S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 13, стр. 716–725 (2016) УДК 512.5
DOI 10.17377/semi.2016.13.056 MSC 20F10

О РАЗРЕШИМОСТИ УРАВНЕНИЙ С ЭНДОМОРФИЗМАМИ В НИЛЬПОТЕНТНЫХ ГРУППАХ

В.А. РОМАНЬКОВ

Abstract. We prove that the conjugacy, twisted conjugacy and bi-twisted conjugacy problems, and the corresponding search problems, are decidable for the class $\mathbf{N}_{fg}$ of all finitely generated nilpotent groups. Also we give a finite description of the equalizer of any pair of endomorphisms of arbitrary group in the class $\mathbf{N}_{fg}$.

Keywords: finitely generated group, (twisted, bi-twisted) conjugacy problem, search problems, fix-point and equalizer problems, algorithm, complexity

1. Введение

Группа G называется *нильпотентной*, если в ней существует конечный *центральный* ряд, т. е. ряд нормальных подгрупп

$$G = G_k > ... > G_1 > G_0 = \{1\}, \tag{1}$$

для которого любой фактор G_{i+1}/G_i принадлежит центру $C(G/G_i)$ фактор группы $G/G_i, i = 0, ..., k-1$. Наименьшая *длина* k такого ряда называется *ступенью нильпотентности* группы G.

Через $\mathbf{N}$ обозначается класс всех нильпотентных групп, а через $\mathbf{N}_{fg}$ – его подкласс, состоящий из всех конечно порожденных нильпотентных групп. Класс $\mathbf{N}$ является одним из наиболее изучаемых в теории групп. Значительное место в этом изучении отводится подклассу $\mathbf{N}_{fg}$. В целом класс $\mathbf{N}$ не является многообразием. Классическими нильпотентными многообразиями служат классы

Roman'kov, V.A., On solvability of equations with endomorphisms in nilpotent groups.

Работа поддержана РНФ (грант 16-11-10002).

Поступила 23 июля 2016 г., опубликована 15 сентября 2016 г.

$\mathbf{N}_k$ всех нильпотентных групп ступени нильпотентности не больше, чем заданное натуральное число k.

Основы теории нильпотентных групп изложены в лекциях Ф. Холла [1] и Г. Баумслага [2]. Многообразиям нильпотентных групп посвящена значительная часть монографии Х. Нейман [3]. См. также монографии М.И. Каргаполова и Ю.И. Мерзлякова [4], Д. Леннокса и Д. Робинсона [5].

Настоящая работа посвящена исследованию разрешимости уравнений с эндоморфизмами в классе $\mathbf{N}_{fg}$. На языке уравнений такого вида записывается целый ряд алгоритмических проблем. В работе доказана алгоритмическая разрешимость некоторых из них, а именно: сопряженности, скрученной сопряженности и бинарно скрученной сопряженности. Также показана разрешимость соответствующих им проблем поиска сопрягающего элемента. Представлены алгоритмы, вычисляющие в классе $\mathbf{N}_{fg}$ подгруппы фиксированных точек эндоморфизмов и эквализаторы пар эндоморфизмов.

Через $\mathbb{N}, \mathbb{Z}$ и $\mathbb{Q}$ обозначаются соответственно множество натуральных чисел, кольцо целых чисел и поле рациональных чисел. Если G – группа, то для ее элементов g, f выражение $g^f = fgf^{-1}$ означает сопряжение, а $[g, f] = gfg^{-1}f^{-1}$ – коммутатор. Через $M_{m\times n}(K)$ обозначается кольцо матриц размера $m \times n$, а через $SL_n(K)$ – группа специальных матриц размера $n\times n$ над кольцом (полем) K.

2. Алгоритические проблемы

Пусть G – конечно порожденная группа, $X = \{x_1, ..., x_n\}$ – множество порождающих G элементов. Предполагается, что группа G задана эффективным образом. В основном мы имеем в виду, что G задана либо конечным, либо рекурсивным представлением через порождающие элементы из X и определяющие соотношения.

В данной работе представляемые ниже алгоритмические проблемы рассматриваются для класса $\mathbf{N}_{fg}$ конечно порожденных нильпотентных групп. Группы из $\mathbf{N}_{fg}$ допускают конечные представления. Это позволяет рассматривать для $\mathbf{N}_{fg}$ следующие алгоритмические проблемы.

