Г.Н. Чеботарев

Основы теории Галуа. Часть 1

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Г11

Г.Н. Чеботарев

Г11 Основы теории Галуа. Часть 1 / Г.Н. Чеботарев – М.: Книга по Требованию, 2017. – 223 с.

ISBN 978-5-458-25761-9

Особенностью предлагаемой книги является возможность не просто ознакомиться с исследуемой теорией, но и проникнуть несравненно глубже детально рассмотреть корни, о которых умалчивается в классическом изложении идеи. Знакомя с основами теории, автор отступает от общепринятого способа определения группы Галуа, введя понятие "функциональных модулей". В книге дается понятие о проблеме построения уравнений с заданными группами, излагаются два метода такого построения. Приводится множество примеров и упражнений для самостоятельной работы читателя. Предназначается для студентов старших курсов, желающих специализироваться по алгебре, аспирантов, а также для математиков-неалгебраистов, желающих познакомиться с основами теории Галуа.

ISBN 978-5-458-25761-9

При изложении основ теории Галуа я отступил от обычного классического способа определения группы Галуа при помощи резольвенты Галуа. Именно, я, следуя примеру Мертенса и Шатуновского, ввел понятие функциональных модулей (глава II, § 4). Мне кажется, что этот путь более соответствует духу теории Галуа и вместе с тем дает возможность непосредственно обозреть все „соотношения между корнями“, которые при классическом изложении оторваны от идеи группы Галуа. Это дает также возможность несравненно легче провести доказательство теоремы 90: „группа сравнения изоморфна с некоторым делителем группы уравнения“.

В тексте решено много примеров, а также дано 47 упражнений для самостоятельной работы читателя. На них читатель убеждается, что нахождение группы Галуа, весьма простое теоретически, на практике достигается путем всевозможных ухищрений, так как иначе необходимые выкладкн были бы непомерио длинны.

Главные приложения современной теории Галуа: связь между арифметической и групповой природой уравнений, а также проблема резольвент, которые требуют знакомства с теорией идеалов и непрерывными группами, будут изложены в дальнейших частях книги.

Н. Чеботарев.

Казань,
31 января 1933 г.

ИСТОРИЧЕСКИЙ ОЧЕРК

1. Под теорией Галуа в ее первом этапе развития разумелась теория, имевшая целью выяснить условия того, чтобы заданное уравнение разрешалось в радикалах. Во всяком случае так понимал ее сам Галуа, который считал основным своим результатом следующий:

> Для того, чтобы заданное уравнение (степень которого есть простое число) решалось в радикалах, необходимо и достаточно, чтобы его корни рационально выражались через любые два из них (см. теорему 69).

2. **Лагранж.** Решение уравнений 3-й и 4-й степени в радикалах было получено еще в XVI столетии. Уравнения 3-й степени решил Тарталья (Tartaglia) [по другим источникам—Кардан (G. Cardano)], 4-й степени — ученик Кардана Феррари (Ferrari). Многочисленные попытки самых блестящих математиков XVII и XVIII столетий—Декарта (R. Descartes), Чирнгаузена (Tschirnhausen), Эйлера (L. Euler), Безу (É. Bézout)—решить эту задачу для уравнений высших степеней—увенчались неудачей.

В 1770—71 гг. знаменитый французский математик Лагранж (Lagrange) публикует в Мемуарах Берлинской Академии свой мемуар „Réflexions sur la résolution algébrique des équations", в котором делает критический пересмотр всех решений уравнений 3-й и 4-й степеней, данных его предшественниками, и замечает, что все они в сущности основаны на следующем принципе. Пусть $x_1, x_2, \ldots, x_n$ будут корни заданного уравнения, и пусть $\varphi(x_1, x_2, \ldots, x_n)$ будет их рациональная функция, принимающая при всевозможных $n!$ перестановках между корнями v значений. Тогда эта функция удовлетворяет уравнению степени v с рациональными коэффициентами. Согласно точке зрения Лагранжа, задача заключается в том, чтобы подобрать функцию $\varphi(x_1, x_2, \ldots, x_n)$ таким образом, чтобы v было меньше n. И вот оказалось, что это при $n > 4$ невозможно. Основной метод, предложенный для этой цели Лагранжем, заключается в следующем. Пусть α будет первообразный корень n-й степени из единицы, т. е. корень уравнения $x^n - 1 = 0$, не удовлетворяющий ни одному уравнению $x^m - 1 = 0$ при $m < n$. Тогда функция

