УДК 512.54
DOI 10.25513/1812-3996.2018.23(2).27-34

АЛГОРИТМЫ ДЛЯ МЕТАБЕЛЕВЫХ ГРУПП
(посвящается 70-летию профессора Виталия Анатольевича Романькова)

А. В. Меньшов[1,2], А. Г. Мясников[1], А. В. Ушаков[1]
[1]*Институт технологий Стивенса, Хобокен, Нью-Джерси, США*
[2]*Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия*

Информация о статье
Дата поступления
11.03.2018

Дата принятия в печать
29.03.2018

Дата онлайн-размещения
25.06.2018

Ключевые слова
Метабелевы группы, проблема равенства, проблема сопряженности, алгоритм, коммутативная алгебра, базисы Гребнера

Финансирование
Исследование первого автора выполнено при финансовой поддержке РНФ в рамках научного проекта № 16-11-10002

Аннотация. Данной статьей мы начинаем систематическое изучение трудоемкости основных алгоритмических проблем в конечно порожденных метабелевых группах. Основной целью этой работы является классификация алгоритмических проблем в метабелевых группах в соответствии с их вычислительной сложностью.

ALGORITHMS FOR METABELIAN GROUPS
(paper dedicated to Professor Vitaly Anatol'evich Roman'kov on the occasion of his 70th birthday)

A. V. Menshov[1,2], A. G. Myasnikov[1], A. V. Ushakov[1]
[1]*Stevens Institute of Technology, Hoboken, NJ, USA*
[2]*Dostoevsky Omsk State University, Omsk, Russia*

Article info
Received
11.03.2018

Accepted
29.03.2018

Available online
25.06.2018

Keywords
Metabelian groups, word problem, power problem, conjugacy problem, algorithm, commutative algebra, Groebner bases

Abstract. In this paper, we begin the study of computational complexity of the principal algorithmic problems in finitely generated metabelian groups. The main goal is to classify the algorithmic problems in metableian groups in terms of their computational complexity.

ISSN 1812-3996

Acknowledgements
The reported study of the first author was funded by RSF to the research project № 16-11-10002

1. Introduction

In this paper we begin the study of computational complexity of the principal algorithmic problems in finitely generated metabelian groups. Our approach here is two-fold: firstly, we rewrite and streamline some classical algorithms in metabelian groups to fit them into the framework of Groebner bases and commutative algebra (sometimes this requires a significant rebuild); secondly, we show that in most cases this reduction to the Groebner bases is in polynomial time. The main goal for the subsequent papers is to classify the algorithmic problems in metableian groups in terms of the logspace and circuit complexities.

In section 2 we introduce necessary definitions and results related to Groebner bases and state Theorem 2.1 and Corollary 2.2 that allow us to compute module presentation of ideals in polynomial rings.

In section 3 we discuss presentation of group rings of finitely generated abelian groups and modules over such rings by polynomials.

In section 4 we interpret submodule computability in terms of Groebner bases.

In section 5 we interpret word, power, and conjugacy problems in finitely generated metabelian groups in terms of Groebner bases.

2. Groebner bases

In this section we will introduce some necessary definitions and results related to Groebner bases. For a detailed exposition we refer to [1] or [2].

Let R be a commutative ring with 1, $\mathrm{X} = \{x_1, \dots, x_n\}$ be a finite set of variables, and $R[X] = R[x_1, \dots, x_n]$. A *term* t in the variables $x_1, \dots, x_n$ is a power product of the form $x_1^{e_1} \cdot \ldots \cdot x_n^{e_n}$ with $e_i \in \mathbb{N}$ for $1 \leq i \leq n$. In particular, $1 = x_1^0 \cdot \ldots \cdot x_n^0$ is a term. We denote by $T(X)$ the set of all terms in these variables. The divisibility relation $|$ on $T(X)$ is defined by $s|t$ iff there exists $s' \in T(X)$ such that $ss' = t$.

A *term order* $\leq$ is a linear order on $T(X)$ that satisfies the following conditions:

1. $1 \leq t$ for all $t \in T(X)$.

2. $t_1 \leq t_2$ implies $t_1 s \leq t_2 s$ for all $s, t_1, t_2 \in T(X)$.

A *monomial* in the variables $\{x_1, \dots, x_n\}$ over R is a polynomial of the form $m = at$ with $0 \neq a \in R$ and $t \in T(X)$. Here, a is called the *coefficient* of m and t the *term* of m. The set of all monomials (in variables $\{x_1, \dots, x_n\}$ over R) is denoted by $M(X, R)$. Multiplication on $M(X, R)$ is defined by $a_1 t_1 \cdot a_2 t_2 = (a_1 a_2)(t_1 t_2)$, and $M(X, R)$ is clearly a commutative monoid.

