Algebra and Logic, Vol. 51, No. 3, July, 2012
(Russian Original Vol. 51, No. 3, May-June, 2012)

UNIVERSAL THEORIES FOR FREE SOLVABLE GROUPS

N. S. Romanovskii*

UDC 512.54.05

Keywords: *universal theory, decidable theory, free solvable group.*

It is proved that a free solvable group of derived length at least 4 *has an algorithmically undecidable universal theory.*

INTRODUCTION

In [1], it was proved that a free solvable group of derived length at least 2 has an algorithmically undecidable elementary theory. In [2], it was stated that a free metabelian group of derived length 2 and some other solvable groups, for instance, left-iterated direct wreath products of torsion-free Abelian groups, have decidable universal theories. In particular, it was pointed out that a noncyclic free metabelian group and a direct wreath product of two nontrivial torsion-free Abelian groups are universally equivalent (i.e., have the same universal theory). Universal theories for free metabelian groups, as well as for groups close to these, were explored further in [3, 4]: axiomatics was worked out, properties of theories were investigated, and so on.

For free solvable groups of derived length at least 3, groups of different ranks are also universally equivalent to each other. The question whether their universal theories are decidable was taken up in [5]. It was established that an arbitrary Diophantine equation over the field of rational numbers is interpreted via $\exists$-formulas in a free solvable group of derived length at least 3; however, the question if the Diophantine problem is decidable over $\mathbb{Q}$ remains open. The main result of the present paper is the following:

THEOREM. A free solvable group F of derived length at least 4 has an undecidable universal theory, or, which is equivalent, an undecidable $\exists$-theory.

*Supported by RFBR, grant No. 12-01-00084.

Sobolev Institute of Mathematics, Siberian Branch, Russian Academy of Sciences, pr. Akad. Koptyuga 4, Novosibirsk, 630090 Russia; Novosibirsk State University, ul. Pirogova 2, Novosibirsk, 630090 Russia; rmnvski@math.nsc.ru. Translated from *Algebra i Logika*, Vol. 51, No. 3, pp. 385-391, May-June, 2012. Original article submitted February 7, 2012.

0002-5232/12/5103-0259

The proof is based on the interpretation of an arbitrary Diophantine equation in a group F over $\mathbb{Z}$ by using methods outlined in [1, 5] and by applying a theorem in [6], which states that the Diophantine problem is undecidable over $\mathbb{Z}$. Possibly, a similar scheme can also be realized for a free solvable group of derived length 3.

1. AUXILIARY STATEMENTS

As usual, if G is a group, and $x, y \in G$, then $x^y = y^{-1}xy$ and $[x, y] = x^{-1}y^{-1}xy$. An ith member in a series of commutator subgroups of G is denoted by $G^{(i)}$.

LEMMA 1. If two elements f_1 and f_2 of a free solvable group F_2 of derived length 2 are linearly independent modulo a commutator subgroup F_2', then an eigenvalue of a commutator $[f_1, f_2]$ is not extracted.

Proof. We may assume that our group has finite rank. Note that the commutator $[f_1, f_2]$ under consideration is left invariant under elementary transformations of a system $\{f_1, f_2\}$ of the form

$$f_i \to f_j^m f_i,\ f_j \to f_j,\ i \neq j,\ m \in \mathbb{Z}.$$

Recall that elements of a free Abelian group of finite rank (such is F_2/F_2' for instance) can be identified with integer-valued rows of respective lengths. A matrix with two rows, via elementary transformations of rows and columns over $\mathbb{Z}$ (column transformations correspond to elementary transformations of a basis for a free Abelian group), can be reduced to a generalized diagonal form, i.e., one where nonzero elements may only capture the positions $(1, 1)$ and $(2, 2)$. Using this argument, we can reduce the problem to the case where $f_1 \equiv x_1^m$, $f_2 \equiv x_2^n \mod F_2'$, $m, n > 0$, and $\{x_1, x_2, \ldots\}$ is a basis for a free solvable group F_2 of derived length 2. We may also assume that the rank of F_2 equals exactly 2, i.e., $F_2 = \langle x_1, x_2 \rangle$.