$$(1) \qquad t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{n-1} x_n$$

при подстановке корней, переводящей x_1 в x_2, x_2 в x_3, и т. д., x_{n-1} в x_n, наконец x_n в x_1 (иначе: подстановке, увеличивающей все значки при корнях на 1, если кратности n отбрасывать), приобретает множитель α^{-1}:

$$x_2 + \alpha x_3 + \ldots + \alpha^{n-1} x_1 = \alpha^{-1}(x_1 + \alpha x_2 + \ldots + \alpha^{n-1} x_n),$$

а потому функция $\theta = t^n$ не меняется при производстве упомянутой подстановки:

$$(x_2 + \alpha x_3 + \ldots + \alpha^{n-1}x_1)^n = (x_1 + \alpha x_2 + \ldots + \alpha^{n-1}x_n)^n.$$

Далее Лагранж рассматривает совокупность подстановок (x, ax), заключающихся в умножении каждого значка на одно и то же число a, взаимно простое с n, и отбрасывании кратностей n. Например при $n = 8$ подстановка $(x, 3x)$ переводит x_1 в x_3, x_2 в x_6, x_3 в x_1, x_4 в x_4, x_5 в x_7, x_6 в x_2, x_7 в x_5, x_8 в x_8. Далее он применяет эти подстановки к θ, получает систему функций

$$\theta_1, \theta_2, \ldots, \theta_m \quad [m = \varphi(n)]$$

и составляет уравнение

$$(\theta - \theta_1)(\theta - \theta_2)\ldots(\theta - \theta_m) = 0, \tag{2}$$

коэффициенты которого удовлетворяют уравнениям степени $\frac{n!}{n \cdot m}$. В частности, если n простое число, то эта степень равна $\frac{n!}{n(n-1)} = (n-2)!$ При $n = 3$ $(n-2)! = 1$, так что этот метод дает полное решение уравнения. При $n = 4$ $\frac{n!}{n\,\varphi(n)} = \frac{4!}{4 \cdot 2} = 3$, так что этот метод дает понижение степени. Но уже при $n = 5$ имеет место $(n-2)! = 6$, так что метод никакого понижения степени не дает.

Эти исследования Лагранжа дали для последующих алгебраистов весьма удобный аппарат. Кроме того, они указали путь, по которому следовало искать доказательства невозможности общего решения уравнений в радикалах. Наконец, уравнение (2) оказалось при простом n имеющим рациональные коэффициенты всякий раз, когда исходное уравнение разрешимо в радикалах. Вместе с тем в этом случае уравнение (2) является циклическим и может быть всегда решено при помощи составления величины (1), носящей название резольвенты Лагранжа.

8. Доказательство невозможности. Руффини и Абель. Дальнейшим этапом в выяснении проблемы решения уравнений в радикалах послужили работы Руффини (P. Ruffini, 1765—1822) и Абеля (N.-H. Abel, 1802—1829). Руффини (1799) предложил доказательство неразрешимости в радикалах уравнений 5-й степени, коэффициенты которого являются независимыми переменными. В своем доказательстве он опирался на уже упоминавшееся нами явление, что рациональная функция от корней уравнения 5-й степени, принимающая при всевозможных перестановках корней более двух различных значений, принимает их по крайней мере 5. Этот факт, обобщенный на любое $n \geqslant 5$ и известный под названием теоремы Бертрана (J. Bertrand), приведен у нас в переводе на язык теории групп в качестве теоремы 29.