1. **Проблема сопряженности (ПС)**: *Для произвольной пары элементов $g, f \in G$ определить, существует ли элемент $x \in G$ такой, что*

$$g^x = f. \tag{2}$$

2. **Проблема скрученной сопряженности (ПСС)**: *Относительно произвольного фиксированного эндоморфизма $\varphi \in End(G)$ для произвольной пары элементов $g, f \in G$ определить, существует ли элемент $x \in G$ такой, что*

$$\varphi(x)g = fx. \tag{3}$$

3. **Проблема бинарно скрученной сопряженности (ПБСС)**: *Относительно произвольной фиксированной пары эндоморфизмов $\varphi, \psi \in End(G)$ для произвольной пары элементов $g, f \in G$ определить, существует ли элемент $x \in G$ такой, что*

$$\varphi(x)g = f\psi(x). \tag{4}$$

Каждое из рассматриваемых отношений, а именно: *сопряженность* $g \sim f$, *скрученная сопряженность* $g \sim_\varphi f$ и *бинарно скрученная сопряженность* $g \sim_{\varphi,\psi} f$, является отношением эквивалентности на G.

Заметим, что ПС является частным случаем ПСС, соответствующим выбору в качестве φ тождественного эндоморфизма id. В свою очередь ПСС – частный случай ПБСС при выборе в качестве ψ тождественного эндоморфизма id.

Приведенным выше алгоритмическим проблемам соответствуют алгоритмические проблемы поиска, имеющие значение в приложениях, в частности, в алгебраической криптографии (см., например, [6] – [8]).

$1'$. **Проблема поиска сопрягающего элемента относительно ПС**: *Для произвольной пары сопряженных элементов $g, f \in G$ определить сопрягающий элемент $x \in G$, для которого выполнено (2).*

$2'$. **Проблема поиска сопрягающего элемента относительно ПСС**: *Для произвольной пары скрученно сопряженных относительно эндоморфизма $\varphi \in End(G)$ элементов $g, f \in G$ определить сопрягающий элемент $x \in G$, для которого выполнено (3).*

$3'$. **Проблема поиска сопрягающего элемента относительно ПБСС**: *Для произвольной пары бинарно скрученно сопряженных относительно эндоморфизмов $\varphi, \psi \in End(G)$ элементов $g, f \in G$ определить сопрягающий элемент $x \in G$, для которого выполнено (4).*

Разрешимость рассматриваемых проблем связана с разрешимостью следующих сопутствующих алгоритмических проблем, представляющих самостоятельный интерес.

4. **Проблема нахождения подгруппы инвариантов (фиксированных точек) (ПИ)**: Для произвольного $\varphi \in End(G)$ дать конструктивное описание подгруппы

$$Fix_{\varphi}(G) = \{g \in G : \varphi(g) = g\}. \tag{5}$$

5. **Проблема нахождения подгруппы би-инвариантов (эквализатора) (ПБИ)**: Для произвольных $\varphi, \psi \in End(G)$ дать конструктивное описание подгруппы

$$Eq_{\varphi,\psi}(G) = \{g \in G : \varphi(g) = \psi(g)\}. \tag{6}$$

В данной работе даются решения проблем $1 - 5$ и проблем $1' - 3'$ для класса $\mathbf{N}_{fg}$. При этом решения получаются без каких-либо ограничений на эндоморфизмы.

Алгоритмическая разрешимость ПСС для произвольного эндоморфизма полициклической группы G установлена автором в [9]. Так как любая конечно порожденная нильпотентная группа является полициклической, то есть обладает конечным субнормальным (в данном случае и нормальным) рядом с циклическими факторами, это показывает разрешимость ПСС для класса $\mathbf{N}_{fg}$. В данной работе мы приводим алгоритм решения более общей ПБСС для $\mathbf{N}_{fg}$. Из него следует более простой алгоритм решения ПСС для $\mathbf{N}_{fg}$, чем соответствующий алгоритм непосредственно извлекаемый из [9]. Также получается достаточно простой алгоритм решения ПС, при котором переход в более широкую эквивалентность скрученной сопряженности позволяет использовать несложные индукционные соображения.

