S. I. Adian, On algorithmic problems in effectively complete classes of groups,
Dokl. Akad. Nauk SSSR, 1958, Volume 123, Number 1, 13–16

Доклады Академии наук СССР
1958. Том 123, № 1

МАТЕМАТИКА

С. И. АДЯН

ОБ АЛГОРИТМИЧЕСКИХ ПРОБЛЕМАХ В ЭФФЕКТИВНО-ПОЛНЫХ КЛАССАХ ГРУПП

(*Представлено академиком И. М. Виноградовым 16 V 1958*)

Целью настоящей заметки является дальнейшее обобщение теорем о неразрешимых алгоритмических проблемах теории групп ([1-3]) *. Мы здесь пользуемся обозначениями работ ([2]), ([3]). В первой части заметки мы приводим ряд замечаний о работе ([3]), позволяющих полностью восстановить доказательство основной леммы этой работы **. Из приводимых ниже замечаний следует доказательство несколько более сильного утверждения, из которого указанная лемма вытекает как следствие. Именно, в первой части будет доказана следующая лемма о группах F_{qA}.

Лемма Б. *Пусть слово A группы F не содержит букв p^σ. Если $A = 1$ в группе F, то F_{qA} является единичной группой. Если $A \neq 1$ в F, то группа F является подгруппой группы F_{qA}.*

Во второй части, используя лемму Б, мы докажем некоторые теоремы о неразрешимых алгоритмических проблемах для эффективно-полных классов конечно-определенных групп (кратко: к.-о. групп).

I. Некоторые замечания о работе ([3]). Аналогия между определяющими соотношениями групп $\mathfrak{A}_{q,A,B}$, построенных в ([2]), и определяющими соотношениями групп F_{qA}, построенных в ([3]), очевидна. В определяющих соотношениях групп F_{qA} роль слов $AB^{-1} \equiv pXpX^+Y^{+^{-1}}p^{-1}Y^{-1}p^{-1}$ играют слова $E \equiv p^2Ap^{-1}Ap^{-1}$. Эта аналогия является глубокой.

Первые два параграфа гл. II работы ([2]) посвящены доказательству леммы 4, § 2, гл. II. При этом используется ряд вспомогательных утверждений, которые содержатся в гл. I. Утверждения, содержащиеся в § 1, гл. I, имеют общий характер и могут быть применены к любой группе. Что же касается утверждений, содержащихся в § 2, гл. I работы ([2]), то они относятся к конкретной группе $\mathfrak{A}_p$ и связаны с особенностями конструкции этой группы. Тем не менее аналогичные утверждения верны для построенной в ([3]) группы $F = F_0 * F_2' * F_3$.

Для каждого из утверждений § 2, гл. I работы ([2]), использованного в первых двух параграфах гл. II, укажем соответствующее утверждение о группе F, которое будет использовано при доказательстве леммы Б.

1) Лемма 1, § 2, гл. I (стр. 242). Этой лемме соответствует следующее очевидное утверждение.

Лемма 1*. *Пусть D есть слово группы F, не содержащее букв p^σ. Если $D = 1$ в F, то в группе F равны* 1 *также проекции слова D на алфавиты групп F_0 и F_2'.*

2) Лемма 3, § 2, гл. I (стр. 243). Этой лемме соответствует лемма 3 работы ([3]) (см. стр. 10). Эта лемма также очевидна.

* В ([3]) на стр. 10 после формулы (8) должна следовать строка: «где через E обозначено слово $p^2Ap^{-1}Ap^{-1}$».

** Теорема 1 работы ([3]) доказана также Рабиным в ([5]).

3) Лемма 4, § 2, гл. I (стр. 244). Эту лемму заменит лемма 2 работы ([3]) (стр. 10). Доказательство леммы 2 работы ([3]) опирается на лемму 1 той же работы, которую мы и докажем сначала.