Доказательство Руффини вызвало длинную полемику, так как оно пользовалось мало очевидным фактом, что в радикальных выражениях корней уравнения каждый радикал может быть выражен, как рациональная функция от всех корней уравнения. Это действительно имеет место при надлежащим образом подобранных радикалах, что может быть например проверено на решении

$$y=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

кубического уравнения

$$y^3+py+q=0,$$

где

$$\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}=\pm\frac{(y_1-y_2)(y_1-y_3)(y_2-y_3)}{6\sqrt{-3}},$$

$$\sqrt[3]{-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}=\frac{y_1}{2}\pm\frac{y_1+2y_2}{2\sqrt{-3}};$$

однако никто не может помешать нам искусственно ввести в радикальные выражения величины, не удовлетворяющие этому требованию. Поэтому доказательство Руффини не может считаться убедительным.

Абель (1826) нашел независимо от Руффини доказательство невозможности общего радикального выражения для корней уравнений выше 4-й степени с переменными коэффициентами. Его доказательство по существу не отличается от доказательства Руффини, но оно дополнено доказательством того, что всякое радикальное выражение корня уравнения всегда можно преобразовать в такое, что каждый входящий в него радикал уже будет выражаться, как рациональная функция от корней уравнения. Таким образом доказательство Абеля убедительно для уравнений, коэффициенты которых являются независимыми переменными, и одновременно делает очевидным несуществование общего радикального выражения для всех уравнений данной степени; но оно не дает никакой возможности судить о разрешимости отдельных численных уравнений.

4. **Галуа.** Вопрос о разрешимости уравнений в радикалах был окончательно разобран, во всяком случае принципиально, в работах Галуа (Évariste Galois, 1811—1832). Личность Галуа представляет собой совершенно исключительное в истории науки явление. Жизнь Галуа, умершего всего на 21 году, протекала крайне бурно. Дважды провалившись на вступительных экзаменах в знаменитую Политехническую школу, Галуа поступил в Подготовительную школу (преобразованную из Высшей нормальной школы во время реакционного правления Карла IX), откуда вскоре после июльского переворота был уволен за печатное выступление против директора школы. После этого Галуа открыл „публичный курс" по алгебре, но политическая жизнь страны быстро вовлекла его в свой водоворот. Имея репутацию ярого республиканца и активного врага Луи-Филиппа, он два раза сидел в тюрьме за политические выступления и в мае 1832 года был убит на дуэли, причины которой остаются до сих пор загадочными.

За свою короткую жизнь Галуа успел создать теорию, которая до сих пор стоит в фокусе математической мысли. Рассматривая численные уравнения, он установил понятие их группы, т. е. совокупности таких подстановок между их корнями, которые не нарушают рациональных соотношений между ними. Эта группа определяет для каждого уравнения алгебраическую структуру его корней. В частности, уравнение разрешимо в радикалах тогда и только тогда, если его группа принадлежит к числу так называемых разрешимых групп (см. теорему 68). Таким образом вопрос о разрешимости каждого данного уравнения в радикалах может быть решен при помощи конечного числа действий.

Исследование всевозможных типов разрешимых групп, начатое самим Галуа, было продолжено работами большого числа математиков, из которых можно назвать Жордана (C. Jordan), Бетти (Betti), О. Ю. Шмидта. Фундаментальный труд Жордана „Traité des substitutions" (Paris, 1870) содержит богатый материал для детального изучения групп, в частности для исследования типов разрешимых групп. Вместе с тем эта книга дает немало приложений теории групп к другим областям математики, например к алгебраическим функциям (группы монодромии), к эллиптическим и модулярным функциям, и т. п.

5. **Клейн и Ли.** Ли (S. Lie) и Клейн (F. Klein), занимаясь в Париже под руководством Жордана, пришли к мысли о группах другой природы, непрерывных группах. Ли положил начало их общей теории и приложил их к дифференциальным уравнениям, руководясь теми же принципами, которые лежат в основе приложения конечных групп к алгебраическим уравнениям, составляющего сущность теории Галуа. При этом интегрируемые системы дифференциальных уравнений соответствуют так называемым интегрируемым группам, структура которых аналогична структуре разрешимых конечных групп.

Клейн положил непрерывные группы в основу классификации различных геометрий: элементарной, проективной, шаровой и т. п. Этим он указал в математике место геометрии, задачи которой были сведены методами аналитической геометрии к задачам анализа, и привел „чисто геометрические" вопросы к изучению свойств непрерывных групп.

