Доклады Академии наук СССР
1955. Том 103, № 4

МАТЕМАТИКА

С. И. АДЯН

АЛГОРИТМИЧЕСКАЯ НЕРАЗРЕШИМОСТЬ ПРОБЛЕМ РАСПОЗНАВАНИЯ НЕКОТОРЫХ СВОЙСТВ ГРУПП

(Представлено академиком И. М. Виноградовым 26 IV 1955)

Мы будем рассматривать только группы, задаваемые конечным числом образующих и определяющих соотношений, не оговаривая это каждый раз.

В работе (1) П. С. Новиков построил группу с алгоритмически неразрешимой проблемой тождества. На основе этого результата им доказана неразрешимость сформулированной в (2) проблемы изоморфизма теории групп.

В настоящей работе доказывается неразрешимость проблемы изоморфизма в том случае, если одну из групп зафиксировать, взяв в качестве нее любую группу, заданную конечным числом образующих и определяющих соотношений. Именно, справедлива следующая теорема:

Теорема 1. *Пусть дана произвольная группа* F_0. *Невозможен алгоритм, распознающий для каждой группы* F, *изоморфна она группе* F_0 *или нет.*

Будем говорить, что свойство β группы F инвариантно, если всякая группа F_1, изоморфная группе F, также обладает этим свойством. Свойство α группы F назовем наследственным, если всякая подгруппа F' группы F также обладает им. Выполнимость или невыполнимость в данной группе некоторого инвариантного свойства не зависит от способа задания этой группы. Очевидно, что всякое наследственное свойство является инвариантным. Наследственное свойство назовем нетривиальным, если этим свойством не обладает некоторая свободная группа с конечным числом образующих.

Теорема 2. *Пусть* α_0 — *произвольное нетривиальное наследственное свойство,* β_0 — *произвольное инвариантное свойство и пусть существует группа* F_1, *обладающая свойством* $(\alpha_0 \& \beta_0)$. *Тогда невозможен алгоритм, распознающий для любой группы* F, *выполнено в ней свойство* $(\alpha_0 \& \beta_0)$ *или нет.*

Теорема 3. *Пусть существует группа* F_0, *в которой выполнено данное инвариантное свойство* α_0, *которое не выполнено ни в какой группе с неразрешимой проблемой тождества. Тогда невозможен алгоритм, распознающий для любой группы* F, *выполнено в ней свойство* α_0 *или нет.*

Теорема 4. *Невозможен алгоритм, распознающий в каких группах разрешима проблема тождества, в каких нет, т. е. неразрешима так называемая метапроблема тождества.*

Теорема 5. *Невозможен алгоритм для распознавания следующих свойств групп:*

1) *быть простой группой;*

2) *быть группой, разложимой в свободное произведение* n *подгрупп при фиксированном* $n > 1$;

3) *иметь свободную подгруппу.*

Обозначим через $\mathfrak{A}_0$ построенную в [1] центрально-симметрическую группу с неразрешимой проблемой тождества. В [1] доказано, что невозможен алгоритм, распознающий, какие из слов вида XpX^+ (где p — опорная буква группы $\mathfrak{A}_0$, а X состоит только из букв левого алфавита) равны и какие не равны. Очевидно, то же самое можно утверждать и насчет слов вида $pXpX^+$, где X — произвольное слово из букв левого алфавита группы $\mathfrak{A}_0$. Две буквы положительного алфавита группы $\mathfrak{A}_0$ назовем однотипными, если они обе из левого или обе из правого алфавита $\mathfrak{A}_0$. В противном случае две буквы алфавита $\mathfrak{A}_0$ назовем разнотипными. Заметим, что в группе $\mathfrak{A}_0$ больше половины всех букв положительного алфавита составляют буквы, обозначаемые в [1] через $l_{a,i}$ и $l^+_{a,i}$. Легко доказывается следующая лемма:

Лемма. *Весь положительный алфавит группы* $\mathfrak{A}_0$ *можно расположить в ряд*

$$a_1, a_2, \ldots, a_{n-1}, a_n, \tag{1}$$

удовлетворяющий следующим свойствам:

1) *при* $i \leqslant n-2$ *буквы* a_i *и* a_{i+2} *разнотипны*;

2) *при четных* i a_i *есть буква вида* $l_{a,i}$ *или* $l^+_{a,i}$;

3) a_{n-2} *есть опорная буква* p *группы* $\mathfrak{A}_0$;

4) a_n *есть буква вида* $l_{a,i}$; a_{n-1} — *вида* $l^+_{a,i}$.

Каждой паре (A, B) слов группы $\mathfrak{A}_0$ вида $pXpX^+$ соотнесем некоторую группу, которую будем обозначать через $\mathfrak{A}_{q,A,B}$. Группу $\mathfrak{A}_{q,A,B}$ определяем заданием положительного алфавита и системы определяющих соотношений. Положительный алфавит группы $\mathfrak{A}_{q,A,B}$ состоит из всех букв ряда (1) и n новых букв

$$q_1, q_2, \ldots, q_{n-1}, q_n. \tag{2}$$

Система определяющих соотношений группы $\mathfrak{A}_{q,A,B}$ содержит все определяющие соотношения группы $\mathfrak{A}_0$:

$$C_\nu = D_\nu \tag{3}$$

и еще следующие соотношения:

$$a_i q_i = q_i AB^{-1} \quad (i = 1, 3, 5, \ldots, n-2), \tag{4}$$

$$q_{j-1} q_j = q_j a_{j-1} \quad (1 < j \leqslant n), \tag{5}$$

$$q_n a_n = a_n q_n AB^{-1} q_n. \tag{6}$$

Следующую теорему также приводим без доказательства ввиду его громоздкости.

