SOME ALGORITHMIC PROBLEMS FOR SOLVABLE GROUPS

N. S. Romanovskii

UDC 519.45

It is said that a group G is defined in a variety $\mathfrak{M}$ by means of the generators $x_1,\dots,x_n$ and defining relations $r_1(x)=1,\dots,r_m(x)=1$ if it is the factor group of the free group of $\mathfrak{M}$ with basis $x_1,\dots,x_n$ by the normal subgroup generated by $r_1,\dots,r_m$. The occurrence problem for such a group is as follows. For any finite collection $g, h_1,\dots,h_k$ of elements of G defined in the form of words in $x_1,\dots,x_n$, does there exist an algorithm that enables us to determine whether or not g belongs to the subgroup generated by $h_1,\dots,h_k$? In the general case the answer to this question is negative; this follows from the existence of a finitely defined group with an unsolvable equality problem [1]. In [2] there is a proof of the algorithmic unsolvability of the occurrence problem for a certain group in the variety of 4-step solvable groups. In this direction we can note that the occurrence problem is solvable for an absolutely free group and for a group in the variety of nilpotent groups of a specified class of nilpotency (these facts are well known) and that the solvability of the occurrence problem carries over to free products of groups but not to direct products [3]. In §1 of the present note the occurrence problem for 2-step solvable groups is solved affirmatively.

The second section deals with groups with a single relation. Theorem 2 establishes the criterion when the factors of the series of commutator groups for a group with a single defining relation (in the variety of all groups) are torsion-free. Note that a similar criterion for the factors of the lower central series of this group follows easily from [4]. Theorem 3 solves the equality problem for a group with a single relation in the variety of solvable groups of a specified class of solvability under certain restrictions on the relation. In this connection let us take note of [2], where a group is constructed that is finitely defined in the variety of 5-step solvable groups and has an unsolvable equality problem.

The use of the techniques of Magnus embeddings is common to both sections. Below we shall require some important definitions and facts about these embeddings from [2] and [5].

Let us agree on the notation. If G is a group, then G' denotes the first commutator group for this group and $G^{(n)}$ the n-th commutator group. Let A and B be subgroups of G. Then $[A,B]$ denotes the commutator of A and B. $A \wr B$ denotes the discrete wreath product of A and B, and $\bar{A}$ its base group.

§1. The Occurrence Problem for 2-Step Solvable Groups

Before stating the main proposition of this section, we prove two lemmas.

1. Let F be a free group; A a free abelian group of the same rank as F; S and R normal subgroups of F. Set $\tilde{F}=F/S$ and $\tilde{R}=RS/S$. Fix a Magnus embedding (see [2]) of F/S' into the wreath product $A \wr \tilde{F}=C$. Assume that RS'/S' as a normal subgroup of F/S' is generated by r_i, $i\in I$. Let us represent each of these elements in the form $r_i=r_i'r_i''$, where $r_i'\in\tilde{F}$ and $r_i''\in\bar{A}$. Let N denote the normal subgroup of C generated by r_i', r_i'', $i\in I$. Then $N=\tilde{R}\,[\tilde{R},\bar{A}]N_1$, where N_1 is contained in $\bar{A}$ and, as a normal subgroup of C, is generated by r_i'', $i\in I$.

Translated from Algebra i Logika, Vol. 13, No. 1, pp. 26-34, January-February, 1974. Original article submitted March 13, 1974.

LEMMA 1. In the above notation

$$F/S' \cap N = RS'/S'.$$

Proof. The assertion of the lemma means that F/RS' is the image of F/S' under the factorization of C by N. Consider $C/\widetilde{R}[\widetilde{R}, A]$. It is isomorphic to $A \wr F/RS$. The image of F/S' under this factorization is $F/(RS)'$. Note that $(RS)' \subseteq RS'$. All this enables us to reduce our problem to the case when $\widetilde{R}$ is the identity subgroup, i.e., $N = N_1$. But then, as is easy to see, N coincides with RS'/S'. This proves the lemma.

2. In this paragraph we examine a certain algorithmic problem for polynomial rings.

Let $K = Z[x_1,\dots,x_n, y_1,\dots,y_m]$ be the ring of polynomials in $x_1,\dots,x_n, y_1,\dots,y_m$ with integral coefficients (we do not exclude the case when $K = Z[x_1,\dots,x_n]$ or $K = Z[y_1,\dots,y_m]$). Set $K_x = Z[x_1,\dots,x_n]$. Let T be a finitely generated free module over K with a specified basis, S a submodule of T defined by a finite collection of generating elements, and ρ a natural number.