Доказательство леммы 1. Пусть к.-о. группа F_2 задана образующими $a_1, a_2, \ldots, a_n$ и определяющими соотношениями $A_i = 1$. В качестве группы F_2' можно взять группу, определенную образующими

$$b_1, b_2, \ldots, b_n, c \tag{1}$$

и определяющими соотношениями $B_i = 1$, где слово B_i получено из слова A_i заменой каждой буквы a_j^σ, $\sigma = \pm 1$, входящей в A_i, словом$(cb_j)^\sigma$. Подгруппа группы F_2', порожденная всеми элементами cb_j, изоморфна группе F_2. Легко также видеть, что образующие (1) имеют в F_2' бесконечный порядок.

Доказательство леммы 2. Все образующие группы F имеют бесконечный порядок в F (для образующих группы F_0 это следует из теоремы 2 стр. 69 работы ([4]), для образующих группы F_2' — из только что доказанной леммы 1, а буква p в определяющих соотношениях группы F не участвует). Любые две разнотипные буквы алфавита группы F являются образующими различных свободных множителей группы F. Следовательно, они будут свободными образующими порожденной ими в F подгруппы. Лемма 2 доказана.

4) Лемма 2′, § 2, гл. I (стр. 245). Эта лемма является следствием того, что a_n и a_{n-1} являются свободными образующими порожденной ими в $\mathfrak{A}_p$ подгруппы. По леммам 3 и 2 работы ([3]) e_k и e_{k-1} являются свободными образующими порожденной ими в F подгруппы. Отсюда следует, что в F для e_k и e_{k-1} верно утверждение леммы 2′.

5) Лемма 7, § 2, гл. I (стр. 254) может быть заменена следующим утверждением.

Лемма 7*. *Пусть A, C, D — произвольные слова группы F, не содержащие букв p^σ, и $A \neq 1$ в F. Если при этом*

$$p^2Ap^{-1}Ap^{-1}DpA^{-1}pA^{-1}p^{-2}C = 1 \quad \text{в } F,$$

то в группе F равны 1 *также слово C и проекции слова D на алфавиты групп F_0 и F_2'.*

Эта лемма является следствием того, что F_0, F_2' и $F_3 = \{p\}$ являются свободными множителями группы F.

6) Лемма 6, § 2, гл. I и следствие из нее (стр. 246 и 253) заменяются следующей леммой.

Лемма 6*. *Пусть слово A группы F не содержит букв p и не равно* 1 *в F. Для того чтобы слово*

$$Q \equiv e^{k_1}(p^2Ap^{-1}Ap^{-1})^{s_1}e^{k_2}\cdots e^{k_\mu}(p_2Ap^{-1}Ap^{-1})^{s_\mu}e^{k_{\mu+1}},$$

где e — произвольная буква алфавита группы F, равнялась 1 *в F, необходимо и достаточно, чтобы соответствующая последовательность чисел $k_1, s_1, k_2, \ldots, k_\mu, s_\mu, k_{\mu+1}$ была вырождающейся.*

Лемма 6* доказывается таким же образом, как в гл. I работы ([2]) доказывались лемма 6 и следствие из нее.

Таким образом, для каждого из вспомогательных утверждений о группе $\mathfrak{A}_p$ (1) — 6)), мы имеем соответствующее утверждение о группе F. Теперь доказательство леммы Б получится дословным повторением всех рассуждений первых двух параграфов главы II работы ([2]).

II. Алгоритмические проблемы в эффективно-полных классах групп. Под проблемой распознавания группового свойства α для групп класса K будем понимать задачу отыскания алгоритма, который для любой группы класса K решал бы вопрос, обладает она свойством α

или нет. В работах ([1-3]) изучался частный вид таких проблем, когда класс K совпадает с классом всех к.-о. групп.

Класс к.-о. групп K назовем эффективно-полным, если существует алгоритм $\mathfrak{R}$, перерабатывающий задание произвольной к.-о. группы F в задание такой группы из класса K, некоторой подгруппе которой изоморфна группа F. При этом алгоритм $\mathfrak{R}$ будем называть алгоритмом, эффективизирующим полноту класса K. Будем говорить, что алгоритм $\mathfrak{R}$ оставляет группу F_0 неподвижной, если он перерабатывает любое задание группы F_0 в задание той же самой группы.

