2004 г. июль — август *т. 59, вып. 4(358)*

УСПЕХИ МАТЕМАТИЧЕСКИХ НАУК

УДК 512.623.3+517.547.59

Памяти Андрея Андреевича Болибруха

О РАЗРЕШИМОСТИ И НЕРАЗРЕШИМОСТИ УРАВНЕНИЙ В ЯВНОМ ВИДЕ

А. Г. Хованский

В обзоре обсуждаются классические результаты Абеля, Лиувилля, Галуа, Пикара, Вессио, Колчина и др. о разрешимости и неразрешимости уравнений в явном виде. Подробно излагается одномерный топологический вариант теории Галуа, описывающий топологические препятствия для представимости функций в квадратурах.

Библиография: 37 названий.

СОДЕРЖАНИЕ

Многочисленные неудачные попытки решения ряда алгебраических и дифференциальных уравнений "в явном виде" привели математиков к убеждению, что явных решений для этих уравнений просто не существует. Настоящий обзор посвящен вопросу о неразрешимости уравнений в явном виде. Этот вопрос имеет богатую историю.

Первые доказательства неразрешимости алгебраических уравнений в радикалах были найдены Абелем и Галуа. Обдумывая задачу о нахождении в явном виде неопределенного интеграла от алгебраической дифференциальной формы, Абель заложил основы теории алгебраических кривых. Лиувилль продолжил работы Абеля и доказал неэлементарность неопределенных интегралов многих алгебраических и элементарных дифференциальных форм. Неразрешимость в квадратурах ряда линейных дифференциальных уравнений тоже впервые была доказана Лиувиллем.

Еще Галуа связал вопрос о разрешимости в радикалах со свойствами некоторой конечной группы (так называемой группы Галуа алгебраического уравнения). Собственно, само понятие конечной группы было введено Галуа именно в связи с этим вопросом. Софус Ли ввел понятие непрерывной группы преобразований, пытаясь явно решать дифференциальные уравнения и приводить их к более простому виду. Пикар с каждым линейным дифференциальным уравнением связал его группу Галуа, которая является группой Ли (и, более того, является алгебраической матричной группой). Пикар и Вессио показали, что именно эта группа отвечает за разрешимость уравнений в квадратурах. Колчин развил теорию алгебраических групп и придал теории Пикара–Вессио законченный вид.

Арнольд обнаружил, что ряд классических вопросов математики неразрешимы из-за топологических причин. В частности, он показал, что общее алгебраическое уравнение степени $\geqslant 5$ не решается в радикалах именно по топологическим причинам. Я бесконечно признателен Владимиру Игоревичу за то, что он заинтересовал меня этой тематикой. Развивая подход Арнольда, в начале семидесятых годов я построил своеобразный одномерный топологический вариант теории Галуа. Согласно этой теории топология расположения римановой поверхности аналитической функции над плоскостью комплексного переменного может препятствовать представимости этой функции при помощи явных формул. На этом пути получаются наиболее сильные из известных результатов о непредставимости функций явными формулами. Недавно мне удалось обобщить эти топологические результаты на случай многих переменных.

Работа выполнена при частичной поддержке гранта OGP 0156833 (Канада).

В обзоре дается полное изложение одномерного топологического варианта теории Галуа. Этот вариант тесно связан как с обычной теорией Галуа, так и с теорией Пикара–Вессио. Конечно, полностью изложить эти классические теории в статье невозможно. Основные теоремы этих теорий формулируются без доказательств, зато подробно объясняется, почему эти теории в принципе отвечают на вопросы о разрешимости алгебрических уравнений в радикалах и о разрешимости линейных дифференциальных уравнений в квадратурах. В обзоре обсуждается также красивое построение Лиувилля класса элементарных функций, класса функций, представимых в квадратурах, и т. д. и его теория, оказавшая большое влияние на все дальнейшие работы в этой области.

Итак, в работе идет речь о трех вариантах теории Галуа – обычном, дифференциальном и топологическом. Эти варианты объединяет общий подход к задачам о разрешимости и неразрешимости уравнений, основанный на теории групп. Неверно, однако, что все результаты о разрешимости и неразрешимости связаны с теорией групп. Ряд ярких результатов, основанных на другом подходе, содержится в теории Лиувилля.

В обзоре не всегда соблюдается историческая последовательность. Например, теорема Пикара–Вессио о разрешимости линейных дифференциальных уравнений в квадратурах была доказана раньше, чем основная теорема дифференциальной теории Галуа. Однако теорема Пикара–Вессио является прямым следствием этой основной теоремы, и именно так она представляется в настоящем обзоре.

Несколько слов о литературе. Изложение метода Лиувилля и близких работ Чебышёва, Мордухай-Болтовского и др. можно найти в замечательной книге [33]. Обычная теория Галуа хорошо излагается во многих местах. Короткое и ясное изложение дифференциальной теории Галуа содержится в [17]. Интересный обзор работ о разрешимости и неразрешимости уравнений вместе с обширной библиографией можно найти в [36].

В свое время я не опубликовал полное изложение одномерного топологического варианта теории Галуа: сначала я не мог разобраться в сложной истории предмета, а потом занялся совсем другой математикой. Много лет спустя Андрей Болибрух попросил меня вернуться к этой теме и подготовить работу для публикации в своем новом журнале. Часть работы была подготовлена тогда же [22]. Здесь работа излагается полностью, обсуждаются ее взаимосвязи с классическими вариантами теории Галуа, приводится новая постановка задачи, необходимая для построения многомерного варианта теории. Без вмешательства Болибруха, скорее всего, одномерный вариант так и не был бы подготовлен к публикации, а многомерный вариант не был бы найден. Я признателен моей жене Т. В. Белокриницкой за помощь при подготовке этого обзора.

Этот обзор посвящается памяти Андрея Андреевича Болибруха – замечательного человека и первоклассного математика.

§ 1. Постановка задачи о разрешимости уравнений в конечном виде

Некоторые алгебраические и дифференциальные уравнения “решаются явно”. Что это значит? Если решение предъявлено, оно само и дает ответ на этот вопрос. Обычно все же попытки явного решения уравнений оказываются безуспешными. Возникает желание доказать, что для тех или иных уравнений явных решений не существует. Тут уже просто необходимо точно определить, о чем идет речь (иначе непонятно, что, собственно, мы собираемся доказать). С современной точки зрения в классических работах недостает четких определений и формулировок теорем. Лиувилль, несомненно, точно понимал, что он доказывает. Он не только сформулировал задачи о разрешимости уравнений в элементарных функциях и квадратурах, но и алгебраизировал эти задачи. После его работ все эти понятия удалось определить над любым дифференциальным полем. Но требования к математической строгости во времена Лиувилля были не такие, как сейчас. Согласно Колчину (см. [26]), даже у Пикара основные определения еще недостаточно продуманы. Работы Колчина вполне современны, но его определения с самого начала даются для абстрактных дифференциальных полей.

Все же решения дифференциального уравнения – это функции, а не элементы абстрактного дифференциального поля. В функциональных пространствах, кроме дифференцирования и арифметических операций, есть, например, абсолютно неалгебраическая операция суперпозиции. Вообще, в функциональных пространствах больше средств для написания “явных формул”, чем в абстрактных дифференциальных полях. Кроме этого, приходится учитывать, что функции бывают многозначными, имеют особенности и т. д.

Формализовать задачу о неразрешимости уравнений в явном виде в функциональных пространствах несложно (в обзоре мы будем интересоваться именно этой задачей). Сделать это можно так: можно выделить тот или иной класс функций и сказать, что уравнение решается явно, если его решение принадлежит этому классу. Разные классы функций соответствуют разным понятиям разрешимости.

1.1. Задание класса функций с помощью списков основных функций и допустимых операций. Класс функций можно выделить, задав список *основных функций* и список *допустимых операций*. После этого класс функций определяется как множество всех функций, которые получаются из основных функций при помощи применения допустимых операций. В п. 1.2 именно таким способом определяются классические классы функций.

Классические классы функций, фигурирующие в задачах о разрешимости в конечном виде, содержат многозначные функции. В связи с этим исходные понятия нужно уточнить. В этом пункте приведены два варианта такого уточнения. При первом чтении этот пункт можно пропустить.

Итак, пусть фиксирован класс основных функций и запас допустимых операций. Выражается ли заданная функция (являющаяся, скажем, решением данного алгебраического или дифференциального уравнения или возникшая из каких-либо других соображений) через основные функции с помощью допустимых операций? Нас интересуют различные *однозначные ветви* многозначных функций над различными областями. Каждую функцию, даже если она является многозначной, мы будем рассматривать как совокупность всех ее однозначных ветвей. Мы будем применять допустимые операции (такие как арифметические операции или операция взятия суперпозиций) лишь к однозначным ветвям функций над различными областями. Так как мы имеем дело с аналитическими функциями, то в качестве областей достаточно рассматривать лишь малые окрестности точек.

Вопрос теперь видоизменяется следующим образом: *выражается ли заданный росток функции в заданной точке через ростки основных функций при помощи* *допустимых операций*? Конечно, ответ зависит от выбора точки и от выбора однозначного ростка в этой точке заданной многозначной функции. Однако оказывается, что (для интересующих нас классов функций) либо искомого выражения не существует ни для какого ростка заданной многозначной функции ни в какой точке, либо, наоборот, "одно и то же" представление обслуживает все ростки заданной многозначной функции почти в любой точке пространства. В первом случае мы будем говорить, что *никакая ветвь заданной многозначной функции не выражается через ветви основных функций при помощи допустимых операций*. Во втором случае мы будем говорить, что такое выражение *существует*.

Возможен и другой, "глобальный" вариант работы с многозначными функциями, приводящий к другому (несколько расширенному) пониманию определения класса функций, заданного списками основных функций допустимых операций. В этом глобальном варианте многозначная функция рассматривается как единый объект. Определяются операции над многозначными функциями. Результат применения этих операций тоже многозначен: результатом является некоторое множество многозначных функций, про каждую из которых говорится, что она получена применением заданной операции к заданным функциям. Класс функций определяется как множество всех (многозначных) функций, которые получаются из основных функций при помощи допустимых операций.

Определим, например, что такое сумма двух многозначных функций одной переменной в смысле этого варианта.

Определение. Возьмем произвольную точку a на комплексной прямой, один из ростков f_a аналитической функции f в точке a и один из ростков g_a аналитической функции g в той же точке a. Будем говорить, что многозначная функция φ, порожденная ростком $\varphi_a = f_a + g_a$, *представима в виде суммы функций f и g*.

Например, легко видеть, что ровно две функции представляются в виде $\sqrt{x} + \sqrt{x}$, это $f_1 = 2\sqrt{x}$ и $f_2 \equiv 0$. Абсолютно аналогично определяются и другие операции над многозначными функциями. *Замкнутость какого-либо класса многозначных функций относительно сложения означает, что этот класс вместе с любыми двумя функциями содержит все функции, представимые в виде их суммы*. То же самое нужно сказать и про все другие операции над многозначными функциями, понимаемые в указанном выше смысле.