LEMMA 2. There exists an algorithm that enables us to convert a given system of generators of S into another system $\Sigma(S, \rho)$, which we call a "canonical basis" and which satisfies the following conditions:

a) the module over the ring K_x, generated by the elements in $\Sigma(S,\rho)$, contains all elements of S whose exponents as a power of the y's do not exceed ρ;

b) a basis for the module of relations among the elements of $\Sigma(S,\rho)$ can effectively be found.

COROLLARY. There exists an algorithm that solves the problem of the occurrence of an element in a submodule of a free module over a polynomial ring with integral coefficients.

This follows immediately from a) if we consider the case where $K = Z[y_1,\dots,y_m]$.

Proof of the Lemma. By induction, we can assume that the lemma and corollary are valid for $K' = Z[x_1,\dots,x_n, y_1,\dots,y_{m-1}]$.

Suppose that the exponents of the elements of a given system of generators of S as powers of y_m do not exceed t, $t \geq \rho$. Noetherian arguments and the inductive assumption enable us to transform this system of generators into another system satisfying the following conditions:

1) This system, which we denote by Ω, is the union of the sets $\Omega_0,\dots,\Omega_t$, where Ω_τ consists of elements having exponent τ as a power of y_m, $0 \leq \tau \leq t$. Let S_τ denote the module over K' generated by the highest (with respect to y_m) terms of the elements in Ω_τ. Then $S_0 \subseteq S_1 \subseteq \dots \subseteq S_t$.

2) Let $\Omega_\tau = \{f_1,\dots,f_\ell\}$. Assume that for some $u_1,\dots,u_\ell$ in K' the exponent of $u_1f_1+\dots+u_\ell f_\ell$ as a power of y_m is less than τ. Then the coefficient of this element for $y_m^{\tau-1}$ lies in $S_{\tau-1}$. Moreover, we shall assume that the highest terms of the elements in Ω_t form a "canonical basis" $\Sigma_t = \Sigma(S_t, \rho)$ for S_t.

Consider the coefficients for y_m^{t-1} of the elements in Ω_t. Suppose that their exponents as powers of $y_1,\dots,y_{m-1}$ do not exceed ρ_{t-1}, $\rho_{t-1} \geq \rho$. Let us transform Ω_{t-1} so that the highest terms of the elements of this system constitute a "canonical basis" $\Sigma_{t-1} = \Sigma(S_{t-1}, \rho_{t-1})$ for S_{t-1}. We continue to proceed in a similar manner, thereby guaranteeing one more condition.

3) The highest terms of the elements in Ω_τ form a canonical basis $\Sigma_\tau = \Sigma(S_\tau, \rho_\tau)$, $\rho_\tau \geq \rho$, for S_τ. If $f \in \Omega_i$, $i > \tau$, then the coefficient of this element for y_m^τ has exponents not exceeding ρ_τ as powers of $y_1,\dots,y_{m-1}$.

Let us find a basis for the module of relations over K among the elements of Ω. Let $\Omega_\tau = \{f_1,\dots,f_\ell\}$ and $\{u^{(\alpha)} = (u_1^{(\alpha)},\dots,u_\ell^{(\alpha)})\}$ a basis of the module of relations over K' among the highest terms of $f_1,\dots,f_\ell$.

Then the relations that express $u_1^{(\alpha)} f_1 + \ldots + u_\ell^{(\alpha)} f_\ell$ in terms of elements in $\Omega_0, \ldots, \Omega_{\tau-1}$ and $y_m f_i$ in terms of elements in $\Omega_0, \ldots, \Omega_{\tau+1}$ over K' constitute the desired basis.

It is not hard to verify that the system Ω satisfying 1), 2), and 3) is the desired system. This proves the lemma.

3. Let us turn to the proof of the main result of this section.

THEOREM 1. There exists an algorithm that solves the occurrence problem for 2-step solvable groups.

Proof. Let G be defined in the variety of 2-step solvable groups by means of the generators $x_1, \ldots, x_n$ and defining relations $\tau_1(x) = 1, \ldots, \tau_m(x) = 1$. G is the factor group of the free 2-step solvable group F with basis $x_1, \ldots, x_n$ by the normal subgroup R generated by $\tau_1, \ldots, \tau_m$. Let F be Magnus-embedded in the wreath product C of free abelian groups $\bar{A}$ and B of rank n. By Lemma 1, choose a normal subgroup C of N such that $F \cap N = R$ and $N = B_1[B_1, \bar{A}]N_1$, where $B_1 \subseteq B$, $N_1 \subseteq \bar{A}$, $N_1 \lhd C$. The group G can be embedded as a subgroup in C/N and so it suffices to learn how to solve the occurrence problem for C/N. Consider the factor group of C by $B_1[B_1, \bar{A}]$; it is isomorphic to $A \wr B/B_1$. The image of N under this factorization is contained in the base group of this wreath product. Therefore, we shall assume from the very beginning that B is a finitely generated abelian group (not necessarily free) and that N is contained in $\bar{A}$ and, as a normal subgroup, is generated by a given finite collection of elements.