Условие Т. Будем говорить, что для пары (K, α), где K — некоторый класс к.-о. групп, а α — любое инвариантное групповое свойство, выполняется условие Т, если можно указать к.-о. группу F_1 из класса K, обладающую свойством α, и такую к.-о. группу F_2, которая не может быть вложена ни в какую к.-о. группу со свойством α.

Теорема 1. *Пусть K — некоторый эффективно-полный класс к.-о. групп. Если инвариантное свойство α таково, что для пары (K, α) выполняется условие* Т, *причем алгоритм $\mathfrak{R}$, эффективизирующий полноту класса K, оставляет группу F_1 со свойством α неподвижной, то проблема распознавания свойства α для групп класса K неразрешима.*

Доказательство. Рассмотрим группу F_2, которая в силу условия Т не вложима ни в какую к.-о. группу со свойством α. Используя лемму 1 работы ([3]), вложим F_2 в к.-о. группу F_2', все образующие которой имеют бесконечный порядок. Далее на основе группы $F = F_0 * F_2' * \{p\}$, где F_0 есть к.-о. группа с неразрешимой проблемой тождества, построим точно так, как это указано в ([3])*, систему групп F_{qA}. Выше мы доказали, что для групп F_{qA} верна лемма Б. Пусть $F_A = F_{qA} * F_1$, где F_1 есть группа класса K, обладающая свойством α. Рассмотрим систему групп $G_A = \mathfrak{R}(F_A)$, где A — произвольное слово группы F_0. Так как алгоритм $\mathfrak{R}$ эффективизирует полноту класса K, то все группы G_A принадлежат классу K. Теорема 1 будет доказана, если мы докажем, что невозможен алгоритм, который проверял бы для любой группы G_A, обладает она свойством α или нет. Для этого же достаточно доказать, что G_A будет обладать свойством α тогда и только тогда, когда $A = 1$ в группе F_0.

Пусть $A = 1$ в F_0. Тогда $A = 1$ в F. По лемме Б в этом случае группа F_{qA} единичная. Следовательно, F_A изоморфна группе F_1, а значит, и G_A изоморфна F_1. А тогда инвариантное свойство α будет выполнено в G_A.

Пусть $A \neq 1$ в F_0. Тогда $A \neq 1$ в F. В этом случае по лемме Б группа F является подгруппой группы F_{qA}. Имеем $F_2 \subset F_2' \subset F \subset F_{qA} \subset F_A \subset \mathfrak{R}(F_A) = G_A$, т. е. группа F_2 вложена в G_A. Тогда, в силу условия Т, группа G_A не может обладать свойством α. Теорема доказана.

Представляет интерес следующий частный случай теоремы 1.

Теорема 2. *Пусть K — эффективно-полный класс к.-о. групп, эффективизирующий алгоритм которого оставляет неподвижной любую группу этого класса. Если инвариантное свойство α таково, что для пары (K, α) выполняется условие* Т, *то проблема распознавания свойства α для групп класса K неразрешима.*

Легко видеть, что теорема 1 работы ([3]) является частным случаем этой теоремы.

Класс к.-о. групп K назовем рекурсивным, если существует алгоритм, который позволяет для любой к.-о. группы проверять, принадлежит она классу K или нет.

Теорема 3. *Пусть K есть рекурсивный и эффективно-полный класс к.-о. групп, а α — некоторое инвариантное групповое свойство. Если для пары (K, α) условие* Т *выполняется, то проблема распознавания свойства α для групп класса K неразрешима.*

---

* См. подстрочное примечание на стр. 13.

