



# ГАЛУА́ ТЕО́РИЯ

Авторы: Л. В. Кузьмин

ГАЛУА́ ТЕО́РИЯ, созданная Э. [Галуа](#) теория алгебраич. уравнений высших степеней с одним неизвестным, т. е. уравнений вида

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a^1x + a_0 = 0,$$

основанная на изучении групп перестановок их корней.

Уравнения 2-й, 3-й и 4-й степеней разрешимы в радикалах. Формула  $x = -p/2 \pm \sqrt{p^2/4 - q}$  для решения уравнения  $x^2 + px + q = 0$  была известна в глубокой древности. Методы решения уравнений 3-й и 4-й степеней были найдены в 16 в. Для уравнения 3-й степени вида  $x^3 + px + q = 0$ , к которому можно привести всякое уравнение 3-й степени, решение даётся т. н. формулой Кардано

$$x = \sqrt[3]{-q/2 + \sqrt{q^2/4 + p^3/27}} + \sqrt[3]{-q/2 - \sqrt{q^2/4 + p^3/27}}.$$

Метод решения в радикалах уравнений 4-й степени был предложен Л. [Феррари](#), оба результата были опубликованы Дж. [Кардано](#) в 1545.

В 16–18 вв. предпринимались попытки найти аналогичные формулы для уравнений 5-й и более высоких степеней. Над этим работали Э. [Безу](#) и Ж. [Лагранж](#). В 1801 К. [Гаусс](#) создал полную теорию решения в радикалах двучленного уравнения вида  $x^n = 1$ , называемого уравнением деления круга; он указал условия для того, чтобы уравнение  $x^n = 1$  решалось в квадратных радикалах. Последняя задача заключалась в отыскании правильных  $n$ -угольников, которые можно построить при помощи циркуля и линейки. Такими оказываются  $n$ -угольники при  $n = 2^m$  и  $n = 2^m p_1 \dots p_k$ , где  $m = 0, 1, 2, \dots$ , а  $p_1, \dots, p_k, k = 1, 2, \dots$ , – разл. гауссовы простые числа, т. е. простые числа вида  $4s + 1, s = 0, 1, 2, \dots$  (см. [Многоугольник](#)). В 1824 Н. [Абель](#) доказал, что общее уравнение 5-й степени (и тем более общие уравнения более высоких степеней) не решается в радикалах. С др. стороны, Абель дал решение в радикалах для одного класса уравнений, содержащего уравнения произвольно высоких степеней, – т. н. абелевых уравнений.

Таким образом, когда Галуа начал свои исследования, в теории алгебраич. уравнений были получены важные результаты, но общей теории, охватывающей все возможные уравнения высоких степеней, ещё не было создано. Нужно было установить необходимые и достаточные условия, которым должно удовлетворять уравнение (1) для того, чтобы оно решалось в радикалах; выяснить, каковы необходимые и достаточные условия для того, чтобы уравнение (1) сводилось к цепи квадратных уравнений, т. е. чтобы корни уравнения (1) можно было построить геометрически с помощью циркуля и линейки. Все эти вопросы Галуа решил в «Мемуаре об условиях разрешимости уравнений в радикалах», найденном в его бумагах после смерти и впервые опубликованном Ж. [Лиувиллем](#) в 1846. Условия разрешимости уравнения (1) в радикалах сформулированы Галуа в терминах [групп теории](#).

Чтобы сформулировать осн. результаты Г. т., рассмотрим некоторое поле  $k$ , содержащее все коэффициенты многочлена  $f(x)$ . Любое поле  $K$ , содержащее  $k$ , называется расширением  $k$  (обозначение  $K/k$ ). Его степень называется размерность  $K$  как линейного векторного пространства над  $k$ . Если эта размерность конечна, то расширение называется конечным. Поле  $K = k(\alpha_1, \dots, \alpha_n)$ , где  $\alpha_1, \dots, \alpha_n$  – все корни уравнения (1), т. е. минимальное расширение  $k$ , в котором  $f(x)$  разлагается в произведение линейных множителей,  $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ , называется полем разложения многочлена  $f(x)$  и является конечным расширением  $k$ . Если  $K$  – поле разложения сепарабельного многочлена, т. е. многочлена, неприводимые множители которого не имеют кратных корней, то  $K/k$  называется расширением Галуа. Такому расширению сопоставляется группа Галуа  $G(K/k)$ , называемая также группой Галуа многочлена  $f$ , состоящая из всех автоморфизмов, т. е. изоморфизмов поля  $K$  на себя, оставляющих неподвижными все элементы  $k$ . Порядок этой группы равен степени расширения  $K/k$ . Любой её элемент определяет некоторую подстановку корней  $\alpha_1, \dots, \alpha_n$  многочлена  $f$ , поэтому  $G(K/k)$  можно рассматривать как подгруппу симметрич. группы  $S_n$  перестановок  $n$  элементов. Осн. теорема Г. т. утверждает, что существует взаимно однозначное соответствие (соответствие Галуа) между всеми промежуточными подполями расширения  $K/k$  и всеми подгруппами группы  $G(K/k)$ . Г. т. даёт необходимые и достаточные условия разрешимости уравнения (1) в радикалах, т. е. оно разрешимо в радикалах тогда и только тогда, когда его группа Галуа разрешима. В частности, теорема Абеля связана с тем, что общее уравнение (1) имеет в качестве группы Галуа симметрич. группу  $S_n$ , которая неразрешима при  $n \geq 5$ . Другое приложение Г. т. – это полное решение идущей из античности задачи о построении циркулем и линейкой.

В Г. т. большое значение имеет обратная задача, состоящая в построении расширения Галуа  $K/k$  с заданной группой Галуа  $G$ . Существует гипотеза о том, что для поля алгебраич. чисел  $k$  обратная задача разрешима для любой конечной группы  $G$ ; доказано это только для симметрических, знакопеременных и некоторых типов простых групп. И. Р. [Шафаревич](#) доказал (1954), что над любым полем алгебраич. чисел существует бесконечно много расширений с заданной разрешимой группой Галуа. Понятия и методы Г. т. широко используются в алгебраич. теории чисел и алгебраич. геометрии. Для некоторых типов полей  $k$ , включающих поля алгебраич. чисел, существует теория (теория полей классов), дающая обзор всех абелевых расширений поля  $k$  (расширений с абелевой группой Галуа).

## Литература

Лит.: Галуа Э. Соч. М.; Л., 1936; Бурбаки Н. Алгебра. Многочлены и поля. Упорядоченные группы. М., 1965; Ленг С. Алгебраические числа. М., 1966; он же. Алгебра. М., 1968; Серр Ж. П. Когомологии Галуа. М., 1968; Artin E. Galois theory. Ann Arbor, 1971; Ван дер Варден Б. Л. Алгебра. М., 1976; Matzat B. Konstruktive Galois theorie. В., 1987; Ишханов В. В., Лурье Б. Б., Фаддеев Д. К. Задача погружения в теории Галуа. М., 1990.