Итак, отмеченные выше алгоритмические проблемы сводятся к исследованию разрешимости в группе G уравнений с эндоморфизмами, общая форма для которых выглядит, как

$$w(\phi_1(x), ..., \phi_n(x)) = v(\phi_1(x), ..., \phi_n(x)), \phi_i \in End(G)\ (i = 1, ..., n), \tag{7}$$

где w и v – полугрупповые слова с коэффициентами из G. Таким образом уравнение (7) имеет вид

$$g_1\phi_{i_1}(x)g_2...\phi_{i_k}(x)g_{k+1} = f_1\phi_{j_1}(x)f_2...\phi_{j_l}(x)f_{l+1}, \tag{8}$$

где $i_1, ..., i_k, j_1, ..., j_l \in \{1, ..., n\}$, $g_1, ..., g_{k+1}, f_1, ..., f_{l+1} \in G$.

Применим к записи (8) эффективный переписывающий процесс переноса коэффициентов $g_1, ..., g_k$ направо и $f_2, ..., f_{l+1}$ – налево. При этом изменяется набор участвующих в записи уравнения эндоморфизмов. Для этого определим внутренние автоморфизмы $\sigma_g(x) = gxg^{-1} = x^g, g \in G$. Нужные для переписки уравнения формулы имеют вид $g\phi(x) = \phi'(x)g, \phi' = \phi\circ\sigma_g$ и $\phi(x)f = f\phi'(x), \phi' = \phi \circ \sigma_{g^{-1}}$. После переписки получаем уравнение вида

$$\varphi_1(x)...\varphi_k(x)g = f\psi_1(x)...\psi_l(x), \tag{9}$$

где $g = g_1...g_{k+1}$ и $f = f_1...f_{l+1}$.

Если G – абелева группа, то уравнение (9) очевидно равносильно уравнению вида (4) для эндоморфизмов φ и ψ, определенных, как $\varphi(x) = \prod_{i=1}^{k}\varphi_i(x), \psi(x) = \prod_{j=1}^{l}\psi_j(x)$.

3. Основные результаты

Пусть G – произвольная (неединичная) конечно порожденная нильпотентная группа ступени нильпотентности k, $X = \{x_1, ..., x_n\}$ – множество порождающих элементов группы G. Пусть

$$G = C_k > C_{k-1} > ... > C_1 > C_0 = \{1\} \tag{10}$$

– *верхний центральный ряд* группы G. Здесь C_1 – центр группы G и C_{i+1} определяется для любого $i = 1, ..., k-1$, как полный прообраз центра $C(G/C_i)$ фактор группы G/C_i в группе G. Известно (см., например, [1] или [4]), что длина k ряда (10) равна ступени нильпотентности группы G.

Хорошо известно (см., например, [10]–[13]), что большинство классических алгоритмических проблем для конечно порожденных нильпотентных групп разрешимы. В частности, разрешима ПС [13]. В то же время существуют неразрешимые алгоритмические проблемы. Среди них числятся проблемы существования решений уравнений и эндоморфной сводимости [14]. Недавно показано [15], что существует конечно порожденная нильпотентная группа G ступени два, в которой алгоритмически неразрешима коммутаторная проблема, т. е. вопрос о разрешимости уравнения вида $[x_1, x_2] = g, g \in G$. Также в [15] построен пример нильпотентной группы G ступени два, для которой неразрешима *проблема ретракта*: будет ли подгруппа H группы G ретрактом, т. е. существует ли эндоморфизм группы G на H, ограничение которого на H является тождественным отображением. Тем самым даны ответы на вопросы А. Мясникова N8a и N9a из [16].

Перейдем к формулировкам результатов и их доказательствам. Случаи абелевых групп и нильпотентных групп ступени нильпотентности не меньше, чем два, рассматриваются раздельно. Результаты, полученные для абелевых групп составляют базу индукции для второго из рассматриваемых случаев.

Абелев случай.

Прежде всего мы рассматриваем случай конечно порожденных абелевых групп. Предлагаемые алгоритмы нельзя рассматривать как абсолютно новые.

Так или иначе они содержатся в разных работах, связанных со скрученной сопряженностью. Нашей задачей было собрать их воедино и представить единообразным образом.

Доказательство следующей леммы можно найти в [17] (элементарное изложение и примеры можно найти в [18]).