For a term order $\leq$ we define the relation $\preccurlyeq$ on $M(X, R)$ by setting

$$as \preccurlyeq bt \quad \text{iff} \quad s \leq t$$

for $0 \neq a, b \in R$ and $s, t \in T(X)$. We will call $\preccurlyeq$ the quasi-order (reflexive and transitive relation) on $M(X, R)$ induced by $\leq$. If m_1, m_2 are two monomials with the same term but with different coefficients, then $m_1 \neq m_2$ but $m_1 \preccurlyeq m_2$ and $m_2 \preccurlyeq m_1$. In this case we will say that m_1 and m_2 are equivalent w.r.t. $\preccurlyeq$ and write $m_1 \sim m_2$. Further we will denote this induced relation $\preccurlyeq$ by $\leq$.

Clearly, every polynomial $f \in R[X]$ has a unique representation in the form $\sum_{i=1}^{k} m_i$ with $m_i \in M(X, R)$ and $m_1 > \cdots > m_k$. The set of monomials occurring in such representation is denoted by $M(f)$ and called the set of monomials of f. The set $T(f)$ of terms of f is the set of all terms of monomials $m \in M(f)$. The set $C(f)$ of all coefficients of f is the set of all coefficients of monomials $m \in M(f)$.

For any finite, non-empty subset A of $M(X, R)$ consisting of pairwise inequivalent monomials, we define $\max(A)$ to be the unique maximal element of A w.r.t. $\leq$. For any non-zero polynomial $f \in R[X]$ we define w.r.t. $\leq$ the *head term* $\mathrm{HT}(f) = \max(T(f))$, the *head monomial* $\mathrm{HM}(f) = \max(M(f))$, and the *head coefficient* $\mathrm{HC}(f)$ to be the coefficient of $\mathrm{HM}(f)$. The *reductum* $\mathrm{red}(f)$ of f w.r.t. $\leq$ is defined as $f - \mathrm{HM}(f)$, i.e., $f = \mathrm{HM}(f) + \mathrm{red}(f)$. A polynomial $f \in R[X]$ is called *monic* w.r.t. $\leq$ if $f \neq 0$ and $\mathrm{HC}(f) = 1$.

For the rest of this section, let R be a PID (or just $\mathbb{Z}$).

Let $m_1 = a_1 t_1$ and $m_2 = a_2 t_2$ be monomials in $R[X]$. We say that m_2 divides m_1 and write $m_2 | m_1$ if there is a monomial $m_3 \in R[X]$ such that $m_1 = m_2 m_3$.

Let $f, g, p \in R[X]$ with $f, p \neq 0$, and let P be a subset of $R[X]$. Then we say that

1. f D-reduces to g modulo p by eliminating m (notation $f \underset{p}{\to} g[m]$), if $m \in M(f)$ is such that $\mathrm{HM}(p) | m$, say $m = m' \cdot \mathrm{HM}(p)$, and $g = f - m'p$.

2. f D-reduces to g modulo p (notation $f \underset{p}{\to} g$), if $f \underset{p}{\to} g[m]$ for some $m \in M(f)$.

ISSN 1812-3996

3. f D-reduces to g modulo P (notation $f \underset{P}{\rightarrow} g$), if $f \underset{p}{\rightarrow} g$ for some $p \in P$.

4. f is D-reducible modulo p if there exists $g \in R[X]$ such that $f \underset{p}{\rightarrow} g$.

5. f is D-reducible modulo P if there exists $g \in R[X]$ such that $f \underset{P}{\rightarrow} g$.

If f is not D-reducible modulo p (modulo P), then we say f is in D-normal form modulo p (modulo P). A D-normal form of f modulo P is a polynomial g that is in D-normal form modulo P and satisfies

$$f \underset{P}{\rightarrow}^* g$$

where $\underset{P}{\rightarrow}^*$ is the reflexive-transitive closure of $\underset{P}{\rightarrow}$. We call $f \underset{p}{\rightarrow} g[m]$ a top-D-reduction of f if $m = \mathrm{HM}(f)$. Whenever a top-D-reduction of f exists (with $p \in P$), we say that f is top-D-reducible modulo p (modulo P).

Let $0 \neq f \in R[X]$. A *standard representation* of f w.r.t. a finite subset P of $R[X]$ is a representation

$$f = \sum_{i=1}^{k} m_i p_i,$$

with monomials m_i and $p_i \in P$ such that $\mathrm{HT}(m_i p_i) \leq$ $\leq \mathrm{HT}(f)$ for $1 \leq i \leq k$.

Lemma ([1], Lemma 10.3): Let P be a finite subset of $R[X]$, $0 \neq f \in R[X]$, and assume that $f \underset{P}{\rightarrow}^* 0$. Then f has a standard representation w.r.t. P.

