О НЕРАЗРЕШИМОСТИ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ В РАДИКАЛАХ И ТЕОРИИ ГРУПП

В. Г. ЗВЯГИН

Воронежский государственный университет

ON NONSOLVABILITY OF ALGEBRAIC EQUATIONS IN RADICALS AND THE GROUP THEORY

V. G. ZVYAGIN

Some ideas and results of group theory are explained and the way to reduce the problem of solvability in radicals of algebraic equation of n-th degree by one variable to some results of the group theory is shown. An example of how such equation can be solved using them is presented.

Даны некоторые понятия и результаты теории групп и показано, каким образом проблема разрешимости в радикалах алгебраического уравнения n-й степени связана с теорией групп и решается с ее помощью.

www.issep.rssi.ru

В курсе средней школы подробно изучают алгебраические уравнения с одним неизвестным 1-й и 2-й степеней. При этом оказывается, что для решения таких уравнений существуют общие формулы, выражающие корни уравнения через его коэффициенты с помощью арифметических операций и радикалов (для уравнений 2-й степени). Подобного типа формулы были установлены еще в XVI веке и для уравнений 3-й (Дж. Кардано) и 4-й (Л. Феррари) степеней. Долгое время математики пытались найти метод решения в радикалах общего уравнения 5-й степени. Однако в 1824 году норвежский математик Нильс Генрик Абель доказал следующую теорему: *Общее алгебраическое уравнение с одним неизвестным степени выше* 4*-й неразрешимо в радикалах, то есть не существует формулы, выражающей корни общего уравнения степени выше* 4*-й через коэффициенты с помощью операций сложения, вычитания, умножения, деления, возведения в натуральную степень и извлечения корней натуральной степени.*

Цель статьи – познакомить читателя с рядом понятий и результатов теории групп и показать, каким образом проблема разрешимости в радикалах алгебраического уравнения n-й степени от одного неизвестного сводится к некоторой проблеме в теории групп и каким образом она там решается.

ГРУППА

Определение 1. *Группой* называется множество G элементов произвольной природы, в котором любой упорядоченной паре (a, b) элементов этого множества поставлен в соответствие третий элемент, который мы будем обозначать символом $a \cdot b$, и при этом предполагаются выполненными следующие условия:

1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ для любых $a, b, c \in G$;

2) в G существует такой элемент e, называемый единицей группы G, для которого $a \cdot e = e \cdot a = a$ для любого элемента $a \in G$;

3) для любого элемента $a \in G$ существует такой элемент a^{-1} в G, называемый обратным к элементу a, для которого $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Множество вещественных чисел с обычной операцией сложения чисел, множество вещественных чисел, отличных от нуля, с операцией умножения чисел – все это простейшие примеры групп.

Мы подробнее обсудим более важный для темы этой статьи пример группы, причем вначале в общей ситуации, а затем и в частной ситуации, в которой он и будет использован ниже.

Определение 2. Пусть X и Y – два множества произвольной природы. Отображение $\varphi: X \longrightarrow Y$ называется *взаимно однозначным отображением*, если для каждого $y \in Y$ существует единственный $x \in X$, такой, что $\varphi(x) = y$.

Пусть M – произвольное множество. Произвольное взаимно однозначное отображение множества M на себя называется преобразованием множества M.