Лемма 1. *Пусть $A \in M_{m\times n}(\mathbb{Z})$. Тогда найдутся матрицы $L \in SL_m(\mathbb{Z})$ и $R \in SL_n(\mathbb{Z})$ такие, что*

$$LAR = D = diag(d_1, ..., d_s, 0, ..., 0), \tag{11}$$

где d_i – положительные целые числа, и $d_i|d_{i+1}$ для $i = 1, ..., s-1$.

Матрица D, в которой вхождение d_{ii} равно d_i для $i = 1, ..., s$, а остальные вхождения нулевые, определяется однозначно, в то время, как матрицы L и R, соответствующие элементарным преобразованиям строк и столбцов матрицы A, соответственно, могут варьироваться. Матрица D называется *формой Смита* для A. Заметим, что построение полиномиального алгоритма для нахождения формы Смита данной матрицы не является тривиальной задачей. Прямое применение элементарных преобразований к строкам и столбцам не дает полиномиального алгоритма. Однако, полиномиальный алгоритм приведения матрицы к форме Смита существует. См. его описание в [19] и [20].

Пусть $A_n = \mathbb{Z}_+^n$ обозначает свободную абелеву группу ранга n относительно операции сложения. Элементы группы A_n – целочисленные векторы длины n. Для произвольных целых положительных чисел m и n рассмотрим гомоморфизм $\lambda : A_m \to A_n$. При фиксированных базисах этих групп гомоморфизм λ задается целочисленной матрицей $A \in M_{m\times n}(\mathbb{Z})$.

Предложение 1. *Пусть m и n – произвольные положительные целые числа. Существует алгоритм, который для любого гомоморфизма $\lambda : A_m \to A_n$ и любого элемента $b \in A_n$ определяет разрешимость относительно неизвестного $x \in A_m$ следующего уравнения:*

$$\lambda(x) = b. \tag{12}$$

В случае разрешимости данного уравнения алгоритм дает эффективное описание всех его решений. В частности, при $b = 0$ алгоритм выписывает порождающие элементы подгруппы $ker(\lambda)$.

Доказательство. При фиксированных базисах групп A_m и A_n уравнение (12) записывается в виде

$$x \cdot A = b, A \in M_{m\times n}(\mathbb{Z}). \tag{13}$$

По лемме 1 найдем матрицы $L \in SL_m(\mathbb{Z})$ и $R \in SL_n(\mathbb{Z})$ такие, что $LAR = D = diag(d_1, ..., d_s, 0, ..., 0)$, где D – форма Смита матрицы A. Уравнение (13) переписывается как диагональная система $y \cdot D = c$, $y = xL^{-1}, c = b \cdot R$. Определить, существует ли решение диагональной системы, и в случае существования выписать общее решение, является легким упражнением. При $b = 0$ решения системы образуют подгруппу группы A_m, а именно: $\ker(\lambda)$. □

Следствие 1. *Существуют полиномиальные алгоритмы, решающие для произвольной свободной абелевой группы следующие алгоритмические проблемы: ПСС, ПБСС, ПИ и ПБИ.*

Доказательство. Для решения ПБПИ относительно эндоморфизмов φ и ψ группы A_m определим эндоморфизм $\lambda = \varphi - \psi$. Тогда $\mathrm{Eq}_{\varphi,\psi}(A_m) = \ker(\lambda)$. Описание $\ker(\lambda)$ дается предложением 1. Решение ПИ определяется и строится как частный случай решения ПБИ, когда $\lambda = \varphi - id$.

Основное уравнение (4) в аддитивной форме $\varphi(x) + g = f + \psi(x)$ для ПБСС относительно эндоморфизмов φ и ψ группы A_m переписывается в эквивалентной форме $\lambda(x) = h$, где $\lambda = \phi - \psi, h = f - g$. Существование решений и их описание в случае разрешимости устанавливается предложением 1. ПСС решается как частный случай ПБСС. □

Пусть A – конечно порожденная абелева группа с операцией сложения. Считаем, что A представлена в виде $B \oplus A_m$, где B – конечная абелева группа (конечная часть $T(A)$ группы A). Известно (см., например, [17], [21]), что указанное представление эффективно строится исходя из конечного представления группы A через порождающие элементы и определяющие соотношения.

Выше рассмотрены гомоморфизмы между свободными абелевыми группами. Для перехода к общему случаю гомоморфизмов между произвольными конечно порожденными группами выделим следующую простую подготовительную лемму.