Definition (D-Gröbner basis, [1], Definition 10.4) A D-Gröbner basis is a finite subset G of $R[X]$ with the property that all D-normal forms modulo G of elements of $\mathrm{Id}(G)$ equal zero. If I is an ideal of $R[X]$, then a D-Gröbner basis of I is a D-Gröbner basis that generates the ideal I.

In other words, G is a D-Gröbner basis if $f \underset{G}{\rightarrow}^* 0$ for every $f \in \mathrm{Id}(G)$.

Theorem 10.14 of [1] provides an algorithm which, when given a finite subset P of $R[X]$, finds a D-Gröbner basis G such that $\mathrm{Id}(P) = \mathrm{Id}(G)$.

Unfortunately, having a D-Gröbner basis G, $\underset{G}{\rightarrow}$ will not give us unique normal forms, which means that $f + \mathrm{Id}(G) = h + \mathrm{Id}(G)$ will not imply $f \underset{G}{\rightarrow}^* q$ and $h \underset{G}{\rightarrow}^*$ q. For example, consider the ring $Z[x]$ and $G = \{2x + 1\}$, then $f(x) = 2x^2 + 2x$ has the two normal forms $h_1 = x$ and $h_2 = -x - 1$.

However, for Euclidean domains with unique remainders (in the sense of [1, Definition 10.16]) the theory can be improved so that we obtain unique normal forms. We note that examples of such domains are $\mathbb{Z}$ and $K[X]$ for any field K.

Now we define a new type of reduction over Euclidean domain with unique reminders.

Definition (E-reduction, [1], Definition 10.18) Let R be a Euclidean domain with unique reminders and $f, g, p \in R[X]$. We say that f E-reduces to g modulo p and write $f \underset{p}{\rightarrow} g$ if there exists a monomial $m = at \in M(f)$ such that $\mathrm{HT}(p) | t$, say $t = s\mathrm{HT}(p)$, and

$$g = f - qsp,$$

where $0 \neq q \in R$ is the quotient of a upon division with unique reminder by $\mathrm{HC}(p)$.

E-reduction modulo a finite subset of $R[X]$, E-reducibility, and E-normal forms are defined in the obvious way. It is clear that E-reduction extends D-reduction, i.e., every D-reduction step is an E-reduction step.

To obtain the desired bases that allow the computation of unique normal forms, we do not need another Gröbner basis algorithm. It will suffice to take a D-Gröbner basis G and E-reduce modulo G [1, Theorem 10.23].

Further, when we refer to Gröbner bases and reductions, we will assume a D-Gröbner bases and E-reductions. In the reset of the section we use the theory above to obtain results required for algorithms in metabelian groups.

Let $P = \{f_1, \dots, f_q\}$ be a finite subset of $R[X]$, where R is a PID. Ideal

$$\mathrm{Id}(P) = \{f_1\alpha_1 + \dots + f_q\alpha_q \mid \alpha_i \in R[X]\}$$

may be treated as the $R[X]$-module generated by $f_1, \dots, f_q$, then $\mathrm{Id}(P) = F/N$, where F is the free $R[X]$-module generated by $\xi_1, \dots, \xi_q$ and N is a submodule of F. Since $R[X]$ is Noetherian, so is F, therefore N is finitely generated, and $\mathrm{Id}(P)$ is finitely presented as an $R[X]$-module. Our purpose will be to find its presentation.

Observe that the set $S = \{(\alpha_1, \dots, \alpha_q) \mid \alpha_i \in R[X]\}$ of all solutions of the equation

$$f_1h_1 + \dots + f_qh_q = 0$$

with indeterminates $h_1, \dots, h_q$ is an $R[X]$-submodule of $R[X]^q$. The set S is called the *(first) module of syzygies* of $(f_1, \dots, f_q)$. Computing a finite set of generators for S is a well known problem, and its solution actually gives us an $R[X]$-module presentation of $\mathrm{Id}(P)$. Proposition 6.1 of [1] solves this problem for the case when R is a field. Below we state analogous results that allows us to compute a presentation of $\mathrm{Id}(P)$ for the case when R is a PID.

Theorem 2.1 Let G be a Gröbner basis. Then there exists an algorithm to find a finite presentation of $R[X]$-module $\mathrm{Id}(G)$ in terms of elements of G.

ISSN 1812-3996

Corollary 2.2 Let P be a finite subset of $R[X]$. Then there exists an algorithm to find a finite presentation of $R[X]$-module $\mathrm{Id}(P)$ in terms of elements of P.

3. Representing group rings and modules by polynomials

Let A be a finitely generated abelian group given by its abelian presentation

$$A = \langle x_1, \dots, x_n \mid r_1(x_1, \dots, x_n), \dots, r_s(x_1, \dots, x_n)\rangle,$$

where $r_i(x_1, \dots, x_n) = x_1^{c_{i1}} \cdot \dots \cdot x_n^{c_{in}}$, $c_{ij} \in \mathbb{Z}$.

