Mathematics

1961

SovietRxiv

Abstract

Full Text

Mathematics

D. S. Faermark

An Algorithm for Establishing the Identity of Words in the Nilpotent Product of Groups Given by a Finite Number of Generators and Defining Relations

(Presented by Academician A. I. Mal' cev on 17 X 1960)

Let the group G_1, given by generators $a_k,\ k = 1, \dots, N_1$, and relations $v_i = 1,\ i = 1, \dots, M_1$, and the group G_2 with generators $b_m,\ m = 1, \dots, N_2$, and relations $w_j = 1,\ j = 1, \dots, M_2$, be such that for them there exists an algorithm for the identity of words. The question is considered of the existence of an identity algorithm in their n-th nilpotent (1,5) product

$$G = G_1(n)G_2.$$

(The notation is introduced so that the lower central series of the group is the series $G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$, and the direct product is the first nilpotent product.) It is known (1) that every element $h \in G$ has a unique "proper" representation of the form

$$h = g_1 g_2 u, \tag{1}$$

where $g_1 \in G_1,\ g_2 \in G_2$, and the element u lies in the mutual commutant $[G_1, G_2]^G$ of the subgroups G_1 and G_2 of the group G. Consequently, $h = h'$ if and only if the equalities

$$g_1 = g_1'; \qquad g_2 = g_2'; \qquad u = u'$$

hold.

An element $h \in G$, written as a word in the generators a_k and b_m of the group G, as indicated in (1), can be brought in a finite number of steps to the form (1).

Since in G_1 and G_2 there exist identity algorithms, in order to solve the question it is necessary to give an identity algorithm in the mutual commutant $[G_1, G_2]^G$. In (2) an algorithm is described for the identity of words in a finitely defined nilpotent group. Since $[G_1, G_2]^G$ is nilpotent (^{1}), it remains to give constructively, through a_k and b_m, a finite system of generators and defining relations for $[G_1, G_2]^G$.

Consider first

$$F = F_1(n)F_2$$

–the nilpotent product of the free groups F_1 and F_2 with free generators $a_k,\ k = 1, \dots, N_1$, and $b_m,\ m = 1, \dots, N_2$. In them are distinguished systems of words $v_i \in F_1,\ i = 1, \dots, M_1$, and $w_j \in F_2,\ j = 1, \dots, M_2$.

Since nilpotent products satisfy MacLane' s postulate (^{6}), we have

$$G \cong F/N,$$

where $N = \{v_i, w_j\}^F$, and

$$[G_1, G_2]^G \cong [F_1, F_2]^F / N \cap [F_1, F_2]^F.$$

The question will be solved if a finite system of generators and defining relations is found for $[F_1, F_2]^F$ and a finite system of elements, written in these generators, generating the subgroup

$$K = N \cap [F_1, F_2]^F.$$

Let A be a free group with a finite number of generators $g_1, \dots, g_m$, and let $g_1, \dots, g_m, \dots, g_r$ be all basic commutators (^{3,4}) of weights from 1 to n inclusive. Then the commutation formulas hold

$$g_j^\varepsilon g_i^\delta \equiv g_i^\delta g_j^\varepsilon g_{j+1}^{\mu_{j+1}} \cdots g_r^{\mu_r} \pmod{A^{(n)}}, \tag{2}$$

where $r \geq j > i$; $\varepsilon, \delta = \pm 1$ and $\mu_s = \mu_s(\varepsilon, \delta, i, j)$. In addition, every element $g \in A$ has a unique canonical representation modulo $A^{(n)}$

$$g \equiv g_1^{\alpha_1} \cdots g_m^{\alpha_m} \cdots g_r^{\alpha_r} \pmod{A^{(n)}}. \tag{3}$$

The algorithm for computing the exponents μ_s and a_i is described in the paper (^{4}). Obviously, "basic" commutators can be constructed on an arbitrary finite set of elements of any group, and formulas (2) and the existence of the representation (3) are preserved, together with the algorithms for computing μ_s (only the uniqueness of the representation (3) will be absent). We formulate, without proof, two obvious properties of a system of basic commutators.

Lemma 1. Let us select from the system σ of all basic commutators of the free group A the subsystem σ' consisting of all those commutators in whose expressions in terms of the free generators g_i only certain fixed free generators g_{i_k} of the group A occur. Then σ' is a system of basic commutators for the group A' generated by the elements g_{i_k}.

Lemma 2. Let k be a commutator (not necessarily basic) whose components are some of the free generators g_{i_k} of the group A. Then in every basic commutator that occurs with nonzero degree in the canonical representation of the element k, each of the generators g_{i_k} occurs.

Let now F_1 and F_2 be free groups with systems of free generators a_k and b_m, respectively, and let $F = F_1(n)F_2$. Construct in F, on the generators a_k and b_m, a system of basic commutators c_s, assuming that $c_s = a_s$ for $1 \leq s \leq N_1$ and $c_s = b_{s-N_1}$ for $N_1 + 1 \leq s \leq N_1 + N_2$.

