Доклады Академии Наук СССР
1952. Том LXXXV, № 4

МАТЕМАТИКА

П. С. НОВИКОВ

ОБ АЛГОРИТМИЧЕСКОЙ НЕРАЗРЕШИМОСТИ ПРОБЛЕМЫ ТОЖДЕСТВА

(Представлено академиком И. М. Виноградовым 31 V 1952)

1. Пусть G — произвольная группа, заданная конечным числом образующих, связанных конечным числом определяющих отношений. Проблема тождества ставится следующим образом: требуется указать алгоритм, позволяющий устанавливать для любых двух элементов группы, равны они между собой или нет.

В некоторых частных случаях эту проблему удается решить. Магнус ([3]) построил алгоритм для случая произвольной группы с одним определяющим соотношением. В ряде работ В. А. Тартаковского ([5–9]) построены алгоритмы, применимые к более широким классам групп. Однако в общем случае вопрос о существовании алгоритма для решения проблемы тождества оставался до настоящего времени открытым. Нами доказана следующая теорема.

Теорема. *Существуют группы, для которых невозможно построить алгоритм, решающий проблему тождества.*

Понятие алгоритма понимается в смысле определения, принятого в современной теории алгоритмов. Мы разрабатываем способ, позволяющий свести вопрос о тождестве элементов группы к ранее решенным задачам о несуществовании алгоритма. Наиболее удобно для этого воспользоваться системой продукций Поста. Мы сводим сначала вопрос об алгоритмической неразрешимости проблемы тождества для групп с конечным числом определяющих соотношений к тому же вопросу для некоторых систем специального вида — с бесконечным числом определяющих соотношений, которые мы называем круговыми системами. Затем вопрос об алгоритмической неразрешимости проблемы тождества для круговых систем мы сводим к тому же вопросу для системы продукций Поста.

2. Определение круговых систем. Мы рассматриваем конечный алфавит и слова в нем, к которым присоединено пустое слово, обозначаемое 1. Система задается конечным числом соотношений, которые мы назовем исходными равенствами:

$$A_i = B_i, \tag{1}$$

где A_i и B_i — слова. Для каждой буквы x существует обратная x^{-1} и в (1) существуют все равенства вида $xx^{-1} = 1$ и $x^{-1}x = 1$. Для обозначения равенства мы употребляем тот же знак $=$, что и в исходных равенствах.

Равенство между словами определяется следующими условиями: 1) равенство рефлективно, симметрично и транзитивно; 2) для любой

буквы a и любого слова A имеет место $aA = Aa$; 3) каковы бы ни были слова A' и A'' (может быть, пустые), имеет место $A'A_iA'' = A'B_iA''$, где A_i и B_i — слова из соотношения (1).

3. Мы будем говорить, что круговая система $\mathfrak{B}$ представима посредством группы $\mathfrak{A}$, если в $\mathfrak{A}$ можно алгоритмически выделить подмножество $\mathfrak{A}'$, которое можно алгоритмически привести во взаимно-однозначное соответствие с системой $\mathfrak{B}$ (иными словами, равные слова системы $\mathfrak{B}$ переходят в равные элементы $\mathfrak{A}'$ и обратно).

Теорема 1. *Для каждой круговой системы $\mathfrak{B}$ с конечным числом образующих и конечным числом исходных равенств существует группа с конечным числом образующих и конечным числом определяющих соотношений, посредством которой можно представить круговую систему $\mathfrak{B}$.*

Построение группы $\mathfrak{A}$ для данной круговой системы $\mathfrak{B}$. Пусть $\mathfrak{B}$ определена равенствами (1) и $a, b, c, \ldots$ — ее образующие. Среди букв группы $\mathfrak{A}$ имеются буквы: опорные p_1, p_2, p_3; основные $a_j, b_j, c_j, \ldots$ с индексами; сигнальные μ_i, λ_i, ν_i с индексами. Основные и сигнальные буквы делятся на 4 рода, отмечаемые индексами 0, 1, 2, 3. Основные буквы каждого рода — все буквы из $\mathfrak{B}$, но снабженные индексами.

Слова группы $\mathfrak{A}$, которые представляют систему $\mathfrak{B}$, имеют вид

$$A_0p_1A_1p_2A_2p_3A_3. \tag{2}$$

При этом слово A_0 отличается от слова A системы $\mathfrak{B}$ только индексами при буквах. Слово A_j состоит только из основных букв j-го рода. Слова (2) являются с точностью до различающих типы индексов и индексов у p центрально-симметричными относительно p_2, а части слова (2) $A_0p_1A_1$ и $A_2p_3A_3$ — центрально-симметричными относительно букв p_1 и p_3. Слово (2) соответствует слову A системы $\mathfrak{B}$.