Во множестве преобразований множества M можно ввести операцию произведения преобразований, а именно пусть $\varphi_1, \varphi_2: M \longrightarrow M$ – два преобразования множества M, тогда произведение преобразований $\varphi_1 \cdot \varphi_2: M \longrightarrow M$ определяется так: $(\varphi_1 \cdot \varphi_2)(m) = \varphi_1(\varphi_2(m))$, $m \in M$, то есть сначала делается преобразование φ_2, затем φ_1. Первое условие определения 1 выполнено, поскольку $[(\varphi_1 \cdot \varphi_2) \cdot \varphi_3](m) = \varphi_1(\varphi_2(\varphi_3(m)))$ и $[\varphi_1 \cdot (\varphi_2 \cdot \varphi_3)](m) = \varphi_1(\varphi_2(\varphi_3(m)))$ для любого $m \in M$. Следовательно, $(\varphi_1 \cdot \varphi_2) \cdot \varphi_3 = \varphi_1 \cdot (\varphi_2 \cdot \varphi_3)$. Роль единицы в условии 2 этого определения играет тождественное отображение множества M на себя. И наконец, поскольку преобразование $\varphi: M \longrightarrow M$ есть взаимно однозначное отображение множества M на себя, то существует обратное отображение $\varphi^{-1}: M \longrightarrow M$, которое также является преобразованием и которое есть обратный элемент для φ во множестве всех преобразований множества M в себя.

Рассмотрим теперь частный случай, когда $M = \{1, 2, ..., n\}$ – множество первых n натуральных чисел. Подстановкой n-й степени будем называть любое преобразование множества M в себя. Таким образом, произвольную подстановку n-й степени можно записать в виде $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, где i_m – образ элемента m при данной подстановке. Заметим, что порядок столбцов в подстановке неважен. Важно только, что m отображается в i_m.

Множество всех подстановок n-й степени обозначают символом S_n. Во множестве S_n аналогично тому, как это сделано в случае произвольного множества M, вводится операция умножения двух подстановок, а именно под умножением двух подстановок будем понимать последовательное выполнение первой подстановки, а затем второй (то есть, другими словами, композицию этих подстановок). Множество S_n с этой операцией является группой.

Два элемента группы G называются перестановочными или коммутирующими, если $a \cdot b = b \cdot a$. Если все элементы группы коммутируют между собой, то такая группа называется коммутативной или абелевой.

Коммутативные группы – наиболее изученные объекты в теории групп. Однако имеется большое число важных для приложений и некоммутативных групп. В частности, группа S_n при $n \geq 3$ является некоммутативной.

ПОДГРУППЫ

В теории групп представляют интерес не произвольные подмножества группы, а подмножества, называемые подгруппами и учитывающие ту операцию, которая определена в группе.

Определение 3. Подмножество H группы G называется *подгруппой*, если H само является группой относительно той же операции, которая задана в G.

Опишем в группе S_n важную для нас подгруппу.

Пусть числа 1, 2, ..., n записаны в строку в некотором произвольном порядке. Скажем, что пара чисел i, j образует инверсию в этой строке, если $i < j$, но j встречается в строке раньше, чем i. Число инверсий характеризует беспорядок в данной строке по отношению к обычному порядку чисел 1, 2, ..., n.

Определение 4. Подстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ называется *четной*, если число инверсий в нижней строке четно.

Множество четных подстановок группы S_n обозначается символом A_n. Легко проверить, что A_n – подгруппа группы S_n, причем при $n \geq 4$ это некоммутативная подгруппа. A_n также называют знакопеременной группой степени n.

Среди всех подгрупп произвольной группы G выделяются нормальные подгруппы. Дадим их определение.

Пусть a – произвольный элемент группы G. Для любого элемента $g \in G$ элемент $g \cdot a \cdot g^{-1}$ называется сопряженным к элементу a.

Определение 5. Подгруппа H группы G называется *нормальной*, если она с каждым своим элементом a содержит все сопряженные элементы gag^{-1}, $g \in G$.

В частности, A_n является нормальной подгруппой в S_n.

РАЗРЕШИМЫЕ ГРУППЫ

Ниже описывается класс групп, близких к коммутативным. Разрешимыми группы из этого класса называются потому, что возможность решить алгебраическое уравнение в радикалах, как увидим ниже, зависит от разрешимости некоторой группы.

Вначале заметим, что степень коммутативности двух элементов группы можно измерить с помощью произведения $a \cdot b \cdot a^{-1} \cdot b^{-1}$, которое равно единице тогда и только тогда, когда элементы a и b перестановочны. Элемент $a \cdot b \cdot a^{-1} \cdot b^{-1}$ называется коммутатором элементов a и b.