Theorem 1. In the group $F = F_1(n)F_2$, those among the basic commutators c_s of weight $\omega(c_s)$, $2 \leq \omega(c_s) \leq n$, in the expression of each of which both elements from the set a_k and elements from the set b_m occur, form a system of generators for $[F_1, F_2]^F$.

Proof. Consider the free product $H = F_1 * F_2$. Every element $h \in H$ has a unique representation of the form

$$h = c_1^{\alpha_1} \cdots c_l^{\alpha_l} u, \tag{4}$$

where $u \in H^{(n)}$. Let $h \in [F_1, F_2]^H$, and let φ be the projection of H onto F_1, i.e. the natural homomorphism of H onto F_1 with kernel $\bar{F}_2^H$. Denote by c_{i_k} the basic commutators composed only of the elements $a_1, \dots, a_{N_1}$. Since $h \in [F_1, F_2]^H$, we have

$$1 = h\varphi = (c_{i_1}\varphi)^{\alpha_{i_1}} \cdots (c_{i_q}\varphi)^{\alpha_{i_q}} (u\varphi);$$

but $u\varphi = F_1^{(n)}\varphi$, and since F_1 is mapped identically onto itself under φ, by Lemma 1, $\alpha_{i_k} = 0$. From this it follows for the group F that, if $g \in [F_1, F_2]^F$, then, since $F = H/H^{(n)} \cap [F_1, F_2]^H$, the element g can be written in the form

$$g = c_{j_1}^{\alpha_{j_1}} \cdots c_{j_p}^{\alpha_{j_p}} u, \tag{5}$$

where the c_{j_r} satisfy the conditions of the theorem, and $u \in F^{(n)}$. But each of the elements c_{j_r} belongs to $[F_1, F_2]^F$, and therefore $u \in F^{(n)} \cap [F_1, F_2]^F = E$ (see (^{5})), i.e. $u = 1$. The theorem is proved.

Put $c_{j_r} = g_r$, preserving the ordering $g_i < g_j$ for $i < j$. In the new notation the representation of the element g has the form

$$g = g_1^{\alpha_1} \cdots g_p^{\alpha_p}, \tag{5'}$$

and it is unique in view of the uniqueness of the representation modulo $F^{(n)}$.

Just as it was proved that $u = 1$ in formula (5), one can show that the congruences (2) for the system $\{g_r\}$ in $[F_1, F_2]^F$ turn into the equalities

$$g_j^{\varepsilon} g_i^{\delta} = g_i^{\delta} g_j^{\varepsilon} g_{j+1}^{\mu_{j+1}} \cdots g_p^{\mu_p}. \tag{6}$$

With the aid of these relations, an arbitrary expression of each element g of $[F_1, F_2]^F$ can be brought to the form (5′). Since this latter expression is unique, the following is true.

Theorem 2. *The relations (6) are a complete system of defining relations for the group $[F_1, F_2]^F$ with respect to the system of generators $g_1, \dots, g_p$.*

Theorems 1 and 2 solve the problem for the case of two factors that are free groups.

Let us pass to the consideration of the general case. Order in the group $F = F_1(n)F_2$ the elements a_k, b_m, v_i, and w_j so that $a_k < b_m < v_i < w_j$. Construct from them the system of basic commutators $\{y_z\}$ up to weight n inclusive. Among these, select the commutators x_s, $\omega(x_s) \geq 2$, satisfying the following two conditions: 1) the expression of each x_s contains at least one element among the v_i or w_j; 2) among the x_s there are none whose expression consists only of elements a_k and v_i, or only of elements b_m and w_j.

Let $N = \{v_i, w_j\}^F$. Obviously, every $x_s \in N \cap [F_1, F_2]^F$.

Theorem 3. *The system of elements $\{x_s\}$ is a system of generators for the subgroup $K = N \cap [F_1, F_2]^F$.*

If the assertion of the theorem is true, the system of equalities (6) and the equalities $x_s = 1$, $s = 1, \dots, l$, where the x_s are rewritten in canonical form through the commutators g_r, will constitute a complete system of defining relations for $[G_1, G_2]^G$ in the system of generators $\{g_r\}$.

For the proof we shall need

Lemma 3. *If in the group $F = F_1(n)F_2$ an element g belonging to the normal divisor N is taken, then g admits an expression of the form*

$$g = y_{r_1}^{\alpha_{r_1}} \cdots y_{r_p}^{\alpha_{r_p}} z, \tag{7}$$

where $z = F^{(n)}$, and all y_{r_i} satisfy condition 1).