For any $a = x_1^{k_1} \dots x_n^{k_n} \in A$ we denote by $T(a)$ the term in variables $x_1, y_1, \dots, x_n, y_n$ of the form $T(a) = s_1^{|k_1|} \dots s_n^{|k_n|}$, where $s_i = x_i$ if $k_i \geq 0$ and $s_i = y_i$ otherwise. Observe that the inverse procedure is obvious.

Take

$$R_A = \mathbb{Z}[x_1, y_1, \dots, x_n, y_n],$$
$$P_A = \{x_1 y_1 - 1, \dots, x_n y_n - $$
$$-1, T(r_1) - 1, \dots, T(r_s) - 1\} \subset R_A,$$

and consider the map

$$\tau_1 : \mathbb{Z}A \to R_A / \mathrm{Id}(P_A),$$

defined for $\alpha = \sum_{i=1}^{m} k_i a_i \in \mathbb{Z}A$ by

$$\tau_1(\alpha) = \sum_{i=1}^{m} k_i T(a_i) + \mathrm{Id}(P_A).$$

Clearly, τ_1 is a ring automorphism.

Remark 3.1 In practice, the element α would be presented as an element of Laurent ring with integer coefficients in variables $x_1, \dots, x_n$. Although α may have different such presentations if A is not free, given a particular presentation, we uniquely pick the polynomial $\sum_{i=1}^{m} k_i T(a_i)$ as a representative of the residue class $\tau_1(\alpha)$. For convenience, we further denote this representative by $p(\tau_1(\alpha))$. Inversely, given any representative g of the residue class $\tau_1(\alpha)$ as a polynomial in R_A, we uniquely pick the corresponding element β of Laurent ring with integer coefficients in variables $x_1, \dots, x_n$ and interpret it as an element of $\mathbb{Z}A$ and as a preimage of g, so that $\tau_1(\beta) = g + \mathrm{Id}(P_A)$.

Further, when we refer to the size of α, we will assume the size of $\tau_1(\alpha)$, which is actually the size of the polynomial $p(\tau_1(\alpha))$.

Let A be a finitely generated abelian group and $\tau : \mathbb{Z}A \to R_\tau / \mathrm{Id}(P_\tau)$ be a ring isomorphism, where R_τ is a ring of polynomials with integer coefficients and $P_\tau \subset R_\tau$ is finite.

Let F be a free right $\mathbb{Z}A$-module with basis $\xi_1, \dots, \xi_q$, then any $f \in F$ can be written uniquely in the form

$$f = \xi_1 \alpha_1 + \dots + \xi_q \alpha_q, (\alpha_i \in \mathbb{Z}A).$$

This form can be naturally viewed as a polynomial in ξ_i with coefficients in $\mathbb{Z}A$. Consider the ring $\mathbb{Z}A[\xi_1, \dots, \xi_q]$ and its ideal $\mathrm{Id}(P_\xi)$, where $P_\xi = \{\xi_i \xi_j \mid 1 \leq i \leq j \leq q\}$, and observe that the factor ring $\mathbb{Z}A[\xi_1, \dots, \xi_q]/\mathrm{Id}(P_\xi)$ is a free $\mathbb{Z}A$-module with basis $\{1, \xi_1, \dots, \xi_q\}$. Hence the natural map $F \to \mathbb{Z}A[\xi_1, \dots, \xi_q]/\mathrm{Id}(P_\xi)$ is a $\mathbb{Z}A$-module monomorphism. Denote

$$R_F = R_\tau[\xi_1, \dots, \xi_q],$$
$$P_F = P_\tau \cup P_\xi \subset R_F,$$

then

$$R_F/\mathrm{Id}(P_F) \simeq R_\tau[\xi_1, \dots, \xi_q]/\mathrm{Id}(P_F) \simeq$$
$$\simeq (R_\tau/\mathrm{Id}(P_\tau))[\xi_1, \dots, \xi_q]/\mathrm{Id}(P_\xi) \simeq$$
$$\simeq \mathbb{Z}A[\xi_1, \dots, \xi_q]/\mathrm{Id}(P_\xi).$$

So we define the embedding

$$\theta_\tau : F \to R_F/\mathrm{Id}(P_F),$$

that maps an element f of the defined above to

$$\theta_\tau(f) = \sum_{i=1}^{q} \xi_i \, \tau(\alpha_i) + \mathrm{Id}(P_\xi) =$$
$$= \sum_{i=1}^{q} \xi_i \, p(\tau(\alpha_i)) + \mathrm{Id}(P_F).$$

We define the size of f w.r.t. θ_τ as the sum of sizes of $\tau(\alpha_1), \dots, \tau(\alpha_q)$.