Определение 6. *Коммутантом $K(G)$ группы G* называется множество всевозможных произведений конечного числа коммутаторов группы G.

Несложно проверить, что коммутант группы является нормальной подгруппой группы.

Итак, пусть G – некоторая группа и $K(G)$ – ее коммутант. Коммутант $K(G)$ сам является группой, и в нем также можно рассмотреть коммутант $K(K(G))$. В полученной группе снова можно рассмотреть коммутант и т.д. Группу $\underbrace{K(K(\ldots(K}_{r}(G))\ldots))$ будем для краткости обозначать $K_r(G)$. Таким образом, $K_{r+1}(G) = K(K_r(G))$.

Определение 7. Группа G называется *разрешимой*, если цепочка групп G, $K(G)$, $K_2(G)$, $K_3(G)$, ... заканчивается при некотором конечном n единичной группой, то есть при некотором n получаем $K_n(G) = \{e\}$.

Конечно, любая коммутативная группа разрешима, так как если G – коммутативная группа, то уже на первом шаге $K(G) = \{e\}$. Также группа G разрешима, если ее коммутант коммутативен, так как в этом случае $K_2(G) = \{e\}$.

Имеет место следующий важный факт.

Теорема 1. *Если группа G некоммутативна и не имеет нормальных подгрупп, отличных от $\{e\}$ и G, то она неразрешима.*

Доказательство. Так как группа G некоммутативна, то коммутант $K(G) \neq \{e\}$. Так как $K(G)$ – нормальная подгруппа в G, то по условию теоремы $K(G) = G$. Следовательно, в цепочке G, $K(G)$, $K_2(G)$, ... все группы совпадают с G и, следовательно, эта цепочка никогда не заканчивается единичной группой, то есть группа G неразрешима. Теорема доказана.

Отметим также следующий результат.

Теорема 2. *Всякая подгруппа разрешимой группы разрешима.*

Доказательство. Пусть группа G разрешима. Тогда существует n, такое, что подгруппа $K_n(G)$ является единичной. Если H – подгруппа группы G, то $K(H)$ содержится в $K(G)$, $K_2(H)$ содержится в $K_2(G)$ и т.д. Тогда $K_n(H)$ содержится в $K_n(G)$ и, следовательно, является единичной группой. Поэтому подгруппа H разрешима. Теорема доказана.

Простой анализ показывает, что знакопеременная группа A_5 степени 5 не содержит нормальных подгрупп, кроме единичной подгруппы и всей группы. Поэтому из теоремы 1 и того факта, что A_5 – некоммутативная группа, следует, что A_5 – неразрешимая группа.

Определение 8. Говорят, что *группа G_1 изоморфна группе G_2*, и записывают это в символах так: $G_1 \cong G_2$, если существует отображение φ: $G_1 \longrightarrow G_2$, обладающее следующими двумя свойствами:

1) φ – взаимно однозначное отображение;

2) $\varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2)$ для всех $a_1, a_2 \in G_1$.

С точки зрения теории групп изоморфные группы обладают одними и теми же свойствами, и поэтому в теории групп изоморфные группы не различаются.

Легко видеть, что группа S_n при $n \geq 5$ содержит подгруппу, изоморфную группе A_5. В самом деле, такой подгруппой является, например, подгруппа, содержащая все подстановки вида

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \ldots & n \\ i_1 & i_2 & i_3 & i_4 & i_5 & 6 & \ldots & n \end{pmatrix}$$

с четным числом инверсий в строке i_1, i_2, i_3, i_4, i_5.

Из этого факта и теорем 1 и 2 следует результат, на котором основано утверждение о неразрешимости алгебраических уравнений степени $n \geq 5$ в радикалах.

