Czechoslovak Mathematical Journal

Petr Sergeevich Novikov

О неразрешимости проблемы тождества слов в группе и некоторых других проблем алгебры

Czechoslovak Mathematical Journal, Vol. 6 (1956), No. 4, 450–454

Persistent URL: `http://dml.cz/dmlcz/100215`

О НЕРАЗРЕШИМОСТИ ПРОБЛЕМЫ ТОЖДЕСТВА СЛОВ В ГРУППЕ И НЕКОТОРЫХ ДРУГИХ ПРОБЛЕМ АЛГЕБРЫ

П. С. НОВИКОВ, Москва.

Прочитано на IV съезде чехословацких математиков в Праге 5/IX 1955 г.

Работы, о которых будет идти речь в этом докладе, принадлежат направлению, возникшему из математической логики. Оно связано с понятием „алгоритма" или закона, позволяющего автоматически решать задачи определенного круга. В математике известно много проблем, состоящих в том, что требуется найти алгоритм для решения задач той или другой серии. Мы будем рассматривать известные алгоритмические проблемы алгебры для групп с конечным числом образующих, заданных конечным числом определяющих соотношений: проблему тождества слов, проблему сопряженности слов и проблему изоморфизма групп. Вопрос о возможности решать алгоритмические проблемы не мог быть поставлен во всей полноте до тех пор, пока понятие алгоритма, хотя и ясно всеми представляемое, не было сколько-нибудь точно определено. При таком положении полностью закрывалась возможность устанавливать несуществование алгоритма для решения того или другого круга задач. Развитие математической логики позволило дать точное определение понятия алгоритма или закона; это было осуществлено в 30 годах нашего столетия в ряде работ (Чёрч, Тюринг и Клин). Впоследствие были даны другие формы определения алгоритма (Пост, Марков, Колмогоров и Успенский). Открытие определения понятия алгоритма позволило обнаружить наличие алгоритмически неразрешимых проблем сначала в математической логике (проблема разрешимости логики предикатов), а затем и в самой математике. Так Марков и Пост доказали неразрешимость проблемы тождества слов в ассоциативных системах. Тюринг показал неразрешимость проблемы тождества слов для полугрупп с сокращениями.

Нами была доказана неразрешимость проблемы тождества слов в группе и неразрешимость проблемы сопряженности слов в группе. Хотя нереарешимость проблемы сопряженности является тривиальным следствимз неразрешимости проблемы тождества слов, мы даем непосредственное доказательство неразрешимости проблемы сопряженности значительно более простое. Это обстоятельство имеет значение для тех геометрических приложений, которые можно извлечь из данной работы. Вместе с тем оказалось, что развивая методы, употребленные для доказательства неразрешимости проблемы сопряженности слов, можно получить значительно более простое доказательство неразрешимости проблемы тождества слов в группе. Правда, при этом результат несколько ослабляется по сравнению с ранее полученным. Прежде строилась конкретная группа с неразрешимой проблемой тождества слов; теперь же доказывается несуществование алгоритма, устанавливающего равенство или неравенство слов, общего для всех групп, заданных конечным числом определяющих соотношений. Доказательство неразрешимости проблемы сопряженности основано на результате Поста. Пост ввел системы преобразований слов, которые называются системами продукций. Эти системы определяются следующим образом: рассматривается определенная совокупность букв, называемая алфавитом системы и произвольная конечная совокупность пар слов (A_i, B_i), $i = 1, 2, \ldots, \lambda$, составленных из этих букв. Преобразования в системе продукций осуществляются по схемам

$$A_iX \to XB_i\,, \quad XB_i \to A_iX\,,$$

где X — любое слово, состоящее из букв алфавита данной системы. Если слово X может быть переработано в слово Y преобразованиями по указанным схемам, то мы будем говорить, что X равно Y в системе продукций. Дополнительно условимся, что равенство в системе продукций рефлексивно и транзитивно. Пост показал, что существует система продукций, для которой нет алгоритма, позвояющего для любой пары слов узнать, равны они или нет. Неразрешимость проблемы сопряженности слов в теории групп является следствием следующей теоремы:

Теорема 1. *Какова бы ни была система продукций $\mathfrak{K}$ существует группа $\mathfrak{A}$ с конечным числом образующих и конечным числом определяющих соотношений такая, что каждому слову $X \in \mathfrak{K}$ можно поставить в соответствие слово $\Phi(X) \in \mathfrak{A}$, причем соответствие Φ обладает следующими свойствами:*

1. *Существует алгоритм, позволяющий по слову X построить слово $\Phi(X)$.*

2. *Если слова X и Y равны (не равны) в $\mathfrak{K}$, то слова $\Phi(X)$ и $\Phi(Y)$ соответственно сопряжены (не сопряжены) в группе $\mathfrak{A}$.*

Опишем группу $\mathfrak{A}$ и соответствие $\Phi(X)$.

Пусть $a_1, \ldots, a_n$ — алфавит системы продукции $\mathfrak{K}$ и (A_iB_i), $i = 1, 2, \ldots, \lambda$ — определяющая система пар слов. Алфавит соответствующей группы $\mathfrak{A}$ состоит из букв

$$\begin{array}{rl} & p_1, p_2\,; \\ a_1, \ldots, a_n\,; & a_1^+, \ldots, a_n^+\,; \\ q\,; & q^+\,; \\ r\,; & r^+\,; \\ l_1, \ldots, l_\lambda\,; & l_1^+, \ldots, l_\lambda^+ \end{array}$$

и обратных им элементов.