6. **Построения при помощи циркуля и линейки.** Идея приложения групп к уравнениям имеет настолько всеобщий характер, что сфера ее применения не могла ограничиться сравнительно узким вопросом о разрешимости уравнений в радикалах. Поэтому вскоре же оказалось, что методы теории Галуа могут быть применены и к другим вопросам, которые приводятся к алгебраическим уравнениям. Например, вопросы о построениях при помощи циркуля и линейки приводятся к вопросу, может ли заданное уравнение быть решено при помощи извлечений квадратных корней, и потому могут быть решены с помощью теории Галуа.

Таким путем была доказана невозможность деления произвольного угла посредством циркуля и линейки на нечетное число частей и тем самым обнаружена бесплодность многочисленных попыток решить задачу „трисекции угла". Вопрос о делении окружности на несколько равных частей был, правда, решен Гауссом (C. F. Gauss) до Галуа. Гаусс показал, что при помощи циркуля и линейки можно делить окружность на числа m типа

$$m = 2^{\lambda} \cdot p \cdot p' \cdot p'' \ldots,$$

где p, p', p'', ... простые числа вида $1+2^s$. Однако только благодаря теории Галуа появилась уверенность в невозможности задачи для других случаев.

7. Теория Галуа и алгебраические числа. Особенно глубокие приложения теории Галуа допускает теория чисел. Вопрос об арифметической природе корней уравнения, как выяснилось, тесно связан со структурой его группы Галуа. Вот первый результат в этом направлении:

> Корни всякого уравнения с абелевой группой Галуа в поле рациональных чисел, как области рациональности, рационально выражаются через некоторые корни из единицы,

который был предугадан Кронекером (L. Kronecker) и впервые строго доказан Вебером (H. Weber). В настоящее время существует около десяти различных доказательств этой теоремы.

Кронекер задался дальнейшим вопросом об уравнениях с абелевой группой в области рациональности, образованной мнимыми корнями квадратного уравнения. Оказалось, что такого рода величины получаются, как значения эллиптических функций, допускающих так называемое *комплексное умножение*. Кронекер предположил, что эти значения дадут корни всех возможных абелевых уравнений в рассматриваемой области рациональности („Jugendtraum"—мечта юности). Это предположение удалось в общем доказать Фуэтеру (R. Fueter), причем оказался один исключительный случай, не включающийся в эти значения.

Исследуя арифметические законы комплексного умножения, Фуэтер пришел к общим законам, имеющим место для уравнений, абелевых в произвольной области рациональности. Эти законы позволяют рассматривать поле корней таких уравнений, как обобщение так наз. Klassenkörper, и связывают степень этих уравнений с *числом идеальных классов* в рассматриваемой области рациональности. Здесь вскрывается глубокая связь между теорией Галуа и теорией *идеалов*, которые являются основным инструментом в теории алгебраических чисел.

Такаги (T. Takagi) дал законченный вывод упомянутых законов.

8. Связь уравнений со сравнениями. В тесной связи с упомянутыми законами стоит закон, открытый Дедекиндом (R. Dedekind), Фробениусом (G. Frobenius) и Гурвицем (A. Hurwitz) и в своей элементарной части могущий быть формулирован так:

> Дан полином $f(x)$. Рассматривая его по модулю некоторого простого числа p (т. е. имея право прибавлять к его коэффициентам кратности p), разложим его на неприводимые множители. Пусть
>
> (3) $$f(x) \equiv f_1(x) \cdot f_2(x) \ldots f_k(x) \pmod p,$$
>
> где $f_1(x)$, $f_2(x)$, ..., $f_k(x)$ неприводимые по модулю p полиномы степеней n_1, n_2, ..., n_k. Тогда группа Галуа уравнения $f(x)=0$ содержит подстановку, состоящую из циклов порядков n_1, n_2, ..., n_k.

Обратно, если группа Галуа уравнения $f(x)=0$ содержит подстановку, состоящую из циклов порядков n_1, n_2, ..., n_k, то существует бесчисленное множество таких простых чисел, для которых имеет место разложение (3) (Фробениус).