В приведенном выше определении важную роль играет не только сама операция сложения, но и операция аналитического продолжения, спрятанная в понятии многозначной функции. Действительно, рассмотрим следующий пример. Пусть f_1 – аналитическая функция, определенная в области U комплексной прямой $\mathbb{C}^1$, не продолжающаяся аналитически за пределы области U, и пусть f_2 – аналитическая функция в области U, определенная равенством $f_2 = -f_1$. Согласно данному определению, функция, тождественно равная нулю, представима в виде $f_1 + f_2$ *на всей комплексной прямой*. Согласно общепринятой точке зрения, равенство $f_1+f_2 = 0$ справедливо только в области U, но не вне ее.

В глобальном варианте работы с многозначными функциями мы не настаиваем на существовании *единой области*, в которой все нужные действия производились бы над однозначными ветвями многозначных функций. Одна операция может производиться в одной области, а другая операция – в другой области над аналитическими продолжениями полученных функций. В сущности, это расширенное понимание операций эквивалентно добавлению операции аналитического продолжения к числу допустимых операций над аналитическими ростками. Для функции одной переменной удается получить топологические ограничения даже и при таком, расширенном, понимании операций над многозначными аналитическими функциями. Говорить о функциях чуть короче, чем говорить о ростках (так как не надо фиксировать точку, в которой рассматривается росток, и не надо уточнять, о каком именно ростке многозначной функции идет речь). *Поэтому ниже при рассмотрении топологических препятствий к принадлежности функции одной переменной тому или иному классу мы будем иметь в виду глобальный вариант определения класса функций с помощью списков основных функций и допустимых операций.* Для функций многих переменных в столь расширенной формулировке это сделать не удается и приходится принять более ограничительную формулировку, связанную с ростками функций, которая, впрочем, не менее (а может быть, даже более) естественна.

1.2. Классические классы функций одной переменной. Перечислим классические классы функций одной переменной. Мы будем задавать эти классы при помощи списков основных функций и допустимых операций.

Функции одной переменной, представимые в радикалах.

Список основных функций: все комплексные константы, независимая переменная x.

Список допустимых операций: арифметические операции и операции извлечения корня $\sqrt[n]{f}$ степени n, $n = 2, 3, \dots$, из заданной функции f.

Функция $g(x) = \sqrt[3]{5x + 2\sqrt[2]{x}} + \sqrt[7]{x^3 + 3}$ доставляет пример функции, представимой в радикалах.

С этим классом связана знаменитая задача о разрешимости уравнений в радикалах. Рассмотрим алгебраическое уравнение

$$y^n + r_1 y^{n-1} + \dots + r_n = 0,$$

в котором r_i – рациональные функции одной переменной. Полный ответ на вопрос о разрешимости таких уравнений в радикалах дает теория Галуа (см. § 3).

Для определения остальных классов нам понадобится список основных элементарных функций. В этот список, в сущности, входят те функции, которые мы проходили в школе и которые часто вносят в клавиатуры калькуляторов.

Список основных элементарных функций.

1) Все комплексные константы и независимая переменная x.

2) Экспонента, логарифм и степенная функция x^α, где α – любая комплексная константа.

3) Тригонометрические функции: синус, косинус, тангенс, котангенс.

4) Обратные тригонометрические функции: арксинус, арккосинус, арктангенс, арккотангенс.

Перейдем теперь к списку классических операций над функциями. Здесь приводится начало списка. Он будет продолжен в п. 2.1.

Список классических операций. 1) *Операция суперпозиции*, сопоставляющая функциям f, g функцию $f \circ g$.

2) *Арифметические операции*, сопоставляющие функциям f и g функции $f+g$, $f-g$, fg и f/g.

3) *Операция дифференцирования*, сопоставляющая функции f функцию f'.

4) *Операция интегрирования*, сопоставляющая функции f ее неопределенный интеграл y (т.е. любую функцию y такую, что $y' = f$; по функции f функция y определена с точностью до аддитивной постоянной).

5) *Операция решения алгебраического уравнения*, сопоставляющая функциям $f_1, \dots, f_n$ функцию y такую, что $y^n + f_1 y^{n-1} + \dots + f_n = 0$ (по функциям $f_1, \dots, f_n$ функция y определена не вполне однозначно, так как алгебраическое уравнение степени n может иметь n решений).

Вернемся теперь к определению классических классов функций одной переменной.

Элементарные функции одной переменной.

Список основных функций: основные элементарные функции.

Список допустимых операций: суперпозиции, арифметические операции, дифференцирование.

Элементарные функции записываются формулами, например следующей:

$$f(x) = \operatorname{arctg}(\exp(\sin x) + \cos x).$$

Функции одной переменной, представимые в квадратурах.

Список основных функций: основные элементарные функции.

Список допустимых операций: суперпозиции, арифметические операции, дифференцирование, интегрирование.

Например, эллиптический интеграл

$$f(x) = \int_{x_0}^{x} \frac{dt}{\sqrt{P(t)}},$$

где P – кубический полином, представим в квадратурах. Но, как доказал Лиувилль, если полином P не имеет кратных корней, то функция f не является элементарной.

Обобщенные элементарные функции одной переменной. Этот класс функций определяется в точности так же, как класс элементарных функций. Нужно лишь к списку допустимых операций добавить операцию решения алгебраических уравнений.

Функции одной переменной, представимые в обобщенных квадратурах. Этот класс функций определяется в точности так же, как класс функций, представимых в квадратурах. Нужно лишь к списку допустимых операций добавить операцию решения алгебраических уравнений.

Определим еще два класса функций, близких к классическим классам.

Функции одной переменной, представимые в k-радикалах. Этот класс функций определяется в точности так же, как класс функций, представимых в радикалах. Нужно лишь к списку допустимых операций добавить операцию решения алгебраических уравнений степени $\leqslant k$.

Функции одной переменной, представимые в k-квадратурах. Этот класс функций определяется в точности так же, как класс функций, представимых в квадратурах. Нужно лишь к списку допустимых операций добавить операцию решения алгебраических уравнений степени $\leqslant k$.

§ 2. Теория Лиувилля

Первые строгие доказательства неразрешимости некоторых уравнений в квадратурах и в элементарных функциях были получены в середине девятнадцатого века Лиувиллем (см. [30]–[36)]). Согласно его теории, "достаточно простые" уравнения либо имеют "достаточно простые " решения, либо вообще не решаются в явном виде. Теория Лиувилля, например, отвечает на следующие вопросы:

1) при каких условиях неопределенный интеграл от элементарной функции является элементарной функцией?

2) при каких условиях все решения линейного дифференциального уравнения представимы в обобщенных квадратурах?

Более полно на второй вопрос отвечает дифференциальная теория Галуа (см. § 4). В настоящем параграфе мы обсудим, как Лиувилль алгебраизировал задачу о разрешимости, и сформулируем некоторые результаты его теории.

2.1. Новые определения классических классов функций. Лиувилль алгебраизировал задачу о разрешимости в элементарных функциях и квадратурах. Главным препятствием на этом пути является абсолютно неалгебраическая операция суперпозиции. Лиувилль обошел это препятствие следующим образом: с каждой функцией g из списка основных функций он связал операцию суперпозиции с этой функцией, переводящую функцию f, к которой применяется эта операция, в функцию $g \circ f$. Лиувилль заметил, что все основные элементарные функции сводятся к логарифму и к экспоненте (см. лемму 2.1 ниже). Суперпозиции $y = \exp f$ и $z = \ln f$ можно рассматривать как решения уравнений $y' = f'y$ и $z' = f'/f$. Таким образом, внутри классических классов функций вместо абсолютно неалгебраической операции суперпозиции достаточно рассматривать операции решения простых дифференциальных уравнений. После этого задача о разрешимости в классических классах функций становится дифференциально-алгебраической и переносится на абстрактные дифференциальные поля. Приступим к реализации этой программы.

Продолжим список классических операций.

Список классических операций (начало списка в п. 1.2).

6) *Операция взятия экспоненты*, сопоставляющая функции f функцию $\exp f$.

7) *Операция взятия логарифма*, сопоставляющая функции f функцию $\ln f$.

Приведем теперь новые определения трансцендентных классических классов функций.

Элементарные функции одной переменной.

Список основных функций: все комплексные константы и независимая переменная x.

Список допустимых операций: взятие экспоненты, взятие логарифма, арифметические операции, дифференцирование.

Функции одной переменной, представимые в квадратурах.

Список основных функций: все комплексные константы.

Список допустимых операций: взятие экспоненты, арифметические операции, дифференцирование, интегрирование.

Обобщенные элементарные функции и функции, представимые в обобщенных квадратурах и k-квадратурах одной переменной, определяются так же, как соответствующие необобщенные классы функций, нужно лишь к списку допустимых операций добавить соответственно операцию решения алгебраических уравнений или операцию решения алгебраических уравнений степени не выше k.

Лемма 2.1. *Основные элементарные функции выражаются с помощью комплексных констант, арифметических операций и суперпозиций через экспоненту и логарифм.*

Доказательство. Для степенной функции x^α нужное выражение доставляет равенство $x^\alpha = \exp(\alpha \ln x)$. Для тригонометрических функций нужные выражения вытекают из формулы Эйлера $e^{a+bi} = e^a(\cos b + i \sin b)$. При вещественных значениях x имеем $\sin x = \dfrac{1}{2i}(e^{ix} - e^{-ix})$ и $\cos x = \dfrac{1}{2}(e^{ix} + e^{-ix})$. В силу аналитичности эти же формулы справедливы и для комплексных x. Функции тангенс и котангенс выражаются через синус и косинус. Покажем, что для вещественных x справедливо равенство $\operatorname{arctg} x = \dfrac{1}{2i} \ln z$, где $z = \dfrac{1+ix}{1-ix}$. Очевидно, что $|z| = 1$, $\arg z = 2\arg(1+ix)$, $\operatorname{tg}(\arg(1+ix)) = x$, что и доказывает нужное равенство. В силу аналитичности это же равенство справедливо и для комплексных значений x. Остальные обратные тригонометрические функции выражаются через arctg. Именно, $\operatorname{arcctg} x = \dfrac{\pi}{2} - \operatorname{arctg} x$, $\arcsin x = \operatorname{arctg} \dfrac{x}{\sqrt{1-x^2}}$, $\arccos x = \dfrac{\pi}{2} - \arcsin x$. Квадратный корень, участвующий в выражении функции arcsin, выражается через экспоненту и логарифм: $x^{1/2} = \exp(1/2)\ln x$. Лемма доказана.

