MATH. SCAND. 3 (1955), 31–43

A BASIS FOR SUBGROUPS OF FREE GROUPS

JAKOB NIELSEN

Recently I took up an earlier subject of my interest [5] with a view to extending its scope. Dr. Wilhelm Magnus, to whom I communicated some results, kindly drew my attention to related publications, some of which are listed in the bibliography. References to that bibliography — which does not pretend to be exhaustive — are indicated by numbers in square brackets. The substance of the result of the present paper is, more or less, covered by earlier publications of F. Levi [4], M. Hall and T. Radó [3][2] and H. Federer and B. Jónsson [1]. However, since the procedure used in the present paper does not involve alphabetical ordering as used in [4] and [2], and does not rest on the use of Schreier systems [3][2], it may not be out of order to publish it. In so doing I have avoided excessive formalization, since the problem is a rather primitive one and can be presented without presupposing expert knowledge in its field. For the same reason the introductory sections state the point of departure rather elaborately, even beyond what is strictly needed in the sequel.

I.

1. Let

$$F = [a_1, a_2, \ldots]$$

denote the free group with the symbols a_ν, $\nu = 1, 2, \ldots$, finite or infinite in number, as a set of free generators. The elements of F are finite, non-commutative products of the a_ν and their inverses a_ν^{-1}. The identity of F will be denoted by 1. If a given "word" in the generators contains the symbols a_ν and a_ν^{-1} as immediate neighbours, it can be shortened by the omission of these two symbols. This process will be called *a-cancellation*. When a "word" $\alpha = \alpha(a)$ indicates an element of F, it is assumed that it is *reduced*, i.e. that it cannot be shortened by a-cancellation. The sum of the absolute values of the exponents of all the a_ν in $\alpha(a)$ is called the *length* of α and denoted by $l(\alpha)$. The identity is the only element of length zero. A product $\alpha(a)\beta(a)$ will, in general, give rise to

Received March 25, 1955.

a-cancellation, hence $l(\alpha\beta) \leqq l(\alpha) + l(\beta)$. The inverse of $\alpha(a)$ contains the symbols of $\alpha(a)$ in the inverse order and with the opposite sign of all exponents.

2. Consider a set

$$S: \quad \alpha_1(a), \alpha_2(a), \ldots,$$

finite or infinite, of reduced elements of F. The α_ν *generate* a certain subgroup of F; let it be denoted by

$$G = [\alpha_1, \alpha_2, \ldots] .$$

G is independent of the order of the α_ν and of the substitution of α_ν^{-1} for α_ν. The set of all α_ν^{-1} will be denoted by S^{-1}, the union of S and S^{-1} by $S \cup S^{-1}$.

The general problem: to decide in a finite number of steps whether a given reduced element $\beta(a)$ of F belongs to G, that is, whether a product of the α_ν and their inverses exists which reduces by a-cancellation to the word $\beta(a)$, has been solved in [5] in the case of a *finite* set S. In the case of an *infinite* set S this problem is still far from solution. The present paper is intended as a modest contribution to this general problem. The importance of the problem is seen from the fact that it contains the "identity problem" of non-free groups as a special case; see sections 15–16, pp. 41–43.

3. It has been known for a long time that every subgroup of a free group is itself free; cf. [6]. Thus G is a free group. This fact will not be used explicitly in the proofs. It is stated here only in order to adapt the wording to existing knowledge. The fact that G is free results by the way from the construction in part II.

Consider a product $P = \prod(\alpha_\nu^{\pm 1})$ of a finite number of elements of $S \cup S^{-1}$. If it reduces to the identity of F by a-cancellation, then $P = 1$ is called a *relation* in the set S. This relation is called trivial if it results by α-cancellation (without inserting the a's explicitly in the α's). Otherwise the relation $P = 1$ is called *essential*. If S admits no essential relations, it is called *unrelated*, otherwise *related*. If S is unrelated, it is a set of free generators of G, and every element of G has a uniquely determined expression in terms of the α's, if it is so written that no α-cancellation is possible. If S contains the identity of F as an element, then S is obviously related.