Кроме своих приложений в теории алгебраических чисел, эта теорема позволяет устанавливать общие критерии для нахождения группы отдельных классов уравнений, а также устанавливать тождество двух заданных полей. Ее неудобство состоит в том, что в ней приходится иметь дело с бесконечным множеством простых чисел.

9. Только что упомянутым неудобством не обладает другой закон, который однако труднее формулировать и который допускает в особых („не-регулярных") случаях большие осложнения. Этот закон касается так называемых критических простых чисел, которые впервые были тщательно изучены Гильбертом (D. Hilbert) в связи с теорией идеалов („Trägheitsgruppen"—группы инерции), но допускают также элементарное определение, если мы вместе с Гензелем (K. Hensel) станем рассматривать разложения алгебраических чисел по возрастающим степеням простого числа. Исходя из аналогии с алгебраическими функциями, где критическим значением переменной z называется значение $z = a$, в окрестности которого функция разлагается по дробным степеням, Гензель рассматривает так называемые p-адические разложения алгебраических чисел (см. гл. II, § 3.3). Простое число такого рода, что заданное алгебраическое число разлагается по его дробным степеням, носит название критического. Критические числа всегда входят в дискриминант уравнения, которому удовлетворяет рассматриваемое алгебраическое число, а потому каждому алгебраическому числу соответствует конечное число критических простых чисел. С другой стороны, каждому иррациональному алгебраическому числу непременно соответствует хотя бы одно критическое простое число.

Каждое алгебраическое число степени n имеет n сопряженных разложений по степеням каждого простого числа p. Если p — критическое простое число для алгебраического числа a, которое разлагается по степеням $p^{\frac{1}{s}}$, то существует s сопряженных разложений, которые, как мы будем говорить, образуют s-членный цикл. Тогда закон, о котором мы говорим, может быть формулирован так:

Если разложения числа a в p-адические ряды разбиваются на циклы порядков $s_1, s_2, \ldots, s_k$, то существует подстановка группы Галуа уравнения, которому удовлетворяет a, состоящая из циклов порядков $s_1, s_2, \ldots, s_k$.

Обратно, в группе Галуа можно выбрать несколько подстановок, цикленный состав которых задается разложениями по степеням критических простых чисел, и которые при композиции воспроизводят всю группу Галуа.

Если, например, группа Галуа уравнения p^k-ой степени циклическая, то должно существовать такое критическое простое число, разложения по степеням которого корней этого уравнения образуют p^k-членный цикл.

10. **Построение уравнений с заданной группой.** Перейдем теперь к некоторым проблемам, стоящим на очереди в современной теории Галуа.

Проблема I. Найти прием для построения уравнений, группы Галуа которых изоморфны с заданной группой $\mathfrak{G}$.

Эта проблема была решена Гильбертом для случая, когда группа $\mathfrak{G}$ есть симметрическая или знакопеременная группа. Возможность такого построения Гильберт основывает на своей следующей „теореме неприводимости":

Если полином $f(x, y)$ от двух переменых x, y неприводим, то можно найти бесконечное множество рациональных значений $y = a$ такого рода, что полином $f(x, a)$ остается неприводимым относительно одного x в любой заданной области рациональности.

Эта теорема является типичной „теоремой существования“, а потому основанный на ней способ построения не может считаться эффективным, т. е. приводящим к цели при помощи конечного числа действий.

Бауэр (M. Bauer), пользуясь законами, описанными в п.п. 9 и 8, предложил два новых различных приема для построения уравнений с симметрической группой. Его приемы дают эффективные решения; с другой стороны, его второй способ (основанный на п. 8), будучи достаточно продолжен, дает все без пропусков существующие уравнения без аффекта.

Э. Нётер (E. Noether) показала, что проблема I может быть решена для таких групп $\mathfrak{G}$, для которых справедлива следующая теорема:

Пусть $A_1, A_2, \ldots, A_n$ элементарно-симметрические функции от переменных $x_1, x_2, \ldots, x_n$ и $\Phi(x_1, x_2, \ldots, x_n)$ функция, принадлежащая к заданной группе $\mathfrak{G}$. Тогда существует n функций

$$\pi_1, \pi_2, \ldots, \pi_n$$

такого рода, что они рационально выражаются через $A_1, A_2, \ldots, A_n$, Φ, и обратно, каждая из функций $A_1, A_2, \ldots, A_n$, Φ может быть рационально выражена через $\pi_1, \pi_2, \ldots, \pi_n$.