Лемма 2. *Пусть A – произвольная конечно порожденная абелева группа, C – конечная абелева группа. Существует алгоритм, который для любого гомоморфизма $\mu : A \to C$ определяет разрешимость относительно неизвестного $x \in A$ следующего уравнения:*

$$\mu(x) = c. \tag{14}$$

В случае разрешимости данного уравнения алгоритм дает эффективное описание всех его решений. В частности, при $c = 0$ алгоритм выписывает порождающие элементы подгруппы $ker(\mu)$.

Доказательство. Пусть t – период группы B. Тогда подгруппа $tA \leq A$ принадлежит $\ker(\mu)$. Нахождение решения (14) сводится к нахождению решения в конечной группе A/tA уравнения $\bar{\mu}(\bar{x}) = c$, где $\bar{\mu} : A/tA \to C$ – индуцированный гомоморфизм. Пусть $\bar{x}_i, i = 1, ..., s$ – все решения этого уравнения. Общее решение уравнения (14) получается как $\cup_{i=1}^{s}(x_i + tA)$, где элементы x_i – фиксированные прообразы для $\bar{x}_i, i = 1, ..., s$. Очевидно, что построенный алгоритм полиномиален. □

Перейдем к рассмотрению общего случая гомоморфизмов между конечно порожденными абелевыми группами.

Предложение 2. *Пусть $G_1 = B_1 \oplus A_m, G_2 = B_2 \oplus A_n$ – произвольные конечно порожденные абелевы группы, где $B_i, i = 1, 2$ – их конечные части. Существует полиномиальный алгоритм, который для любого гомоморфизма $\nu : G_1 \to G_2$ и любого элемента $g \in G_2$ определяет разрешимость относительно неизвестного $x \in A$ следующего уравнения:*

$$\nu(x) = g. \tag{15}$$

В случае разрешимости алгоритм дает общее решение.

Доказательство. Определим индуцированные гомоморфизмы $\nu_1 : G_1 \to B_2, \nu_2 : G_1 \to A_n, \nu_3 : A_m \to A_n$. Если $g \in B_2$, то уравнение (15) равносильно уравнению $\nu_1(x) = g$, поэтому работает алгоритм, описанный в лемме 2. Пусть $g = b + d, b \in B_2, d \in A_n$, причем $d \neq 0$. По предложению 1 находим $x_1 \in A_m$, для которого $\nu_3(x) = d$. Так как $B_1 \leq \ker(\nu_2)$, если x_1 не существует, то уравнение (15) не имеет решения. В противном случае общее решение уравнения имеет вид

$$x = x_1 + ker(\nu_1) + ker(\nu_3). \tag{16}$$

Составляющие $\ker(\nu_1)$ и $\ker(\nu_3)$ общего решения находятся по лемме 2 и предложению 1, соответственно. Полиномиальность алгоритма вытекает из полиномиальности алгоритмов леммы 2 и предложения 1. □

Следствие 2. *Пусть G – произвольная конечно порожденная абелева группа. Существуют полиномиальные алгоритмы, решающие для G следующие алгоритмические проблемы: ПСС, ПБСС, ПИ и ПБИ и проблемы поиска $2' - 3'$.*

Доказательство. Для решения ПБИ относительно эндоморфизмов φ и ψ группы G определим эндоморфизм $\lambda = \varphi - \psi$. Тогда $\mathrm{Eq}_{\varphi,\psi}(G) = \ker(\lambda)$. Описание $\ker(\lambda)$ дается предложением 2. Решение ПИ определяется и строится как частный случай решения ПБИ, когда $\lambda = \varphi - id$.

Основное уравнение (4) в аддитивной форме $\varphi(x) + g = f + \psi(x)$ для ПБСС относительно эндоморфизмов φ и ψ группы G переписывается в эквивалентной форме $\lambda(x) = h$, где $\lambda = \phi - \psi, h = f - g$. Существование решений и их описание в случае разрешимости устанавливается предложением 2. ПСС решается как частный случай ПБСС.