Теорема 2.2. *Для каждого из трансцендентных классических классов функций новое и старое определения* (см. настоящий параграф и п. 1.2) *эквивалентны.*

Доказательство. В одну сторону теорема очевидна: ясно, что каждая функция, принадлежащая некоторому классическому классу функций, понимаемому в смысле нового определения, принадлежит тому же классу, понимаемому в смысле старого определения.

Докажем теорему в другую сторону. Согласно лемме 2.1, основные элементарные функции лежат в классах элементарных и обобщенных элементарных функций, понимаемых в смысле нового определения. Из этой же леммы вытекает, что классы функций, представимые в квадратурах, обобщенных квадратурах и k-квадратурах, понимаемые в смысле нового определения, тоже содержат основные элементарные функции. Действительно, независимая переменная x принадлежит этим классам, так как она получается интегрированием константы 1, ибо $x' = 1$. Вместо операции взятия логарифма, которой нет среди допустимых операций в этих классах, можно использовать операцию интегрирования, так как $(\ln f)' = f'/f$.

Нам осталось показать, что классические классы функций, понимаемые в смысле нового определения, замкнуты относительно суперпозиций. Дело здесь в следующем: операция взятия суперпозиции коммутирует со всеми операциями, фигурирующими в новых определениях классов функций, за исключением операций дифференцирования и интегрирования. Так, например, результат применения операции exp к суперпозиции $g \circ f$ совпадает с результатом применения операции взятия суперпозиции к функциям $\exp g$ и f, т.е. $\exp(g \circ f) = (\exp g) \circ f$. Аналогично $\ln(g \circ f) = (\ln g) \circ f$, $(g_1 \pm g_2) \circ f = (g_1 \circ f) \pm (g_2 \circ f)$, $(g_1 g_2) \circ f = (g_1 \circ f)(g_2 \circ f)$, $(g_1/g_2) \circ f = (g_1 \circ f)/(g_2 \circ f)$.

Если функция y удовлетворяет уравнению $y^n + g_1 y^{n-1} + \dots + g_n = 0$, то функция $(y \circ f)$ удовлетворяет уравнению

$$(y \circ f)^n + (g_1 \circ f)(y \circ f)^{n-1} + \dots + (g_n \circ f) = 0.$$

Для операций дифференцирования и интегрирования имеем следующие простые коммутационные соотношения с операцией суперпозиции: $(g)' \circ f = (g \circ f)'(f')^{-1}$ (если функция f – константа, то функция $(g)' \circ f$ – тоже константа) и если y – неопределенный интеграл функции g, то $y \circ f$ – неопределенный интеграл функции $(g \circ f)f'$ (другими словами, интегрированию функции g при суперпозиции с функцией f соответствует интегрирование функции $g \circ f$, домноженной на функцию f').

Отсюда и вытекает замкнутость классических классов, понимаемых в смысле нового определения, относительно суперпозиций. Действительно, если функция g получается из констант (или из констант и независимой переменной) при помощи операций, которые мы обсуждали выше, то функция $g \circ f$ получается применением тех же или почти тех же операций, как в случае интегрирования и дифференцирования, из функции f. Теорема доказана.

Замечание. Легко видеть, что операцию дифференцирования тоже можно исключить из списков допустимых операций классических классов функций. Для доказательства достаточно воспользоваться явным вычислением производных экспоненты и логарифма и правилами дифференцирования формул, включающих суперпозиции и арифметические операции. Однако исключение операции дифференцирования никак не помогает в задаче о разрешимости уравнений в конечном виде.

2.2. Расширения Лиувилля абстрактных и функциональных дифференциальных полей. Поле K называется *дифференциальным полем*, если задано аддитивное отображение $a \to a'$, удовлетворяющее соотношению Лейбница $(ab)' = a'b + ab'$. Элемент y дифференциального поля K называется *константой*, если $y' = 0$. Все константы дифференциального поля образуют подполе, которое называется *полем констант*. Во всех интересующих нас случаях полем констант является поле комплексных чисел. *Мы всегда в дальнейшем предполагаем, что дифференциальное поле имеет нулевую характеристику и алгебраически замкнутое поле констант.* Элемент y дифференциального поля называется: *экспонентой элемента* a, если $y' = a'y$; *экспонентой интеграла элемента* a, если $y' = ay$; *логарифмом элемента* a, если $y' = a'/a$; *интегралом элемента* a, если $y' = a$.

Пусть дифференциальное поле K и множество M лежат в некотором дифференциальном поле F. *Присоединением* к дифференциальному полю K множества M называется минимальное дифференциальное поле $K\langle M\rangle$, содержащее поле K и множество M.

Дифференциальное поле F, содержащее дифференциальное поле K и имеющее то же поле констант, называется *элементарным расширением* поля K, если существует цепочка дифференциальных полей $K = F_1 \subseteq \dots \subseteq F_n = F$ таких, что при каждом $i = 1, \dots, n-1$ поле $F_{i+1} = F_i\langle x_i\rangle$ получается присоединением к полю F_i элемента x_i, причем x_i – экспонента или логарифм некоторого элемента a_i поля F_i. Элемент $a \in F$ называется *элементарным* над K, $K \subset F$, если он содержится в каком-либо элементарном расширении поля K.

Обобщенное элементарное расширение, *расширение Лиувилля*, *обобщенное расширение Лиувилля* и *k-расширение Лиувилля* поля K определяются аналогично. При построении обобщенных элементарных расширений допускаются присоединения экспонент, логарифмов и алгебраические расширения. При построении расширений Лиувилля допускаются присоединения интегралов и экспонент интегралов. В обобщенных расширениях Лиувилля и k-расширениях Лиувилля кроме этого допускаются соответственно алгебраические расширения и присоединения решений алгебраических уравнений степени не выше k. Элемент $a \in F$ называется *обобщенно-элементарным* над K, $K \subset F$ (*представимым в квадратурах*, в *обобщенных квадратурах*, в *k-квадратурах* над K), если a содержится в каком-либо обобщенно-элементарном расширении (расширении Лиувилля, обобщенном расширении Лиувилля, k-расширении Лиувилля) поля K.

Замечание. Уравнение для экспоненты интеграла проще, чем уравнение для экспоненты. Поэтому при определении расширений Лиувилля и т. д. используются присоединения экспонент интегралов. Вместо этого можно было бы отдельно присоединять экспоненты и отдельно интегралы.

Перейдем к функциональным дифференциальным полям. Именно с такими полями мы будем иметь дело в обзоре (хотя некоторые результаты без труда переносятся на абстрактные дифференциальные поля).

Всякое подполе K поля всех мероморфных функций в связной области U на сфере Римана, содержащее все комплексные константы и замкнутое относительно дифференцирования (т.е. если $f \in K$, то $f' \in K$), доставляет пример функционального дифференциального поля. Дадим теперь общее определение. Пусть V, v – пара, состоящая из связной римановой поверхности V и мероморфного векторного поля v на ней. Производная Ли L_v вдоль векторного поля v действует на поле F всех мероморфных функций на поверхности V и задает дифференцирование $f' = L_v f$ в этом поле. *Функциональное дифференциальное поле* – это любое дифференциальное подполе поля F, содержащее все комплексные константы.

Иногда удобнее использовать другое определение дифференцирования поля функций, в котором вместо мероморфного векторного поля фигурирует мероморфная 1-форма α. Производную f' функции f можно определить следующей формулой: $f' = df/\alpha$ (частное двух мероморфных 1-форм является корректно определенной мероморфной функцией). Описанное дифференцирование – это производная Ли L_v вдоль векторного поля v, связанного с формой α следующим соотношением: значение формы α на поле v тождественно равно единице.

Для расширения функциональных полей полезна следующая конструкция. Пусть K – некоторое подполе поля мероморфных функций на связной римановой поверхности V, снабженной мероморфной формой α, инвариантное относительно дифференцирования $f' = df/\alpha$ (т.е. если $f \in K$, то $f' \in K$). Рассмотрим любую связную риманову поверхность W вместе с аналитическим отображением $\pi\colon W \to V$. Фиксируем на W форму $\beta = \pi^*\alpha$. Дифференциальное поле F всех мероморфных функций на W с дифференцированием $\varphi' = d\varphi/\beta$ содержит дифференциальное подполе π^*K, состоящее из функций вида π^*f, где $f \in K$. Дифференциальное поле π^*K изоморфно дифференциальному полю K, и оно лежит внутри дифференциального поля F. Если удачно подобрать поверхность W, то расширение поля π^*K, изоморфного полю K, можно произвести внутри поля F.

Пусть требуется расширить поле K, скажем, интегралом y некоторой функции $f \in K$. Это можно сделать следующим образом. Над римановой поверхностью V можно рассмотреть риманову поверхность W неопределенного интеграла y формы $f\alpha$. По самому определению римановой поверхности W существует естественная проекция $\pi\colon W \to V$ и функция y является однозначной мероморфной функцией на поверхности W. Дифференциальное поле F мероморфных функций на W с операцией дифференцирования $f' = df/\pi^*\alpha$ содержит как элемент y, так и поле π^*K, изоморфное полю K. Поэтому расширение $\pi^*K\langle y\rangle$ определено и является подполем дифференциального поля F. Именно эту конструкцию расширения мы имеем в виду, когда говорим о расширениях функциональных дифференциальных полей. Эта же конструкция позволяет присоединить к функциональному дифференциальному полю K логарифм, экспоненту, интеграл или экспоненту интеграла от любой функции f из поля K. Для любых функций $f_1, \dots, f_n \in K$ можно таким способом присоединить к K решение y алгебраического уравнения $y^n + f_1y^{n-1} + \dots + f_n = 0$ или все решения $y_1, \dots, y_n$ этого уравнения (присоединение всех решений $y_1, \dots, y_n$ можно осуществить на римановой поверхности вектор-функции $\mathbf{y} = (y_1, \dots, y_n)$). Таким же способом для любых функций $f_1, \dots, f_{n+1} \in K$ можно присоединить к K n-мерное аффинное пространство над $\mathbb{C}$ всех решений линейного дифференциального уравнения $y^{(n)} + f_1y^{(n-1)} + \dots + f_ny + f_{n+1} = 0$. (Напомним, что росток любого решения линейного дифференциального уравнения аналитически продолжается вдоль кривой на поверхности V, не проходящей через полюсы функций $f_1, \dots, f_{n+1}$.)

Итак, *все упомянутые выше расширения функциональных дифференциальных полей можно осуществить, не выходя из класса функциональных дифференциальных полей.* Говоря о расширениях функциональных дифференциальных полей, мы всегда имеем в виду именно эту процедуру.

Дифференциальное поле, состоящее из всех комплексных констант, и дифференциальное поле, состоящее из всех рациональных функций от одной переменной, можно рассматривать как дифференциальные поля функций, определенных на сфере Римана.

Сформулируем снова теорему 2.2, используя определения из абстрактной дифференциальной алгебры и конструкцию расширения функциональных дифференциальных полей.