4. A set

$$T: \quad \beta_1(a), \beta_2(a), \ldots$$

is called *equivalent* to the set S, if T generates the same group G as S. Thereby a distribution of all subsets of elements of F into equivalence classes is constituted. A necessary and sufficient condition for the equivalence of S and T is that every β can be expressed as a product of the α's (in general by a-cancellation) and *vice versa*.

A way of transforming a set into an equivalent set is the following: Let ϱ and σ be two indices of the set S. If one puts

$$\alpha'_\sigma = \alpha_\varrho \alpha_\sigma, \qquad \alpha'_\nu = \alpha_\nu \text{ for all } \nu \neq \sigma,$$

one gets an aquivalent set S'; the inverse substitution

$$\alpha_\sigma = \alpha'^{-1}_\varrho \alpha'_\sigma, \qquad \alpha_\nu = \alpha'_\nu \text{ for all } \nu \neq \sigma,$$

leads back to S. The substitution used constitutes an automorphism of the free group generated by the symbols α as free generators, not taking into account their expression by the a's. Therefore, if S is unrelated, then S' is unrelated too and *vice versa*. If a set S is unrelated, every subset of S is unrelated.

Since the replacement of an α by α^{-1} is also an automorphism of the free group defined by the symbols α as free generators, it is evident that the same results hold if instead of the above substitutions one applies the substitutions

$$\alpha'_\sigma = \alpha_\varrho^{-1} \alpha_\sigma, \qquad \alpha'_\sigma = \alpha_\sigma \alpha_\varrho, \qquad \alpha'_\sigma = \alpha_\sigma \alpha_\varrho^{-1}.$$

5. A finite or infinite set of reduced elements

$$B: \quad \alpha_1(a), \alpha_2(a), \ldots$$

will be called *basic*, if it satisfies the following two conditions, which refer to a-cancellation in products of elements of B:

(1) *In no product of two elements of the set $B \cup B^{-1}$, where these two factors are not inverse, does more than half of any of the two factors cancel.*

(2) *In no product of three elements of the set $B \cup B^{-1}$, where no two neighbouring factors are inverse, does half of the central factor cancel to the left and half to the right.*

Since this concept of a basic set is the central concept of the present investigation, it may be useful to elucidate it by some remarks.

Condition (1) states that $l(\alpha_\varrho^\varepsilon \alpha_\sigma^\eta)$, where ε and η are $+1$ or -1, exceeds or equals both $l(\alpha_\varrho)$ and $l(\alpha_\sigma)$, except when the two factors are inverse. Since it is easy to see that $l(\alpha^2) > l(\alpha)$ for any non-empty, reduced "word" $\alpha(a)$, the real content of (1) concerns the case $\varrho \neq \sigma$.

Condition (2) concerning a product of three factors $\alpha_\varrho{}^\varepsilon \alpha_\sigma \alpha_\tau{}^\eta$, $\varepsilon = \pm 1$, $\eta = \pm 1$, has a real content only if $l(\alpha_\sigma)$ is an even number. If taken together with (1), it states that the central factor α_σ cannot disappear completely by a-cancellation, unless the first or last factor is its inverse.

Since the existence of elements of even length requires a good deal of special consideration in the sequel, another formulation of condition (2) recommends itself: Consider an element $\alpha_\mu = \alpha'_\mu \alpha''_\mu$ of B of even length, and let $\alpha'_\mu(a)$ and $\alpha''_\mu(a)$ be its half-parts, thus $l(\alpha'_\mu) = l(\alpha''_\mu) = \frac{1}{2} l(\alpha_\mu)$. Then α'_μ will be called *an isolated first half-part in* B, if α_μ is the only element in $B \cup B^{-1}$ which begins with the sequence of a-symbols $\alpha'_\mu(a)$. Likewise α''_μ will be called *an isolated second half-part in* B, if α_μ is the only element in $B \cup B^{-1}$ which ends with the sequence $\alpha''_\mu(a)$. It should be noted that in the latter case $\alpha''_\mu{}^{-1}$ is an isolated first half-part in B. An equivalent formulation of condition (2) is then the following:

(2) *In any element of B whose length is an even number at least one half-part is isolated.*

6. The following are consequences of the property of B of being basic: In any product $P = \Pi(\alpha_\nu{}^{\pm 1})$ of a finite number of elements of the set $B \cup B^{-1}$ in which no α-cancellation is possible every factor leaves a contribution to the element $P(a)$ after full a-cancellation. No participating factor has a length greater than $l(P(a))$; this is evident from induction. A basic set is unrelated; for in a non-empty product of the α's, such as the P just mentioned, $P(a)$ cannot be the identity of F, since every factor yields a contribution to $P(a)$. The set B is therefore a set of free generators for the group which it generates, and every element of this group has a uniquely determined representation as a product of the elements of B. The set B will be called a *basis* for the subgroup of F which it generates. On the other hand, of course, an unrelated set need not be basic.

7. The main importance of basic sets lies in the fact that the general problem described in section 2 is easily treated as soon as a basic set of generators is known for the group in question. Let the finite or infinite set

$$B: \quad \alpha_1(a), \alpha_2(a), \ldots$$

be basic, and let G be the group generated by B. A decision is sought as to whether or not a given element $\beta(a)$ of F belongs to G. Only those elements α_ν of B can come into play as factors in $\beta(a)$ for which $l(\alpha_\nu) \leqq l(\beta)$.

Assume that β is contained in G, and thus is a uniquely determined product of the α_ν. The first factor in this product leaves more than half

or exactly half of its symbols a in $\beta(a)$. Assume the first case. One has to look for such an element in $B \cup B^{-1}$ that more than the first half of its symbols occur in the same order at the beginning of $\beta(a)$; there can only be one such element according to (1). Let $\alpha_{\nu_1}^{\varepsilon}$, $\varepsilon = \pm 1$, be that element. Then $\beta_1 = \alpha_{\nu_1}^{-\varepsilon}\beta$ has a smaller length than β and also belongs to G. Hence this process, which we may term the *decrease process*, can be continued as long as a reduction of the length of the element is obtained. If the process goes on until β is completely absorbed, then a representation of β as a product of elements of B results. Suppose the process stops at an element β_r which is not yet 1. If the decrease process does not apply to β, then β_r means β itself, and we start with the second case. The first α-factor in β_r must then leave exactly half of its a-symbols as its contribution to β_r. Its length is thus an even number, and its first half-part is isolated, since the second is not, because it is absorbed by the next α-factor, see condition (2). Hence in examining the beginning of β_r one has to look for an element with even length in $B \cup B^{-1}$ such that its first half-part is isolated and occurs at the beginning of β_r, and that the second half-part is not isolated. There is exactly one such element $\alpha_{\nu_{r+1}}^{\varepsilon}$, $\varepsilon = \pm 1$, in $B \cup B^{-1}$. Thus β_r is replaced by $\beta_{r+1} = \alpha_{\nu_{r+1}}^{-\varepsilon}\beta_r$, which has the same length. One may call this the *level process*. It may now happen that the decrease process is applicable to β_{r+1}. If not, the level process has to be applied again. Now β_{r+1} begins with the first half-part of $\alpha_{\nu_{r+1}}^{-\varepsilon}$, which is not isolated. Hence the element of even length $\alpha_{\nu_{r+2}}^{\eta}$, $\eta = \pm 1$, whose first half-part occurs at the beginning of β_{r+1} must satisfy the condition $l(\alpha_{\nu_{r+2}}) > l(\alpha_{\nu_{r+1}})$, because its first half-part has to be isolated. The level process can therefore only continue a limited number of times, because at each step an element of increasing length is involved and, on the other hand, the length cannot surpass the length of β_r. Sooner or later the decrease process thus becomes applicable again and, in the end, β is fully absorbed and thus represented as a product of elements from $B \cup B^{-1}$.

If $\beta(a)$ does not belong to G, the whole procedure stops before $\beta(a)$ is fully absorbed.

