

## Annals of Mathematics

---

Recursive Unsolvability of Group Theoretic Problems

Author(s): Michael O. Rabin

Source: *The Annals of Mathematics*, Second Series, Vol. 67, No. 1 (Jan., 1958), pp. 172-194

Published by: Annals of Mathematics

Stable URL: <http://www.jstor.org/stable/1969933>

Accessed: 15/02/2010 02:45

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=annals>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



*Annals of Mathematics* is collaborating with JSTOR to digitize, preserve and extend access to *The Annals of Mathematics*.

<http://www.jstor.org>

## RECURSIVE UNSOLVABILITY OF GROUP THEORETIC PROBLEMS\*

By MICHAEL O. RABIN

(Received March 25, 1957)

Finitely presented groups, i.e. groups defined by a finite system of generators and relations between these generators, arise in a natural way in several mathematical contexts especially in algebraic topology. Very often decision problems spring into the foreground. In the theory of knots, for example, there corresponds to every knot a certain finitely presented group; given the knot it is possible to actually compute a presentation of its group. The knot is trivial if and only if its group is infinite cyclic. Thus the problem of classifying knots into trivial and non-trivial ones reduces to a decision problem concerning presentations.

P. S. Novikov proved [13] that the word problem for groups is not effectively solvable. In fact he exhibited a specific finite presentation  $\Pi_0$  and proved that there does not exist a general and effective method of deciding for every given word on the generators of  $\Pi_0$  whether it equals one as a consequence of the defining relations.

The word problem is a decision problem concerning elements of an algebraic system. Algebraists are usually more interested in questions related to whole algebraic systems. Thus we are naturally led to consider decision problems of a higher category, namely problems concerning presentations and properties of the algebraic systems defined by them. Markov led the way in this direction. In [9, 10] he showed that for many algebraic properties of semigroups there does not exist an effective procedure of deciding, for every given presentation, whether the semigroup defined by it possesses the property in question. Addison [1] and Feeney [3] obtained similar results for cancellation semigroups. The main theorem of the following paper, and the general method of its proof, were inspired by the ideas of Markov.

In Chapter I we combine Novikov's result with a certain algebraic construction to show that for a very extensive class of group theoretic properties there does not exist a general and effective method of deciding,

---

\* This work constitutes part of a doctoral dissertation written under the supervision of Prof. A. Church at Princeton University and submitted in October, 1956. The author wishes to thank Prof. Church for his kind encouragement during the preparation of the thesis. The results (except those in Chapter III) were presented before the New York meeting of the American Mathematical Society in April, 1956.

for every given presentation, whether the group defined by it has the property in question (Theorem 1.1). Since every group presentation can also be written as a presentation of a semigroup, or cancellation semigroup, the results of Markov, Addison, and Feeney follow as special cases. Also follow the results on groups announced, without proofs, by Adjan [2]; see review in Zentralblatt, September 1956, our source.

The usual method of proving that a problem is not solvable by means of an effective decision procedure is to "translate" a problem known not to be effectively solvable into the problem in question. When dealing with algebraic systems this translation process involves proofs that certain mappings are isomorphisms, or at least map distinct elements into distinct elements. These proofs were usually obtained by combinatorial analysis. One checked what products, cancellations, and equations can occur and showed, by inspection and inductive arguments, that certain equations between products are impossible. In the following work we were however successful in avoiding combinatorial arguments and used methods of a more algebraic nature instead. In particular the free product with amalgamated subgroups turned out to be a useful tool. The comparative simplicity of proofs of this kind does in fact raise hope that one can replace the combinatorial arguments in previous papers on similar subjects by group theoretic procedures and thereby obtain much simpler proofs for the same results.

Chapter II is devoted to the direct and indirect consequences of the main theorem. It turns out that for such basic algebraic properties as cyclicity, finiteness, simplicity, solvability, being decomposable into a direct product, and many others, there does not exist a general and effective method of ascertaining from presentations whether the groups defined by them have that property. Novikov's result is supplemented (in Section 2.6.) by showing that it is impossible, in general, to decide whether the word problem of a presentation is recursively solvable.

In Section 3.1. we prove that the isomorphism problem for groups is not recursively solvable, a result which can be rephrased by saying that there does not exist a finite complete system of computable isomorphism invariants. Now for certain equivalence problems in algebraic topology one constructs infinite sequences of equivalence invariants which are usually also computable. Though the construction of a complete countable sequence of computable equivalence invariants does not furnish an effective decision procedure for that equivalence problem, it is probably the next best thing after it. In Section 3.2. we demonstrate the impossibility of even a countably infinite complete system of computable isomorphism

invariants. Thus a program for the classification of presentations, similar to the program of algebraic topology, is not feasible.

### 0.1. Effective decision procedures

A decision problem arises when we are given a set  $S$  of mathematical objects together with a subset  $P$  of  $S$ , and we want a general method of deciding, for every given element  $x \in S$ , whether  $x \in P$ .

In most cases it is possible to replace the original problem, given by the pair  $(S, P)$ , by a new problem concerning a set  $S'$  and a subset  $P' \subseteq S'$ , where  $S'$  is a subset of the set of non-negative integers. This is done by the so-called device of Gödel numbering. Let  $S$  be, for example, the set of all polynomials in one variable with non-negative integral coefficients and let  $P$  be a subset of  $S$ . The set  $S$  can be Gödel numbered by associating with each polynomial  $f \in S$ ,  $f(x) = a_0 + a_1x + \cdots + a_nx^n$ , the integer  $i(f)$

$$i(f) = \prod_{j=0}^n p_j^{a_j}, \quad p_j = j^{\text{th}} \text{ prime.}$$

The function  $i$  clearly maps  $S$  one to one onto the positive integers  $I$  and maps  $P$  onto a subset  $P' = i(P)$  of  $I$ ; given a polynomial  $f \in S$  one can compute in a finite number of steps the integer  $i(f)$ ; given any integer  $k$  one can find in a finite number of steps the polynomial  $i^{-1}(k)$ . Any solution of the decision problem  $(I, P')$  therefore leads to a solution of the original decision problem.

By using Gödel numbering most decision problems are thus reducible to the form: Given a subset  $P$  of the integers  $I$ , to find a test for membership in  $P$ . With  $P$  we can now associate its characteristic function  $f$

$$f(n) = \begin{cases} 1 & \text{if } n \in P, \\ 0 & \text{if } n \notin P. \end{cases}$$

Having an effective test for membership in  $P$  is thus equivalent to  $f$  being an effectively computable function.

The question how to define the concept of an effectively computable function is treated in the theory of recursive functions [5, pp. 217-386]. There one defines a certain set  $C$  of so-called *recursive functions* and then agrees to call a function  $f$  (from integers to integers) *effectively computable* if and only if  $f \in C$ . For the motivation for identifying effective computability with recursiveness see [5, pp. 317-323].

We can now give a precise meaning to the notion of the effective solvability of a decision problem. We say that the decision problem  $(S, P)$  is *effectively (recursively) solvable* if, when mapping  $S$  by a Gödel numbering onto the integers  $I$ ,  $P$  is mapped on a set of integers having an

effectively computable characteristic function. In this case we shall call  $P$  a *recursive* subset of  $S$ . The statement that a decision problem is not effectively solvable of course means that the aforementioned characteristic function is not effectively computable. These remarks clearly show that the non-existence of an effective solution for a decision problem  $(S, P)$  has nothing to do with the existence of an element  $x \in S$  "for which we cannot decide whether  $x \in P$ " (whatever that means).

I. A THEOREM CONCERNING THE SET OF ALL PRESENTATIONS

1.1. The main theorem

Since we intend to ask questions concerning the recursiveness of subsets of the set of all (finite) presentations, we must first of all define the latter set. Unless we define precisely the set of all presentations it is meaningless to talk of its subsets and even more so to talk about recursiveness or non-recursiveness of subsets. What we have to do is, essentially, to fix upon a definite notation for presentations.