Полиномиальность алгоритмов вытекает из полиномиальности алгоритма предложения 2. □

Теорема 1. *Пусть G – конечно порожденная абелева группа. Существует полиномиальный алгоритм, определяющий для G разрешимость произвольной конечной системы уравнений с эндоморфизмами, и в случае разрешимости этой системы выписывающий ее общее решение.*

Доказательство. Любое уравнение вида (9), значит и (8), в абелевом случае по очевидным соображениям равносильно расщепимому уравнению вида $\varphi(x) = g, g \in G$. Произвольная конечная система с эндоморфизмами над G эквивалентна системе вида

$$\varphi_p(x) = h_p, \varphi_p \in End(G), h_p \in G, p = 1, ..., n. \tag{17}$$

По предложению 2 определяем разрешимость каждого из уравнений системы (17). Считаем, что все они разрешимы, иначе данная система не имеет решения. Запишем общее решение p-го уравнения системы в виде $x = x_p + H_p$, где x_p – частное решение p-го уравнения, $H_p = \ker(\varphi_p)$, $p = 1, ..., n$.

Общее решение системы (17) записывается как пересечение $\cap_{p=1}^{n}(x_p + H_p)$. Система разрешима, если это пересечение непусто. Пусть $\tilde{x}$ – частное решение системы. Оно находится полиномиальным алгоритмом. Для любого другого решения x разность $x - \tilde{x}$ принадлежит пересечению $H_{\bar{n}} = \cap_{i=1}^{n} H_i$. Легко видеть, что общее решение системы имеет вид $x = \tilde{x} + H_{\bar{n}}$. Порождающие элементы пересечения подгрупп конечно порожденной абелевой группы вычисляются

известным полиномиальным алгоритмом, что завершает доказательство теоремы. □

Неабелев случай.

Перейдем к рассмотрению неабелевых конечно порожденных нильпотентных групп.

Теорема 2. *Пусть G – конечно порожденная нильпотентная группа. Существует алгоритм, который по любой паре эндоморфизмов φ и ψ группы G находит конечное множество порождающих элементов эквализатора $Eq_{\varphi,\psi}(G)$.*

Доказательство. Если группа абелева, то заявленный в теореме алгоритм существует по следствию 2.

Пусть ступень нильпотентности группы G равна $k \geq 2$. Также предположим, что утверждение теоремы верно для любой конечно порожденной нильпотентной группы ступени нильпотентности не больше, чем $k-1$. Рассмотрим нижний центральный ряд

$$G = \gamma_1 G > \gamma_2 G > ... > \gamma_k G > \gamma_{k+1} G = \{1\} \tag{18}$$

группы G, где по определению $\gamma_{i+1}G = [\gamma_i G, G] = \mathrm{gp}([u, f] : u \in \gamma_i G, f \in G)$, $i = 1, ..., k$. Ступень нильпотентности группы G совпадает с длиной k ряда (18), что объясняет корректность обозначений. Подгруппа $D = \gamma_k G$ принадлежит центру C группы G. Она инвариантна относительно всех эндоморфизмов группы G, значит, можно говорить об индуцируемых эндоморфизмах группы $\bar{G} = G/D$. Относительно деталей приведенных фактов см., например, [1], [2] или [4].

Группа $\bar{G}$ имеет ступень нильпотентности $k-1$. Пусть $\bar{\varphi}$ и $\bar{\psi}$ – эндоморфизмы группы $\bar{G}$, индуцированные φ и ψ, соответственно. Согласно индукционному предположению существует алгоритм, выписывающий множество порождающих элементов эквализатора $\mathrm{Eq}_{\bar{\varphi},\bar{\psi}}(\bar{G})$. Пусть G_1 – полный прообраз $\mathrm{Eq}_{\bar{\varphi},\bar{\psi}}(\bar{G})$ в группе G. Обозначим его $\mathrm{Eq}_{D,\varphi,\psi}(G)$ и назовем *D-эквализатором* группы G. По определению

$$Eq_{D,\varphi,\psi}(G) = \{g \in G : \varphi(g) = d_g \psi(g), \text{ где } d_g \in D\}. \tag{19}$$

Определим гомоморфизм $\beta : Eq_{D,\varphi,\psi}(G) \to D$, полагая $\beta(g) = d_g$. Так как группа D абелева, коммутант $Eq_{D,\varphi,\psi}(G)'$ принадлежит $\ker(\beta)$. Ясно, что $\mathrm{Eq}_{\varphi,\psi}(G) = \ker(\beta)$. Описание $\mathrm{Eq}_{\varphi,\psi}(G)$ сводится таким образом к описанию ядра индуцированного гомоморфизма $\bar{\beta} : Eq_{D,\varphi,\psi}(G)_{ab} \to D$ конечно порожденных абелевых групп. Такое описание дается предложением 2. Заметим, что для этого необходимо знать структуру этих абелевых групп. Соответствующие алгоритмы приведены в [17]. □