8. Concerning the whole question of deciding whether or not a given element $\beta(a)$ is contained in the group G generated by a given basic set B the following remark has to be made: The number of *steps*, each consisting in the replacement of β_i by β_{i+1}, is in all cases finite. If B is a finite set, the number of *tests* to be made in finding suitable factors $\alpha_{\nu_{i+1}}^{\pm 1}$ is likewise finite. If B is an infinite set, but F has a finite number of generators $a_1, \ldots, a_n$, then the number of tests is still finite, because

the number of elements of length not greater than $l(\beta)$ is then finite in F and *a fortiori* in G and hence in B, and only those elements can come into play (section 6). If F has an infinite number of generators, and B contains infinitely many elements, then the decision may not be obtainable by a finite number of tests unless the very structure of the basic set B indicates that, for other reasons, only a finite number of its elements can possibly come into play in relation to the given element $\beta(a)$.

II.

9. The aim of this part II is to show that for any subgroup G of a free group

$$F = [a_1, a_2, \ldots]$$

there exists a set of generators of G which is basic with respect to this (finite or infinite) set of free generators of F and is thus a *basis* for G.

Assume all elements of G to be written as reduced products of the a_ν. Each, except the identity, has a certain positive length. Let

$$0 < l_1 < l_2 < l_3 < \ldots \tag{3}$$

be the increasing sequence of those integers which occur as lengths of elements of G. Let A_k denote the subset of elements of G with length l_k and G_k the subgroup of G generated by the union $A_1 \cup A_2 \cup \ldots \cup A_k$ of the subsets $A_1, \ldots, A_k$.

10. We first set out to prove the existence of a basis B_1 for the subgroup G_1 generated by A_1.

If B_1 is such a basis, then any element of A_1 is a product of elements of B_1. The length of the factors then is smaller than or equal to l_1 (section 6), and hence equal to l_1, because l_1 is the smallest positive length in G. On the other hand, these elements of B_1 then generate G_1 and thus constitute the complete basis B_1. Hence B_1 has to be a certain subset of A_1 and is thus obtained from A_1 by the elimination of certain elements of A_1.

In the existence proof, let

$$A_1: \quad \alpha_1, \alpha_2, \alpha_3, \ldots \tag{4}$$

be an enumeration in an arbitrary order of all elements of length l_1 in G with the restriction that only one of every two inverse elements of length l_1 is actually inserted in the sequence (4). Without affecting the procedure envisaged one may always substitute α_μ^{-1} for α_μ in the sequence, if that is convenient.

The elements of (4) satisfy (1), because if $l(\alpha_\varrho^{\varepsilon}\alpha_\sigma^{\eta}) < l_1$, this length has to be zero, i.e. the two factors are inverse. If l_1 is an odd number, they also satisfy (2), and the set A_1 is then basic and is thus the required basis B_1.

So one has to consider the case that l_1 is even. Let

$$\alpha_\mu = \beta_1\gamma, \qquad l(\beta_1) = l(\gamma) = \tfrac{1}{2}l_1 ,$$

be the first element in the sequence (4), if any, in which at least one half-part is not isolated in (4), that is in $A_1 \cup A_1^{-1}$. Since we can replace the element by its inverse, if necessary, we may assume that γ is not isolated. If an element of (4) begins with γ^{-1}, substitute its inverse, which ends with γ. Then let

(5) $$\beta_1\gamma, \beta_2\gamma, \beta_3\gamma, \ldots$$

be the subsequence of (4) containing all elements of (4) with γ as second half. Here all β_r, $r = 1, 2, \ldots$, are different, because no element is written twice in the sequence. Assume that β_r is not an isolated first half-part in (4). Thus there is in (4), but outside (5), at least one element of the form $(\beta_r\delta)^{\pm 1}$ where $\delta \neq \gamma$. Then the element

$$(\beta_r\delta)^{-1}(\beta_r\gamma) = \delta^{-1}\gamma$$

has its length equal to l_1. Since it belongs to G it belongs also to A_1, and hence to (5), and

$$\beta_r\delta = (\beta_r\gamma)(\delta^{-1}\gamma)^{-1}$$

is the product of two elements of (5). Therefore, if one keeps all the elements (5) in the sequence, one can eliminate all other elements of (4) which begin with β_r, $r = 1, 2, \ldots$, or end with β_r^{-1}. None of the elements α_ϱ, $\varrho < \mu$, if any, are among these, because both of their half-parts are isolated. After this elimination all elements (5) have an isolated first half-part in the remaining subsequence of (4).