DEFINITION 1.1. The set  $Q$  of presentations is the set of all presentations

$$\Pi = (x_1, \dots, x_n : r_1(x) = 1, \dots, r_m(x) = 1)$$

where: (1) the generators  $x_1, \dots, x_n$  are the first  $n$  ( $n$  is arbitrary) symbols of the infinite sequence  $x_1, x_2, \dots$ ; (2) the words  $r_1(x), \dots, r_m(x)$  are all in reduced form; (3) the words  $r_1(x), \dots, r_m(x)$  are pairwise different and are arranged according to the lexicographic ordering induced by arranging the generators and their inverses in the order:  $x_1, x_1^{-1}, x_2, x_2^{-1}, \dots$ <sup>1</sup>

The set  $Q$  will also be referred to as *the set of all presentations*. Every statement containing this more intuitive phrase can however be made entirely precise by referring back to the definition of  $Q$ .

Viewing  $Q$  as the set of all presentations is justified because, given any presentation  $\Pi'$ , it differs from some  $\Pi \in Q$  by at most an alphabetic change of the generators, a reduction of the defining relations to words in reduced forms, a deletion of repetitious relations, and a rearrangement of the defining relations.

It is now possible to introduce a Gödel numbering of  $Q$  and thereby give precise meaning to notions such as *recursive set of presentations* (i.e. recursive subset of  $Q$ ), *recursive function from  $Q$  into  $Q$* , etc. We shall not carry out the actual Gödel numbering, the reader can carry out the formal details of the process if he wishes to do so.

<sup>1</sup> Clause (1), in one form or another, is indispensable; as to (2) and (3) their purpose is to avoid occurrence of a multiplicity of presentations which are essentially the same.

**THEOREM 1.1.** *Let  $P$  be an algebraic property (i.e. a property preserved under isomorphisms) of finitely presentable (f.p.) groups such that (1) there exists at least one f.p. group  $G_1$  which has the property  $P$ ; (2) there exists at least one f.p. group  $G_2$  which does not have the property  $P$  and is not isomorphic to any subgroup of a f.p. group having  $P$ . The set  $S(P)$*

$$S(P) = \{\Pi \mid \Pi \in Q, G_\pi \text{ has } P\}^2$$

*of all presentations (in  $Q$ ) of groups having the property  $P$  is not a recursive set.*

In more intuitive language: there does not exist a general and effective procedure of deciding, for every presentation  $\Pi$ , whether  $G_\pi$  (the group defined by  $\Pi$ ) possesses the property  $P$ .

Let us consider a concrete example. The property of being a cyclic group clearly satisfies conditions (1) and (2), thus there does not exist a general and effective procedure of deciding, for every presentation  $\Pi$ , whether  $G_\pi$  is a cyclic group. In special cases such as  $\Pi = (x_1 : x_1^5 = 1)$  the answer is of course clear, but what we have in mind is a general decision method which is applicable to all presentations and which is effective; such a method does not exist.

### 1.2. Test groups

Before proceeding to prove Theorem 1.1 we will introduce the notion of *test groups* and state Theorem 1.2 concerning this concept. We shall then prove Theorem 1.1, using Theorem 1.2. After doing this we shall take up the proof of Theorem 1.2; this is actually the most difficult and substantial task in Chapter I.

**DEFINITION 1.2.** Let  $\tau$  be a function assigning to each pair  $(\Pi, w)$  where  $\Pi \in Q$  and  $w$  is a word on the generators of  $\Pi$ , a presentation  $\tau((\Pi, w)) \in Q$ ; denote  $\tau((\Pi, w))$  by  $\Pi_w$ , thus:

$$\tau : (\Pi, w) \rightarrow \Pi_w, \quad \Pi_w \in Q.$$

The function  $\tau$  is a *test group construction* if (1)  $\tau$  is a recursive function (i.e., given  $\Pi$  and  $w$ , one can obtain  $\Pi_w$  effectively), (2) if  $\vdash_\pi w = 1$  then  $G_{\pi_w} \approx 1$ ,<sup>3</sup> (3) if  $\vdash_\pi w = 1$  does not hold, then  $G_\pi$  is isomorphic to a subgroup of  $G_{\pi_w}$ .

$G_{\pi_w}$  will be called the *test group corresponding to  $\Pi$  and  $w$* .<sup>4</sup>

<sup>2</sup>  $G_\pi$  denotes the group defined by the presentation  $\Pi$ .

<sup>3</sup> The notation  $\vdash_\pi w = 1$  means that  $w$  equals to one as a consequence of the defining relations of  $\Pi$ .

<sup>4</sup> The reason for this name is that  $G_{\pi_w}$  can be used for testing whether  $\vdash_\pi w = 1$ , since  $\vdash_\pi w = 1$  holds if and only if  $G_{\pi_w} \approx 1$ .

**THEOREM 1.2.** *There exists a function  $\tau$  which is a test group construction, i.e. which satisfies (1), (2), and (3), of Definition 1.2.*

We shall prove Theorem 1.2 by exhibiting a particular function and showing that (1), (2), and (3) are satisfied. When reading the following proof the reader should assume that the  $\Pi$  and  $\Pi_w$  used there are those to be exhibited later on in the proof of Theorem 1.2.

**1.3. Proof of Theorem 1.1**

Let  $G_1$  and  $G_2$  be as in the assumptions of Theorem 1.1 and let  $\Pi_1$  and  $\Pi_2$  be presentations of  $G_1$  and  $G_2$  respectively.

Let  $\Pi_0$  be a presentation for which the word problem is not recursively solvable (this is the point where we use Novikov's result [12, 13] to the effect that such a presentation does exist).

Form the free product

$$(1.1) \quad G = G_2 * G_{\pi_0};$$

$G$  is a finitely presentable group, in fact a presentation  $\Pi \in Q$  can be explicitly obtained from  $\Pi_2$  and  $\Pi_0$ . Thus we have  $G = G_\pi$ .

Since  $G_{\pi_0}$  is isomorphic to a subgroup of  $G$  it follows that the word problem of  $\Pi$  is not recursively solvable.

Let  $w$  be an arbitrary word on the generators of  $\Pi$ . Let  $\Pi_w$  be the presentation of the test group  $G_{\pi_w}$  corresponding to  $\Pi$  and  $w$ .

Form the free product

$$(1.2) \quad G(w) = G_1 * G_{\pi_w}.$$

If  $\vdash_{-\pi} w = 1$  then, by clause (2) of Definition 1.2,  $G_{\pi_w} \approx 1$  and hence  $G(w) \approx G_1$ ;  $G(w)$  therefore has property  $P$ . If  $\vdash_{-\pi} w = 1$  does not hold then, by clause (3) of Definition 1.2,  $G_\pi$  (i.e.  $G$ ) is isomorphic to a subgroup of  $G_{\pi_w}$ ; combining this fact with (1.1) and (1.2) we get that  $G_2$  is isomorphic to a subgroup of  $G(w)$ . But  $G_2$  cannot be isomorphic to a subgroup of a finitely presentable group having property  $P$ ; thus  $G(w)$  does not have the property  $P$ .

Assume now that we have a general effective method of deciding, for every presentation  $\Pi' \in Q$ , whether  $G_{\pi'}$  has property  $P$ . If  $w$  is any word on the generators of  $\Pi$ , we can effectively obtain the presentation  $\Pi_w$  of the test group  $G_{\pi_w}$ . From  $\Pi_1$  and  $\Pi_w$  we can effectively obtain a presentation  $\Pi(w) \in Q$  of  $G(w)$ . According to our assumption we can effectively recognize from  $\Pi(w)$  whether  $G(w)$  has the property  $P$ ; by the previous paragraph we thus have a general effective method of deciding whether  $\vdash_{-\pi} w = 1$ . But the word problem of  $\Pi$  is not recursively solvable, thus

Theorem 1.1 is proven by *reductio ad absurdum*.