Arguments of Remark 3.1 apply to representation of f as well. In the same way, by $p(\theta_\tau(f)) \in R_F$ we denote the representative of the residue class $\theta_\tau(f)$.

4. Submodule computability

All modules under consideration will be right modules. Let R be a ring. If M is an R-module generated by $a_1, \dots, a_q$, then we write

$$M = \mathrm{mod}_R(a_1, \dots, a_q).$$

If F is a free R-module with basis $\xi_1, \dots, \xi_q$, then any $f \in F$ can be written uniquely in the form

$$f = \xi_1 r_1 + \dots + \xi_q r_q, (r_i \in R).$$

Let $\phi : F \to M$ be an R-module epimorphism define by $\phi(\xi_i) = a_i$, $i = 1, \dots, q$. If $K = \ker\phi$ is the submodule of F generated by the words

$$\{w_1(\xi_1, \dots, \xi_q), \dots, w_p(\xi_1, \dots, \xi_q)\},$$

where the $w_i(\xi_1, \dots, \xi_q)$ are given explicitly as words in $\xi_1, \dots, \xi_q$, then we write

$$M = \langle a_1, \dots, a_q \mid w_1(a_1, \dots, a_q), \dots, w_p(a_1, \dots, a_q)\rangle$$

for the corresponding presentation of M. If R is right Noetherian, then any finitely generated R-module M has a finite presentation where the number of relations is finite. By Hall's results [3] this is the case for $R = \mathbb{Z}G$ where G is a polycyclic-by-finite group, and, in particular, for $R = \mathbb{Z}A$ where A is a finitely generated abelian group.

If M is presented as above, then a word of M is an R-linear combination of the form $a_1 r_1 + \cdots + a_q r_q$, ($r_i \in R$). Membership in a submodule L of M is decidable if there is an algorithm which determines for any word w of M whether or not w belongs to L (i.e. represents an element of L).

If R is a right Noetherian ring, then any finitely generated R-module M is finitely presented and submodules of M are always finitely generated, hence finitely presented.

Definition 4.1 An R-module M over a right Noetherian ring R is called submodule computable if for any finite set $\{v_1, \dots, v_n\}$ of words of M there is

1. an algorithm to compute a finite presentation of the submodule L of M generated by $\{v_1, \dots, v_n\}$ on the given generators.
2. an algorithm to decide membership in L.

Definition 4.2 A right Noetherian ring R is called submodule computable if finitely presented R-modules M are submodule computable uniformly in the presentation for M.

One of the principal results of [4] is the following theorem.

Theorem 4.3 ([4], Theorem 2.12) Integral group ring of a polycyclic-by-finite group is submodule computable.

In particular, integral group ring of a finitely generated abelian group is submodule computable, so for any finitely generated metabelian group G its derived subgroup G' is submodule computable as a $\mathbb{Z}G_{ab}$-module.

In the rest of this section we provide a practical proof in terms of Groebner bases for Theorem 4.3 for the case of integral group rings of finitely generated abelian groups.

Let A be a finitely generated abelian group, M be a finitely presented $\mathbb{Z}A$-module given by its presentation, and F be a free $\mathbb{Z}A$-module on $\xi_1, \dots, \xi_q$, so $M \simeq \frac{F}{K}$ where K is the submodule of F generated by $w_1(\xi_1, \dots, \xi_q), \dots, w_p(\xi_1, \dots, \xi_q)$. Let $v_1(a_1, \dots, a_q), \dots, v_n(a_1, \dots, a_q) \in M$ and L is the $\mathbb{Z}A$-submodule of M generated by these words. Denote by N the full preimage of L under the natural homomorphism $F \to F/K$, clearly it is a submodule of F generated by the words

$$\{w_1(\xi_1, \dots, \xi_q), \dots, w_p(\xi_1, \dots, \xi_q), v_1(\xi_1, \dots, \xi_q), \dots, v_n(\xi_1, \dots, \xi_q)\},$$

and $L \simeq N/K$.

A word $w(a_1, \dots, a_q) \in M$ belongs to L iff $w(\xi_1, \dots, \xi_q)$ belongs to N. In particular, $w(a_1, \dots, a_q) = 0$ in M iff $w(\xi_1, \dots, \xi_q)$ belongs to the submodule K of F. So it is sufficient to decide membership for finitely generated submodules of free $\mathbb{Z}A$-modules.

Analogously, if N has a $\mathbb{Z}A$-module presentation

$$N = \langle w_1, \dots, w_p, v_1, \dots, v_n \mid z_1, \dots, z_t \rangle,$$

where z_i are words in the given generators, then

$$L \simeq \langle v_1, \dots, v_n \mid z_1', \dots, z_t' \rangle,$$

where z_i' is obtained from z_i by replacing w_j with 0. So it is sufficient to compute presentations of finitely generated submodules of free $\mathbb{Z}A$-modules.