Теорема 2.2$'$. *Функция одной комплексной переменной (возможно, многозначная) принадлежит:*

1) *классу элементарных функций, если и только если она принадлежит некоторому элементарному расширению поля всех рациональных функций одной переменной;*

2) *классу обобщенных элементарных функций, если и только если она принадлежит некоторому обобщенному элементарному расширению поля рациональных функций;*

3) *классу функций, представимых в квадратурах, если и только если она принадлежит некоторому расширению Лиувилля поля всех комплексных констант;*

4) *классу функций, представимых в k-квадратурах, если и только если она принадлежит некоторому k-расширению Лиувилля поля всех комплексных констант;*

5) *классу функций, представимых в обобщенных квадратурах, если и только если она принадлежит обобщенному расширению Лиувилля поля всех комплексных констант.*

2.3. Некоторые результаты теории Лиувилля. В этом пункте мы приведем без доказательства формулировки ряда результатов теории Лиувилля.

2.3.1. Неэлементарность неопределенных интегралов. Когда мы начинаем учить анализ, нас учат интегрировать элементарные функции, и это оказывается далеко не простым занятием. Как доказал Лиувилль, неопределенный интеграл от элементарной функции обычно не является элементарной функцией.

ТЕОРЕМА 2.3 (об интегралах). *Неопределенный интеграл y функции f, лежащей в функциональном дифференциальном поле K, принадлежит некоторому обобщенно-элементарному расширению этого поля, если и только если этот интеграл представим в виде*

$$y(x) = \int_{x_0}^{x} f(t)\,dt = A_0(x) + \sum_{i=1}^{n} \lambda_i \ln A_i(x), \tag{1}$$

где A_i при $i = 0, 1, \dots, n$ – некоторые функции из поля K.

Условие (1) из теоремы Лиувилля в дифференциальной форме означает, что элемент $f \in K$ представим в виде

$$f = A_0' + \sum_{i=1}^{n} \lambda_i \frac{A_i'}{A_i}, \tag{2}$$

где A_i при $i = 0, 1, \dots, n$ – некоторые элементы поля K. В абстрактной дифференциальной алгебре справедлив аналог теоремы Лиувилля [34]. В формулировке абстрактной теоремы в качестве K нужно взять абстрактное дифференциальное поле и воспользоваться условием (1) в дифференциальной форме (2).

СЛЕДСТВИЕ 2.4. *Неопределенный интеграл y от обобщенной элементарной функции f является обобщенной элементарной функцией, если и только если он представим в виде*

$$y(x) = A_0(x) + \sum_{i=1}^{n} \lambda_i \ln A_i(x),$$

где A_i при $i = 0, 1, \dots, n$ – рациональные функции с комплексными коэффициентами от функции f и ее производных.

Априори, интеграл от элементарной функции f мог бы быть очень сложной элементарной функцией. Теорема Лиувилля показывает, что ничего такого случиться не может. Или интеграл от элементарной функции неэлементарен, или он имеет описанный в следствии простой вид.

Берется ли интеграл от алгебраической функции в явном виде? Этому вопросу были посвящены пионерские работы Абеля, заложившие основы теории алгебраических кривых и абелевых интегралов и вдохновившие Лиувилля на создание его теории. Грубо говоря, ответ на этот вопрос такой. Если риманова поверхность алгебраической функции имеет нулевой род, то ее интеграл всегда берется в обобщенных элементарных функциях. Если же род римановой поверхности положителен, то интеграл, как правило, не элементарен и берется в обобщенных элементарных функциях в исключительных случаях. Более подробный ответ дает формулируемая ниже теорема Лиувилля об абелевых интегралах.

Теорема 2.5 (об абелевых интегралах). *Неопределенный интеграл y от алгебраической функции A комплексной переменной x берется в обобщенных элементарных функциях, если и только если он представим в виде*

$$y(x) = \int_{x_0}^{x} A(t)\,dt = A_0(x) + \sum_{i=1}^{k} \lambda_i \ln A_i(x),$$

где A_i при $i = 0, 1, \ldots, k$ – алгебраические функции, однозначные на римановой поверхности W подынтегральной функции A.

Доказательство. Теорема вытекает из теоремы Лиувилля об интегралах элементарных функций, примененной к полю F всех мероморфных функций на поверхности W, снабженному следующим дифференцированием: $f' = df/\alpha$, где $\alpha = \pi^* dx$ и $\pi\colon W \to \overline{C}$ – естественная проекция римановой поверхности функции A на сферу Римана $\overline{C}$ комплексного переменного x.

Замечание. Теорема Лиувилля об абелевых интегралах восходит к Абелю. Абель рассматривал более частную задачу о представимости абелевых интегралов в виде рациональных функций от алгебраических функций и их логарифмов и пришел к аналогичным выводам.

Сформулируем критерий Лиувилля интегрируемости в явном виде функций экспоненциального типа и приведем примеры неберущихся интегралов.

Критерий Лиувилля. *Рассмотрим неопределенный интеграл вида*

$$I(x) = \int_{x_0}^{x} f(t) e^{g(t)}\,dt,$$

где f и g – рациональные функции, причем функция g непостоянная, а f не обращается в тождественный нуль. Если существует рациональная функция a такая, что $a' + ag' = f$, то $I = ae^g + c$, где c – комплексная константа. Если же уравнение $a' + ag' = f$ неразрешимо в рациональных функциях, то интеграл I не является обобщенной элементарной функцией.

Примеры неберущихся интегралов. *Неопределенные интегралы $\int e^{t^2}\,dt$, $\int \frac{e^t}{t}\,dt$, $\int \frac{dt}{\ln t}$, $\int \frac{\sin t}{t}\,dt$ не являются обобщенными элементарными функциями.*

2.3.2. Критерий Лиувилля–Мордухай-Болтовского. Лиувиллю принадлежит первый результат о неразрешимости линейных дифференциальных уравнений в явном виде (см. [32], [33]).

Теорема 2.6 (Лиувилль). *Уравнение $y'' + py' + qy = 0$ с коэффициентами из функционального дифференциального поля K, все элементы которого представимы в обобщенных квадратурах, решается в обобщенных квадратурах, если и только если оно имеет решение вида $y_1(x) = \exp \int_{x_0}^{x} f(t)\,dt$, где f – функция, удовлетворяющая алгебраическому уравнению с коэффициентами в поле K.*

В одну сторону теорема очевидна. Если известно одно решение y_1 линейного дифференциального уравнения второго порядка, то его можно решить, понизив порядок уравнения. Доказать теорему в другую сторону достаточно трудно.

Потребовалось более полувека, чтобы обобщить теорему Лиувилля на уравнения n-го порядка. Мордухай-Болтовский доказал в 1910 году методом Лиувилля следующий критерий, позволяющий сводить вопрос о разрешимости уравнения к вопросу о разрешимости другого уравнения меньшего порядка.

Критерий Лиувилля–Мордухай-Болтовского. *Уравнение n-го порядка*

$$y^{(n)} + p_1 y^{(n-1)} + \dots + p_n y = 0$$

с коэффициентами из функционального дифференциального поля K, все элементы которого представимы в обобщенных квадратурах, решается в обобщенных квадратурах, если и только если оно, во-первых, имеет решение вида $y_1(x) = \exp \int_{x_0}^{x} f(t)\,dt$, где f – функция, лежащая в некотором алгебраическом расширении K_1 поля K, и, во-вторых, если дифференциальное уравнение $(n-1)$-го порядка на функцию $z = y' - \frac{y_1'}{y_1} y$ с коэффициентами из поля K_1, полученное из исходного уравнения процедурой понижения порядка (*см. п.* 4.1.2), *решается в обобщенных квадратурах над полем K_1.*

В этом же 1910 году появилась теорема Пикара–Вессио, в которой вопрос о разрешимости линейных дифференциальных уравнений решается абсолютно по-другому, с точки зрения дифференциальной теории Галуа.

Ниже мы обсудим основные положения этой теории. Критерий Лиувилля–Мордухай-Болтовского, по существу, эквивалентен теореме Пикара–Вессио. Теория Пикара–Вессио не только объясняет этот критерий, но и дает возможность довести его до явного алгоритма, позволяющего для уравнения с коэффициентами из поля рациональных функций (имеющих рациональные коэффициенты) определить, разрешимо уравнение в обобщенных квадратурах или нет (см. [37] и п. 4.7).

§ 3. Разрешимость алгебраических уравнений в радикалах и теория Галуа

Решается ли заданное алгебраическое уравнение в радикалах? Можно ли решать заданное алгебраическое уравнение степени n, используя решение вспомогательных алгебраических уравнений меньшей степени и радикалы? В этом параграфе мы обсуждаем, как теория Галуа решает эти вопросы. Мы обращаем главное внимание именно на вопросы разрешимости и неразрешимости и приводим без доказательства основную теорему теории Галуа. Без доказательства используются также хорошо известные свойства разрешимых групп и группы $S(k)$. В п. 3.4.1 доказывается значительно менее известное характеристическое свойство подгрупп группы $S(k)$. Эти факты из теории групп применяются как в обычной теории Галуа, так и в ее дифференциальном и топологическом вариантах.

"Разрешительная" часть теории Галуа (см. п. 3.3.2), позволяющая решать уравнение в радикалах, весьма проста. Она не использует ни основную теорему теории Галуа, ни вообще теорию полей и относится, по существу, к линейной алгебре. Только эти линейно-алгебраические соображения применяются в топологическом варианте теории Галуа при обсуждении вопроса о представимости алгебраических функций в радикалах. (Однако достаточное условие разрешимости уравнения с помощью решения вспомогательных уравнений меньшей степени и радикалов опирается не только на линейную алгебру, но и на основную теорему теории Галуа.)

Приведенные выше задачи о разрешимости алгебраических уравнений по своей природе являются чисто алгебраическими и могут быть поставлены над любым полем K. *В этом параграфе мы будем предполагать, что поле K имеет нулевую характеристику и содержит все корни из единицы.* Этот случай немного проще общего, а для нас основной интерес представляют функциональные дифференциальные поля, которые содержат все комплексные константы.

3.1. Группа Галуа алгебраического уравнения. Рассмотрим некоторое алгебраическое уравнение

$$a_nx^n + \cdots + a_1x + a_0 = 0 \tag{3}$$

с коэффициентами из поля K. Мы считаем, что поле K вложено в некоторое большее поле, содержащее все корни уравнения. *Соотношением*, определенным над полем K, между корнями уравнения (3) называется любой полином Q, принадлежащий кольцу $K[x_1, \dots, x_n]$, который обращается в нуль в точке $(x_1^0, \dots, x_n^0)$, где $x_1^0, \dots, x_n^0$ – упорядоченный набор корней уравнения (3).