#### 1.4. Algebraic lemmas

The method of constructing the test group  $\Pi_w$  corresponding to a pair  $(\Pi, w)$  is to add to  $\Pi$  new generators and new defining relations connecting these generators with  $w$  in such a fashion that if  $\vdash_{\pi} w = 1$  then the new generators become equal to one; and also add relations connecting the new generators with the original generators in such a way that setting the new generators equal to one will imply equality to one of the original generators and thus reduce  $\Pi_w$  to triviality. At the same time we must guarantee that when  $\vdash_{\pi} w = 1$  does not hold, no new relations arise between the original generators. To achieve the construction along these lines we need the following Lemmas 1–7.

If  $\Pi$  is a presentation then  $G_{\pi}$  will be called *the group defined by  $\Pi$* . In the following we shall often have occasion to modify a presentation

$$\Pi = (x_1, \dots, x_n : r_1(x), \dots, r_m(x)),$$

by adding to it generators and defining relations, into a presentation

$$\Pi' = (x_1, \dots, x_n, \dots, x_{n'} : r_1(x), \dots, r_m(x), \dots, r_{m'}(x)).$$

When we say that  $G_{\pi}$  is *embedded* in  $G_{\pi'}$  we mean that mapping the generators of  $\Pi$  identically onto the same generators of  $\Pi'$ ,  $x_i \rightarrow x_i$ ,  $i = 1, \dots, n$ , induces an isomorphic mapping of  $G_{\pi}$  into  $G_{\pi'}$ . If  $G_{\pi}$  is embedded in  $G_{\pi'}$  we shall refer to the subgroup of  $G_{\pi'}$  generated by  $x_1, \dots, x_n$  as *the subgroup  $G_{\pi}$  of  $G_{\pi'}$* .

LEMMA 1. *In the group  $F$  defined by*

$$(1.3) \quad (u, t : ut = t^2u),$$

*$u$  and  $t$  have infinite order and an equation  $u^i = t^r$  can hold only if  $i = r = 0$ .*

For a proof see [4].

LEMMA 2. *Let  $H_0$  be the group defined by*

$$\Pi_0 = (x_1, \dots, x_{n+1} : r_1(x), \dots, r_m(x)) = (x : r(x)),$$

*and let  $u(x)$  have infinite order in  $H_0$ . The group  $H_0$  is embedded in the group  $H_1$  defined by*

$$\Pi_1 = (x, t : r(x), u(x)t = t^2u(x)),$$

*and an equation  $p(x) = t^r$  can hold in  $H_1$  only if  $r = 0$ ; in particular  $t$  has infinite order in  $H_1$ .*

PROOF.  $u(x)$  generates an infinite cyclic subgroup of  $H_0$ , and  $u$



generates, by Lemma 1, an infinite cyclic subgroup of  $F$ . We can therefore form the free product of  $H_0$  and  $F$  with the amalgamation  $u(x) = u$ ; denote this product by  $H'_1$

$$H'_1 = (H_0 * F)_{u(x)=u} .$$

$H'_1$  is presented by

$$\Pi'_1 = (x, t, u : r(x), ut = t^2u, u(x) = u) .$$

By the theorem about free products with amalgamated subgroups,  $H_0$  and  $F$  are embedded in  $H'_1$ . Furthermore, since  $p(x) \in H_0$  and  $t^r \in F$ , an equation  $p(x) = t^r$  can hold in  $H'_1$  only if  $t^r$  is in the amalgamated subgroup, i.e. only if  $t^r = u^i$  holds in  $F$  for some integer  $i$ ; Lemma 1 now implies  $r = 0$ .

To complete the proof observe that the relation  $ut = t^2u$  of  $\Pi'_1$  can be replaced by the relation  $u(x)t = t^2u(x)$  (since  $u(x) = u$ ), thus we get a presentation

$$\Pi''_1 = (x, t, u : r(x), u(x)t = t^2u(x), u(x) = u)$$

of the same group  $H'_1$ .

$\Pi''_1$  differs from  $\Pi_1$  by having the extra generator  $u$  and this  $u$  appears only in the relation  $u(x) = u$ . The mapping

$$x_i \rightarrow x_i, i = 1, \dots, n + 1, t \rightarrow t, u \rightarrow u(x),$$

therefore induces an isomorphism of  $H'_1$  onto  $H_1$ ; this completes the proof.

In the following Lemmas 3-7 the notations  $H_0$  and  $u(x)$  retain the same meaning as in Lemma 2.

LEMMA 3.  $H_0$  is embedded in the group  $H_2$  defined by

$$\Pi_2 = (x, t, a : r(x), u(x)t = t^2u(x), ta = a^2t) .$$

Furthermore the subgroup of  $H_2$  generated by  $x_1, \dots, x_{n+1}, a$ , call it  $H_a$ , is the free product of the subgroup generated by  $a$  with the subgroup generated by  $x_1, \dots, x_{n+1}$ .

PROOF. Since  $t$  has infinite order in  $H_1$ , it is a corollary of Lemma 2 that  $H_1$  is embedded in  $H_2$ . But  $H_0$  is embedded in  $H_1$ , hence  $H_0$  is embedded in  $H_2$ .

To prove the second assertion we must show that there is no non-trivial relation between products of  $x_1, \dots, x_{n+1}$  and powers of  $a$ . Let  $F'$  be defined by

$$(1.4) \quad (u, a : ua = a^2u) .$$

Form the free product with amalgamation

$$(1.5) \quad H'_2 = (H_1 * F^n)_{t=u};$$

from (1.4) and (1.5) we see that  $H'_2$  is presented by

$$\Pi'_2 = (x, t, a, u: r(x), u(x)t = t^2u(x), ua = a^2u, t = u).$$

Any non-trivial relation in  $H'_2$  between products of  $x_1, \dots, x_{n+1}$  and powers of  $a$  can be reduced to the form

$$(1.6) \quad a^{i_1}p_1(x) \cdots a^{i_r}p_r(x) = 1$$

where

$$(1.7) \quad i_j \neq 0, p_j(x) \neq 1, \quad j = 1, \dots, r.$$

Now (1.7) implies that  $a^{i_j}$  is not in the subgroup of  $F^n$  generated by  $u$ , and, by Lemma 2, that  $p_j(x)$  is not in the subgroup of  $H_1$  generated by  $t$ . Therefore an equation (1.6) cannot hold in the free product with amalgamation (1.5). Hence there does not exist in  $H'_2$  any non-trivial relation between products of the generators  $x$  and powers of  $a$ .

Considerations similar to those used at the end of the proof of Lemma 2 (i.e. application of Tietze transformations) show that  $H'_2$  is actually isomorphic to  $H_2$  under a mapping which acts identically on  $x_1, \dots, x_{n+1}$ , and  $a$ . This completes the proof of the second assertion.

Since the subgroup of  $H_2$  generated by  $x_1, \dots, x_{n+1}$  is  $H_0$ , the second assertion can be summarized by

$$(1.8) \quad H_a = H_0 * (a).$$

Notice that  $(a)$  is infinite cyclic.