Следствие 3. *Существуют алгоритмы, решающие для произвольной конечно порожденной нильпотентной группы алгоритмические проблемы ПБИ и ПИ.*

Переходим к рассмотрению алгоритмических проблем ПС, ПСС и ПБСС и соответствующих проблем поиска $1' - 3'$ для конечно порожденных нильпотентных групп.

Теорема 3. *Пусть G – конечно порожденная нильпотентная группа. Существует алгоритм, который решает ПБСС и соответствующую ей проблему поиска $3'$ относительно G.*

Доказательство. Используем индукцию по ступени нильпотентности k группы G. В абелевом случае заявленный алгоритм существует по следствию 1. Считаем, что $k \geq 2$. Предположим, что аналогичное утверждение верно для любой конечно порожденной нильпотентной группы ступени нильпотентности не больше, чем $k-1$.

Допустим, что ПБСС решается относительно пары эндоморфизмов $\varphi, \psi \in \mathrm{End}(G)$. Пусть g, f – пара элементов группы G, для которых выясняется их бинарно скрученная сопряженность, то есть определяется разрешимость уравнения (4). Пусть σ_g обозначает внутренний автоморфизм группы G, соответствующий сопряжению элементом g^{-1}. Полагаем $\phi = \varphi \circ \sigma_g$. Уравнение (4) равносильно уравнению

$$\phi(x) = h\psi(x), h = g^{-1}f. \tag{20}$$

Пусть $D = \gamma_k G$ – последний неединичный член нижнего центрального ряда (18) группы G. Подгруппа D инвариантна относительно любого эндоморфизма группы G. Обозначим $\bar{G} = G/D$. Рассмотрим эндоморфизмы $\bar{\phi}$ и $\bar{\psi}$ группы $\bar{G}$, индуцированные ϕ и ψ, соответственно. Пусть $\bar{u}$ – естественный образ произвольного элемента u в $\bar{G}$. По индукционному предположению существует алгоритм, определяющий разрешимость относительно неизвестной $\bar{x}$ в группе $\bar{G}$ уравнения

$$\bar{\phi}(\bar{x}) = \bar{h}\bar{\psi}(\bar{x}), \tag{21}$$

и в случае его разрешимости, представляющий общее решение этого уравнения.

Если уравнение (21) не имеет решения, то не имеет решения и уравнение (20), значит, $g \not\sim_{\varphi,\psi} f$ в уравнении (4). Предположим, что решение $\bar{x}$ уравнения (21) существует. Зафиксируем один из его прообразов x_1 в группе G. Тогда $\phi(x_1) = c_1 h\psi(x_1), c_1 \in D$. Если $\bar{x_2}$ – другое решение уравнения (21), x_2 – его прообраз в G, $\phi(x_2) = c_2 h\psi(x_1), c_2 \in D$, то выполнено равенство

$$\phi(x_2^{-1}x_1) = c\psi(x_2^{-1}x_1), c = c_2^{-1}c_1 \in D. \tag{22}$$

Решение $x = x_2$ уравнения (20) существует тогда и только тогда, когда в (22) $c = c_1$. По теореме 2 эффективно строится конечное множество порождающих элементов для $\mathrm{Eq}_{\bar{\phi},\bar{\psi}}(G)$. Взяв прообразы этих элементов в G и присоединив к ним порождающие элементы подгруппы D, получим конечное множество $\{g_1, ..., g_t\}$ порождающих элементов для $\mathrm{Eq}_{D,\phi,\psi}(G)$. Тогда

$$\phi(g_i) = d_i\psi(g_i), d_i \in D, i = 1, ..., t. \tag{23}$$

Определим гомоморфизм $\mu : \mathrm{Eq}_{D,\phi,\psi}(G) \to D$, полагая $\mu(g_i) = d_i, i = 1, ..., t$. Как уже замечено выше, уравнение (21) имеет решение тогда и только тогда, когда элемент c_1 принадлежит подгруппе $\mu(\mathrm{Eq}_{D,\phi,\psi}(G)) = \mathrm{gp}(d_1, ..., d_t)$. Проблема вхождения в классе конечно порожденных абелевых групп полиномиально разрешима, что заканчивает доказательство. □

References

[1] P. Hall, *Edmonton notes on nilpotent groups*, Queen Mary College Math. Notes. Math. Dept., Queen Mary College, London, 1969.