Пусть слово A имеет вид $a_{s_1}a_{s_2}\ldots a_{s_k}$; условимся, что символ A^+ обозначает слова $a_{s_k}^+\,a_{s_{k-1}}^+\ldots a_{s_1}^+$. Тогда определяющие соотношения группы $\mathfrak{A}$ могут быть записаны следующим образом:

$$A_i^+p_1A_i = q^+l_i^+p_1l_iq\,, \quad i = 1, 2, \ldots, \lambda\,;$$
$$r^+p_1r = p_1\,;$$
$$B_ip_2B_i^+ = rl_ip_2l_i^+r_i^+\,; \quad i = 1, 2, \ldots, \lambda\,;$$
$$qp_2q^+ = p_2\,;$$
$$q_ia_j = a_jq_i^2\,; \quad a_j^+q_i^+ = q_i^{+2}a_j^+\,;$$
$$r_i^2a_j = a_jr_i\,; \quad a_j^+r_i^{+2} = r_i^+a_i^+\,.$$

Соответствие $\Phi(X)$ определяется следующим образом:

$$\Phi(X) \equiv p_1Xp_2X^+\,.$$

Полученный результат имеет следующее геометрическое приложение. Вопрос о гомотопии путей на двумерном полиэдре равносилен вопросу о сопряженности элементов фундаментальной группы этого полиэдра. С другой стороны каждая группа с конечным числом образующих и конечным числом определяющих соотношений является фундаментальной группой некоторого двумерного полиэдра. Из полученного результата вытекает, что существует двумерный полиэдр с неразрешимой проблемой гомотопии путей.

Для доказательства неразрешимости проблемы тождества слов для всех групп с конечным числом определяющих соотношений мы определяем некоторые специальные соотношения между словами. Мы называем слова X и Y группы дедуктивно - эквивалентными, если, присоединив к определяющим соотношениям группы равенство $X = 1$, можно вывести равенство $Y = 1$ и обратно.

Для групп описанного выше типа имеет место следующая теорема:

Теорема 2. *Дедуктивная эквивалентность слов $(p_1Xp_2X^+)^2$ и $(p_1Yp_2Y^+)^2$, где X и Y — слова из букв подалфавита $a_1, \ldots, a_n$, равносильна сопряженности слов $p_1Xp_2X^+$ и $p_1Yp_2Y^+$.*

Так как существуют группы указанного типа, для которых не существует алгоритма, решающего вопрос о сопряженности слов вида $p_1Xp_2X^+$, то для тех же групп нет так же алгоритма, решающего вопрос о дедуктивной эквивалентности слов вида $(p_1Xp_2X^+)^2$. Вместе с тем очевидно, что существование групп с неразрешимой задачей дедуктивной эквивалентности означает неразрешимость проблемы тождества для всех групп.

Summary

THE UNSOLVABILITY OF THE PROBLEM OF THE EQUIVALENCE OF WORDS IN A GROUP AND SEVERAL OTHER PROBLEMS IN ALGEBRA

P. S. NOVIKOV, Moscow.

Presented at the Fourth Congress of Czechoslovak Mathematicians in Prague on 5th September, 1955.

TURING has proved that the problem of the equivalence of words for semigroups (with cancellation) is unsolvable. Starting out from this result, the author of the present paper proved that the problem of the equivalence of words for groups is unsolvable (Works of the Steklov Mathematical Institute XLIV, 1955). A trivial consequence of the above result is the unsolvability of the problem of conjugate words in groups. The latter result can, however, be proved directly and much more simply than in the quoted paper. The possibility of a simpler proof of the original problem, i. e. the unsolvability of the problem of the equivalence of words (in a somewhat weaker form) then follows. The present paper is devoted to the main ideas of these proofs.

The new proof of the unsolvability of the problem of conjugate words (for groups with a finite number of generators and defining relations) is based on a certain result of POST. Post introduced so-called systems of production and proved for them that the problem of the equivalence of words is unsolvable. The author of this paper has proved the following theorem:

Theorem 1. *To each system of production $\mathfrak{K}$ it is possible to find a group $\mathfrak{A}$ with a finite number of generators and defining relations such that to each word $X \in \mathfrak{K}$ it is possible to associate the word $\Phi(x) \in \mathfrak{A}$ in such a way that the transformation Φ has the following properties*:

1. *There exists an algorithm by means of which it is possible to find, to each word $X \in \mathfrak{K}$, the corresponding word $\Phi(x) \in \mathfrak{A}$.*

2. *If the words X, Y are equivalent (non-equivalent) in $\mathfrak{K}$, then the words $\Phi(X)$, $\Phi(Y)$ are (are not) conjugate in $\mathfrak{A}$.*

By means of this theorem the unsolvability of the problem of conjugate words for groups with a finite number of generators and defining relations is reduced to the unsolvability of the problem of the equivalence of words in Post's systems of production. The construction of the group $\mathfrak{A}$ is described.

The simplification of the proof is important for several problems in algebraic topology. For instance, from the unsolvability of the problem of conjugate words for groups with a finite number of generators and defining relations it follows that there exists a two-dimensional polyhedron for which the problem of the homotopy of its paths is unsolvable.

In the above-mentioned paper of the author, the unsolvability of the problem of the equivalence of words for groups is proved by the construction of a concrete group with a finite number of generators and defining relations for which the problem is unsolvable. The author now derives a somewhat weaker result:

There does not exist an algorithm which would, for each group with a finite number of generators and defining relations, permit a decision on the equivalence of its words.

In the proof the concept of so-called deductive equivalence of words in a group is used: the words X, Y of a group are deductively equivalent if, on adding the equality $X = 1$ to the defining relations of the group, it is possible to derive the equality $Y = 1$ and conversely. The unsolvability of the problem of the equivalence of words for all groups with a finite number of generators and defining relations is reduced to the unsolvability of the problem of the deductive equivalence of words and, using the second fundamental theorem which the author presents in this paper, to the problem (already solved) of the unsolvability of the problem of conjugate words.