Next, let α_ν, $\nu > \mu$, be the first element, if any, in the remaining sequence, but outside (5), in which at least one half-part is not isolated. This element α_ν then gives rise to the procedure analogous to the one applied to α_μ, and none of the elements α_ϱ, $\varrho < \mu$, and (5) are affected by this process, because neither their isolated half-parts nor γ are among the half-parts which come into play by the new process.

This procedure is continued, step by step, as long as the sequence (4) is not exhausted. An element of (4) whose half-parts are both isolated in (4) remains in the sequence during all steps. An element of (4) with at least one half-part which is not isolated becomes involved in one of the steps of the process. If it is not eliminated in that step, it remains

in the sequence during all the following steps. Hence one gets a uniquely determined subsequence B_1 of (4) consisting of those elements which are not eliminated in any of the steps. This subsequence is infinite if (4) is infinite, because a finite number of half-parts of length $\frac{1}{2}l_1$ can only combine into a finite number of elements of length l_1. Every element of B_1 contains at least one isolated half-part. Hence B_1 satisfies (1) and (2) and is thus basic. Every element of (4) which is eliminated is a product of elements which remain in B_1; therefore B_1 generates G_1 and is thus a basis for G_1.

11. Next we prove that the group G_k, $k=1, 2, \ldots$, has a basis. We proceed by induction with respect to k. Let B_{k-1} be a basis for G_{k-1}. It consists of elements of length not exceeding l_{k-1}, because G_{k-1} has a set of generators not exceeding that length. Hence B_{k-1} is a certain subset of the set $A_1 \cup A_2 \cup \ldots \cup A_{k-1}$. Let

$$A'_k: \quad \sigma_1, \sigma_2, \sigma_3, \ldots \tag{6}$$

be an enumeration of those elements of A_k, if any, which do not belong to G_{k-1}, with the same restriction as for A_1, namely that only one of every two inverse elements of A'_k is inserted in (6). If A'_k is empty, then B_{k-1} is also a basis B_k of $G_k = G_{k-1}$. Assume that A'_k is not empty.

No element σ of (6) can be shortened by multiplication with an element of G_{k-1}, because the product, and hence σ itself, would belong to G_{k-1}, and this has been excluded. Hence no element of (6), nor its inverse, begins with more than half of an element of B_{k-1} or, this is always understood, the inverse of such an element. If an element of (6), or its inverse, say σ_μ, begins with a first half-part β' of an element $\beta = \beta'\beta''$ of B_{k-1}, and if β' is isolated in B_{k-1}, then σ_μ may be eliminated from (6), because if $\sigma_\mu = \beta'\gamma$, then $\sigma_\mu = \beta(\beta''^{-1}\gamma)$ is the product of an element β from B_{k-1} and an element $\beta''^{-1}\gamma$ which is contained in (6), because it has the length l_k and cannot belong to G_{k-1}. It should be noted that $l(\gamma) = l_k - l(\beta') > \frac{1}{2}l_{k-1}$.

Assume now that also $\beta''^{-1}\gamma$ begins with the first half-part δ' of an element $\delta = \delta'\delta''$ of B_{k-1} different from β''^{-1}. If $l(\delta') < l(\beta'')$, this half-part δ' is not isolated in B_{k-1}. If $l(\delta') > l(\beta'')$, the half-part δ' may well be isolated in B_{k-1}. If this is the case, then β''^{-1} is not an isolated first half-part, thus β'' is not an isolated second half-part. Hence we proceed as follows: the elimination process described is carried out first in respect of all elements of smallest even length in B_{k-1}, for instance in the order in which they appear in an enumeration of B_{k-1} (they do not interfere with each other, because only different half-parts of equal length are

involved), then in respect of all elements in B_{k-1} of the next even length occurring in (3), and so on up to the greatest even length occurring in B_{k-1}, which is smaller than or equal to l_{k-1}.