Определение. *Группой Галуа алгебраического уравнения* (3) над полем K называется подгруппа G группы $S(n)$ всех перестановок корней уравнения, сохраняющих все соотношения между корнями, определенные над полем K (т.е. если перестановка $\sigma \in S(n)$ принадлежит группе Галуа G, то полином σQ, полученный из соотношения Q перестановкой σ переменных $x_1, \dots, x_n$, тоже обращается в нуль в точке $(x_1^0, \dots, x_n^0)$).

Определение. Поле P называется *расширением Галуа* поля K, если существует алгебраическое уравнение (3) с коэффициентами в поле K такое, что поле P получается присоединением к полю K всех корней этого уравнения. *Группой Галуа расширения Галуа P* над полем K называется группа всех автоморфизмов поля P, оставляющих на месте все элементы поля K.

Каждый элемент σ из группы Галуа поля P над полем K переставляет корни уравнения (3) и сохраняет все соотношения между ними, определенные над полем K. Таким образом, группа Галуа поля P над K имеет представление в группе Галуа G уравнения (3), определяющего расширение P. Очевидно, что это представление является изоморфизмом групп, т.е. группа Галуа уравнения и группа Галуа заданного им расширения изоморфны.

Для доказательства неразрешимости уравнений нам понадобятся следующие простые “оценки сверху” групп Галуа.

Лемма 3.1. *Группа Галуа уравнения $x^n - a = 0$ над полем K, $a \in K$, является подгруппой циклической группы из n элементов.*

Доказательство. Фиксируем любой корень x_0 уравнения $x^n - a = 0$ и любой первообразный корень ξ степени n из единицы. Занумеруем корни уравнения $x^n - a = 0$ вычетами i по модулю n, положив x_i равным $\xi^i x_0$. Пусть преобразование g из группы Галуа переводит корень x_0 в корень x_i. Тогда $g(x_k) = g(\xi^k x_0) = \xi^{k+i} x_0 = x_{k+i}$. То есть всякое преобразование группы Галуа задает циклическую перестановку корней.

Следующая лемма непосредственно вытекает из определения группы Галуа алгебраического уравнения.

Лемма 3.2. *Группа Галуа уравнения степени $m \leqslant k$ изоморфна подгруппе группы $S(k)$.*

3.2. Основная теорема теории Галуа. Пусть P – расширение Галуа поля K и G – его группа Галуа.

Определены следующие отображения между множеством полей, лежащих между K и P, и множеством подгрупп группы Галуа G.

1) *Отображение Fd*, сопоставляющее каждой подгруппе Γ группы G поле $Fd(\Gamma)$, состоящее из элементов поля P, остающихся неподвижными при действии подгруппы Γ (ясно, что $K \subseteq Fd(\Gamma)$).

2) *Отображение Gp*, сопоставляющее каждому промежуточному полю F, $K \subseteq F \subseteq P$, подгруппу $Gp(F) \subseteq G$, являющуюся группой Галуа расширения Галуа P поля F (P является расширением Галуа поля K, и поэтому оно автоматически является расширением Галуа промежуточного поля F, $K \subseteq F \subseteq P$).

Отображения Fd и Gp устанавливают *соответствие Галуа* между подгруппами группы Галуа и промежуточными полями расширения Галуа.

Приведем без доказательства следующую теорему.

Основная теорема 3.3 (теории Галуа). *Для всякого расширения Галуа P поля K с группой Галуа G*

1) *композиция отображений Fd и Gp является тождественным отображением множества промежуточных полей в себя: если F – поле и $K \subseteq F \subseteq P$, то $Fd(Gp(F)) = F$;*
2) *композиция отображений Gp и Fd является тождественным отображением множества подгрупп группы Галуа в себя: если Γ – подгруппа группы Галуа, $\Gamma \subset G$, то $Gp(Fd(\Gamma)) = \Gamma$;*
3) *промежуточное поле F, $K \subseteq F \subseteq P$, является расширением Галуа поля K, если и только если группа $Gp(F)$ является нормальным делителем группы G; при этом группа Галуа расширения Галуа F поля K является фактор-группой группы G по нормальному делителю $Gp(F)$.*

Поле P является расширением Галуа поля K, если и только если существует конечная группа Γ автоморфизмов поля P такая, что она оставляет неподвижными все элементы поля K и только их.

Что произойдет с группой Галуа уравнения, если поле коэффициентов K расширить, заменив его большим полем K_1? Этот вопрос особенно интересен в том случае, когда поле K_1 является расширением Галуа поля K. Обозначим через G_1 группу Галуа расширения K_1 поля K. Результаты о неразрешимости алгебраических уравнений основаны на следующей теореме.

Теорема 3.4 (об изменении группы Галуа уравнения при расширении Галуа поля коэффициентов). *При замене поля коэффициентов K его расширением Галуа K_1 группа Галуа G уравнения заменяется некоторым своим нормальным делителем H. Фактор-группа G/H группы G относительно этого нормального делителя изоморфна некоторой фактор-группе группы Галуа G_1 нового поля коэффициентов K_1 над старым полем коэффициентов K.*

Доказательство. Пусть Q – наименьшее расширение Галуа поля K, содержащее расширения P и K_1 поля K. (Расширение Q получается присоединением к K всех корней произведения полиномиальных уравнений, определяющих расширения Галуа P и K_1 поля K.) Поле K неподвижно при действии группы Галуа Γ_Q расширения Q, а поля K_1 и P инвариантны относительно этого действия. Следовательно, поле $K_1 \cap P$ инвариантно относительно действия группы Γ_Q и является поэтому расширением Галуа поля K.

Группа Галуа H расширения Галуа P поля $K_1 \cap P$ является нормальным делителем группы Галуа расширения Галуа P поля K, так как $K_1 \cap P$ – расширение Галуа поля K и $K_1 \cap P \subset P$. С другой стороны, группа H является фактор-группой группы Галуа расширения Галуа K_1 поля K, поскольку $K_1 \cap P$ – расширение Галуа поля K и $K_1 \cap P \subset K_1$.

Осталось показать, что группа Галуа H поля P над $K_1 \cap P$ совпадает с группой Галуа Γ поля Q над K_1. Действительно, группа Γ является подгруппой в H, так как каждое соотношение над полем $K_1 \cap P$ является, в частности, соотношением между корнями того же уравнения над полем K_1. Пусть $\Gamma \neq H$. Согласно основной теореме, примененной к расширению P поля K, поле инвариантов F относительно действия Γ на P строго больше, чем $K_1 \cap P$. С другой стороны, все элементы поля F лежат как в поле P, так и в поле K_1. Противоречие доказывает, что $\Gamma = H$.

3.3. Разрешимость в радикалах. Решается ли заданное алгебраическое уравнение в радикалах? Теория Галуа была создана для ответа на этот вопрос. Начнем с формального определения.

Алгебраическое уравнение над полем K *разрешимо в радикалах*, если существует цепочка расширений $K = K_0 \subset \cdots \subset K_N$, в которой поле K_{i+1} получается из поля K_i, $i = 0, 1, \ldots, N-1$, присоединением радикала, а поле K_N содержит все корни исходного алгебраического уравнения.

Теорема 3.5. *Алгебраическое уравнение решается в радикалах, если и только если его группа Галуа разрешима.*

Доказательство. Достаточное условие разрешимости группы Галуа для разрешимости уравнения в радикалах мы докажем ниже в п. 3.3.1 (см. следствие 3.10). Покажем, что если алгебраическое уравнение решается в радикалах, то его группа Галуа разрешима. Проследим, что происходит с группой Галуа уравнения при переходе от поля коэффициентов K_i к полю коэффициентов K_{i+1}. Обозначим через G_i группу Галуа нашего уравнения над полем K_i. Тогда, согласно теореме 3.4, группа G_{i+1} является нормальной подгруппой в группе G_i, причем фактор-группа G_i/G_{i+1} является одновременно фактор-группой группы Галуа поля K_{i+1} над полем K_i. Так как поле K_{i+1} получается из поля K_i присоединением радикала, то согласно лемме 3.1 группа Галуа поля K_{i+1} над полем K_i коммутативна. Так как все корни алгебраического уравнения по условию лежат в поле K_N, то группа Галуа G_N алгебраического уравнения над полем K_N тривиальна. Итак, у группы Галуа G существует цепочка подгрупп $G = G_0 \supset \cdots \supset G_N$, в которой группа G_{i+1} является нормальным делителем группы G_i с коммутативной фактор-группой G_i/G_{i+1}, а группа G_N тривиальна. То есть группа Галуа G разрешима.

3.3.1. Достаточное условие разрешимости в радикалах. Пусть K – подполе поля P, и пусть на P действует конечная группа автоморфизмов G, оставляющая неподвижными все элементы поля K и только их. Если поле P получено из поля K присоединением всех корней алгебраического уравнения над полем K, то такая группа автоморфизмов G существует (и изоморфна группе Галуа уравнения). Существование группы G никак не самоочевидно и представляет собой один из центральных фактов теории Галуа (см. п. 3.2). Однако в ряде важных случаев группа G задана априори. Так, например, обстоит дело, если K – поле рациональных функций одной переменной, P – поле, полученное присоединением к K всех ветвей алгебраической функции, и G – монодромии этой алгебраический функции (см. п. 5.1.2). Другой пример доставляет общее алгебраическое уравнение степени n (см. п. 3.3.3).

Пусть в рассматриваемой ситуации группа G разрешима. Тогда любой элемент поля P представим в радикалах через элементы поля K. Конструкция представления элемента в радикалах, в основном, относится к линейной алгебре. Она очень слабо использует то обстоятельство, что мы имеем дело с полями. Чтобы подчеркнуть это, мы опишем эту конструкцию, взяв вместо поля алгебру V, которая может быть и некоммутативной. В дальнейшем нам даже не понадобится перемножать разные элементы этой алгебры. Мы будем использовать лишь операцию возведения в целую неотрицательную степень k и однородность этой операции относительно умножения на элементы основного поля $(\lambda a)^k = \lambda^k a^k$ при $a \in V$, $\lambda \in K$. Итак, пусть V – алгебра над полем нулевой характеристики K, содержащем все корни из единицы.

Утверждение 3.6. *Пусть A – автоморфизм конечного порядка n алгебры V, $A^n = I$ и V_0 – подалгебра инвариантов. Пусть поле нулевой характеристики K содержит все корни степени n из единицы. Тогда каждый элемент x алгебры V представим в виде суммы $x = x_1 + \cdots + x_n$ элементов $x_i \in V$ таких, что $x_i^n \in V_0$.*

Доказательство. Рассмотрим конечномерное линейное пространство в алгебре V, натянутое на орбиту $x, A(x), \ldots, A^{n-1}(x)$ элемента x относительно действия автоморфизма A и его степеней. Так как A^n по условию является тождественным преобразованием пространства V и поле K содержит все собственные числа линейного преобразования $A\colon V \to V$, то V раскладывается в прямую сумму собственных подпространств $V = V_1 \oplus \cdots \oplus V_n$ оператора A с собственными числами ξ_k, $1 \leqslant k \leqslant n$, – корнями n-й степени из единицы (некоторые из пространств V_i могут быть нулевыми). Поэтому вектор x представим в виде $x = x_1 + \cdots + x_n$, где $A(x_k) = \xi_k x_k$. Следовательно, $A(x_k^n) = (A(x_k))^n = \xi_k^n x_k^n = x_k^n$. То есть элемент x_k^n принадлежит алгебре инвариантов автоморфизма A.

