, then v_1, v_2 would have to be powers of one and the same element; as both have length 4, they would then have to be equal or inverse to each other; and inspection shows that they are not.

COROLLARY 5.1. *Under the conditions of the lemma, the elements*

$$v_1^{-i} v_2 v_1^{i}, \qquad i = 0, \pm 1, \pm 2, \ldots ,$$

are independent.

Cf. e.g. [8, Corollary (4.4)].

COROLLARY 5.2. *There exists no effective procedure to decide whether certain words in the generators s, t, u_1, u_2 of G_0 (the finitely presented group of the proof of Theorem* 1) *represent independent elements.*

The words are

$$v_1^{-i} v_2 v_1^{i}, \qquad i = 1, 2, \ldots, r ,$$

where v_1, v_2 are defined by (4.1) in terms of $w = w(u_1, u_2)$; they are independent if, and only if, $w \neq 1$.

To prove Theorem 2, we consider words $t_1^*, t_2^*, \ldots, t_r^*$ defined by

$$t_i^* = t_i v_1^{-i} v_2 v_1^{i} ,$$

and the subgroup T^* of G_P generated by the elements they represent. They depend on the word $w = w(u_1, u_2)$ that enters the definition of v_1, v_2. If $w = 1$, then $v_1 = v_2 = 1$, and $T^* = T$ has property P. If $w \neq 1$, then T^* is a free group of rank r, as is seen from Corollary 5.1, using the retractive homomorphism of G_P onto G_0; in this case then T^* has non-P. Hence an effective procedure to decide whether a finitely generated subgroup of G_P has P will also decide whether $w = 1$ in U. There is no such effective procedure, and Theorem 2 follows.

4. An example. Barely anything is known about groups that can be embedded in finitely presented groups. In the present section we answer one question, namely whether a finitely presented group can have a subgroup that is finitely generated but not finitely related. An example will show that the answer is in the affirmative. This is not in itself surprising, and the example is simple enough; but the proof that it has the stated properties is surprisingly long.

Let D be the group generated by two elements, a, b subject to the defining relation

$$a^{-1}ba = b^2 .$$

In this group, b has a unique square root, namely

$$b^{\frac{1}{2}} = aba^{-1} ,$$

and this in turn has a unique square root, and so on. The elements of D can be written, uniquely, in the form

$$d = a^{\alpha} b^{\beta},$$

where α is an integer and β a dyadic fraction, that is a rational number whose denominator is a power of 2.

Next we take a free group F of rank 2, generated by two elements p, q, and we form the group of our example as the direct product of D and F,

$$E = D \times F .$$

This is generated by a, b, p, q, and defined by the relations

$$a^{-1}ba = b^2 ,$$

$$[a, p] = [a, q] = [b, p] = [b, q] = 1 ;$$

thus it is evidently finitely presented. The subgroup to be studied is that generated by b, p, and

$$c = aq;$$

let us denote it by C. The subgroup of C generated by b and c is isomorphic to D. In fact it is defined by the relation

$$c^{-1}bc = b^2;$$

for clearly this relation is satisfied, so that the mapping φ generated by $a\varphi = c$, $b\varphi = b$ is a homomorphism; and the retractive homomorphism of E onto D induces the homomorphism ψ generated by $c\psi = a$, $b\psi = b$; as φ and ψ are evidently inverse to each other, they are isomorphisms.

The elements generated by b and c can then be written uniquely in the form

$$d' = c^{\alpha}b^{\beta},$$

where α is an integer and β a dyadic fraction. The (dyadic) fractional powers of b lie in D and therefore permute with p. Thus in particular p permutes with all transforms of b by powers of c.

LEMMA 6.1. *The relations*

$$c^{-1}bc = b^2, \tag{6.11}$$

$$[p, c^ibc^{-i}] = 1, \qquad i = 0, 1, 2, \ldots, \tag{6.12}$$

form a system of defining relations of C.

We have seen that these relations are satisfied in C; it only remains to show that they suffice to define C. Now these relations suffice to reduce every word in b, c, p to the form

$$f(c, p)\, b^{\beta},$$

where $f(c, p)$ is a word in c and p, that is an element of the free group they generate, and β is a dyadic fraction. Hence any further relation in C could be reduced to the form

$$f(c, p)\, b^{\beta} = 1.$$

The retractive homomorphism of E onto F would lead from this to

$$f(q, p) = 1;$$

thus f must be trivial, and the relation reduces to

$$b^{\beta} = 1.$$

This is, however, only valid if $\beta = 0$. Thus any relation between b, c, p that is valid in C reduces to the trivial relation, using the relations (6.11), (6.12). These then suffice to define C, and the lemma follows.