LEMMA 4.  $H_0$  is embedded in the group  $H_3$  defined by

$$(1.9) \quad \Pi_3 = (x, t, a, s, b: r(x), u(x)t = t^2u(x), ta = a^2t, \\ u(x)s = s^2u(x), sb = b^2s).$$

Furthermore the subgroup  $H_{a,b}$  of  $H_3$  generated by  $x_1, \dots, x_n, a, b$  is isomorphic to the free product

$$H_0 * (a, b).^5$$

PROOF.  $\Pi_3$  is obtained from  $\Pi_2$  by adding two new generators  $s, b$ , and adding the defining relations

$$u(x)s = s^2u(x), sb = b^2s.$$

Now  $u(x)$  has infinite order in  $H_2$ ; thus Lemma 3, with  $H_2$  instead of  $H_0$  and  $H_3$  instead of  $H_2$ , applies. This implies that  $H_2$  is embedded in  $H_3$ ; since  $H_0$  is embedded in  $H_2$  this yields the first assertion.

<sup>5</sup>  $(a, b)$  is the free group on the generators  $a$  and  $b$ .

Again by Lemma 3 (for  $H_2$  and  $H_3$ ) the subgroup of  $H_3$  generated by  $x_1, \dots, x_{n+1}, t, a, b$ , is the same as

$$(1.10) \quad H_2 * (b).$$

But the subgroup of  $H_3$  generated by  $x_1, \dots, x_{n+1}, a$ , i.e.  $H_a$ , is contained in the first factor of (1.10), i.e. in  $H_2$ , combining with the preceding statement this yields

$$H_{a,b} = H_a * (b).$$

By (1.8) we now get

$$H_{a,b} = (H_0 * (a)) * (b) = H_0 * ((a) * (b)) = H_0 * (a, b),$$

the last step following from the fact that  $(a)$  and  $(b)$  are infinite cyclic.

LEMMA 5. *In the free group  $(a, b)$  the elements*

$$(1.11) \quad a, bab^{-1}, \dots, b^{n+1}ab^{-n-1}, \text{ and } b^{n+2}aba^{-1}b^{-n-2},$$

*are free generators of the subgroup they generate, i.e. they do not satisfy any non-trivial relation.*

PROOF. The following equations obviously hold for all positive and negative integers  $k$ :

$$(b^i ab^{-i})^k = b^i a^k b^{-i} [i = 0, \dots, n + 1], (b^{n+2} aba^{-1} b^{-n-2})^k = b^{n+2} a^k a^{-1} b^{-n-2}.$$

Keeping these equations in mind it is readily seen that in any non-trivial product of powers of the elements (1.11) the adjacent powers of  $b$  never cancel out; the product therefore reduces to a non-trivial product of powers of  $a$  and powers of  $b$  and consequently is not equal to 1.

LEMMA 6. *In the group  $H_3$ , defined by (1.9) in Lemma 4, the elements*

$$(1.12) \quad a, x_i b^i a b^{-1} [i = 1, \dots, n + 1], b^{n+2} aba^{-1} b^{-n-2}$$

*are free generators of the subgroup  $U$  they generate. Thus  $U$  is a free group on  $n + 3$  generators.*

PROOF. All these elements lie in the subgroup of  $H_3$  generated by  $x_1, \dots, x_{n+1}, a, b$ . By Lemma 4 this subgroup is isomorphic to  $H_0 * (a, b)$ .

The mapping  $x_i \rightarrow 1, i = 1, \dots, n + 1$ , induces the trivial homomorphism  $\varphi$  of  $H_0$  into  $(a, b)$ . The mapping  $a \rightarrow a, b \rightarrow b$ , induces a homomorphism  $\psi$  of  $(a, b)$  into  $(a, b)$  ( $\psi$  being in fact an isomorphism onto). It follows from the basic properties of the free product that  $\varphi$  and  $\psi$  can be extended to a homomorphism  $\eta$

$$\eta : H_0 * (a, b) \rightarrow (a, b).$$

Since  $\eta$  extends both  $\varphi$  and  $\psi$ :

$$(1.13) \quad \eta(x_i) = 1 [i = 1, \dots, n + 1], \eta(a) = a, \eta(b) = b.$$

Let  $p$  be a non-trivial product of the elements (1.12), thus  $p \in H_0^*(a, b)$ . Because of (1.13) these elements go under  $\eta$  into the elements (1.11). The element  $\eta(p)$  is therefore a non-trivial product of the words (1.11), hence by Lemma 5  $\eta(p) \neq 1$ ; since  $\eta$  is a homomorphism this implies  $p \neq 1$ .

LEMMA 7.  $H_0$  is embedded in the group  $H_1$  defined by

$$\begin{aligned} \Pi_1 &= (x_1, \dots, x_{n+1}, t, a, s, b, c, d: r(x), u(x)t = t^2u(x), ta = a^2t, \\ u(x)s &= s^2u(x), sb = b^2s, a = c, x_i b^i a b^{-i} = d_i c d^{-i} [i = 1, \dots, n + 1], \\ & b^{n+2} a b a^{-1} b^{-n-2} = d^{n+2} c d c^{-1} d^{-n-2}). \end{aligned}$$

PROOF. Let  $F''$  be the free group defined by  $(c, d)$ . The elements

$$c, d c d^{-1}, \dots, d^{n+1} c d^{-n-1}, d^{n+2} c d c^{-1} d^{-n-2},$$

constitute, by Lemma 5,  $n + 3$  free generators of the free subgroup  $V$  they generate. Recalling Lemma 6 we see that the correspondence

$$a \leftrightarrow c, x_i b^i a b^{-i} \leftrightarrow d^i c d^{-i} [i = 1, \dots, n + 1], b^{n+2} a b a^{-1} b^{-n-2} \leftrightarrow d^{n+2} c d c^{-1} d^{-n-2},$$

induces an isomorphism between  $U$  (Lemma 6) and  $V$ . Using this isomorphism we can form the free product with amalgamated subgroups

$$(H_3 * F'')_{U=V}.$$

Comparing with the presentation (1.9) of  $H_3$ , we see that  $\Pi_1$  is precisely the presentation of this free product with amalgamation, thus

$$H_1 = (H_3 * F'')_{U=V}.$$

$H_3$  is therefore embedded in  $H_1$ ; by Lemma 4,  $H_0$  is embedded in  $H_3$ , hence  $H_0$  is embedded in  $H_1$ .

### 1.5. The case $u(x) = 1$

Lemmas 2-7 were proved under the assumption that  $u(x)$  has infinite order in  $H_0$ . Note that if on the other hand  $u(x) = 1$  in  $H_0$  then  $\Pi_1$  defines the trivial unit-element group. Indeed,  $u(x) = 1$  and  $u(x)t = t^2u(x)$  imply  $t = 1$ , combining with  $ta = a^2t$  we get  $a = 1$ ; similarly  $s = 1$  and  $b = 1$ ;  $a = c$  now implies  $c = 1$ , and  $b^{n+2} a b a^{-1} b^{-n-2} = d^{n+2} c d c^{-1} d^{-n-2}$  implies (since  $a = b = c = 1$ ) that  $d = 1$ ; finally  $x_i b^i a b^{-i} = d^i c d^{-i}$  implies  $x_i = 1$  for  $i = 1, \dots, n + 1$ . Thus, assuming that  $u(x) = 1$ , all the generators of  $H_1$  are equal to 1, hence  $H_1 \approx 1$ .

### 1.6. Proof of Theorem 1.2

Given a pair  $(\Pi, w)$ , where

$$Q \ni \Pi = (x_1, \dots, x_n: r(x))$$

and  $w$  is a word on the generators of  $\Pi$ , define a presentation  $\Pi_w \in Q$  as follows

- (a) add to  $\Pi$  the generators  $x_{n+1}, x_{n+2}, \dots, x_{n+7}$ ;
- (b) add the defining relations resulting from

$$\begin{aligned} u(x)t &= t^2u(x), \quad ta = a^2t, \quad u(x)s = s^2u(x), \quad sb = b^2s, \quad a = c, \\ x_i b^i a b^{-i} &= d^i c d^{-i} \quad [i = 1, \dots, n + 1], \\ b^{n+2} a b a^{-1} b^{-n-2} &= d^{n+2} c d c^{-1} d^{-n-2}, \end{aligned}$$

by substituting  $x_{n+2}, x_{n+3}, \dots, x_{n+7}$  for  $t, a, s, b, c, d$ , respectively, and substituting  $x_{n+1} w x_{n+1}^{-1} w$  for  $u(x)$ ;

- (c) rearrange the totality of relations now present (i.e. the relations  $r(x)$  plus the new relations added) so as to conform with requirements (2) and (3) of Definition 1.1.