After all these eliminations have been carried out in (6), let the remaining subsequence of (6) be

$$A''_k: \quad \tau_1, \tau_2, \tau_3, \ldots . \tag{7}$$

The situation is now as follows: consider the set $B_{k-1} \cup A''_k$, the union of the basis B_{k-1} of G_{k-1} and the subset A''_k of A_k. For the elements of $B_{k-1} \cup A''_k$ condition (1) holds, if at least one of the two factors belongs to B_{k-1}, since A''_k is part of A'_k. Condition (2) holds, if the central factor belongs to B_{k-1}, because every element of even length in B_{k-1} has at least one half-part which is isolated not only in B_{k-1} but in the enlarged set $B_{k-1} \cup A''_k$ according to the above procedure of elimination of certain elements of A'_k. (Note that in respect of such elements of B_{k-1} for which *both* half-parts are isolated in B_{k-1}, we have in fact selected one half-part arbitrarily and arranged for it to become isolated even in the enlarged set, while the other is not, if eliminations have taken place at all in respect of that element.) Moreover, the set $B_{k-1} \cup A''_k$ generates G_k, because at every elimination the element eliminated is the product of an element of B_{k-1} and an element of (6) which remains at that elimination.

In order to arrive at a basis for G_k we first have to enforce the validity of (1) for any two factors drawn from A''_k, since (1) is already satisfied if at least one factor belongs to B_{k-1}. Consider the product $\tau_1^{\varepsilon} \tau_\mu^{\eta}$, $\mu > 1$, $\varepsilon = \pm 1$, $\eta = \pm 1$. If its length is inferior to l_k, the product belongs to G_{k-1}, and τ_μ can thus be eliminated, being the product of $\tau_1^{\pm 1}$ and factors from B_{k-1}. After all τ_μ with this property have been eliminated, proceed to the first τ after τ_1 in the remaining sequence and repeat the process for that element (which does not re-involve τ_1), and so on. Let

$$A'''_k: \quad \omega_1, \omega_2, \ldots \tag{8}$$

be the remaining sequence after this process has been fully carried out. Then the set $B_{k-1} \cup A'''_k$ satisfies (1).

Finally, it remains to enforce the validity of (2) for products of three elements from $B_{k-1} \cup A'''_k$, where the central factor is drawn from A'''_k and has an even length. If such a product $\beta \omega_\mu \gamma$ does not satisfy (2), the first half-part of ω_μ cancels in the product $\beta \omega_\mu$. If β belonged to B_{k-1}, one would have $l(\beta) < l(\omega_\mu)$, hence $l(\beta \omega_\mu) < l(\omega_\mu)$, which would contradict (1). Hence β, and likewise γ, must also belong to A'''_k. The situation in A'''_k is therefore completely analogous to the situation in

A_1 in section 10; the elements of A'''_k satisfy (1) and, if l_k is odd, they also satisfy (2), and $B_{k-1} \cup A'''_k$ is then a basis for G_k. If l_k is even, the process applied to the sequence (4) in section 10 applies without any change to the sequence (8) and reduces it to a subsequence A''''_k satisfying (2). Then every element of A''''_k has at least one half-part which is isolated in A''''_k, hence also in $B_{k-1} \cup A''''_k$, and

$$B_k = B_{k-1} \cup A''''_k \tag{9}$$

is thus a basis for G_k, since it generates G_k and satisfies (1) and (2).

12. The preceding section has shown that there is, for every k, a basis B_k of G_k which is either identical with B_{k-1} or is obtained from B_{k-1} by the addition of a certain set of elements of length l_k as expressed in (9). Consider now the union B of all the B_k, $k = 1, 2, \ldots$. Any two or three elements of B belong to a B_k for a sufficiently large value of k and therefore satisfy (1) and (2), since B_k is basic. Hence B is basic.