Введем следующее определение.

Определение. Скажем, что элемент x алгебры V получается *операцией извлечения n-й степени из элемента a*, если выполняется равенство $x^n = a$.

Пользуясь этим определением, утверждение 3.6 можно интерпретировать следующим образом: каждый элемент x в алгебре V представляется в виде суммы корней n-й степени из элементов алгебры инвариантов. Утверждение 3.6 легко обобщается на случай действия конечной коммутативной группы автоморфизмов.

Утверждение 3.7. *Пусть G – конечная коммутативная группа порядка n автоморфизмов алгебры V, и пусть V_0 – подалгебра инвариантов. Тогда каждый элемент x алгебры V представим в виде суммы $x = x_1 + \dots + x_n$ элементов $x_i \in V$ таких, что $x_i^m \in V_0$, где m – наименьшее общее кратное порядков элементов группы G.*

Доказательство утверждения 3.7 почти дословно повторяет доказательства утверждения 3.6, нужно только воспользоваться тем, что конечная коммутативная группа линейных преобразований в некотором базисе приводится к диагональному виду.

Теорема 3.8. *Пусть G – конечная разрешимая группа автоморфизмов алгебры V, и пусть V_0 – подалгебра инвариантов. Тогда каждый элемент x алгебры V получается из элементов алгебры инвариантов V_0 при помощи извлечения корней и суммирований.*

Докажем сначала следующее простое утверждение о действии группы на множестве.

Пусть группа G действует на множестве X, пусть H – нормальный делитель группы G, и пусть X_0 – подмножество X, состоящее из неподвижных точек относительно действия группы G.

Утверждение 3.9. *Подмножество X_H множества X, состоящее из неподвижных точек относительно действия нормального делителя H, инвариантно относительно действия группы G. На множестве X_H естественно действует фактор-группа G/H с неподвижным множеством X_0.*

Доказательство. Пусть $g \in G$ и $h \in H$. Тогда элемент $g^{-1}hg$ принадлежит нормальному делителю H. Пусть $x \in X_H$. Тогда $g^{-1}hg(x) = x$, или $h(gx) = g(x)$, что означает, что элемент $g \in X$ неподвижен при действии нормального делителя H. Итак, множество X_H инвариантно относительно действия группы G. При этом действии элементам нормального делителя H соответствуют тождественные преобразования. Поэтому действие группы G на X_H сводится к действию фактор-группы G/H.

Перейдем теперь к доказательству теоремы 3.8.

Доказательство. Так как группа G разрешима, то у нее существует цепочка вложенных подгрупп $G = G_0 \supset \dots \supset G_m = e$ такая, что группа G_m совпадает с единичным элементом e и при $i = 1, \ldots, m$ группа G_i является нормальным делителем группы G_{i-1}, причем фактор-группа G_{i-1}/G_i коммутативна.

Такая цепочка подгрупп существует ввиду разрешимости группы G.

Обозначим через $V_0 \subset \cdots \subset V_m = V$ цепочку подалгебр инвариантов алгебры V относительно действия групп $G_0, \ldots, G_m$. Согласно утверждению 3.9, коммутативная фактор-группа G_{i-1}/G_i естественно действует на алгебры инвариантов V_i, оставляя неподвижной подалгебру инвариантов V_{i-1}. Согласно утверждению 3.7, каждый элемент алгебры V_i выражается при помощи суммирования и извлечения корней через элементы алгебры V_{i-1}. Последовательно повторяя это рассуждение, мы выразим каждый элемент алгебры V через элементы подалгебры V_0 цепочкой извлечения корней и суммирования.

Замечание. Цепочку нормальных делителей конечной разрешимой группы G можно выбрать таким образом, что все фактор-группы G_i/G_{i-1} будут не только коммутативными, но и циклическими. Поэтому для доказательства теоремы вполне достаточно использовать утверждение 3.6.

Закончим доказательство теоремы 3.5 о разрешимости уравнений в радикалах.

Следствие 3.10. *Если группа Галуа алгебраического уравнения над полем K разрешима, то уравнение решается в радикалах над этим полем.*

Доказательство. Согласно основной теореме теории Галуа, поле инвариантов относительно действия группы Галуа совпадает с полем K. Поэтому следствие вытекает из теоремы 3.8.

3.3.2. Решения уравнений второй, третьей и четвертой степени. Теорема 3.8 объясняет, почему уравнения маленькой степени решаются в радикалах.

Пусть $K[x_1, \ldots, x_n]$ – кольцо многочленов от переменных $x_1, \ldots, x_n$ над полем нулевой характеристики K, содержащем все корни из единицы. Группа $S(n)$ перестановок n элементов действует на этом кольце, переставляя переменные $x_1, \ldots, x_n$ в многочленах из этого кольца. Алгебра инвариантов $K_S[x_1, \ldots, x_n]$ относительно этого действия состоит из симметричных многочленов. Каждый многочлен этой алгебры явным образом представляется в виде многочлена от переменных $\sigma_1, \ldots, \sigma_n$, где $\sigma_1 = x_1 + \cdots + x_n$, $\sigma_2 = \sum_{i<j} x_i x_j$, $\ldots$, $\sigma_n = x_1 \cdots x_n$. При $n = 2, 3, 4$ группа $S(n)$ разрешима. Применяя теорему 3.8, получаем, что каждый полином от $x_1, \ldots, x_n$ при $n \leqslant 4$ выражается через основные симметрические многочлены $\sigma_1, \ldots, \sigma_n$ при помощи извлечения корней, суммирования и умножения на рациональные числа. Рассмотрим алгебраическое уравнение

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

Согласно формулам Виета, коэффициенты этого уравнения с точностью до знака совпадают с основными симметрическими функциями от его корней $x_1, \ldots, x_n$, поэтому *теорема* 3.8 *при* $n = 2, 3, 4$ *дает явное выражение корней уравнения* (4) *через коэффициенты этого уравнения при помощи извлечения корней, суммирования и умножения на рациональные числа.*

3.3.3. Общее алгебраическое уравнение и теорема Абеля. Общим алгебраическим уравнением степени n называется алгебраическое уравнение

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \tag{5}$$

коэффициенты $a_1, \dots, a_n$ которого являются независимыми комплексными переменными. Общее алгебраическое уравнение определено над полем K рациональных функций от переменных $a_1, \dots, a_n$. Пусть a^0 – некоторая точка в пространстве $\mathbb{C}^n$ с координатами $a_1, \dots, a_n$, в которой дискриминант уравнения (5) не обращается в нуль. В малой окрестности U точки a^0 существует n алгебраических функций $x_1, \dots, x_n$, удовлетворяющих уравнению (5). Рассмотрим поле P_U мероморфных функций в области U, порожденное функциями $x_1, \dots, x_n$ над полем K_U, изоморфное полю K и состоящее из ограничений рациональных функций на область U. По определению поле P является расширением Галуа поля K_U, соответствующим уравнению (5) над K_U.

Пусть $V\colon \mathbb{C}^n \to \mathbb{C}^n$ – отображение Виета, переводящее точку $x = (x_1, \dots, x_n)$ в точку $a(x)$ с координатами $a_1 = -(x_1 + \dots + x_n), \dots, a_n = (-1)^n x_1 \cdots x_n$. На пространстве-прообразе действует группа $S(n)$ перестановок координат $x_1, \dots, x_n$. Действие $S(n)$ переносится на поле $R[x_1, \dots, x_n]$ рациональных функций от переменных $x_1, \dots, x_n$. Поле инвариантов $R_S[x_1, \dots, x_n]$ относительно этого действия состоит из симметричных рациональных функций от $x_1, \dots, x_n$.

Утверждение 3.11.

1) *Пара полей $K_U \subset P_U$ изоморфна паре полей $R_S[x_1, \dots, x_n] \subset R[x_1, \dots, x_n]$.*

2) *Группа Галуа уравнения* (5) *изоморфна симметрической группе $S(n)$.*

Доказательство. 1) Функции $x_1, \dots, x_n$, удовлетворяющие уравнению (5) в малой окрестности U, задают локальное обращение отображения Виета, т.е. $V(x(a)) = a$, где $x(a) = (x_1(a), \dots, x_n(a))$. Обозначим через U_0 образ области U при этом локальном обращении. Рассмотрим пару функциональных полей $V^*K_U \subset V^*P_U$ на области U_0, индуцированных при отображении V из функциональных полей $K_U \subset P_U$ на области U. Поле V^*P_U изоморфно полю $R[x_1, \dots, x_n]$ всех рациональных функций от $x_1, \dots, x_n$. Поле V^*K_U изоморфно полю $R_S[x_1, \dots, x_n]$ всех симметричных рациональных функций от $x_1, \dots, x_n$. Действительно, согласно теореме о симметричных рациональных функциях, каждая такая функция является рациональной функцией от $x_1 + \dots + x_n, \dots, x_1 \cdots x_n$.

2) Группа $S(n)$ перестановок координат действует без ядра на поле рациональных функций, причем полем инвариантов является поле симметричных рациональных функций. Согласно основной теореме теории Галуа (см. п. 3.2), группа Галуа расширения Галуа $R_S[x_1, \dots, x_n] \subset R[x_1, \dots, x_n]$ изоморфна группе $S(n)$.

Теорема 3.12 (Абель). *Общее алгебраическое уравнение степени $\geqslant 5$ не решается в радикалах.*

Доказательство. Группа $S(n)$ при $n \geqslant 5$ неразрешима.

Замечание. Эта теорема была доказана Абелем еще до возникновения теории Галуа и теории групп. Его оригинальное доказательство ближе к методу Лиувилля, чем к теории Галуа.

3.4. Понижение степени уравнения. Можно ли выразить корни данного алгебраического уравнения степени n через его коэффициенты, используя арифметические операции, присоединение радикалов и присоединение решений и алгебраических уравнений степени k меньше, чем n? В п. 3.4.2 мы даем ответ на этот вопрос в терминах группы Галуа уравнения. Для этого нам понадобятся свойства подгрупп группы перестановок.

3.4.1. Подгруппы группы перестановок k элементов. Нам понадобится следующая лемма.

Лемма 3.13 [21]. *Группа Γ изоморфна подгруппе $S(k)$, если и только если группа Γ обладает набором подгрупп Γ_i, $i = 1, \ldots, m$, таким, что*

1) *группа $\bigcap_{i=1}^m \Gamma_i$ не содержит нормальных делителей группы Γ, отличных от тривиального;*
2) $\sum_{i=1}^m \operatorname{ind}(\Gamma, \Gamma_i) \leqslant k$.