Доказательство. Пусть $\mathfrak{N}$ — эффективизирующий алгоритм класса K, а $\mathfrak{M}$ — алгоритм, который позволяет проверять для любой к.-о. группы, принадлежит она классу K или нет. Используя эти два алгоритма, легко строим такой эффективизирующий полноту класса K алгоритм $\mathfrak{N}^*$, который оставляет неподвижной каждую группу класса K, чем и доказывается теорема 3.

В качестве нетривиального примера рекурсивного и эффективно-полного класса к.-о. групп можно указать класс к.-о. групп, совпадающих со своим коммутантом.

Всякая система нетривиальных тождественных соотношений

$$L_i \equiv 1 \quad (i = 1, 2, \ldots, k), \tag{2}$$

записанных с помощью переменных символов $x_1, x_2, \ldots, x_r$, определяет класс групп, условно-единичных относительно этой системы тождественных соотношений (см. ([3]), стр. 11).

Теорема 4. *Пусть K_1 есть класс условно-единичных групп относительно системы нетривиальных тождественных соотношений* (2). *Если инвариантное групповое свойство α таково, что для пары* (K_1, α) *выполняется условие* T, *то проблема распознавания свойства α для групп класса K_1 неразрешима.*

Доказательство. Сначала вложим группу F_2 по лемме 1 работы ([3]) в группу F'_2, все образующие которой имеют бесконечный порядок. При этом мы возьмем группу F'_2 такой, чтобы она содержала свободную подгруппу с двумя образующими b_1 и b_2. Пусть $B_1, B_2, \ldots, B_r$ — свободные образующие порожденной ими подгруппы в свободной группе с образующими b_1 и b_2. Подставим в словах L_i всюду вместо переменных $x_1, x_2, \ldots, x_r$ слова $B_1, B_2, \ldots, B_r$. Полученные слова группы $\{b_1, b_2\}$ обозначим через Y_i ($i = 1, 2, \ldots, k$). Так как все тождественные соотношения (2) по условию нетривиальны, то ни одно Y_i не равно 1 в группе $\{b_1, b_2\}$. Тогда $Y_i \neq 1$ и в F'_2. Пусть C — произвольное слово группы F_0. Положим

$$A = [\ldots[[C, Y_1], Y_2]\ldots Y_k], \tag{3}$$

где квадратные скобки обозначают взятие коммутатора. A есть слово группы $F = F_0 * F'_2 * \{p\}$.

Легко видеть, что $A = 1$ в F тогда и только тогда, когда $C = 1$ в F_0. Поэтому невозможен алгоритм, который проверял бы для любого слова A типа (3), равно оно 1 в F или нет. Заметим также, что добавление к соотношениям группы F какого-нибудь из тождественных соотношений (2) превращает в 1 соответствующее слово Y_i, а вместе с ним и слово A.

Рассмотрим теперь систему групп F_{qA}, построенных так же, как это делалось в ([3]), которые соответствуют словам (3) при всевозможных $C \in F_0$. В силу леммы Б каждая из этих групп будет условно-единичной относительно системы (2), т. е. все эти группы входят в класс K_1. Очевидно, каждая группа $F_A = F_{qA} * F_1$, где F_1 — группа, которая по условию T входит в K_1 и обладает свойством α, также входит в класс K_1. Теорема 4 будет доказана, если мы докажем, что невозможен алгоритм, который проверял бы для любой группы F_A, обладает она свойством α или нет. А для этого достаточно доказать, что группа F_A обладает свойством α тогда и только тогда, когда $A = 1$ в группе F. Это доказывается так же, как в теореме 1.

Математический институт им. В. А. Стеклова
Академии наук СССР

Поступило
15 V 1958

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] С. И. Адян, ДАН, 103, № 4 (1955). [2] С. И. Адян, Тр. Московск. матем. общ., 6 (1957). [3] С. И. Адян, ДАН, 117, № 1 (1957). [4] П. С. Новиков, Тр. Матем. инст. им. В. А. Стеклова, 44 (1955). [5] M. Rabin, Ann. Math., 67, № 1 (1958).