Теорема 1°. *Если* $A = B$ *в группе* $\mathfrak{A}_0$, *то* $\mathfrak{A}_{q,A,B}$ *есть единичная группа. Если* $A \neq B$ *в группе* $\mathfrak{A}_0$, *то* $\mathfrak{A}_0$ *является подгруппой группы* $\mathfrak{A}_{q,A,B}$.

Из этой теоремы непосредственно следует, что невозможен алгоритм, распознающий по заданию группы, является она единичной или нет. Непосредственным следствием этой теоремы является также теорема 4. Остальные теоремы, сформулированные в начале статьи, тоже доказываются на основе теоремы 1°.

Приведем краткое доказательство теоремы 1. Пусть группа F_0 задана образующими

$$b_1, b_2, \ldots, b_\lambda \tag{7}$$

и определяющими соотношениями

$$E_k = L_k \quad (k = 1, 2, \ldots, m). \tag{8}$$

Каждой паре слов (AB) вида $pXpX^+$ соотнесем группу $\mathfrak{A}'_{q,\,A,\,B}$, заданную образующими (1), (2) и (7) и определяющими соотношениями (3), (4), (5), (6) и (8). Каждая группа $\mathfrak{A}'_{q,\,A,\,B}$ есть свободное произведение соответствующей группы $\mathfrak{A}_{q,\,A,\,B}$ на группу F_0. Из теоремы 1° следует, что при $A = B$ в $\mathfrak{A}_0$ группа $\mathfrak{A}'_{q,\,A,\,B}$ будет изоморфна группе F_0. Докажем теперь, что в случае $A \neq B$ в $\mathfrak{A}_0$ группа $\mathfrak{A}'_{q,\,A,\,B}$ не будет изоморфна F_0. Пусть $A \neq B$ в $\mathfrak{A}_0$ и $\mathfrak{A}'_{q,\,A,\,B}$ изоморфная F_0. Тогда ни $\mathfrak{A}_{q,\,A,\,B}$ ни F_0 не будут единичными группами, а $\mathfrak{A}'_{q,\,A,\,B}$ будет их свободным произведением. F_0 как группа, изоморфна группе $\mathfrak{A}'_{q,\,A,\,B}$ будет иметь свободное разложение из двух множителей F'_1 и F_1, изоморфных, соответственно, группам $\mathfrak{A}_{q,\,A,\,B}$ и F_0. Тогда $\mathfrak{A}'_{q,\,A,\,B}$ имела бы свободное разложение из трех множителей $\mathfrak{A}_{q,\,A,\,B}$, F'_1 и F_1. Продолжая эти рассуждения, мы находим, что если при $A \neq B$ в $\mathfrak{A}_0$ группы $\mathfrak{A}'_{q,\,A,\,B}$ и F_0 изоморфны, то группа $\mathfrak{A}'_{q,\,A,\,B}$ имеет свободные разложения из сколь угодно большого числа множителей. Но это невозможно, ибо известно ([2]), что число множителей в свободном разложении группы с конечным числом образующих ограничено сверху числом образующих. Значит, при $A \neq B$ в $\mathfrak{A}_0$ группа $\mathfrak{A}'_{q,\,A,\,B}$ не изоморфна F_0. Это и доказывает теорему 1, так как невозможен алгоритм для распознавания $A = B$ в $\mathfrak{A}_0$ или нет.

Для доказательства теоремы 2 строим систему групп $\mathfrak{A}'_{q,\,A,\,B}$, беря вместо группы F_0 группу F_1, в которой выполнено свойство $(\alpha_0 \,\&\, \beta_0)$. Тогда получаем, что для выполнимости в группе $\mathfrak{A}'_{q,\,A,\,B}$ свойства $(\alpha_0 \,\&\, \beta_0)$ необходимо и достаточно, чтобы выполнялось $A = B$ в $\mathfrak{A}_0$.

Достаточность. Если $A = B$ в $\mathfrak{A}_0$, то по теореме 1° группа $\mathfrak{A}'_{q,\,A,\,B}$ будет изоморфна группе F_1 и, по условию теоремы 2, в ней будет выполнено инвариантное свойство $(\alpha_0 \,\&\, \beta_0)$.

Необходимость. Достаточно доказать, что при $A \neq B$ в $\mathfrak{A}_0$ уже свойство α_0 не будет выполнено в $\mathfrak{A}'_{q,\,A,\,B}$. По теореме 1° при $A \neq B$ в $\mathfrak{A}_0$ группа $\mathfrak{A}_0$ будет подгруппой группы $\mathfrak{A}_{q,\,A,\,B}$, а, значит, и группы $\mathfrak{A}'_{q,\,A,\,B}$. Но группа $\mathfrak{A}_0$, как видно из ([1]), имеет свободную подгруппу с двумя образующими, которая в свою очередь имеет свободные подгруппы с любым конечным числом образующих ([2]). Значит, при $A \neq B$ в $\mathfrak{A}_0$ группа $\mathfrak{A}'_{q,\,A,\,B}$ имеет свободные подгруппы с любым конечным числом образующих, и поэтому в ней не может быть выполнено нетривиальное наследственное свойство α_0.

Теоремы 3 и 5 доказываются аналогично.

Московский государственный
педагогический институт
им. В. И. Ленина

Поступило
12 IV 1955

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] П. С. Новиков, Тр. Матем. инст. им. В. А. Стеклова, 44, 1 (1955). [2] А. Г. Курош, Теория групп, 1953.