Доказательство. Пусть Γ является подгруппой $S(k)$. Рассмотрим представление группы Γ как некоторой подгруппы перестановок множества M, содержащего k элементов. Пусть под действием группы Γ множество M распадается на m орбит. Выберем в каждой орбите по точке x_i. Набор стационарных подгрупп Γ_i точек x_i удовлетворяет условиям леммы.

Обратно, пусть группа Γ обладает набором подгрупп, удовлетворяющим условиям леммы. Обозначим через P непересекающееся объединение множеств $P_i = \{P_i^j\}$ – множеств правых классов смежности P_i^j группы Γ по подгруппе Γ_i. Группа Γ обладает естественным действием на множестве P. Возникающее представление группы Γ в группу $S(P)$ точное, так как ядро этого представления лежит в группе $\bigcap_{i=1}^m \Gamma_i$. Группа $S(P)$ вкладывается в группу $S(k)$, так как в множестве P содержится $\sum_{i=1}^m \operatorname{ind}(\Gamma, \Gamma_i) \leqslant k$ элементов.

Следствие 3.14. *Фактор-группа подгруппы симметрической группы $S(k)$ изоморфна подгруппе симметрической группы $S(k)$.*

Доказательство. Пусть группа G изоморфна подгруппе группы $S(k)$ и Γ_i – набор ее подгрупп, удовлетворяющих условию леммы 3.13. Пусть π – произвольный гомоморфизм группы G. Тогда совокупность подгрупп $\pi(\Gamma_i)$ в группе $\pi(G)$ тоже удовлетворяет условиям леммы.

Определение. Скажем, что *нормальный делитель H* в группе G *имеет глубину, не превосходящую k*, если в группе G существует подгруппа G_0 индекса, не превосходящего k, такая, что нормальный делитель H является пересечением всех подгрупп, сопряженных с подгруппой G_0. Будем говорить, что *группа G имеет глубину, не превосходящую k*, если единичный элемент этой группы является ее нормальным делителем глубины, не превосходящей k.

Определение. *Нормальной башней* группы G называется вложенная цепочка подгрупп $G = G_0 \supset \cdots \supset G_n = e$, в которой группа G_0 совпадает с исходной группой G, группа G_n тривиальна и для каждого $i = 0, 1, \ldots, n-1$ группа G_{i+1} является нормальным делителем группы G_i.

Следствие 3.15. *Если группа G является подгруппой группы $S(k)$, то у группы G существует нормальная башня $G = G_0 \supset \cdots \supset G_n = e$, в которой для каждого $i = 1, \ldots, n$ группа G_i имеет в группе G_{i-1} глубину, не превосходящую k.*

Доказательство. Пусть Γ_i – совокупность подгрупп в группе G, удовлетворяющих условиям леммы 3.13. Обозначим через F_i нормальный делитель группы G, равный пересечению всех подгрупп, сопряженных группе Γ_i. Цепочка подгрупп $G_0 = F_0$, $G_1 = F_0 \cap F_1, \ldots, G_m = F_0 \cap \cdots \cap F_m$ удовлетворяет требованиям следствия.

3.4.2. Условие понижаемости степени уравнения при помощи радикалов. Начнем с формальных определений.

Определение. Алгебраическое уравнение над полем K *решается при помощи радикалов и корней уравнений степени не выше* k (или, короче, *решается в* k*-радикалах*), если существует цепочка расширений $K = K_0 \subset \cdots \subset K_N$, в которой поле K_i получается из поля K_{i-1}, $i = 1, \dots, N$, либо присоединением радикала, либо присоединением всех корней алгебраического уравнения степени не выше k с коэффициентами в поле K_{i-1}, а поле K_N содержит все корни исходного алгебраического уравнения.

Определение. Группа G называется k-разрешимой, если у нее существует нормальная башня

$$G = H_0 \supset \cdots \supset H_N = e$$

такая, что для каждого i, $i = 1, \dots, N$, либо глубина нормального делителя H_i в группе H_{i-1} не превосходит k, либо фактор-группа H_{i-1}/H_i коммутативна.

Теорема 3.16. *Алгебраическое уравнение решается в* k*-радикалах, если и только если его группа Галуа* G k*-разрешима.*

Справедлива следующая лемма.

Лемма 3.17. *Пусть на поле* P *действует конечная группа автоморфизмов с полем инвариантов* P_0. *Пусть орбита точки* $x \in P$ *содержит ровно* m *элементов. Тогда* x *удовлетворяет некоторому алгебраическому уравнению степени* m *с коэффициентами из поля* P_0.

Доказательство. Пусть $x_1, \dots, x_m$ – точки орбиты. Основные симметрические функции $\sigma_1, \dots, \sigma_m$ от этих точек остаются неподвижными при действии группы и, следовательно, принадлежат полю инвариантов. Точки орбиты являются корнями алгебраического уравнения степени m

$$x^m - \sigma_1 x^{m-1} + \cdots + (-1)^m \sigma_m = 0$$

с коэффициентами из поля инвариантов P_0.

Лемма 3.18. *Пусть на поле* P *действует конечная группа автоморфизмов* G *с полем инвариантов* P_0. *Пусть глубина группы* G *не превосходит* k. *Тогда поле* P *можно получить из поля* P_0 *присоединением всех корней некоторого алгебраического уравнения степени, не превосходящей* k, *с коэффициентами из поля* P_0.

Доказательство. Пусть G_0 – подгруппа группы G индекса m, не превосходящего k, такая, что пересечение всех подгрупп, сопряженных с G_0, содержит лишь единичный элемент группы G. Согласно основной теореме теории Галуа, подгруппе G_0 соответствует некоторое промежуточное поле P_1; $P_0 \subseteq P_1 \subseteq P$. Поле P_1, как и любое другое конечное алгебраическое расширение поля P_0, порождается над полем P_0 некоторым элементом x. Точка x обладает следующим свойством: элемент g группы G оставляет точку x на месте, если и только если $g \in G_0$. Орбита точки x относительно действия группы G содержит ровно m точек, поскольку индекс стационарной подгруппы точки x равен m. Неединичный элемент группы G задает отличную от тождественной перестановку точек орбиты, поскольку пересечение подгрупп, сопряженных с группой G_0, совпадает с единичным элементом группы G. Поле, порожденное над P_0 элементами орбиты, совпадает с полем P. Действительно, это поле соответствует тривиальной подгруппе группы Галуа. Лемма 3.18 теперь вытекает из леммы 3.17.

Вернемся к доказательству теоремы 3.16.

Доказательство теоремы 3.16. 1) Необходимость условия на группу Галуа доказывается так же, как необходимость разрешимости группы Галуа для разрешимости уравнения в радикалах. Нужно лишь рассмотреть, что происходит с группой Галуа G_i нашего уравнения над полем K_i при переходе к полю K_{i+1}, если поле K_{i+1} получено из поля K_i присоединением всех корней уравнения степени $\leqslant k$. В этом случае группа Галуа поля K_{i+1} над полем K_i является подгруппой группы $S(k)$ (см. лемму 3.2). Согласно теореме 3.4 о поведении группы Галуа при изменении основного поля, фактор-группа G_i/G_{i+1} является фактор-группой некоторой подгруппы в $S(k)$. Согласно следствиям 3.14 и 3.15, у группы G_i/G_{i+1} существует нормальная башня $G_i/G_{i+1} = \Gamma_0 \supset \cdots \supset \Gamma_m = e$ такая, что группа Γ_{i+1} имеет в группе Γ_i глубину $\leqslant k$. Между группами $G_i \supset G_{i+1}$ достаточно вставить цепочку подгрупп

$$G_i = \Gamma_{0i} \supset \cdots \supset \Gamma_{mi} = G_{i+1},$$

где Γ_{pi} – прообраз группы Γ_p при гомоморфизме факторизации $G_i \to G_i/G_{i+1}$. Ясно, что группа $\Gamma_{p+1,i}$ является нормальным делителем глубины $\leqslant k$ в группе Γ_{pi}. Это и доставляет недостающее звено в доказательстве необходимости условия на группу Галуа.

2) Достаточность условия на группу Галуа доказывается индукцией по длине N нормальной башни в группе G. Группа G имеет k-разрешимый нормальный делитель H_1 с нормальной башней длины $N-1$. Обозначим через P_1 поле инвариантов группы H_1. Согласно индукционному предположению, поле P получается из поля P_1 при помощи присоединений радикалов и корней уравнений степени не выше k. Фактор-группа G/H_1 действует на поле P_1 с полем инвариантов P_0. Если фактор-группа G/H_1 коммутативна, то поле P_1 получается из поля P_0 при помощи присоединения радикалов (см. утверждение 3.7). Если фактор-группа G/H_1 имеет глубину, не превосходящую k, то поле P_1 получается из поля P присоединением всех корней алгебраического уравнения степени не выше k (см. лемму 3.18).

Теорема 3.19. *Общее алгебраическое уравнение* (см. п. 3.3.3) *степени $n \geqslant 5$ не решается при помощи радикалов и корней алгебраических уравнений степени меньше n.*

Доказательство. Группа Галуа общего алгебраического уравнения степени n изоморфна группе $S(n)$ (см. п. 3.3.3).

При $n \geqslant 5$ группа $S(n)$ имеет всего лишь две различных башни нормальных подгрупп: тривиальную башню $e \subset S(n)$ и башню $e \subset A(n) \subset S(n)$, где e – единичная подгруппа, а $A(n)$ – знакопеременная подгруппа. Поэтому группа $S(n)$ при $n \geqslant 5$ не является разрешимой.

§ 4. Разрешимость линейных дифференциальных уравнений в квадратурах и теория Пикара–Вессио

Пикар обратил внимание на аналогию между линейными дифференциальными уравнениями и алгебраическими уравнениями и начал строить дифференциальный аналог теории Галуа. Венцом этой теории является теорема Пикара–Вессио, в которой вопрос о разрешимости или неразрешимости линейного дифференциального уравнения связывается с вопросом о разрешимости или неразрешимости некоторой алгебраической группы Ли.

4.1. Аналогия между линейными дифференциальными уравнениями и алгебраическими уравнениями. Напомним простейшие свойства линейных дифференциальных уравнений и их аналоги для алгебраических уравнений.