Определяющие соотношения группы $\mathfrak{A}$ обладают в известном смысле подобной же симметрией. Так, если это соотношение содержит только буквы нулевого и первого рода, а среди опорных букв только p_1, то существует соответствующее ему определяющее соотношение, получаемое из данного заменой p_1 на p_3, букв нулевого рода — соответствующими буквами третьего рода, букв первого — буквами второго, а также изменением порядка написания входящих в соотношение слов на обратные. Мы напишем поэтому все определяющие соотношения, содержащие центральную опорную букву p_2. Остальные определяющие соотношения напишем только для образующих первых двух родов, как основных, так и сигнальных, и буквы p_1. Основные буквы каждого рода j разделяются на два подрода, отмечаемые штрихами. Вместе с основной буквой x_j в группе существуют основные буквы x'_j. Для произвольной основной буквы x_0 нулевого рода имеются сигнальные буквы того же рода μ_0^{1, x_0}, μ_0^{2, x_0} и λ_0^{1, x_0, y_0}, $\lambda_0^{1, x_0, y_0, z_0}$, λ_0^{2, x_0, y_0} и $\lambda_0^{2, x_0, y_0, z_0}$. Имеем следующие соотношения:

1) $x_0 = \mu_0^{1, x_0}\mu_0^{2, x_0}$;
2) $\mu_0^{1, x_0}\mu_0^{2, x_0} = \mu_0^{2, x_0}\mu_0^{1, x_0}$;
3) $\mu_0^{2, x_0}y_0 = y'_0\mu_0^{2, x_0}\lambda_0^{2, x_0, y_0}$;
4) $\mu_0^{1, x_0}y'_0 = y_0\mu_0^{1, x_0}\lambda_0^{1, x_0, y_0}$,

где y_0 — произвольная буква нулевого рода, отличная от x_0. Пусть z_0 и u_0 — любые другие буквы того же рода (может быть, совпадающие с x_0 или y_0).

5) $\lambda_0^{2, x_0, y_0}z_0 = z_0\lambda_0^{2, x_0, y_0}\lambda^{2, x_0, y_0, z_0}$;
6) $\lambda_0^{2, x_0, y_0, z_0}u_0 = u_0\left(\lambda_0^{2, x_0, y_0, z_0}\right)^2$;
7) $\lambda_0^{1, x_0, y_0}z'_0 = z'_0\lambda_0^{1, x_0, y_0}\lambda_0^{1, x_0, y_0, z_0}$;
8) $\lambda^{1, x_0, y_0, z_0}u'_0 = u'_0\left(\lambda_0^{1, x_0, y_0, z_0}\right)^2$;

9) $\lambda_0^{2,x_0,y_0,z_0}p_1\lambda_1^{2,x_1,y_1,z_1}=p_1$; 10) $\lambda_0^{2,x_0,y_0}p_1\lambda_1^{2,x_1,y_1}=p_1$;

11) $\lambda^{1,x_0,y_0,z_0}\mu_0^{2,x_0}p_1\mu_1^{2,x_1}\lambda_1^{1,x_1,y_1,z_1}=\mu_0^{2,x_0}p_1\mu_1^{2,x_1}$;

12) $\lambda_0^{1,x_0,y_0}\mu_0^{2,x_0}p_1\mu_1^{2,x_1}\lambda_1^{1,x_1,y_1}=\mu^{2,x_0}p_1\mu_1^{2,x_1}$;

13) $x_1=\mu_1^{2,x_1}\mu_1^{1,x_1}$, $\mu_1^{2,x_1}\mu_1^{1,x_1}=\mu_1^{1,x_1}\mu_1^{2,x_1}$,

где x_1, y_1 и z_1 — буквы первого рода, соответствующие буквам x, y, z системы $\mathfrak{B}$.

14) $y_1\mu_1^{2,x_1}\nu_1^{2,x_1,y_1}=\lambda_1^{2,x_1,y_1}\mu_1^{2,x_1}y_1'$; 15) $u_1'\lambda_1^{1,x_1,y_1,z_1}=(\lambda_1^{1,x_1,y_1,z_1})^2\,u_1'$;

16) $y_1'\mu_1^{1,x_1}\nu_1^{1,x_1,y_1}=\lambda_1^{1,x_1,y_1}\mu_1^{1,x_1}y_1$; 17) $\nu_1^{2,x_1,y_1}z_1'=z_1'\nu_1^{2,x_1,y_1}\nu_1^{2,x_1,y_1,z_1}$;

18) $z_1\lambda_1^{2,x_1,y_1}=\lambda_1^{1,x_1,y_1,z_1}\lambda_1^{2,x_1,y_1}z_1$; 19) $\nu_1^{2,x_1,y_1,z_1}u_1'=u_1'(\nu_1^{2,x_1,y_1,z_1})^2$;

20) $z_1'\lambda_1^{1,x_1,y_1}=\lambda_1^{1,x_1,y_1,z_1}\lambda_1^{1,x_1,y_1}z_1'$; 21) $\nu_1^{1,x_1,y_1}z_1=z_1\nu_1^{1,x_1,y_1}\nu_1^{1,x_1,y_1,z_1}$;

22) $u_1\lambda_1^{2,x_1,y_1,z_1}=(\lambda_1^{2,x_1,y_1,z_1})^2\,u_1$; 23) $\nu_1^{1,x_1,y_1,z_1}u_1=u_1(\nu_1^{1,x_1,y_1,z_1})^2$.