Let A be a free Abelian group with basis $\{a_1, a_2\}$ and T a right free $\mathbb{Z}A$-module with basis $\{t_1, t_2\}$. In view of [7], if we put

$$x_1 = \begin{pmatrix} a_1 & 0 \\ t_1(a_1 - 1) & 1 \end{pmatrix},\ x_2 = \begin{pmatrix} a_2 & 0 \\ t_2(a_2 - 1) & 1 \end{pmatrix},$$

then we obtain an embedding of F_2 in a matrix group $\begin{pmatrix} A & 0 \\ T & 1 \end{pmatrix}$. In this case

$$\begin{pmatrix} a & 0 \\ t_1u_1 + t_2u_2 & 1 \end{pmatrix} \in F_2 \Longleftrightarrow u_i \in (a_i - 1) \cdot \mathbb{Z}A,\ u_1 + u_2 = a - 1. \tag{1}$$

In particular,

$$\begin{pmatrix} a & 0 \\ t_1u_1 + t_2u_2 & 1 \end{pmatrix} \in F_2' \Longleftrightarrow a = 1,\ u_1 = -u_2 = (a_1 - 1)(a_2 - 1)u, \quad u \in \mathbb{Z}A. \tag{2}$$

Let $f_1 = x_1^m g_1$ and $f_2 = x_2^n g_2$, $g_1, g_2 \in F_2'$. We have

$$[f_1, f_2] = [x_1^m, x_2^n][x_1^m, g_2][g_1, x_2^n],\ [x_1^m, x_2^n] = \begin{pmatrix} 1 & 0 \\ (t_1 - t_2)(a_1^m - 1)(a_2^n - 1) & 1 \end{pmatrix}.$$

Let

$$[f_1, f_2] = \begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix},\ g_1 = \begin{pmatrix} 1 & 0 \\ w_1 & 1 \end{pmatrix},\ g_2 = \begin{pmatrix} 1 & 0 \\ w_2 & 1 \end{pmatrix}.$$

By virtue of (2),

$$w_1 = (t_1 - t_2)(a_1 - 1)(a_2 - 1)u_1,\ w_2 = (t_1 - t_2)(a_1 - 1)(a_2 - 1)u_2,$$

where $u_1, u_2 \in \mathbb{Z}A$. Consequently,

$$w = (t_1 - t_2)((a_1^m - 1)(a_2^n - 1) + (a_1 - 1)(a_2 - 1)(u_1(a_2^n - 1) - u_2(a_1^m - 1))).$$

Assume on the contrary that a pth root, where p is a prime, of $[f_1, f_2]$ is extracted. This means that modulo p, i.e., in the group ring of A over a field $\mathbb{Z}/p\mathbb{Z}$ consisting of p elements, the following equality holds:

$$(a_1^m - 1)(a_2^n - 1) = (a_1 - 1)(a_2 - 1)(-u_1(a_2^n - 1) + u_2(a_1^m - 1)). \tag{3}$$

Let $m = p^k r$ and $n = p^l s$, where r and s are relatively prime to p. Then (3) is equivalent to

$$(a_1^r - 1)^{p^k}(a_2^s - 1)^{p^l} = (a_1 - 1)(a_2 - 1)(-u_1(a_2^s - 1)^{p^l} + u_2(a_1^r - 1)^{p^k}). \tag{4}$$

If we expand the left-hand side of (4) in powers of $a_1 - 1$ and $a_2 - 1$, then a monomial of minimal degree in this expansion will be equal to $(a_1 - 1)^{p^k}(a_2 - 1)^{p^l}$. Therefore, we may assert that the left-hand side does not belong to the ideal of the group ring generated by elements $(a_1 - 1)(a_2 - 1)^{p^l + 1}$ and $(a_2 - 1)(a_1 - 1)^{p^k + 1}$. This fact becomes obvious if we embed the ring $\mathbb{Z}/p\mathbb{Z}[A]$ in a ring of formal power series in $b_1 = a_1 - 1$ and $b_2 = a_2 - 1$ over $\mathbb{Z}/p\mathbb{Z}$. However, the right-hand side of (4) belongs to the ideal mentioned. The lemma is proved.