Теорема 3. *При $n \geq 5$ группа S_n неразрешима.*

АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ n-Й СТЕПЕНИ. КОМПЛЕКСНЫЕ ЧИСЛА

Алгебраическим уравнением с одним неизвестным степени n называется уравнение вида

$$b_0x^n + b_1x^{n-1} + \ldots + b_{n-1}x + b_n = 0, \qquad (1)$$

где $b_0, b_1, \ldots, b_n$ – коэффициенты этого уравнения, причем $b_0 \neq 0$.

Если предположить, что все коэффициенты уравнения (1) – вещественные числа, и попытаться искать решение уравнения (1) во множестве вещественных чисел, то хорошо известно, что эта попытка окажется неудачной. Так, например, уравнение $x^2 + 1 = 0$ не имеет действительных корней. Попытка найти решение этого уравнения в более широком множестве, чем множество вещественных чисел, приводит к понятию комплексного числа. Перейдем к определению этого понятия.

Рассмотрим всевозможные упорядоченные пары действительных чисел, то есть пары вида (a, b), где a и

b – действительные числа. На множестве таких пар определим две операции – сложение и умножение:

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Определение 9. Множество всевозможных упорядоченных пар действительных чисел с указанными выше операциями сложения и умножения называется *множеством комплексных чисел.*

Положим $i = (0, 1)$ и отождествим пару $(a, 0)$ с действительным числом a. Тогда $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1)$, что позволяет записать комплексное число (a, b) в виде $a + bi$. Эта форма записи комплексного числа называется алгебраической и является одной из наиболее часто используемых.

Если на плоскости зафиксировать некоторую прямоугольную систему координат, то каждое комплексное число $a + bi$ можно отождествить с точкой этой плоскости с координатами (a, b). Если произведено такое отождествление, то такая плоскость называется комплексной плоскостью.

Далее отметим, что во множестве комплексных чисел определены не только операции сложения и умножения, но и обратные к ним операции вычитания и деления на числа, отличные от нуля.

Следующая теорема и обусловливает в значительной степени то значение, которое имеют комплексные числа в математике.

Теорема 4. *Всякое алгебраическое уравнение, то есть уравнение вида*

$$b_0 z^n + b_1 z^{n-1} + \ldots + b_{n-1} z = a, \qquad (2)$$

где a и все b_i – комплексные числа, $n \geq 1$ и $b_0 \neq 0$, имеет по крайней мере одно решение во множестве комплексных чисел.

Эта теорема иногда называется основной теоремой алгебры комплексных чисел. Она была доказана в 1799 году немецким математиком К.Ф. Гауссом.

На самом деле, из теоремы 4 несложно следует, что уравнение (2) имеет n решений, среди которых, правда, могут быть повторяющиеся. Однако имеется только конечное число комплексных чисел a, для которых уравнение (2) имеет повторяющиеся решения. Для всех остальных значений a уравнение (2) имеет n различных решений $z_1, z_2, \ldots, z_n$.

ГРУППА ГАЛУА МНОГОЗНАЧНОЙ ФУНКЦИИ

Рассмотрим следующую многозначную функцию: каждой точке a поставим в соответствие $z(a)$ – множество решений уравнения (2). Мы уже знаем, что если коэффициенты $b_0, b_1, \ldots, b_{n-1}$ фиксированы, то $z(a)$ состоит ровно из n различных комплексных чисел $z_1(a), z_2(a), \ldots, z_n(a)$ для всех комплексных чисел a, за исключением конечного числа таких чисел. В этом конечном множестве "плохих" чисел a функция $z(a)$ имеет меньше, чем n значений.

Итак, пусть $z(a)$ – многозначная функция, рассмотренная выше. Зафиксируем в некоторой точке a_0 одно из значений z_i функции $z(a_0)$, и пусть C – непрерывная кривая, идущая из точки a_0 в некоторую точку a_1 (рис. 1). Будем двигаться по кривой C, выбирая для каждой точки a, лежащей на C, одно из значений функции $z(a)$ так, чтобы выбираемые значения изменялись непрерывно при движении точки a по кривой C, начиная со значения z_i. При этом, когда мы достигнем точки a_1, получим вполне определенное значение $w_i \in z(a_1)$. Скажем, что w_i – значение $z(a_1)$, определенное по непрерывности вдоль кривой C при условии исходного выбора $z_i \in z(a_0)$. Если таким образом выбрать значения функции $z(a)$ для всех точек кривой C и затем изобразить на плоскости z, то должна получиться непрерывная кривая, которая начинается в точке z_i и оканчивается в точке w_i. Эта кривая является одним из непрерывных образов кривой C при отображении $z = z(a)$.