Пусть $A^{(i)}=B^{(i)}$ — произвольное определяющее соотношение круговой системы $\mathfrak{B}$. Тогда слово $A_k^{(i)}$ состоит из тех же букв, что и $A^{(i)}$, только снабженных индексом k ($k=0, 1, 2, 3$); при этом, если k четно, то буквы $A_k^{(i)}$ выписаны в том же порядке, как у $A^{(i)}$, а если k нечетно, то в обратном порядке. Такой же смысл имеет обозначение $B_k^{(i)}$. Тогда имеем следующее определяющее соотношение:

24) $A_0^{(i)}p_1A_1^{(i)}=B_0^{(i)}p_1B_1^{(i)}\rho_1^{(i)}$ и $\rho_1^{(i)}x_1=x_1(\rho_1^{(i)})^2$.

Кроме того, имеется столько же соотношений, написанных по симметрии для букв второго и третьего рода. Последние из них имеют вид

24′) $A_2^{(i)}p_3A_3^{(i)}=\rho_2^{(i)}B_2^{(i)}p_3B_3^{(i)}$ и $x_2\rho_2^{(i)}=(\rho_2^{(i)})^2x_2$.

Наконец, имеются еще соотношения:

а) $\nu_1^{1,x_1,y_1,z_1}p_2\nu_2^{1,x_2,y_2,z_2}=p_2$ и $\nu_1^{1,x_1,y_1}p_2\nu_2^{1,x_2,y_2}=p_2$;

б) $\nu_1^{2,x_1,y_1,z_1}\mu_1^{1,x_1}p_2\mu_2^{1,x_2}\nu_2^{2,x_2,y_2,z_2}=\mu_1^{1,x_1}p_2\mu_2^{1,x_2}$ и $\nu_1^{2,x_1,y_1}\mu_1^{1,x_1}p_2\mu_2^{1,x_2}\nu_2^{2,x_2,y_2}=$
$=\mu_1^{1,x_1}p_2\mu_2^{1,x_2}$;

в) $\rho_1^{(i)}p_2\rho_2^{(i)}=p_2$.

Здесь x_2, y_2 и z_2 — буквы второго рода, соответствующие буквам x, y, z круговой системы $\mathfrak{B}$, а μ_2^{1,x_2}, λ_2^{1,x_2,y_2}, $\lambda_2^{1,x_2,y_2,z_2}$ и μ_2^{2,x_2}, λ_2^{2,x_2,y_2}, $\lambda_2^{2,x_2,y_2,z_2}$ — буквы, соответствующие по симметрии буквам μ_1^{1,x_1}, λ_1^{1,x_1,y_1}, $\lambda_1^{1,x_1,y_1,z_1}$ и μ_1^{2,x_1}, λ_2^{2,x_1,y_1}, $\lambda_1^{2,x_1,y_1,z_1}$.

Пусть A — произвольное слово системы $\mathfrak{B}$, а $A_0p_1A_1p_2A_2p_3A_3$ — соответствующее слово в группе $\mathfrak{A}$.

Теорема 2. *Слово группы $\mathfrak{A}$ вида $A_0p_1A_1p_2A_2p_3A_3$ равно слову $B_0p_1B_1p_2B_2p_3B_3$ тогда и только тогда, когда $A=B$ в круговой системе $\mathfrak{B}$.*

После этого вопрос о разрешимости задачи тождества слов в группах сводится к той же задаче для круговых систем.

4. Равенство слов в круговой системе можно свести к задаче равенства слов в системе Поста ([10]). Эта система состоит из определенных правил переработки любого слова, или продукций. Правила преобразования исходного слова A следующие.