The function  $\tau$

$$\tau : (\Pi, w) \rightarrow \Pi_w,$$

assigning to each pair  $(\Pi, w)$  the presentation  $\Pi_w \in Q$  described above, is a test group construction.

It is indeed clear that the instructions (a), (b), and (c), are effective and  $\tau$  is therefore a recursive function.

Denote by  $\Pi_0$  the presentation obtained by taking  $\Pi$  together with the generator  $x_{n+1}$  (compare Lemma 2).  $\Pi_w$  has, apart from obvious changes of letters, the form of  $\Pi_1$  of Lemma 7.

If  $\vdash_{\pi} w = 1$ , then  $\vdash_{\pi_0} x_{n+1} w x_{n+1}^{-1} w = 1$ ; the remark in Section 1.5 now implies that  $G_{\pi_w} \approx 1$ .

If  $\vdash_{\pi} w = 1$  does not hold, then  $x_{n+1} w x_{n+1}^{-1} w$  has infinite order in  $G_{\pi_0}$ . Indeed, by our definition

$$(1.14) \quad G_{\pi_0} = G_{\pi} * (x_{n+1});$$

therefore, since  $w \in G_{\pi}$  and  $w \neq 1$ , a product

$$(x_{n+1} w x_{n+1}^{-1} w)^m = x_{n+1} w x_{n+1}^{-1} w x_{n+1} w x_{n+1}^{-1} w \dots$$

cannot be equal to 1 in the free product (1.14);  $u(x) = x_{n+1} w x_{n+1}^{-1} w$  thus has infinite order in  $G_{\pi_0}$ . By Lemma 7,  $G_{\pi_0}$  is therefore embedded in  $G_{\pi_w}$ ; hence, by (1.14),  $G_{\pi}$  is embedded in  $G_{\pi_w}$ .

## II. CONSEQUENCES OF THE MAIN THEOREM

### 2.1. Hereditary properties

Many of the consequences of the main theorem are immediate corollaries of the following result.

**THEOREM 2.1.** *Let  $P$  be an algebraic property of finitely presentable (f.p.) groups such that (1) there exist at least one f.p. group  $G_1$  having property  $P$ , and at least one f.p. group  $G_2$  which does not have the property  $P$ , (2)  $P$  is hereditary, i.e. if a f.p. group has the property  $P$  then all its f.p. subgroups have  $P$ . There does not exist a general and effective method of deciding, for every given presentation, whether the group defined by it has the property  $P$ .*

**PROOF.** This is a special case of Theorem 1.1. Indeed, because of condition 2,  $G_2$  is not isomorphic to any subgroup of a f.p. group possessing  $P$ . Thus  $P$  satisfies the two conditions of Theorem 1.1.

## 2.2. Immediate corollaries

Each of the algebraic properties enumerated in Theorems 2.2–2.8 is hereditary. In each case it is also clear that there exist f.p. groups having the property and also f.p. groups which do not have it. Therefore, by Theorem 2.1, there does not exist a general and effective method of deciding, for every given presentation  $\Pi$ , whether  $G_\pi$  has the property in question.

**THEOREM 2.2. Triviality.** (I.e. there does not exist a general and effective method of deciding, for every given presentation  $\Pi$ , whether  $G_\pi \approx 1$ . The other theorems should be read in a similar fashion.)

**THEOREM 2.3. Cyclicity.**

**THEOREM 2.4. Finiteness.**

**THEOREM 2.5. Being locally infinite.**<sup>6</sup>

**THEOREM 2.6. Being a free group.** (That every subgroup of a free group is a free group is the content of the Nielsen-Schreier theorem, see [11, 14; 7, pp. 33–36].)

**THEOREM 2.7. Commutativity.**

**THEOREM 2.8. Solvability.**

To each presentation there belongs a group which is uniquely and completely defined by it. For this reason presentations can be used for defining various groups. The above given results indicate however that though a group is completely defined by a presentation in general one can obtain from this presentation very little information about the group itself. This fact is most strikingly exemplified by Theorem 2.2; in general we know so little about a group given by a presentation that we cannot even say whether the group is trivial or not.<sup>7</sup> Compare with Kuroš's remarks in [6, pp. 131–132]; for all the group theoretic proper-

<sup>6</sup> A group is *locally infinite* if, excepting the unit element, each of its elements has infinite order.

<sup>7</sup> I am indebted to Professor W. Magnus for this remark.

ties he discusses there we have proved the non-existence of an effective decision procedure.

### 2.3. Free and direct products

**THEOREM 2.9.** *There does not exist a general and effective method of deciding, for every presentation  $\Pi$ , whether  $G_\pi$  is decomposable into a non-trivial free product.*

**PROOF.** Let  $F$  be the group defined by  $(x_1 : x_1^2 = 1)$ .  $F$  is a non-trivial group which is not decomposable into a free product. Let  $\Pi_1 = (x_1, \dots, x_n : r(x))$  be any presentation whatsoever. Form the presentation  $\Pi$ ,  $\Pi = (x_1, \dots, x_n, x_{n+1} : r(x), x_{n+1}^2 = 1)$ . Obviously  $G_\pi \approx G_{\pi_1} * F$ . Thus  $G_\pi$  is decomposable if and only if  $G_{\pi_1} \neq 1$ . Theorem 2.2 now yields the desired result.

**THEOREM 2.10.** *There does not exist a general effective method of deciding, for every presentation  $\Pi$ , whether  $G_\pi$  is decomposable into a non-trivial direct product.*

The proof of this theorem parallels so closely the previous proof that it need not be given here.

The following theorem was suggested to me by Mr. S. Kochen.

**THEOREM 2.11.** *There does not exist a general and effective method of deciding, for every given presentation  $\Pi$ , whether  $G_\pi$  is a free product of finite groups.*

**PROOF.** The property of being a free product of finite groups is certainly an algebraic property. Furthermore every finite group has this property (here we do not insist on non-triviality of the product).

Let  $G$  be the group defined by  $(x_1, x_2 : x_1 x_2 = x_2 x_1)$ .  $G$  is commutative, infinite, but not cyclic. We claim that  $G$  is not isomorphic to any subgroup of a free product of finite groups. Indeed, let  $H$  be a free product of finite groups  $H = H_1 * \dots * H_n$ ,  $1 \leq n$ ,  $H_i$  finite. By the Kuroš Subgroup Theorem (see [7, pp. 17-26]), every subgroup  $H' \subseteq H$  has the form

$$(2.1) \quad H' = F * H'_1 * \dots * H'_n$$

where  $F$  is a free group and  $H'_i$  is conjugate, in  $H$ , to a subgroup of  $H_i$ . If  $H'$  is commutative, then the number of non-trivial factors in (2.1) cannot exceed one. Thus  $H' = F$  and  $F$  is infinite cyclic, or  $H' = H'_i$  for some  $i$ . If we further assume that  $H'$  is infinite then the second possibility is ruled out because the  $H'_i$  are finite groups. Every commutative infinite subgroup of a free product of finite groups is thus cyclic.  $G$  which is commutative, infinite, but not cyclic, is not isomorphic to such a subgroup.