This set of relations is not irredundant; in fact no set of defining relations of C is irredundant; any one, or more, of the relations (6.12) can be omitted, as long as infinitely many of them are retained.

LEMMA 6.2. *No finite subset of the set of defining relations* (6.11), (6.12) *suffices to define* C.

Consider the group defined by some finite subset of the defining relations of C. After (possibly) restoring the relation (6.11) and some of the relations (6.12), we obtain the group C^*, say, defined by

$$c^{-1}bc = b^2$$

and

$$[p, c^ibc^{-i}] = 1, \qquad i = 0, 1, \ldots, N .$$

If we introduce

$$b^* = c^Nbc^{-N} ,$$

then C^* can also be generated by b^*, c, p, and defined by the relations

$$c^{-1}b^*c = b^{*2} ,$$

$$[p, c^{-i}b^*c^i] = 1, \qquad i = 0, 1, \ldots, N .$$

Of these latter, only the first need be retained; for

$$c^{-i}b^*c^i = b^{*2^i} ,$$

and

$$[p, b^*] = 1$$

implies

$$[p, b^{*2^i}] = 1 .$$

Thus C^* is defined by the two relations

$$c^{-1}b^*c = b^{*2}, \qquad [p, b^*] = 1 .$$

It follows that C^* is the free product of the group generated by c, b^* (which is isomorphic to D) and the group generated by p, b^* (which is free abelian of rank 2), amalgamating the infinite cyclic group generated by b^*; and it then follows that in C^* the square root cb^*c^{-1} of b^* does not permute with p. (Cf. the similar reasoning applied in [8, Section 21].) But in C the square root of b^* does commute with p; hence C and C^* are not isomorphic, and the lemma follows.

COROLLARY 6.3. *The finitely generated subgroup C of the finitely presented group E is not finitely related.*

This follows from the known fact [7, Corollary 12] that if a group has one finite set of generators in which it cannot be finitely defined, then it cannot be finitely defined in any set of generators.

5. Some further results. We finally collect some miscellaneous results that are similar to Corollary 3 but not direct consequences of Theorem 2.

THEOREM 7. *There are finitely presented groups G (depending on the property considered) such that no effective procedure exists to determine whether the elements represented by a finite set of words generate* (i) *a finitely related subgroup of G*; (ii) *a subgroup of finite index in G*; (iii) *a subgroup with finitely many conjugates in G*; (iv) *a normal subgroup of G.*

PROOF. For (i) we use the method of proof of Theorem 2—in fact (i) could be subsumed under a slightly more general form of Theorem 2, using the groups G_0 of Section 2 and E of Section 4: We put

$$G = E * G_0 = E * S * U$$

and consider the words

$$c^* = cv_2, \qquad b^* = b\,v_1^{-1}v_2v_1, \qquad p^* = p\,v_1^{-2}v_2v_1^{2},$$

where v_1, v_2 are again defined by (4.1) in terms of a word $w = w(u_1, u_2)$. The subgroup of G generated by c^*, b^*, p^* is free, and therefore (trivially) finitely related, if $w \neq 1$, but isomorphic to C, and thus not finitely related, if $w = 1$, by Corollary 6.3. Then (i) follows by the argument used in Section 3.

For (ii), (iii), and (iv) we use the group G_0 of Section 2 and consider the subgroup H generated by t, u_1, u_2 and

$$s^*(w) = s^{-1}\, w(u_1, u_2)\, s^2 .$$

Clearly H depends on the element of U represented by the word $w = w(u_1, u_2)$. If $w = 1$, then $s^* = s$ and $H = G_0$. If $w \neq 1$, then we apply the following lemma.

LEMMA 8. *Let P be the free product of two groups V, W, and let Q be the subgroup of P generated by W and the element*

$$v^* = vwv' ,$$

where $v \in V$, $v' \in V$, $w \in W$ and

$$vv' \neq 1, \qquad w \neq 1 .$$

Then the normalizer of Q in P intersects V trivially only.

For the proof, see below. To apply it, we look upon G_0 as the free product P of the group W, say, generated by t, u_1, u_2, and the infinite cyclic group V, say, generated by s; we have $w \neq 1$, and we put $v = s^{-1}$, $v' = s^2$, so that $s^* = v^*$ and $H = Q$. By the lemma, the normalizer of H

in G_0 contains no power $\neq 1$ of s and therefore has infinite index in H. It follows at once that H itself has infinite index in G_0, that H is not normal in G_0, but on the contrary has infinitely many conjugates in G_0. Hence (ii), (iii), (iv) follows, and the proof of the theorem is completed.