Suppose that N is a submodule of F generated by $u_1, \dots, u_n$, where $u_i = \sum_{k=1}^{q} \xi_k \, \alpha_{ik}$, $\alpha_{ik} \in \mathbb{Z}A$, and $i = 1, \dots, n$. We map elements of F to $R_F/\mathrm{Id}(P_F)$ using θ_τ as defined in section 3.

Lemma 4.4 Let $w \in F$, then $w \in N$ iff $\theta_\tau(w)$ belongs to the ideal I of $R_F/\mathrm{Id}(P_F)$ generated by $\theta_\tau(u_1), \dots, \theta_\tau(u_n)$.

Corollary 4.5 Let $w \in F$, then $w \in N$ iff $p(\theta_\tau(w))$ belongs to the ideal J of R_F generated by $P_F \cup \{p(\theta_\tau(u_i)) \mid i = 1, \dots, n\}$.

These results reduce submodule membership problem for F to ideal membership problem for polynomial ring R_F over integers, which can be solved using Gröbner bases technics, see [1], [2].

Lemma 4.6 Submodule N of F and ideal I of $R_F/\mathrm{Id}(P_F)$ generated by $\theta_\tau(u_1), \dots, \theta_\tau(u_n)$ are isomorphic as $\mathbb{Z}A$-modules. Given a $\mathbb{Z}A$-module presentation of I, one can compute the corresponding $\mathbb{Z}A$-module presentation of N.

Corollary 4.7 Given an R_F-module presentation of the ideal J of R_F generated by $P_F \cup \{p(\theta_\tau(u_i)) \mid i = 1, \dots, n\}$, one can compute the corresponding $\mathbb{Z}A$-module presentation of I.

So computation of submodules' presentations in F reduces to computation of ideals' presentations in polynomial ring R_F over integers, which can be done by Corollary 2.2.

5. Algorithmic problems in metabelian groups

Denote by $\mathcal{A}^2$ the variety of all metabelian groups. It is known that finitely generated metabelian groups are finitely presented in $\mathcal{A}^2$, which means that any finitely generated metabelian group G has a presentation of the form

$$G = \langle x_1, x_2, \dots, x_n \mid r_1, \dots, r_p \rangle_{\mathcal{A}^2},$$

meaning that $G \simeq M_n/N$, where $M_n = F_n/F_n^{(2)}$ is the free metabelian group of rank n, F_n is the free group of rank n, and N is the normal closure of $r_1, \dots, r_p$ in M_n. The presentation above is called $\mathcal{A}^2$-presentation or metabelian presentation of G.

A metabelian group G is an extension of abelian normal subgroup G' by abelian group $G_{ab} = G/G'$. The group G_{ab} acts on G' by conjugation $b(aG') = b^a$, where $b \in G'$ and $a \in G_{ab}$. This action naturally extends to the action of the group ring $\mathbb{Z}G_{ab}$ on G':

$$b\left(\sum_{i=1}^{n} k_i a_i\right) = \prod_{i=1}^{n} (b^{a_i})^{k_i}.$$

Thus derived subgroup G' of a finitely generated metabelian group G is a module over the finitely generated commutative ring $\mathbb{Z}G_{ab}$.

For algorithmic problems, it is advantageous to work with special $\mathcal{A}^2$-presentations. For our convenience, we slightly alter the original definition from [5].

Definition 5.1 (Preferred presentation) By a preferred presentation of a finitely generated metabelian group G we mean a finite $\mathcal{A}^2$-presentation of the form

$$G = \langle x_1, x_2, \dots, x_n \mid R_1 \cup R_2 \rangle_{\mathcal{A}^2},$$

where:

1. R_1 is a finite set of words of the form

$$\prod_{\{(i,j) \mid 1 \le i < j \le n\}} [x_j, x_i]^{\alpha_{ij}},$$

where $\alpha_{ij} \in \mathbb{Z}G_{ab}$.

2. R_2 is a finite set of words r_i of the form

$$x_1^{m_{i1}} \cdot \ldots \cdot x_n^{m_{in}} w,$$

where $m_{ij} \in \mathbb{Z}$, w is a word of the form that elements of R_1 have, and the matrix $M = (m_{ij})$ is full rank.

So the words in R_2 determine a finite presentation of the group G_{ab}, while those in R_1, as we will show later, form a part of relations for a finite $\mathbb{Z}G_{ab}$-presentation of G' in the generators $[x_j, x_i] = x_j^{-1} x_i^{-1} x_j x_i$, $1 \le i < j \le n$.

Below we state Theorem 9.5.1 of [6] for our version of the definition of preferred presentation.