COROLLARY. Let F_m be a free solvable group of derived length $m \geq 3$ and f_1 and f_2 be elements which lie in $F_m^{(i)} \setminus F_m^{(i+1)}$ and are linearly independent modulo $F_m^{(i+1)}$. Then for $i \leq m - 2$ the centralizer of an element $[f_1, f_2]$ coincides with a cyclic subgroup generated by this element.

Proof. We know from [1] that the centralizer of any element of a free solvable group, which does not sit in the last nontrivial commutator subgroup, is cyclic. Therefore, it suffices to observe that a root of $[f_1, f_2]$ in F_m is not extracted. This follows from the fact that the subgroup $F_m^{(i)}$ is isolated in F_m and $F_m^{(i)}/F_m^{(i+2)}$ is a free solvable group of derived length 2, and from the statement of Lemma 1. The corollary is proved.

LEMMA 2. Let F be a free solvable group. Then the conditions

$$x \in F^{(i)},\quad x \equiv y \mod F^{(i)},$$

as well as their negations, are written in a group signature by using $\exists$-formulas in free variables x or x, y, respectively.

Proof. The required statement follows from [1] (where it is proved that the condition $x \in F^{(i)}$ is expressed via a $\forall$-formula) and from [5] (where it is stated that this condition is expressed via an $\exists$-formula as well). A more general statement, in which an arbitrary rigid solvable group with a respective rigid series is taken in place of F, was proved in [8, Prop. 5].

2. PROOF OF THE THEOREM

Thus we are proving that a free solvable group F of derived length $m \geq 4$ has an undecidable $\exists$-theory. By Lemma 2, the conditions $x \in F^{(4)}$ and $x \notin F^{(4)}$ are expressed via $\exists$-formulas. Under the passage to a factor group $F/F^{(4)}$, therefore, the problem reduces to the case where F is a free solvable group of derived length 4.

We make some more comments. If $a \in F' \setminus F''$ and $b \in F \setminus F'$, then a and a^b lie in $F' \setminus F''$ and are linearly independent modulo F''. By the corollary to Lemma 1, the centralizer of an element $c = [a, a^b]$ coincides with a cyclic subgroup generated by this element. Note also that elements c and $d = c^b$ lie in $F'' \setminus F^{(3)}$ and are linearly independent modulo $F^{(3)}$.

Since the Diophantine problem is undecidable over $\mathbb{Z}$ [6], to prove the theorem, it suffices to use an $\exists$-formula to interpret in the group under consideration an arbitrary formula

$$\exists z_1, \ldots, z_n \ (P(z_1, \ldots, z_n) = 0),$$

where $P(z_1, \ldots, z_n)$ is an integer polynomial and values for variables z_i are sought for in $\mathbb{Z}$. The formula $\exists z_1, \ldots, z_n \ (P(z_1, \ldots, z_n) = 0)$ is equivalent to some formula

$$\exists y_1, \ldots, y_m \ \Phi(y_1, \ldots, y_m), \tag{5}$$

where $\Phi(y_1, \ldots, y_m)$ is a conjunction of equalities like $y_i + y_j = y_k$, $y_i y_j = y_k$, $y_i = 1$, and $y_i = 0$. We will interpret y_i as exponents of the above element c. More specifically, with formula (4) in a ring signature we associate a formula in a group signature, namely,

$$\begin{aligned} \exists a, b, c, d, x_1, \ldots, x_m \ (a \in F' \setminus F'' \ \wedge \ b \in F \setminus F' \ \wedge \ c = [a, a^b] \\ \wedge \ d = c^b \ \wedge \ [x_1, c] = 1 \ \wedge \ldots \\ \wedge \ [x_m, c] = 1 \ \wedge \ \Psi(x_1, \ldots, x_m)), \end{aligned} \tag{6}$$

where $\Psi(x_1, \ldots, x_m)$ is obtained from $\Phi(y_1, \ldots, y_m)$ by making the following replacements:

$y_i + y_j = y_k \ \rightarrow \ x_i x_j = x_k$;

$y_i = 1 \ \rightarrow \ x_i = c$;

$y_i = 0 \ \rightarrow \ x_i = 1$;

$y_i y_j = y_k \ \rightarrow \ \exists u, v, w \ ([u, x_i d] = 1 \wedge [v, d] = 1 \wedge [w, cd] = 1 \wedge w \equiv x_j v \mod F^{(3)} \wedge u \equiv x_k v \mod F^{(3)})$.