We have shown that all the conditions of the Main Theorem 1.1 are

fulfilled so the desired result now follows.

#### 2.4. Simple groups

**THEOREM 2.12.** *There does not exist a general effective method of deciding, for every given presentation  $\Pi$ , whether  $G_\pi$  is a simple group.*

**PROOF.** Repeat word by word the construction given in the proof of Theorem 2.9. Note that the group  $F$  is simple and that, therefore,  $G_\pi$  is simple if and only if  $G_{\pi_1} \approx 1$ . Now apply Theorem 2.2.

#### 2.5. Groups with one defining relation

These groups, which are in a sense quite similar to free groups, were the subject of an extensive study by a number of algebraists. In particular positive results concerning decision problems were obtained. W. Magnus showed [8] that the word problem of every group with one defining relation is effectively solvable. J. H. C. Whitehead gave in [16] an algorithm for deciding, for every presentation  $\Pi$  having only one defining relation, whether  $G_\pi$  is a free group. On the other hand the isomorphism problem for groups with one defining relation is still open.

**THEOREM 2.13.** *There does not exist a general effective method of deciding, for every given presentation  $\Pi$ , whether  $G_\pi$  is definable by a single relation, i.e. whether there exists a presentation  $\Pi'$  having only one defining relation such that  $G_\pi \approx G_{\pi'}$ .*

**PROOF.** The property of being definable by a single relation is certainly algebraic. Furthermore there are groups possessing this property.

Let  $\Pi$  be a presentation for which the word problem is not recursively solvable. By the Magnus Theorem, the word problem of a presentation having one defining relation is recursively solvable. Theorem 2.15 now implies that  $G_\pi$  is not isomorphic to any subgroup of a group defined by a presentation with a single relation.

Thus the two conditions of the Main Theorem 1.1 are satisfied and our assertion follows.

An alternative proof of this last result can be obtained by combining Whitehead's theorem with Theorem 2.6.

#### 2.6. Presentations with a solvable word problem

Following the terminology and definitions of Section 0.1 we say that the word problem of a presentation  $\Pi$  is *effectively solvable* if the characteristic function of the set of words  $w$  for which  $\vdash_\pi w = 1$  is effectively computable (recursive). The *meta word problem* is the problem of deciding, for every given presentation  $\Pi$ , whether the word problem of  $\Pi$  is



effectively solvable; we intend to show that the meta word problem itself is not effectively solvable. This will follow from Theorem 2.1 but since we are dealing with a property of presentations (whereas Theorem 2.1 deals with properties of groups) some care must be exercised in the proof; we need in fact two preliminary theorems.

**THEOREM 2.14.** *If  $\Pi$  and  $\Pi'$  are presentations such that  $G_\pi \approx G_{\pi'}$ , then the word problems of  $\Pi$  and  $\Pi'$  are either both effectively solvable or both not effectively solvable.*

This shows that the effective solvability of the word problem of a presentation  $\Pi$  has algebraic meaning inasmuch as it is determined by the algebraic structure of  $G_\pi$ .

**THEOREM 2.15.** *If  $\Pi$  and  $\Pi'$  are presentations such that  $G_\pi$  is isomorphic to a subgroup of  $G_{\pi'}$  and if the word problem of  $\Pi$  is effectively solvable, then the word problem of  $\Pi'$  is effectively solvable.*

The analogues, for the case of finitely presented semigroups, of Theorems 2.14 and 2.15, are implicitly contained in Markov's paper [10].

Proofs for these two results will be given elsewhere.

**THEOREM 2.16.** *There does not exist a general and effective method of deciding, for every given presentation  $\Pi$ , whether the word problem of  $\Pi$  is effectively solvable.*

**PROOF.** The property of having at least one presentation with an effectively solvable word problem is an algebraic property of f.p. groups. The trivial group possesses this property. Let  $\Pi_0$  be a presentation for which the word problem is not effectively solvable then  $G_{\pi_0}$  does not have, by Theorem 2.14, any presentation with an effectively solvable word problem. Finally the property is, by Theorem 2.15, hereditary.

Hence, by Theorem 2.1, there does not exist a general and effective procedure of deciding, for every  $\Pi$ , whether  $G_\pi$  has a presentation with an effectively solvable word problem. But  $G_\pi$  has some presentation with an effectively solvable word problem if and only if the word problem of  $\Pi$  itself is effectively solvable.

### III. THE ISOMORPHISM PROBLEM AND ISOMORPHISM INVARIANTS

#### 3.1. The isomorphism problem

An important problem in the theory of finitely presented groups is the isomorphism problem. Two apparently different presentations may define groups which are isomorphic and we would like to have a decision procedure for ascertaining when this is happening. It turns out that there does not exist a general and effective procedure of deciding, for every

two presentations  $\Pi$  and  $\Pi'$ , whether  $G_\pi \approx G_{\pi'}$ . We shall prove even more, namely that for every *fixed*  $\Pi$  the decision problem, which now becomes a problem involving only the variable presentation  $\Pi'$ , is not effectively solvable.

**THEOREM 3.1.** *Let  $G_0$  be a fixed f.p. group. There does not exist a general and effective procedure of deciding, for every given presentation  $\Pi_1$ , whether the group defined by it is isomorphic to  $G_0$ .*

**PROOF.** Let  $\Pi_0$  be a fixed (finite) presentation of  $G_0$ . For every presentation  $\Pi$  construct the free product  $G_1 = G_0 * G_\pi$ . A presentation  $\Pi_1$  of  $G_1$  can be effectively obtained from  $\Pi_0$  and  $\Pi$ .

It is a consequence of Grusko's theorem [7, p. 58] that the minimal number of generators for  $G_1$  equals the sum of the corresponding two numbers of  $G_0$  and  $G_\pi$ ; hence  $G_0 \approx G_1$  if and only if  $G_\pi \approx 1$ . An effective procedure of deciding for every given presentation  $\Pi_1$  whether the group defined by it is isomorphic to  $G_0$  would thus lead to an effective method of deciding, for every  $\Pi$ , whether  $G_\pi \approx 1$ ; this would contradict Theorem 2.2.

### 3.2. Infinite systems of isomorphism invariants

When dealing with a mathematical system in which the objects are divided into equivalence classes (e.g. the system of all finite simplicial complexes, the equivalence relation being homeomorphism), one sometimes tries to solve the equivalence problem by constructing a complete system of equivalence invariants.

In the case of the set of all finitely generated commutative groups, for example, the Betti number and torsion coefficients of a group form a complete system of isomorphism invariants; i.e., two commutative groups are isomorphic if and only if their respective Betti numbers and torsion coefficients agree. This system of invariants has the additional features that (a) their number, for each particular group, is finite, (b) given a presentation  $\Pi$  of a commutative group one can effectively compute from it the Betti number and torsion coefficients of the corresponding group.

The previous result implies that a finite and complete system of computable isomorphism invariants for the set of all presentations is not possible. At this point there naturally arises the question whether it is possible to construct an infinite and complete system of computable isomorphism invariants. Let us first of all define the latter concept in a precise manner.

Assume that the set  $Q$  of all presentations has been indexed in some effective fashion (i.e. that we have a Gödel numbering of  $Q$ ) and let  $i$  be

the indexing function.  $i(\Pi)$  is then the index of  $\Pi$  and  $\Pi_n$  is the presentation having the integer  $n$  as index.

DEFINITION 3.1. An *infinite system of isomorphism invariants* is a function  $f(n, m)$  from integers to integers such that for every two presentations  $\Pi_n$  and  $\Pi_{n'}$ , if

$$G_{\pi_n} \approx G_{\pi_{n'}}$$

then

$$f(n, m) = f(n', m), \quad m = 0, 1, \dots$$

The system is *complete* if

$$G_{\pi_n} \not\approx G_{\pi_{n'}}$$

implies that

$$f(n, m) \neq f(n', m) \quad \text{for some integer } m.$$

If  $f$  is a computable (recursive) function then we call it an *infinite system of computable invariants*.