Proof of Lemma 8. The elements of Q can be written in the form

$$q = w_0 v^{*^{n(1)}} w_1 v^{*^{n(2)}} w_2 \ldots v^{*^{n(k)}} w_k , \tag{8.1}$$

where $w_0, w_1, \ldots, w_k \in W$, $w_1 \neq 1$, $w_2 \neq 1, \ldots, w_{k-1} \neq 1$, and $n(1)$, $n(2)$, $\ldots$, $n(k)$ are non-zero integers. Now writing v^{*^n} in its normal form (relative to the free decomposition $P = V * W$), we see that its length is

$$\lambda(v^{*^n}) = 2|n| + 1 ,$$

when $n \neq 0$. Introducing the normal forms of the powers of v^* into (8.1), we see that no cancellations or amalgamations occur, and the length of q is

$$\lambda(q) = 2\Sigma |n(i)| + 2k - 1 + \lambda(w_0) + \lambda(w_k) , \tag{8.2}$$

if $k > 0$. Assume that v_0 is an element both of V and of the normalizer of Q. Then

$$q_0 = v_0^{-1} w v_0 \in Q ,$$

and this must be of the form (8.1). If $v_0 \neq 1$, then $\lambda(q_0) = 3$, and we see from (8.2) that $k = 1$, $n(1) = \pm 1$, $\lambda(w_0) = \lambda(w_1) = 0$; but this would imply

$$q_0 = vwv' \quad \text{or} \quad q_0 = v'^{-1} w^{-1} v^{-1} ,$$

that is simultaneously $v = v_0^{-1}$, $v' = v_0$ (and possibly also $w = w^{-1}$). This, however, contradicts the assumption that $vv' \neq 1$; it follows that $v_0 = 1$, and the lemma is proved.

To conclude, we state a fact, typical again of many, about automorphisms of finitely presented groups.

Theorem 9. *There is no effective procedure to decide whether a given automorphism of the group G_0 of Section 2 is inner.*

We consider the mapping α of G_0 into itself generated by

$$t\alpha = t, \quad u_1\alpha = u_1, \quad u_2\alpha = u_2 ,$$

$$s\alpha = [t, w(u_1, u_2)]s .$$

This depends on the element of U represented by the word $w(u_1, u_2)$. If $w(u_1, u_2) = 1$, then α is the identity automorphism, hence inner. If $w(u_1, u_2) \neq 1$, then α is an automorphism, but not inner. The verification of these statements is easy, and we omit it.

REFERENCES

1. S. I. Adyan, *The algorithmic unsolvability of the problem of checking certain properties of groups*, Doklady Akad. Nauk SSSR 103 (1955), 533–535. (Russian.)
2. S. I. Adyan, *Finitely generated groups and algorithms*, Uspehi Mat. Nauk 12 (1957), No. 3, 248–249. (Russian.)
3. W. W. Boone, *The word problem*, submitted to Ann. of Math.; cf. also Proc. Nat. Acad. Sci. USA 44 (1958), 1061–1065.
4. J. L. Britton, *The word problem for groups*, Proc. London Math. Soc. (3) 8 (1958), 493–506.
5. A. G. Kuroš, *Teoriya Grupp* (2nd ed.), Moscow 1953.
6. A. G. Kurosh, *The theory of groups* 1–2, New York, 1955–1956. (Translation of 5.)
7. B. H. Neumann, *Some remarks on infinite groups*, J. London Math. Soc. 12 (1937), 120–127.
8. B. H. Neumann, *An essay on free products of groups with amalgamations*, Phil. Trans. Roy. Soc. London (A) 246 (1954), 503–554.
9. P. S. Novikov, *On the algorithmic unsolvability of the identity problem*, Doklady Akad. Nauk SSSR 85 (1952), 709–712, and Trudy Mat. Inst. Steklov No. 44 (1955). (Russian.)
10. P. S. Novikov, *On the algorithmic unsolvability of the word problem in groups*, Amer. Math. Soc. Translations (2) 9 (1958). (Translation of 9.)
11. Michael O. Rabin, *Recursive unsolvability of group theoretic problems*, Bull. Amer. Math. Soc. 62 (1956), 396; and Ann. of Math. 67 (1958), 172–194.

THE UNIVERSITY, MANCHESTER, ENGLAND
UNIVERSITY OF ILLINOIS, URBANA, ILL., U. S. A.
THE UNIVERSITY, MANCHESTER, ENGLAND