[2] G. Baumslag, *Lectures on nilpotent groups*, CBMS Regional Conference Ser. 2, Amer. Math. Soc., Providence R.I., 1969.

[3] H. Neumann, *Varieties of groups*, Springer, New York, 1967. Zbl 0251.20001

[4] M.I. Kargapolov, Yu.I. Merzlyakov, *Foundations of Group Theory*, Springer, New York, 1979. Zbl 0549.20001

[5] J.C. Lennox, D.J.S. Robinson, *The Theory of Infinite Soluble Groups*, Oxford math. monographs, Clarendon Press, Oxford, 2004. Zbl 1059.20001

[6] A. Myasnikov, V. Shpilrain, A. Ushakov, *Group-based Cryptography*, Advanced Courses in Math., CRM Barselona, Birkhauser, Basel, Boston, Berlin, 2008. Zbl 1248.94004

[7] A. Myasnikov, V. Shpilrain, A. Ushakov, *Non-commutative Cryptography and Complexity of Group Theoretic Problems*, Mathematical Surveys and Monographs, **177**, AMS, Providence, Rhode Island, 2011. Zbl 1248.94006

[8] V.A. Roman'kov, *Algebraic cryptography*, OmSU, Omsk, 2013.

[9] V. Roman'kov, *The twisted conjugacy problem for endomorphisms of polycyclic groups*, J. Group Theory, **13** (2010), 355–364. Zbl 1197.20027

[10] M.I. Kargapolov, V.N. Remeslennikov, N.S. Romanovskij, V.A. Roman'kov, V.A. Churkin, *Algorithmic problems for σ-power groups*, Algebra and Logic, **8** (1969), 364–373.

[11] V.N. Remeslennikov, V.A. Roman'kov, *Model-theoretic and algorithmic questions of group theory*, Journal of Soviet Math., **31** (1985), 2887–2939. Zbl 0573.20031

[12] V.A. Roman'kov, *Equations over groups*, Groups Complexity Cryptology, **4** (2012), 191–239. Zbl 1304.20058

[13] N. Blackburn, *Conjugacy in nilpotent groups*, Proc. Amer. Math. Soc., **16** (1965), 143–148. Zbl 0127.01302

[14] V.A. Roman'kov, *Unsolvability of the endomorphism reducibility problem in free nilpotent groups and in free rings*, Algebra and Logic, **16** (1977), 457–471. Zbl 0411.20021

[15] V.A. Roman'kov, *Diophantine questions in the class of finitely generated nilpotent groups*, J. Group Theory, **19** (2016), 497–514. Zbl 06582601

[16] G. Baumslag, A. Myasnikov, V. Shpilrain, *Open problems in combinatorial group theory*, Contemporary Math., **296** (2002), 1–38; extended version: http://grouptheory.info , Open Problems. Zbl 1065.20042

[17] B.L. van der Waerden, *Algebra I*, Springer, Berlin, 1966. Zbl 0137.25403

[18] F. Lazebnik, *On systems of linear Diophantine equations*, Math. Magazine, **69** (1996), 261–266. Zbl 1055.11507

[19] R. Kannan, A. Bachem, *Polynomial time algorithms to compute Hermite and Smith normal forms of an integer matrix*, SIAM J. Computing, **8** (1979), 499–507. Zbl 0446.65015

[20] T.-W.J. Chou, G.E. Collins, *Algorithms for the solution of systems of linear Diophantine equations*, SIAM J. Computing, **11** (1982), 687–708. Zbl 0498.65022

[21] C.C. Sims, *Computations with Finitely Presented Groups*, Encyclopedia of Mathematics and its Applications, Cambridge Univ. Press, Cambridge, 1994. Zbl 0828.20001

Vitalii Anatolievich Roman'kov
Dostoevsky Omsk State University,
pr. Mira, 55-A,
644077, Omsk, Russia
E-mail address: romankov48@mail.ru