Thus we assume that (5) is satisfied on F. Then appropriate values for x_i will be of the form c^{y_i}, where $y_i \in \mathbb{Z}$. We claim that for a given tuple $(y_1, \ldots, y_m)$, $\Phi(y_1, \ldots, y_m)$ will be satisfied. This follows from the fact that for $(x_1, \ldots, x_m) = (c^{y_1}, \ldots, c^{y_m})$, the relations below hold:

(1) $y_i + y_j = y_k \Leftrightarrow x_i x_j = x_k$;

(2) $y_i = 1 \Leftrightarrow x_i = c$;

(3) $y_i = 0 \Leftrightarrow x_i = 1$;

(4) $y_i y_j = y_k \Leftrightarrow \exists u, v, w\, ([u, x_i d] = 1 \wedge [v, d] = 1 \wedge [w, cd] = 1 \wedge w \equiv x_j v \mod F^{(3)} \wedge u \equiv x_k v \mod F^{(3)})$.

Relations (1)-(3) are obvious; (4) was proved in [5]. We give a short proof for (4). Since u, v, and w commute with $x_i d$, d, and cd, respectively, it follows that $u = (x_i d)^{r_1}$, $v = d^{r_2}$, and $w = (cd)^{r_3}$, where r_1, r_2, and r_3 are, broadly speaking, rational numbers (here use is made of the fact that F satisfies the condition of being unique for extraction of roots). Further, we consider congruences modulo $F^{(3)}$. We have $u \equiv c^{y_i r_1} d^{r_1}$ and $w \equiv c^{r_3} d^{r_3}$. From $w \equiv x_j v$, we derive $c^{r_3} d^{r_3} \equiv c^{y_j} d^{r_2}$, and hence $r_3 = y_j = r_2$. From $u \equiv x_k v$, we obtain $c^{y_i r_1} d^{r_1} \equiv c^{y_k} d^{r_2}$, whence $r_1 = r_2 = y_j$ and $y_k = y_i y_j$.

Thus the fact that formula (5) is valid on F implies being valid for (4) on $\mathbb{Z}$. It is easy to see that the converse is also true. The theorem is proved.

REFERENCES

1. A. I. Mal'tsev, "Free solvable groups," *Dokl. Akad. Nauk SSSR*, **130**, No. 3, 495-498 (1960).
2. O. Chapuis, "Universal theory of certain solvable groups and bounded Ore group rings," *J. Alg.*, **176**, No. 2, 368-391 (1995).
3. O. Chapuis, "∀-free metabelian groups," *J. Symb. Log.*, **62**, No. 1, 159-174 (1997).
4. V. Remeslennikov and R. Stohr, "On the quasivariety generated by a non-cyclic free metabelian group," *Alg. Colloq.*, **11**, No. 2, 191-214 (2004).
5. O. Chapuis, "On the theories of free solvable groups," *J. Pure Appl. Alg.*, **131**, No. 1, 13-24 (1998).
6. Yu. V. Matiyasevich, "Being Diophantine for enumerable sets," *Dokl. Akad. Nauk SSSR*, **191**, No. 2, 279-282 (1970).
7. N. S. Romanovskii, "Shmel'kin embeddings for abstract and profinite groups," *Algebra Logika*, **38**, No. 5, 598-612 (1999).
8. A. G. Myasnikov and N. S. Romanovskii, "Universal theories for rigid soluble groups," *Algebra Logika*, **50**, No. 6, 802-821 (2011).