Let H be a subgroup of C defined by a finite collection of generating elements and g an element of C. We need to determine whether or not g belongs to HN. The problem can easily be reduced to the case when g lies in $\bar{A}$. Let $B = B_1 B_2$, where B_1 is the periodic part of B and B_2 is torsion-free. The group $C' = B_2 \bar{A}$ is isomorphic to the wreath product of A^{B_1} and B_2. Its subgroup $H' = H \cap C'$ is finitely generated, and a system of generators for H' can be effectively found. Then, if N, as a normal subgroup of C, is generated by $\tau_1, \ldots, \tau_m$, then in C' it is generated by the set $\{\tau_1^{B_1}, \ldots, \tau_m^{B_1}\}$. On the basis of this, in what follows we shall assume that B is torsion-free.

Let $b_1, \ldots, b_\lambda$ be a basis of B and $t_1, \ldots, t_n$ a basis of A. $\bar{A}$ is the additive group of a free left module T with basis $t_1, \ldots, t_n$ over $\mathbb{Z}[B]$. The normal subgroups of C lying in $\bar{A}$ are precisely the submodules of T. Choose a system of generators $h_1, \ldots, h_K, u_1, \ldots, u_\ell$ for H such that $h_1, \ldots, h_K$ are linearly independent modulo $\bar{A}$, and $u_1, \ldots, u_\ell$ lie in $\bar{A}$. Then $K \leq \lambda$, and we can assume that $h_i = b_i^{n_i}$ modulo $\bar{A}$, $n_i > 0$, $i = 1, \ldots, K$. The set $H \cap \bar{A}$ is a module over the ring $\mathbb{Z}[b_1^{n_1}, b_1^{-n_1}, \ldots, b_K^{n_K}, b_K^{-n_K}]$, generated by $u_1, \ldots, u_\ell$ and all possible commutators $[h_i, h_j]$. Note that we can simplify the construction by assuming $n_1 = \ldots = n_K = 1$. This follows from the fact that T can be regarded as a free module over $\mathbb{Z}[b_1^{n_1}, b_1^{-n_1}, \ldots, b_K^{n_K}, b_K^{-n_K}, b_{K+1}, b_{K+1}^{-1}, \ldots, b_\lambda, b_\lambda^{-1}]$ with basis $\{b_1^{\alpha_1} \ldots b_K^{\alpha_K} t_i \mid i = 1, \ldots, n,\ 0 \leq \alpha_j < n_j\}$. Finally $\mathbb{Z}[B]$ is a factor ring of a polynomial ring. All this reduces our problem to the following one. Let T be a finitely generated free module over the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$; N a submodule of T defined by a finite collection of generating elements; H the module over $\mathbb{Z}[x_1, \ldots, x_n]$ generated by this finite set of elements of T. We must discover an algorithm that solves the occurrence problem in $H + N$. Consider an element g of T for which we wish to determine whether or not it lies in $H + N$. Assume that the exponents of g and the elements of H as powers of all the y_i do not exceed p. By Lemma 2, choose a "canonical basis" $\Sigma = \Sigma(N, p)$ for N and consider the module over $\mathbb{Z}[x_1, \ldots, x_n]$ generated by the elements of Σ, which we denote by N'. It is easy to see that g lies in $H + N$ if and only if g lies in $H + N'$. The occurrence problem in $H + N'$ is algorithmically solvable (corollary of Lemma 2). This proves the theorem.

§2. Groups Given by a Single Defining Relation

THEOREM 2. Let the group G be given by means of the generators $x_1, \ldots, x_n$ and single defining relation $\tau(x) = 1$. In other words, G is the factor group of the free group F with basis $x_1, \ldots, x_n$ by the normal subgroup generated by τ. The factors of the series of commutator groups for G are torsion-free if and only if τ is primitive, i.e., is not a power of another element modulo $F^{(K+1)}$, where the number K is such that $\tau \in F^{(K)} \setminus F^{(K+1)}$.