В действительности при определении такой однозначной ветви многозначной функции мы можем столкнуться с такой неприятностью, что в некоторых точках нарушается однозначность выбора образа для функции $z(a)$. Точки, в которых нарушается однозначность выбора непрерывных образов кривых, будем называть точками неоднозначности данной функции. Ниже мы будем рассматривать для данной функции только те кривые, которые не проходят через эти точки неоднозначности данной функции.

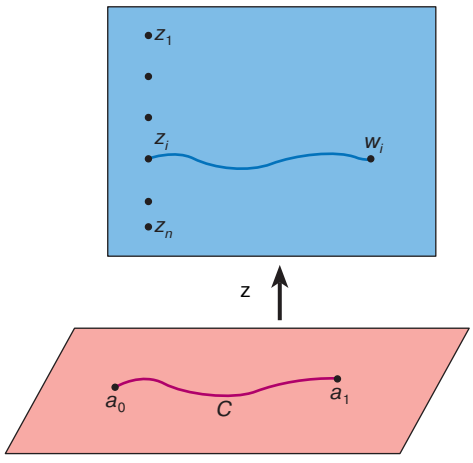

Рис. 1

Итак, пусть точка a_0 не является точкой неоднозначности многозначной функции $z(a)$ и пусть $z_1, z_2, ..., z_n$ – все значения функции $z(a)$ в точке a_0. Рассмотрим некоторую непрерывную кривую C, начинающуюся и кончающуюся в точке a_0 и не проходящую через точки неоднозначности функции $z(a)$. Если для каждого значения $z_i \in z(a_0)$ определим новое значение $z_{i_k} \in z(a_0)$ по непрерывности вдоль кривой C, то при этой конструкции разным значениям z_i отвечают различные значения z_j (рис. 2).

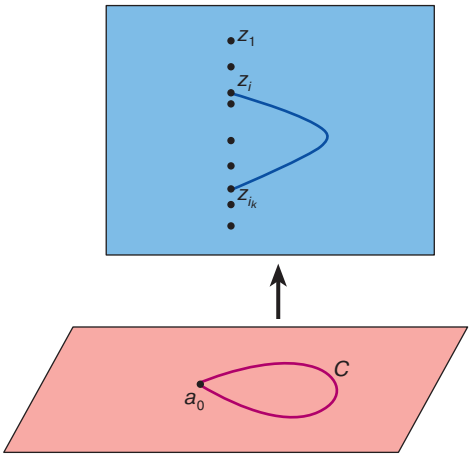

Рис. 2

Таким образом, кривой C соответствует некоторая подстановка

$$\begin{pmatrix} 1 & 2 & ... & i & ... & n \\ i_1 & i_2 & ... & i_k & ... & i_n \end{pmatrix},$$

определяемая преобразованиями значений $z_1, z_2, ..., z_n$. При этом если кривой C соответствует подстановка g, то кривой C^{-1} соответствует подстановка g^{-1}, и если кривым C_1 и C_2 (с концами в точке a_0) соответствуют подстановки g_1 и g_2, то кривой C_1C_2 соответствует подстановка $g_2\, g_1$.

Таким образом, если рассмотреть всевозможные кривые, начинающиеся и кончающиеся в точке a_0, то соответствующие им подстановки будут образовывать некоторую группу подстановок значений $z(a_0)$.

Можно показать, что группы подстановок значений $z(a_0)$ для всех точек a_0, для которых она определена, изоморфны между собой и являются фактически одной и той же группой. Эту группу будем называть группой Галуа многозначной функции $z(a)$.