Any element of G belongs to a certain G_k and is thus a product of elements of B_k, thus of B. Hence B generates G.

This shows that B is a basis for G. — It follows that G is a free group.

III.

13. In the case that F has a finite number of generators, there are only a finite number of elements of given length l in F and hence *a fortiori* in every subgroup G of F. Therefore, in this case, the sets A_k introduced in section 9 are finite, and the procedures used for deriving B_1 in section 10 and for deriving B_k from B_{k-1} in section 11 involve only a finite number of steps. If also G may be generated by a finite number of its elements, then for some k the union $A_1 \cup A_2 \cup \ldots \cup A_k$ contains a set of generators of G; hence $G = G_k$, and $B = B_k$ is a basis of G.

If a set S of elements of F is given, and if G denotes the group generated by S, one does not know beforehand the sets A_k used in the above existence proof. If however S is finite, a direct construction of a basis B for G in a finite number of steps has been given in [5] by the application to S of transformations of the kind described in section 4; see also [7]. In this case only the finite number of generators of F which appear in S come into play, and F can thus, without restriction, be considered as finitely generated.

14. If F is finitely generated and a basis B for a subgroup G of F is known, it may be decided in a finite number of tests whether or not a

given element $\beta(a)$ of F belongs to G, because only the subset B_l consisting of those elements of B whose length does not exceed $l=l(\beta)$ can come into play, and B_l is finite.

If G is determined by a given, infinite, related or non-related set

$$S: \quad \alpha_1, \alpha_2, \ldots \tag{10}$$

of elements generating G, then there exists a function $L(l)$ such that all elements of G of length not exceeding l are contained in the subgroup G_L generated by the part $\alpha_1, \ldots, \alpha_L$ of (10); and for G_L a basis can be constructed in a finite number of steps (section 13). However, the dependence of L on l cannot, in general, be determined unless some further information can be gained from the structure of S. It is therefore only for finitely generated groups G that the identification of their elements can be assured unconditionally in a finite number of tests.

15. Before concluding we mention briefly the connection of these considerations with the decision problem for non-free groups.

Let a group $H=[a_1, a_2, \ldots; R_1(a)=1, R_2(a)=1, \ldots]$ be defined by a finite or infinite system of generators

$$a_1, a_2, \ldots \tag{11}$$

and a finite or infinite system of relations

$$R_1(a)=1, \quad R_2(a)=1, \quad \ldots . \tag{12}$$

On denoting by F the free group with (11) as free generators, H is the factor group in F of the normal subgroup of F

$$G = [\ldots, \Phi R_i \Phi^{-1}, \ldots] \tag{13}$$

generated by all elements $\Phi R_i \Phi^{-1}$ where R_i ranges over the set (12) and Φ ranges over all elements of F. To decide whether an element $\beta(a)$ of F is equal to 1 in H means to decide whether it belongs to G, and this can be done if a basis of G is known. The solution of the decision problem for non-free groups may thus become possible in such cases where a basis for the corresponding group G can be found in some short-cut way.

16. In order to illustrate the procedure in such cases, an example — which is completely trivial in itself — may be put here with the sole view of demonstrating the line of reasoning to be followed. Let

$$H = [a, b;\ a^{2p+1} = 1], \qquad p \geqq 1 . \tag{14}$$

Consider in the free group $F=[a, b]$ generated by a and b the elements

$$\Psi\, a^{2p+1}\, \Psi^{-1} \tag{15}$$

for all $\Psi = a^{x_1}b^{y_1}a^{x_2}b^{y_2}\ldots a^{x_r}b^{y_r}$ satisfying the conditions

$$\left\{\begin{array}{l} 1)\ r = 0 \text{ means that } \Psi \text{ is the empty word.} \\ 2)\ \text{If } r > 0, \text{ none of the exponents } y_1, \ldots, y_r \text{ is zero.} \\ 3)\ \text{If } r > 1, \text{ none of the exponents } x_2, \ldots, x_r \text{ is zero.} \\ 4)\ |x_\nu| \leqq p \text{ for all } \nu = 1, 2, \ldots, r. \end{array}\right. \tag{16}$$