THEOREM 3.2. *Every infinite system of computable isomorphism invariants is not complete.*

The idea lying behind the proof is that a complete infinite system of computable isomorphism invariants would furnish an effective enumeration of all presentations  $\Pi' \in Q$  which define a group *not* isomorphic to the group defined by a fixed presentation  $\Pi$ . For, if  $i(\Pi) = i_0$ , one can compute on the one hand the invariants  $f(i_0, 0), f(i_0, 1), \dots$ , of  $\Pi$  and on the other hand the totality of invariants  $f(n, m)$  arranged in some fixed sequence; whenever  $f(n, m) \neq f(i_0, m)$  one knows that  $G_{\pi_n} \not\approx G_{\pi}$  and every  $\Pi'$  for which  $G_{\pi'} \not\approx G_{\pi}$  will be discovered in this way. In the next section we shall prove that the presentations  $\Pi''$  which define the same group as  $\Pi$  are also effectively enumerable. We would now have the following effective solution for the isomorphism problem. Given two presentations  $\Pi$  and  $\Pi'$ , enumerate effectively the sequence  $\Gamma_1$  of presentations defining a group not isomorphic to  $G_{\pi}$ , and enumerate effectively the sequence  $\Gamma_2$  of presentations defining the same group as  $\Pi$ ; the presentation  $\Pi'$  must appear, after a finite number of steps, either in  $\Gamma_1$  or in  $\Gamma_2$ , when it appears we know whether  $G_{\pi} \not\approx G_{\pi'}$  or not. But the isomorphism problem is not effectively solvable; this contradiction shows that a complete infinite system of computable isomorphism invariants does not exist.

The rigorous proof of Theorem 3.2 will be given in Section 3.4. The next section is devoted to the necessary preliminaries concerning effective

enumerability of sets of presentations.

### 3.3. Recursive enumerability

Let us retain the indexing of the set  $Q$  introduced in Section 3.2. A set  $P$  of integers is called *recursively enumerable* if there exists an effectively computable function  $f$  such that  $P = \{f(n) \mid n = 0, 1, \dots\}$ . In that case we shall also say that  $f$  *effectively enumerates*  $P$ .

**THEOREM 3.3.** *There exists an effectively computable (recursive) function  $e(n, k)$  from integers to integers such that for every integer  $n$  the set*

$$P_n = \{\Pi_{e(n,k)} \mid k = 0, 1, \dots\}$$

*consists precisely of all presentations  $\Pi \in Q$  for which  $G_\pi \approx G_{\pi_n}$ .*

*Fixing  $n$  and letting  $k$  run through the integers,  $e(n, k)$  thus effectively enumerates the indices of all presentations defining the same abstract group as  $\Pi_n$ .*

**PROOF.** The proof is obtained by using the so-called Tietze transformations which allow us to modify a presentation without changing the group defined by it [15], [7, pp. 70–75]. Let  $\Pi = (x, r(x))$  and  $\Pi' = (x: r(x), w(x) = 1)$  where  $w(x)$  is a word on the generators  $x$  such that  $\vdash_\pi w(x) = 1$ , then  $\Pi$  and  $\Pi'$  define the same group. Thus adding, or deleting, a defining relation which is a consequence of the remaining relations (Tietze transformation of the first kind) does not change the group. If

$$\Pi = (x:r(x)) \text{ and } \Pi'' = (x, b:r(x), bu(x) = 1)$$

where  $b$  is a generator not appearing among the generators  $x$  and  $u(x)$  is a word on the generators  $x$ , then  $\Pi$  and  $\Pi''$  define the same abstract group. Thus adding, or deleting, a generator which is defined by means of the remaining generators and at the same time adding, or deleting, the relation giving that generator as a product of the remaining generators (Tietze transformation of the second kind), yields a group isomorphic to the original group. Tietze's theorem states that if two finite presentations  $\Pi^{(0)}$  and  $\Pi$  define isomorphic groups then they can be linked by a finite number of presentations  $\Pi^{(0)}, \Pi^{(1)}, \dots, \Pi^{(k)} = \Pi$  such that for all  $i$ ,  $\Pi^{(i+1)}$  is obtained from  $\Pi^{(i)}$  by a Tietze transformation. Thus to enumerate all the presentations defining the same group as a given presentation  $\Pi_n$  one should apply to  $\Pi_n$  all possible sequences of Tietze transformations. Note however that to recognize whether a transition from  $\Pi = (x:r(x))$  to  $\Pi = (x:r(x), w(x) = 1)$  is a Tietze transformation involves deciding whether  $\vdash_\pi w(x) = 1$ , which decision problem is not effectively solvable. In order to obtain an effective enumeration we shall

proceed as follows.

Call an equation  $p(x) = w(x)$ , where  $p(x)$  and  $w(x)$  are words on  $x_1, x_2, \dots, x_n$ , a *deduction of  $w(x) = 1$  from the relations  $r_1(x) = 1, \dots, r_m(x) = 1$* , if  $p(x)$  is a concatenation of words of the form  $(t_i(x)r_i(x)t_i^{-1}(x))^{\pm 1}$  where the  $t_i(x)$  are words on the generators  $x$ , and if  $w(x)$  is the reduced form of  $p(x)$ . There is, obviously, a general and effective procedure of deciding, for every given system of relations  $r(x)$  and equation  $p(x) = w(x)$ , whether  $p(x) = w(x)$  is a deduction of  $w(x) = 1$  from the relations  $r(x)$ .

A sequence  $\langle A_0, A_1, \dots, A_i \rangle$ , where each  $A_i$  is either a presentation or an equation, will be called a *proof of isomorphy* if  $A_0$  and  $A_k$  are presentations and if for all  $0 < i$  for which  $A_i$  is a presentation, either  $A_i$  is obtained from  $A_{i-2}$  by a Tietze transformation of the first kind and  $A_{i-1}$  is an equation which is a deduction, from the remaining relations of  $A_{i-1}$ , of the relation added or deleted during the transformation; or  $A_{i-1}$  is a presentation and  $A_i$  is obtained from  $A_{i-1}$  by a Tietze transformation of the second kind. It is again clear that there is a general and effective procedure of deciding, for every given sequence, whether it is a proof of isomorphy.

Let  $\Gamma = S_0, S_1, \dots$ , be a fixed and effective enumeration of all finite sequences  $S = \langle A_0, \dots, A_m \rangle$  ( $m$  is arbitrary), where each  $A_i$  is either a finite presentation or an equation on the generators  $x_1, x_2, \dots$  (compare Definition 1.1). Define a function  $e(n, k)$  from integers to integers as follows: If  $S_i = \langle A_0, \dots, A_m \rangle$  is the  $k^{\text{th}}$  element of  $\Gamma$  such that  $S_i$  is a proof of isomorphy and  $A_0 = \Pi_n$  and  $A_m \in Q$ , then  $e(n, k)$  is the index of  $A_m$  (under the indexing of  $Q$  introduced in Section 3.2).

The enumeration of  $\Gamma$ , the procedure of recognizing whether an element of  $\Gamma$  is a proof of isomorphy, and the computation of the index of a presentation in  $Q$ , are all effective processes; the function  $e(n, k)$  is therefore effectively computable. Since  $S_i$  is a proof of isomorphy and  $A_0 = \Pi_n, A_m = \Pi_{e(n,k)}$ , it follows that  $\Pi_n$  and  $\Pi_{e(n,k)}$  define isomorphic groups. Finally, Tietze's theorem implies that if  $\Pi' \in Q$  is any presentation such that  $G_{\pi_n} \approx G_{\pi'}$  then there exists a proof of isomorphy  $S = \langle A_0, \dots, A_m \rangle$  such that  $A_0 = \Pi_n$  and  $A_m = \Pi'$ , hence  $i(\cdot)\Pi = e(n, k)$  for some  $k$ . The function  $e(n, k)$  thus fulfills the conditions of the theorem.