Proof. Let τ be primitive modulo $F^{(\kappa+1)}$. Consider some factor $G^{(m-1)}/G^{(m)}$ of the series of commutator groups for G, $m > \kappa$. Set $F_i = F/F^{(i)}$, $i = 1, 2, \ldots$. The group $G/G^{(m)}$ is the factor group of F_m by the normal subgroup R, generated by the image of τ under the canonical homomorphism of F onto F_m. Denote this image by τ'. Let us Magnus-embed F_m in the wreath product $A \wr F_{m-1} = C$, where A is a free abelian group of rank n. Note [2] that $F_m^{(m-1)}$ is contained in $\bar{A}$ and is isolated there. Let $\tau' = \tau_1 \tau_2$, where $\tau_1 \in F_{m-1}$ and $\tau_2 \in \bar{A}$. By Lemma 1, C contains a normal subgroup N such that $N \cap F_m = R$ and $N = R_1[R_1, \bar{A}]N_1$, where $R_1 \lhd F_{m-1}$ and $N_1 \subseteq \bar{A}$. By construction, R_1 is the normal subgroup of F_{m-1} generated by τ_1, and N_1 is the normal subgroup of C generated by τ_2. Consider the factor group of C by $R_1[R_1, \bar{A}]$. It is isomorphic to $A \wr B = H$, where $B = F_{m-1}/R_1$. In turn, B is isomorphic to $G/G^{(m-1)}$. By induction, we assume that the factors of the series of commutator groups for this group are torsion-free. Let T denote the image of R under the homomorphism of C onto H induced by the canonical homomorphism of F_{m-1} onto B. T, as a normal subgroup, is generated by the image of τ', which we denote by t. Note that t is a primitive element in H. Indeed, by hypothesis, the image of τ, which we denote by $\bar{\tau}$, in $F/F^{(\kappa+1)}$ is a primitive element. This group can be embedded in $A \wr F_\kappa$. In Lemma 6 of [5] it was proved that there exists a homomorphism ν of H onto $A \wr F_\kappa$ under which $\nu(t) = \bar{\tau}$. Since $\bar{\tau}$ is primitive in $A \wr F_\kappa$ (recall that $F_{\kappa+1}^{(\kappa)}$ is isolated in $A \wr F_\kappa$), then t is also primitive. Let $\bar{A}$ be the base of $A \wr B$. To prove the theorem, it suffices to show that T is isolated in $\bar{A}$. Assume the contrary – that some element x in T has a root of prime degree p in $\bar{A}$ but does not have such root in T. Let us represent this element in the form $x = t^{m_1 u_1} \ldots t^{m_s u_s} = t^{\sum m_i u_i}$, where $u_i \in B$ and the m_i are integers, at least one of which is not a multiple of p. We can regard $\bar{A}$ as the additive group of a free left module of rank n over $\mathbb{Z}[B]$. Conjugating $\bar{A}$ by elements of B is equivalent to multiplying the module by these elements. Passing to the language of modules, we rewrite x in the form $x = (\sum m_i u_i) \cdot t$. Let $\mathbb{Z}_p$ denote the ring of residues modulo p. The canonical homomorphism of $\mathbb{Z}[B]$ onto $\mathbb{Z}_p[B]$ induces a homomorphism φ of $\bar{A}$ onto a free left module of rank n over $\mathbb{Z}_p[B]$. By assumption, $\varphi(x) = 0$. Since $\sum \bar{m}_i u_i \neq 0$ and $\varphi(t) \neq 0$, this means that $\mathbb{Z}_p[B]$ has zero divisors. It is known [6] that if B is solvable and the factors of the series of commutator groups are torsion-free, then $K[B]$ has no zero divisors, where K is a field. The resulting contradiction proves the theorem in one direction. The converse is obvious.

The proof of the following theorem is rather tedious and is primarily based on the construction developed in Theorem 2. Therefore, we shall not present it.

THEOREM 3. Let G be given in the variety of n-step solvable groups by means of the generators $x_1, \ldots, x_n$ and defining relation $\tau(x) = 1$, i.e., $G = F/R$, where F is a free group of this variety with basis $x_1, \ldots, x_n$, and R is the normal subgroup generated by τ. Let $\tau \in F^{(\kappa)} \setminus F^{(\kappa+1)}$. Assume that τ is primitive modulo $F^{(\kappa+1)}$. Then the equality problem is algorithmically solvable in G.

LITERATURE CITED

1. P. S. Novikov, "On the algorithmic unsolvability of the identity problem," Dokl. Akad. Nauk SSSR, 85, 709-712 (1952).
2. V. N. Remeslennikov, "An example of a group finitely defined in the variety with an unsolvable equality problem," Algebra i Logika, 12, No. 5, 577-602 (1973).
3. K. A. Mikhailova, "The occurrence problem for free products of groups," Matem. Sb., 75, No. 2, 199-211 (1968).
4. J. P. Labute, "On the descending central series of groups with a single defining relation," J. Algebra, 14, No. 1, 16-23 (1970).
5. N. S. Romanovskii, "A freeness theorem for groups with a single defining relation in varieties of solvable and nilpotent groups of given classes," Matem. Sb., 89, No. 1, 93-99 (1972).
6. A. A. Bovdi, "On group rings of torsion-free groups," Sibirsk. Matem. Zh., 1, No. 4, 555-558 (1960).