The system B consisting of those elements (15) which satisfy (16) is basic. Firstly, Ψ ends with a power of b, if Ψ is not void. Thus the elements of B are written in reduced form. Secondly, the lengths of all elements of B are odd numbers, thus condition (2) becomes void. Finally, in order that more than half of an element of B with exponent ± 1 can cancel by multiplication on the right with another element of the same kind, this other element must begin with the same Ψ and after that have at least the sequel $a^{\mp(p+1)}$. But then it can only be the inverse of the first element. Hence (1) holds.

Now consider an arbitrary element

$$\Phi\, a^{2p+1}\, \Phi^{-1} \tag{17}$$

corresponding to the general form (13). If Φ is empty, (17) is one of the elements of B. Assume

$$\Phi = a^{\xi_1}b^{\eta_1}\ldots a^{\xi_r}b^{\eta_r}, \qquad r \geqq 1\,. \tag{18}$$

If η_r were zero, even a^{ξ_r} could be omitted from Ψ by cancellation of a power of a in (17), thus replacing r by $r-1$. It can thus be assumed that Φ satisfies conditions 2) and 3) of (16). If some $|\xi_i| > p$, let i be the first mark for which this takes place, and let

$$\xi_i = q(2p+1) + \xi'_i, \qquad |\xi'_i| \leqq p\,.$$

Then one can write

$$\Phi = a^{\xi_1}b^{\eta_1}\ldots b^{\eta_{i-1}}\, a^{q(2p+1)}\, b^{-\eta_{i-1}}\ldots b^{-\eta_1}a^{-\xi_1}\, \Phi'$$

$$\Phi' = a^{\xi_1}b^{\eta_1}\ldots b^{\eta_{i-1}}a^{\xi'_i}b^{\eta_i}\ldots a^{\xi_r}b^{\eta_r}\,.$$

The factor of Φ' is a power of some element of B. If $\xi'_i = 0$, replace $b^{\eta_{i-1}}\, b^{\eta_i}$ by $b^{\eta_{i-1}+\eta_i}$ in Φ'. If the exponent $\eta_{i-1}+\eta_i$ is also 0, take the two neighbouring powers of a together, and so on. In any case, Φ' reduces

to a word of the same form as (18) and with a length shorter than $l(\Phi)$. Therefore, after a finite number of steps, Φ is replaced by a product of elements from B followed by a word Ψ satisfying all conditions (16), and on inserting this in (17) it results that (17) is itself a product of elements of B. Thus the whole group G generated by the elements (17) may be generated by B.

Hence the set of all elements (15) satisfying (16) constitutes a basis for the normal subgroup G of the free group $F=[a, b]$ whose elements become the identity of H. This fact solves the identity problem for H in a finite number of tests.

REFERENCES

1. H. Federer and B. Jónsson, *Some properties of free groups*, Trans. Amer. Math. Soc. 68 (1950), 1–27.
2. M. Hall, *Coset representations in free groups*, Trans. Amer. Math. Soc. 67 (1949), 421–432.
3. M. Hall and T. Radó, *On Schreier systems in free groups*, Trans. Amer. Math. Soc. 64 (1948), 386–408.
4. F. Levi, *Über die Untergruppen der freien Gruppen*, Math. Z. 32 (1930), 315–318.
5. J. Nielsen, *Om regning med ikkekommutative faktorer og dens anvendelse i gruppeteorien*, Mat. Tidsskr. B 1921, 77–94.
6. O. Schreier, *Die Untergruppen der freien Gruppen*, Abh. Math. Sem. Hamburg. Univ. 5 (1927), 161–183.
7. J. H. C. Whitehead, *On equivalent sets of elements of a free group*, Ann. of Math. 37 (1936), 782–800.

UNIVERSITY OF COPENHAGEN, DENMARK