Дается конечное число пар слов (P_i, Q_i). Каждое слово вида P_iX преобразуется в слово XQ_i и обратно. Эта операция называется продукцией. Пусть A — некоторое слово. Путем продукций можно, исходя из A, получить совокупность слов. Все эти слова называются равными слову A. Известно ([10]), что можно построить такую конкретную систему пар (P_i, Q_i) и указать такое слово A, что не существует алгоритма,

позволяющего решать вопросы равенства между словами в данной системе. Напишем теперь исходные равенства, определяющие круговую систему, для которой вопрос об отыскании алгоритма для решения задачи равенства слов прямо сводится к такому же вопросу для системы Поста. Пусть Ω — некоторая система Поста и A — исходное слово системы Поста, а (A_i, B_i) — пары слов, определяющих продукции. Мы строим круговую систему $\mathfrak{B}$, алфавит которой содержит каждую букву системы, но в двойном числе, так что имеются буквы двух родов, отмеченные индексами 1 и 2.

Эти буквы назовем основными буквами системы $\mathfrak{B}$. Две буквы p_1 и p_2 назовем опорными и, наконец, буквы $l_1^{(i)}$, $q_1^{(i)}$, $r_1^{(i)}$ и $l_2^{(i)}$, $q_2^{(i)}$, $r_2^{(i)}$ — сигнальными (здесь i пробегает столько же чисел, сколько есть пар (A_i, B_i)).

Пусть x_1 и x_2 — произвольные основные буквы соответственно первого и второго рода, а $(A_1^{(i)}, B_1^{(i)})$ и $(A_2^{(i)}, B_2^{(i)})$ — i-е пары слов, буквы которых соответственно отмечены индексами 1 и 2.

1) $A_1^{(i)} p_1 A_2^{(i)} = q_1^{(i)} l_1^{(i)} p_1 l_2^{(i)} q_2^{(i)}$; 2) $x_1 q_1^{(i)} = (q_1^{(i)})^2 x_1$;

3) $q_2^{(i)} x_2 = x_2 (q_2^{(i)})^2$; 4) $x_1 l_1^{(i)} = l_1^{(i)} x_1$;

5) $l_2^{(i)} x_2 = x_2 l_2^{(i)}$; 6) $q_1^{(i)} p_2 q_2^{(i)} = p_2$;

7) $r_1^{(i)} p_1 r_2^{(i)} = p_1$; 8) $q_1^{(i)} l_1^{(i)} p_2 l_2^{(i)} q_2^{(i)} = B_1^{(i)} p_2 B_2^{(i)}$.

К этим восьми равенствам присоединяются все равенства вида $uu^{-1} = 1$ и $u^{-1}u = 1$, где u — произвольная буква системы $\mathfrak{B}$.

Рассмотрим слово

$$p_1 A_1 p_2 A_2, \tag{3}$$

где A_1 и A_2 — слова, отвечающие слову A системы Ω, только записанные во взаимно-противоположном порядке, так что A_2 есть зеркальное отражение A_1 относительно центра p_2.

Пусть A имеет вид $A_i x$; тогда преобразование слова $p_1 A_1^{(i)} x_1 p_2 x_2 A_2^{(i)}$ после исчезновения сигнальных букв приводит к слову $p_1 x_1 B_1^{(i)} p_2 B_2^{(i)} x_2$.

Это значит, что происшедшее при этом преобразование части данного слова, являющегося словом A_1, есть продукция, определяемая парой $(A_1^{(i)}, B_1^{(i)})$. То же справедливо и для симметрического слова A_2.

Теорема 3. *Всякое преобразование слова* (3) *путем равенств* (2), *после которого исчезают все сигнальные буквы и отсутствуют буквы в отрицательных степенях, приводит к слову* $p_1 B_1 p_2 B_2$, *где* B_1 *преобразуется из* A_1 *в результате применения продукций системы* Ω.

Этим заканчивается доказательство сводимости задачи об алгоритмической разрешимости проблемы тождества в теории групп к такому же вопросу для систем продукций. Но так как можно построить конкретную систему продукций, для которой не может быть алгоритма, решающего задачу равенства слов, то можно построить и конкретную группу, для которой проблема тождества неразрешима.

Поступило
29 V 1952

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] А. И. Мальцев, Матем. сборн., **6** (48), 331 (1939). [2] А. И. Мальцев, там же, **8** (50), 251 (1940). [3] В. Магнус, Усп. матем. наук, **8**, 365 (1941). [4] В. А. Тартаковский, ДАН, **58**, № 8, 1605 (1947). [5] В. А. Тартаковский, ДАН, **58**, № 9, 1909 (1947). [6] В. А. Тартаковский, Матем. сборн., **25** (67), 3 (1949). [7] В. А. Тартаковский, там же, **25** (67), 251 (1949). [8] В. А. Тартаковский, Изв. АН СССР, сер. матем., **13**, № 6, 283 (1949). [9] В. А. Тартаковский, Матем. сборн., **30** (72), 39 (1952). [10] E. Post, Bull. Am. Math. Soc., **50**, No. 5 (1944). [11] Н. Г. Чеботарев, Усп. матем. наук, **8**, 336 (1941).