Theorem 5.2 There is an algorithm which, when given a finitely generated metabelian group G by its finite $\mathcal{A}^2$-presentation, finds a preferred $\mathcal{A}^2$-presentation of G.

Let G be a metabelian group generated by $x_1, \dots, x_n$. Its derived subgroup G' is a $\mathbb{Z}G_{ab}$-module generated by $[x_j, x_i]$. Since the ring $\mathbb{Z}G_{ab}$ is Noetherian, G' is finitely presented as a $\mathbb{Z}G_{ab}$-module. Thus a finite description of G' exists, even if it is not finitely generated as a group.

The module $M_n{}'$ of the free metabelian group M_n with basis $\{x_1, \dots, x_n\}$ for $n = 2$ is free over $\mathbb{Z}A^2$ (where A^2 is the free abelian group of rank 2) with generating element $[x_2, x_1]$. For $n \ge 3$ the module $M_n{}'$ is not free. All relations in the generators $[x_j, x_i]$, $1 \le i < j \le n$, follow from Jacobi relations

$$[x_i, x_j]^{x_k - 1} [x_j, x_k]^{x_i - 1} [x_k, x_i]^{x_j - 1} = 1,$$

for $i, j, k = 1, \dots, n$.

The following result is fundamental and admits an effective proof.

Theorem 5.3 ([5], Theorem 3.1) There is an algorithm which, when given a finitely generated metabelian group G by its finite $\mathcal{A}^2$-presentation, finds a finite $\mathbb{Z}G_{ab}$-presentation of G'.

In the rest of the section we review some classical algorithmic problems, namely, word, power, and conjugacy problems, that have been studied earlier in [5], [7], [8], [9]. We show that all these problems can be interpreted in a unified way in terms of Groebner bases. We note that conjugacy problem, in addition to Groebner bases, requires additional tool called Noskov's Lemma.

Word problem. Solvability of the word problem in finitely generated metabelian group G may be proved by observing that G is residually finite and finitely presented in the variety $\mathcal{A}^2$, so the standard procedure enumerating all finite quotients of G and consequences of defining relations in G solves the problem.

A simpler solution of the word problem was later provided by Timoshenko in [8].

Having all the machinery introduced above, it is now easy to reduce the word problem in a finitely generated metabelian group G to the ideal membership problem in a multivariate polynomial ring over integers.

Suppose that G is given by its metabelian presentation and $w \in G$. For any $g \in G$ we denote $\overline{g} = gG' \in G_{ab}$. To check whether or not $w = 1$ in G perform the following steps:

1. Compute a preferred presentation of G using Theorem 5.2.

2. Check if $\overline{w} = 1$ in G_{ab}. It is possible since relations from R_2 give us a presentation of G_{ab}. If $\overline{w} \ne 1$, then $w \ne 1$ in G, so further we assume $\overline{w} = 1$.

3. Rewrite w as an element of G', i.e. in the form $w = \prod [x_j, x_i]^{\alpha_{ij}}$, where $\alpha_{ij} \in \mathbb{Z}G_{ab}$.

4. Compute $\mathbb{Z}G_{ab}$-presentation of G' using Theorem 5.3

$$G' = \langle \{\xi_{ji} \mid 1 \le i < j \le n\} \mid w_1(\xi_{ji}), \dots, w_p(\xi_{ji}) \rangle.$$

5. Using Corollary 4.7, check if in the free $\mathbb{Z}G_{ab}$-module F generated by ξ_{ji} the word $w(\xi_{ji})$ belongs to the submodule generated by $w_1(\xi_{ji}), \dots, w_p(\xi_{ji})$.

Power problem. By the *power problem* in a group G we mean the problem of deciding for given $u, v \in G$ whether or not $v = u^k$ for some $k \in \mathbb{Z}$.

For a finitely generated metabelian group G, we first consider this problem for elements of G'.

Using the fact that we can get normal forms modulo an ideal in a polynomial ring over integers, one proves the following

Lemma 5.4 There is an algorithm which, when given a finitely generated abelian group Q, a finitely generated $\mathbb{Z}Q$-module M, and elements $a, b \in M$, decides if there exists $k \in \mathbb{Z}$ such that $b = ak$.

Then the general case can be reduced to Lemma 5.4.

Theorem 5.5 There is an algorithm which, when given a finitely generated metabelian group G by its finite $\mathcal{A}^2$-presentation and elements $u, v \in G$, decides if there exists $k \in \mathbb{Z}$ such that $v = u^k$.

Conjugacy problem. The conjugacy problem in finitely generated metabelian groups was solved by Noskov [9]. The proof utilizes the following algorithm for rings.

Lemma 5.6 (Noskov's Lemma) There is an algorithms which, when given a finitely generated commutative ring R and a finite subset X of the group of units $U(R)$, finds a finite presentation of the subgroup $\langle X \rangle$.