Говорят, что многозначная функция $h(z)$ выражается в радикалах, если она может быть получена из функции $f(z) = z$ и постоянных функций $g(z) \equiv c$ (c – произвольное фиксированное комплексное число) с помощью операций сложения, вычитания, умножения, деления, возведения в натуральную степень и извлечения корней натуральной степени.

Оказывается, имеет место следующий фундаментальный в этой теории факт:

Теорема 5. *Если многозначная функция $h(z)$ выражается в радикалах, то группа Галуа функции $h(z)$ разрешима.*

ТЕОРЕМА АБЕЛЯ

Рассмотрим уравнение

$$3z^5 - 25z^3 + 60z - a = 0. \qquad (3)$$

Будем считать, что в этом уравнении a является параметром, и для каждого комплексного значения a будем искать все комплексные корни $z(a)$ этого уравнения. Мы уже знаем, что уравнение (3) (как и каждое уравнение 5-й степени) имеет пять корней, некоторые из которых могут совпадать.

Несложно убедиться, что повторяющиеся корни уравнения (3) могут быть лишь для $a = \pm 38$ и $a = \pm 16$, при остальных значениях a функция $z(a)$ принимает пять различных значений. Таким образом, группа подстановок значений $z(a)$ является подгруппой группы S_5. На самом деле оказывается, она совпадает со всей группой S_5!

Итак, группа Галуа для функции $z(a)$, соответствующей уравнению (3), – это группа S_5 всех подстановок 5-й степени, которая неразрешима. Таким образом, функция $z(a)$ не выражается в радикалах, поскольку в противном случае соответствующая ей группа Галуа должна быть разрешимой.

Далее, рассматривая уравнение

$$(3z^5 - 25z^3 + 60z - a)z^{n-5} = 0, \qquad n > 5, \qquad (4)$$

и замечая, что группа Галуа для функции $z_1(a)$, соответствующей левой части уравнения (4), совпадает с группой Галуа, соответствующей функции $z(a)$, выражающей корни уравнения (3) через параметр a, то есть с группой S_5 всех перестановок 5-й степени, которая неразрешима, делаем также заключение, что функция $z_1(a)$ не выражается в радикалах.

Отсюда следует

Теорема Абеля. *При $n \geq 5$ общее алгебраическое уравнение степени n*

$$b_0z^n + b_1z^{n-1} + ... + b_{n-1}z + b_n = 0, \qquad b_0 \neq 0,$$

с комплексными коэффициентами, неразрешимо в радикалах, то есть не существует формулы, выражающей корни этого уравнения через коэффициенты с помощью операций сложения, вычитания, умножения, деления, возведения в натуральную степень и извлечения корней натуральной степени.

В самом деле, если бы такая формула существовала, то, подставив в нее коэффициенты уравнения (3) для $n = 5$ или коэффициенты уравнения (4) для $n > 5$, мы получили бы, что в первом случае функция $z(a)$, а во втором случае функция $z_1(a)$ выражались бы в радикалах, что, как мы выяснили выше, невозможно.

Тем читателям, которые заинтересовались материалом, изложенным в данной статье, рекомендуем продолжить знакомство с этой тематикой по книгам [1–3].

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. *Алексеев В.Б.* Теорема Абеля в задачах и решениях. М.: Наука, 1976. 208 с.

2. *Постников М.М.* Теория Галуа. М.: Физматгиз, 1963. 124 с.

3. *Чеботарев Н.Г.* Основы теории Галуа. М.: ОНТИ–ГТТИ, 1934. 221 с.

Рецензент статьи И.Б. Симоненко

* * *

Виктор Григорьевич Звягин, доктор физико-математических наук, профессор, зав. кафедрой алгебры и топологических методов анализа Воронежского государственного университета. Область научных интересов – нелинейный функциональный анализ, топологические и алгебраические методы анализа и их приложения к нелинейным проблемам уравнений в частных производных. Автор более 100 научных статей в отечественных и зарубежных журналах.