While we are at it let us get further results along these lines.

**THEOREM 3.4.** *If  $P \subseteq Q$  is a recursively enumerable subset of  $Q$  then  $\bar{P}$ , the closure of  $P$  under isomorphisms,*

$$\bar{P} = \{ \Pi \mid \Pi \in Q, \text{ exists } \Pi' \in P \text{ such that } G_{\pi} \approx G_{\pi'} \},$$

*is also recursively enumerable.*

PROOF. Let  $f(n)$  be the computable function enumerating the indices of the presentations in  $P$ . Let  $a(n)$  and  $b(n)$  be a pair of computable functions such that  $\langle a(n), b(n) \rangle$  enumerates all ordered pairs of integers. It is readily seen that the function  $e(f(a(n)), b(n))$  enumerates the set  $\bar{P}$  and is effectively computable.

It follows immediately from this theorem that the sets of all presentations of finite groups, or free groups, or commutative groups, are all recursively enumerable. Compare these statements with the results of Section 2.2 where we prove that all the aforementioned sets are not recursive.

### 3.4. Proof of Theorem 3.2

The reader should consult the end of Section 3.2 about the motivation for the following proof.

Assume to the contrary that  $f(n, m)$  is a complete infinite system of computable invariants.

Let  $e(n, k)$  be the enumerating function introduced in Theorem 3.3. Consider the function  $d(n, p, m)$  from integers to integers defined by

$$d(n, p, m) = \overline{\text{sg}}(|f(n, m) - f(p, m)|)(e(n, m) - p).^8$$

Since  $f$  is a computable function by assumption, and since  $e$  is computable by Theorem 3.3, it follows that  $d$  is a computable function.

Let  $n$  and  $p$  be any two integers. If

$$G_{\pi_n} \approx G_{\pi_p},$$

then  $p$  must appear as a value of the enumerating function  $e(n, m)$  and hence for some  $m_1$  we have  $d(n, p, m_1) = 0$ .

If

$$G_{\pi_n} \not\approx G_{\pi_p}$$

then, since  $f$  is a complete system of invariants, there exists an integer  $m_2$  for which  $f(n, m_2) \neq f(p, m_2)$  and hence  $d(n, p, m_2) \neq 0$ .

The function  $s(n, p)$  defined by

$$s(n, p) = (\mu m)(d(n, p, m) = 0)$$

is therefore a well defined and computable function ( $\mu$  is the minimalization operator, i.e.  $(\mu y)(g(x, y) = 0)$  is the least integer  $y$  such that  $g(x, y) = 0$ ; the reader can verify that if there exists for every  $x$  at least one  $y$  such that  $g(x, y) = 0$ , and if  $g(x, y)$  is computable function of

<sup>8</sup>  $\overline{\text{sg}}(n)$  is the function which assumes the value 1 for  $n = 0$ , and the value 0 for  $n > 0$ .

$x$  and  $y$ , then  $(\mu y)(g(x, y) = 0)$  is a computable function of  $x$ , see [5, pp. 279-282]).

We now have the following effective decision procedure. Given any two presentations  $\Pi \in Q$ ,  $\Pi' \in Q$ , we can find effectively their indices  $i(\Pi) = n$ ,  $i(\Pi') = p$ . Then we can effectively compute  $s(n, p)$  and also  $e(n, s(n, p))$ . Now  $e(n, s(n, p)) = p$  if and only if  $G_{\pi_n} \approx G_{\pi_p}$ , i.e. if and only if  $G_\pi \approx G_{\pi'}$ . We thus have a general and effective method of deciding, for any two given presentations, whether they define isomorphic groups and this contradicts Theorem 3.1. The assumption that  $f$  is a complete infinite system of invariants is therefore false.

### 3.5. Remarks concerning topological problems

An interesting and important prolongation of the study of effective solvability of decision problems would be to carry it over to the classification problems of algebraic topology.

The fact that the isomorphism problem for finite presentations is not effectively solvable, taken in conjunction with the properties of  $K(\Pi, 1)$  space, implies that the homotopy type classification problem for the at most countable simplicial complexes is not effectively solvable (even when restricted to those complexes which, like  $K(\Pi, 1)$  spaces, are given explicitly).

But it seems that the really strong and satisfying results are those which one hopes to get for the strictly finite structures such as finite simplicial complexes. Thus we conjecture that the homeomorphism problem for finite simplicial complexes is not effectively solvable. It even seems plausible that, in analogy to Theorem 3.2 for finite presentations, this classification problem can not be solved by means of a countably infinite system of numerical equivalence invariants. If this last conjecture turns out to be true, it would entail that any system of computable topological invariants similar say to the homology sequence, could not possibly be complete.

At the present moment it is difficult to predict how a proof for these results will be achieved. In view of the connections between finitely presented groups and topological structures it is possible that the results obtained in this paper may be applied. On the other hand, it may be that an entirely new and different approach is necessary.

PRINCETON UNIVERSITY

### BIBLIOGRAPHY

1. J. W. ADDISON, Jr., On some points of the theory of recursive functions, Dissertation, University of Wisconsin, 1954.

2. S. I. ADJAN, *The algorithmic unsolvability of problems concerning certain properties of groups* (Russian) Doklady Akad. Nauk SSSR, vol. 103 (1955), pp. 533-535.
3. W. J. FEENEY, Certain unsolvable problems in the theory of cancellation semi-groups, Dissertation, Catholic University of America, 1954.
4. G. HIGMAN, *A finitely generated infinite simple group*, J. London Math. Soc., vol. 26 (1951), pp. 61-64.
5. S. C. KLEENE, Introduction to Metamathematics, Van Nostrand Co., New York, 1952.
6. A. G. KUROŠ (KUROSH), Theory of Groups, Vol. I, (translated into English from the second Russian edition), Chelsea Publishing Co., New York, 1955.
7. ———, Theory of Groups, Vol. II, (translated into English from the second Russian edition), Chelsea Publishing Co., New York, 1955.
8. W. MAGNUS, *Das Identitätsproblem für Gruppen mit einer definierenden Relation*, Math. Annal., vol. 106 (1932), pp. 295-307.
9. A. MARKOV, *Impossibility of certain algorithms in the theory of associative systems* (Russian), Doklady Akad. Nauk SSSR., vol. 77 (1951), pp. 19-20.
10. ———, *Impossibility of algorithms for recognizing some properties of associative systems* (Russian), Doklady Akad. Nauk SSSR., vol. 77 (1951), pp. 953-956.
11. J. NIELSEN, *Om Regning med ikkekommutative Faktorer og dens Anvendelse i Gruppeteorien*, Mat. Tidsskrift B (1921), pp. 77-94.
12. P. S. NOVIKOV, *On the algorithmic unsolvability of the word problem* (Russian), Doklady Akad. Nauk SSSR., vol. 85 (1952), pp. 708-712.
13. ———, *On the algorithmic unsolvability of the identity problem for groups* (Russian), Trudy Mat. Inst. Steklov, vol. 44, 1955.
14. O. SCHREIER, *Die Untergruppen der freien Gruppen*, Hamb. Abh., vol. 5 (1927), pp. 161-183.
15. H. TIETZE, *Über die topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten*, Monatsh. Math. Phys., vol. 9 (1908), pp. 1-118.
16. J. H. C. WHITEHEAD, *On equivalent sets of elements in a free group*, Ann. of Math., vol. 37 (1936), pp. 782-800.