Эта теорема (называемая теоремой Люрота (P. Lüroth) или теоремой о рациональном базисе) справедлива для $n = 1$ и $n = 2$; для $n = 3$ она уже не имеет места в общем случае.

Нётер строит свой результат на Гильбертовой теореме неприводимости. Однако можно построить его на втором приеме Бауэра, чем обеспечивается эффективность приема построения.

Фуртвенглер (Ph. Furtwängler) и Бройер (S. Breuer) предложили приемы построения уравнений, имеющих разрешимые группы некоторых типов.

И. Шур (I. Schur) нашел, что некоторые хорошо известные полиномы имеют симметрическую или знакопеременную группу. Этим путем ему удалось эффективно решить проблему I для знакопеременных групп, за исключением случаев, когда $n = 8k + 2$.

11. **Проблема резольвент.** Как мы видели, задача решения уравнений в радикалах допускает положительный ответ лишь в сравнительно немногих исключительных случаях. Поэтому является естественным найти такое обобщение этой задачи, которое бы включало решение в радикалах, как частный случай, и вместе с тем имело бы виды на практическое значение. Такой задачей безусловно является проблема, которую можно формулировать так:

Проблема II. Дано уравнение

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0 \tag{4}$$

с переменными коэффициентами $a_1, a_2, \ldots, a_n$. Требуется найти для него такое рациональное преобразование, чтобы преобразованное уравнение зависело от возможно меньшего числа k параметров.

В коэффициенты преобразования можно при необходимости вводить иррациональности, зависящие от уравнений с меньшим числом переменных параметров. Задача например допускает более низкое значение для k, если ввести квадратный корень из дискриминанта D уравнения (4), так как тогда группа Галуа уравнения (4) понижается с симметрической до знакопеременной.

Бринг (Bring) привел общее уравнение 5-ой степени при помощи преобразований, в выражения которых входят иррациональности не выше 4-ой степени, к так называемому Бринг-Жерраровскому типу

$$x^5 + \alpha x + \beta = 0, \tag{5}$$

которое путем простого преобразования $x = \sqrt[4]{\alpha} \cdot y$ превращается в однопараметрическое.

Клейн перешел от общего уравнения 5-й степени к однопараметрическому, вводя в коэффициенты преобразования только квадратичные иррациональности. Его приведенное уравнение имеет вид

$$y^6 + 15 y^4 - 10\gamma \cdot y^2 + 3\gamma^2 = 0, \tag{6}$$

причем в коэффициенты преобразования входят только иррациональности $\sqrt{D}$, $\sqrt{-3}$ и $\sqrt{5}$.

Клейн поставил в общем виде так называемую „Formenproblem", которая по существу приводится к нашей проблеме II. Оказывается, что решение этой проблемы зависит от группы уравнения (4). Именно, вопрос приводится к представлению элементов группы аналитическими преобразованиями от возможно меньшего числа k переменных. Например для уравнения 5-й степени знакопеременная группа может быть представлена, как группа дробных линейных преобразований:

$$z \to \frac{az+b}{cz+d}$$

одной комплексной переменной z. В связи с этим общее уравнение 5-й степени и допускает резольвенту (6) с одним переменным параметром.

Гильберт обобщил задачу, ставя себе целью привести общее уравнение n-ой степени к нескольким уравнениям, каждое из которых содержит возможно меньшее число k параметров. При этом он получил для каждого $n \leqslant 9$ следующие значения k:

n	5	6	7	8	9
$k \leqslant$	1	2	3	4	4

Виман (A. Wiman), обобщая результат Гильберта, получил, что при всяком $n \geqslant 9$ имеет место $n - k \geqslant 5$.

Эта проблема ставит на очередь вопрос о нахождении всевозможных непрерывных групп, имеющих данную конечную группу в качестве подгруппы („одевание конечных групп непрерывными").