As with power problem, the proof consists of two steps, where the first one requires Noskov's lemma.

Lemma 5.7 ([5], Lemma 3.7) There is an algorithm which, when given a finitely generated abelian group Q, a finitely generated $\mathbb{Z}Q$-module M, and elements $a, b \in M$, decides if a and b are Q-conjugate, i.e. if there exists $q \in Q$ such that $b = aq$.

From the lemma above, the general case follows:

Theorem 5.8 ([5], Theorem 2.3) There is an algorithms which, when given a finitely generated metabelian group G and elements $x, y \in G$, decides if x and y are conjugate in G.

REFERENCES (СПИСОК ЛИТЕРАТУРЫ)

1. *Becker T., Weispfenning V.* Groebner bases: a computational approach to commutative algebra. In cooperation with Heinz Kredel. N. Y. : Springer, 1993.

2. *Adams W. W., Loustaunau P.* An Introduction to Groebner Bases. Providence, Rhode Island : American Mathematical Society, 1994.

3. *Hall P.* Finiteness conditions for solvable groups // Proc. London Math. Soc. 1954. Vol. 4. P. 419–436.

4. *Baumslag G., Cannonito F. B., Miller III C. F.* Computable algebra and group embeddings // J. Algebra. 1981. Vol. 69. P. 186–212.

5. *Baumslag G., Cannonito F. B., Robinson D. J. S.* The algorithmic theory of finitely generated metabelian groups // Transactions of Amer. Math Soc. 1994. Vol. 344. P. 629–648.

6. *Lennox J. C., Robinson D. J. S.* The Theory of Infinite Soluble Groups. Oxford : Oxford University Press, 2004.

7. *Romanovskii N. S.* Some algorithmic problems for solvable groups // Algebra and Logic. 1974. Vol. 13. P. 13–16.

8. *Timoshenko E. I.* Algorithmic problems for metabelian groups // Algebra and Logic. 1973. Vol. 12. P. 132–137.

9. *Noskov G. A.* On conjugacy in metabelian groups // Math. Notes. 1982. Vol. 31. P. 495–507.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Меньшов Антон Владимирович – кандидат физико-математических наук, сотрудник докторантуры отделения математических наук, *Институт технологий Стивенса,* Хобокен, Нью-Джерси, США; *ИМИТ (Институт математики и информационных технологий), Омский государственный университет им. Ф.М. Достоевского,* 644077, Россия, г. Омск, пр. Мира, 55а; e-mail: manton@stevens.edu, menshov.a.v@gmail.com.

Мясников Алексей Георгиевич – доктор физико-математических наук, профессор, руководитель отделения математических наук, *Институт технологий Стивенса,* Хобокен, Нью-Джерси, США; e-mail: amiasnik@stevens.edu.

INFORMATION ABOUT THE AUTHORS

Menshov Anton Vladimirovich – Candidate of Physical and Mathematical Sciences, Postdoctoral Fellow, the Department of Mathematical Sciences, *Stevens Institute of Technology*, 1, Castle Point Terrace, Hoboken, NJ, 07030, USA; *IMIT (the Institute of Mathematics and Information Technologies), Dostoevsky Omsk State University,* 55a, pr. Mira, Omsk, 644077, Russia; e-mail: manton@stevens.edu, menshov.a.v@gmail.com.

Myasnikov Alexei Georgievich – Doctor of Physical and Mathematical Sciences, Professor, Department Chair, the Department of Mathematical Sciences, *Stevens Institute of Technology,* 1, Castle Point Terrace, Hoboken, NJ, 07030, USA; e-mail: amiasnik@stevens.edu.

ISSN 1812-3996

Ушаков Александр Владимирович – доктор философии, профессор отделения математических наук *Институт технологий Стивенса,* Хобокен, Нью-Джерси, США; e-mail: aushakov@stevens.edu.

Ushakov Alexander Vladimirovich – Doctor of Philosophy, Associate Professor, the Department of Mathematical Sciences, *Stevens Institute of Technology,* 1, Castle Point Terrace, Hoboken, NJ, 07030, USA; e-mail: aushakov@stevens.edu.

ДЛЯ ЦИТИРОВАНИЯ

Меньшов А. В., Мясников А. Г., Ушаков А. В. Алгоритмы для метабелевых групп // Вестн. Ом. ун-та. 2018. Т. 23, № 2. С. 27–34. DOI: 10.25513/1812-3996.2018.23(2).27-34. (На англ. яз.).

FOR CITATIONS

Menshov A.V., Myasnikov A.G., Ushakov A.V. Algorithms for metabelian groups. *Vestnik Omskogo universiteta = Herald of Omsk University*, 2018, vol. 23, no. 2, pp. 27–34. DOI: 10.25513/1812-3996.2018.23(2).27-34.