Proof. We shall write elements of N in the form of products of elements a_k, b_m, v_i, and w_j, without performing cancellations between the generators a_k, b_m and the words v_i and w_j, for example, by enclosing v_i and w_j in parentheses. Consider elements $g \in N$ of the form

$$g = h^{-1} v_i h, \qquad h \in F. \tag{8}$$

By rules analogous to (2), g can be rewritten in the form (7). If the length of the word h in (8) is equal to 1, then the y_{r_i} satisfy condition 1). Assuming that the assertion is true when the length of the element h in the generators a_k and b_m is $s-1$, for the element $h_1 = ha_k$, for example, we obtain

$$g = a_k^{-1} h^{-1} v_{iha} k = a_k^{-1} y_{r_1}^{\alpha_{r_1}} \cdots y_{r_p}^{\alpha_{r_p}} z a_k = a_k^{-1} y_{r_1}^{\alpha_{r_1}} \cdots y_{r_p}^{\alpha_{r_p}} a_{kz} (z, a_k).$$

The commutators arising in the transpositions from right to left can be rewritten, by Lemma 2, through basic ones satisfying condition 1). It is clear that a product of elements of the form (7) can also be written in such a form.

We now pass to the proof of Theorem 3. Let $g \in K$, and in its expression (7) select the factors y_{q_i} such that their components are only a_k and v_i, and the elements y_{p_j} whose components are only b_m and w_j. Moving first the y_{q_i} successively past the elements standing to their right, we

we shall ensure that the notation for g assumes the form

$$g = t_1 y_{q_1}^{\alpha_{q_1}} \dots y_{q_m}^{\alpha_{q_m}} z.$$

Proceeding analogously with y_{p_j}, we obtain

$$g = t y_{p_1}^{\alpha_{p_1}} \dots y_{p_n}^{\alpha_{p_n}} y_{q_1}^{\alpha_{q_1}} \dots y_{q_m}^{\alpha_{q_m}} z,$$

where t is a product of commutators satisfying conditions 1) and 2). Let us prove that $y_{p_1}^{\alpha_{p_1}} \dots y_{p_n}^{\alpha_{p_n}} \in F^{(n)}$ and $y_{q_1}^{\alpha_{q_1}} \dots y_{q_m}^{\alpha_{q_m}} \in F^{(n)}$. Let $F\varphi = F_1$, and since $g \in K$, we have

$$g\varphi = \left(y_{q_1}^{\alpha_{q_1}} \dots y_{q_m}^{\alpha_{q_m}} \right) \varphi z \varphi = 1. \tag{9}$$

But $z\varphi \in (F, \varphi)^{(n)}$, and therefore $\left(t y_{q_1}^{\alpha_{q_1}} \dots y_{q_m}^{\alpha_{q_m}} \right) \varphi \in (F_1 \varphi)^{(n)}$, and consequently, $y_{q_1}^{\alpha_{q_1}} \dots y_{q_m}^{\alpha_{q_m}} \in F_1^{(n)} \subset F^{(n)}$. Similarly we verify that $y_{p_1}^{\alpha_{p_1}} \dots y_{p_n}^{\alpha_{p_n}} \in F_n$. Thus, $g = tq$, where $t \in [F_1, F_2]^F$, and $q \in F^{(n)}$. Hence $q \in F^{(n)} \cap [F_1, F_2]^F = E$, and, consequently, $q = 1$. By Lemma 2, every commutator in the notation for t can be rewritten in terms of the basic commutators x_s satisfying conditions 1) and 2). The theorem is proved.

Thus, the algorithm for the identity of words in the nilpotent product of two groups consists of the following. We find the regular notation (1) of the word under consideration. We determine whether the regular components g_1 and g_2 in (1) are equal to 1. If they are equal to 1, then we proceed to investigate the component u. By means of formulas (6) we reduce u to the canonical form (5). If the factors are free groups, then $u = 1$ if and only if all exponents in the canonical notation are equal to 0. If, however, the factors are defined by systems of generators and defining relations, then, in order to decide whether the component u is equal to 1, it is necessary to express the elements x^s in their notation through $g_1, \dots, g_p$ and to apply the algorithm described in work [2] for a nilpotent group given by the system of generators $g_1, \dots, g_p$ and by the systems of relations (6) and $x_s = 1$ $(s = 1, \dots, l)$ as the system of defining relations.

Since nilpotent products of groups are associative [1], the identity algorithm can be constructed for any finite number of factors.

Moscow State University
named after M. V. Lomonosov

Received
27 IX 1960

REFERENCES

[1] O. N. Golovin, *Matem. sborn.*, 27 (69), 427 (1950).
[2] A. I. Mal' cev, *Matem. sborn.*, 37, 567 (1955).
[3] M. Hall, *The Theory of Groups*, 1959, p. 165.
[4] N. P. Gol' dina, *UMN*, 13, No. 3, 183 (1958).
[5] S. Moran, *Proc. London Math. Soc.*, 6, No. 24, 581 (1956).
[6] R. R. Struik, *Trans. Am. Math. Soc.*, 81, 425 (1956).

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.