4.1.1. Деление с остатком и наибольший общий делитель дифференциальных операторов. Линейным дифференциальным оператором порядка n над дифференциальным полем K называется оператор $L = a_nD^n + \cdots + a_0$, где $a_i \in K$ и $a_n \neq 0$, действующий на элементы y поля K по формуле

$$L(y) = a_ny^{(n)} + \cdots + a_0y.$$

Для операторов L_1 и L_2 над K их произведение $L = L_1 \circ L_2 = L_1(L_2)$ тоже является оператором над K. Произведение операторов, вообще говоря, некоммутативно, но в старшем члене эта некоммутативность не проявляется. Именно, *старший член a_nD^n оператора L для $L = L_1 \circ L_2$ равен $b_mc_kD^{m+k}$, где b_mD^m и c_kD^k – старшие члены операторов L_1 и L_2.*

Для операторов L и L_2 порядков n и k над K существуют и единственны операторы L_1 и R над K такие, что $L = L_1 \circ L_2 + R$ и порядок оператора R строго меньше, чем k. Оператор R называется *остатком от деления справа* оператора L на оператор L_2. Операторы L_1 и R строятся по операторам L и L_2 явно: алгоритм деления операторов с остатком основан на приведенной выше формуле для старшего члена произведения операторов и абсолютно аналогичен алгоритму деления с остатком полиномов от одной переменной.

Для любых двух операторов L_1 и L_2 над K можно явно найти их правый наибольший общий делитель N, т.е. оператор N над K наибольшего возможного порядка, который делит справа операторы L_1 и L_2, т.е. $L_1 = M_1 \circ N$ и $L_2 = M_2 \circ N$, где M_1 и M_2 – некоторые операторы над K. Нахождение операторов M_1, M_2 и N по операторам L_1 и L_2 абсолютно аналогично алгоритму Евклида нахождения наибольшего общего делителя двух полиномов от одной переменной и основано на алгоритме деления операторов с остатком. Как и в коммутативном случае, наибольший общий делитель N представим в виде $N = AL_1 + BL_2$, где A, B – некоторые операторы над K.

Ясно, что y является решением уравнения $N(y) = 0$, если и только если $L_1(y) = 0$ и $L_2(y) = 0$.

4.1.2. Понижение порядка линейного дифференциального уравнения как аналог теоремы Безу. Пусть L – линейный дифференциальный оператор над K, y_1 – ненулевой элемент поля K, $p = \dfrac{y_1'}{y_1}$ – его логарифмическая производная и $L_2 = D - p$ – оператор первого порядка, аннулирующий y_1. Остаток R от деления справа L на L_2 является оператором умножения на c_0, где $c_0 = \dfrac{1}{y_1}L(y_1)$. Действительно, нужное равенство получается при подстановке $y = y_1$ в тождество $L(y) \equiv L_1 \circ L_2(y) + c_0 y$. Оператор L делится справа на оператор L_2, если и только если элемент y_1 удовлетворяет тождеству $L(y_1) \equiv 0$.

Используя ненулевое решение y_1 уравнения n-го порядка $L(y) = 0$, можно понизить порядок этого уравнения. Для этого надо представить оператор L в виде $L = L_1 \circ L_2$, где L_1 – оператор $(n-1)$-го порядка. *Коэффициенты оператора L_1 лежат в расширении дифференциального поля K логарифмической производной p элемента y_1.* Если известно какое-либо решение u уравнения $L_1(u) = 0$, то по нему можно построить некоторое решение y исходного уравнения $L(y) = 0$. Для этого достаточно решить уравнение $L_2(y) = y' - py = u$. Описанная процедура называется *понижением порядка дифференциального уравнения.*

Замечание. Оператор, аннулирующий y_1, определен с точностью до умножения на произвольную функцию, и от выбора этой функции зависит процедура понижения порядка. Легче делить на оператор $\widetilde{L}_2 = D \circ y_1^{-1}$, являющийся композицией умножения на элемент y_1^{-1} и дифференцирования. Для этого достаточно вычислить оператор $L_3 = L \circ y_1$, являющийся композицией умножения на элемент y_1 и оператора L. Оператор L_3 делится справа на D, т.е. $L_3 = \widetilde{L}_1 \circ D$, так как $L_3(1) \equiv L \circ y_1(1) \equiv 0$. Видно, что $L = \widetilde{L}_1 \circ \widetilde{L}_2$. Исходное уравнение $L(y) = 0$ сводится к уравнению $\widetilde{L}_1(u) = 0$ меньшего порядка. Обычно именно такую процедуру понижения порядка приводят в учебниках по дифференциальным уравнениям. Отметим, что коэффициенты оператора $\widetilde{L}_1$ лежат в расширении дифференциального поля K самим элементом y_1, а не его логарифмической производной p, что иногда делает оператор $\widetilde{L}_1$ менее удобным, чем оператор L_1.

В алгебре есть следующие аналоги приведенных фактов: 1) остаток от деления полинома P переменной x на $(x - a)$ равен значению полинома P в точке a (теорема Безу); 2) если известно одно решение x_1 уравнения $P(x) = 0$, то его степень можно понизить: остальные корни полинома P удовлетворяют уравнению меньшей степени $Q(x) = 0$, где $Q = P : (x - x_1)$. Кроме аналогии здесь имеется и отличие: решения дифференциального уравнения, полученного процедурой понижения порядка, вообще говоря, не являются решениями исходного уравнения.

Замечание. Экспоненты являются собственными функциями дифференциальных операторов $P(D)$ с постоянными коэффициентами. Этот факт эквивалентен теореме Безу. Действительно, если $P = Q(x-a) + P(a)$, то $P(D) = Q(D) \circ (D-a) + P(a)$. Поэтому решение y_1 дифференциального уравнения $(D - a)y = 0$ является собственным вектором оператора $P(D)$ с собственным числом $P(a)$.

4.1.3. Аналог формул Виета для дифференциальных операторов. Если известны все корни $x_1, \ldots, x_n$ полинома P степени n со старшим коэффициентом 1, то полином P можно восстановить: по формулам Виета $P(x) = x^n + p_1 x^{n-1} + \cdots + p_n$, где $p_1 = -\sigma_1$, $\ldots$, $p_n = (-1)^n \sigma_n$ и $\sigma_1 = x_1 + \cdots + x_n$, $\ldots$, $\sigma_n = x_1 \cdots x_n$. Функции $\sigma_1, \ldots, \sigma_n$ не меняются при перестановке корней и называются основными симметрическими функциями.

Аналогично этому, если известны n линейно независимых решений $y_1, \ldots, y_n$ линейного дифференциального уравнения n-го порядка $L = 0$, где L – оператор, у которого коэффициент при старшей производной равен единице, то оператор L можно восстановить. Действительно, прежде всего такой оператор не более чем один: разность $L_1 - L_2$ двух операторов, обладающих этими свойствами, является оператором порядка $< n$, имеющим n линейно независимых решений, что возможно, лишь если L_1 совпадает с L_2.

Вронскиан W от n независимых решений $y_1, \dots, y_n$ линейного дифференциального уравнения не равен нулю. Рассмотрим уравнение $W(y, y_1, \dots, y_n) = 0$, где $W(y, y_1, \dots, y_n)$ – вронскиан от неизвестной функции y и функций $y_1, \dots, y_n$. Раскрывая вронскиан

$$W(y, y_1, \dots, y_n) = \begin{vmatrix} y & y_1 & \dots & y_n \\ \vdots & \vdots & & \vdots \\ y^{(n)} & y_1^{(n)} & \dots & y_n^{(n)} \end{vmatrix}$$

по первому столбцу и деля его на W, получим уравнение

$$y^{(n)} + p_1 y^{(n-1)} + \dots + p_n y = 0, \tag{6}$$

в котором $p_1 = -\varphi_1, \dots, p_n = (-1)^n \varphi_n$, где

$$\varphi_1 = \frac{\begin{vmatrix} y_1 & \dots & y_n \\ \vdots & & \vdots \\ y_1^{(n-2)} & \dots & y_n^{(n-2)} \\ y_1^{(n)} & \dots & y_n^{(n)} \end{vmatrix}}{W}, \quad \dots, \quad \varphi_n = \frac{\begin{vmatrix} y_1' & \dots & y_n' \\ \vdots & & \vdots \\ y_1^{(n-1)} & \dots & y_n^{(n-1)} \\ y_1^{(n)} & \dots & y_n^{(n)} \end{vmatrix}}{W}. \tag{7}$$

Функции $y_1, \dots, y_n$ и их линейные комбинации является решениями уравнения (6). Формулы (6), (7) вполне аналогичны формулам Виета.

Функции $\varphi_1, \dots, \varphi_n$ являются рациональными функциями от функций $y_1, \dots, y_n$ и от их производных до порядка n. Эти функции зависят лишь от линейного пространства V, натянутого на функции $y_1, \dots, y_n$, но не зависят от выбора конкретного базиса $y_1, \dots, y_n$ в пространстве V. Другими словами, функции $\varphi_1, \dots, \varphi_n$ являются $GL(V)$ инвариантными функциями от $y_1, \dots, y_n$ и от их производных. Функции $\varphi_1, \dots, \varphi_n$ будем называть *основными дифференциальными инвариантами* от $y_1, \dots, y_n$.

4.1.4. Аналог теоремы о симметричных функциях для дифференциальных операторов. Как известно из алгебры, всякая рациональная функция от переменных $x_1, \dots, x_n$, не меняющаяся при перестановках переменных, на самом деле является рациональной функцией основных симметрических функций $\sigma_1, \dots, \sigma_n$ переменных $x_1, \dots, x_n$. Другими словами, всякое рациональное выражение, симметрично зависящее от корней полинома степени n, рационально выражается через коэффициенты этого полинома.

Аналогичная теорема для линейных дифференциальных уравнений была открыта Пикаром.

ТЕОРЕМА 4.1. *Всякая рациональная функция R от линейно независимых функций $y_1, \dots, y_n$ и их производных, которая является $GL(V)$-инвариантной* (т.е. которая не изменится, если функции $y_1, \dots, y_n$ заменить их линейными комбинациями $z_1 = a_{11}y_1 + \dots + a_{1n}y_n, \dots, z_n = a_{n1}y_1 + \dots + a_{nn}y_n$ при условии, что матрица $A = \{a_{ij}\}$ невырождена), *на самом деле является рациональной функцией* *от основных дифференциальных инвариантов $\varphi_1,\dots,\varphi_n$ функций $y_1,\dots,y_n$ и от производных этих инвариантов.*

Доказательство. Каждая функция y в пространстве V, натянутом на $y_1,\dots,y_n$, удовлетворяет тождеству $y^{(n)}-\varphi_1y^{(n-1)}+\dots+(-1)^n\varphi_ny=0$. Дифференцируя это тождество, можно выразить любую производную функции y порядка $\geqslant n$ через функцию y, ее производные порядка $< n$, основные дифференциальные инварианты и их производные. Подставляя найденные выражения старших производных функций $y_1,\dots,y_n$ в рациональную функцию R, мы получим рациональную функцию $\widetilde{R}$ от функций $\varphi_1,\dots,\varphi_n$, их производных и от элементов фундаментальной матрицы Y, где

$$Y=\begin{vmatrix} y_1 & \dots & y_n\\ \vdots & & \vdots\\ y_1^{(n-1)} & \dots & y_n^{(n-1)}\end{vmatrix}.$$

Функция $\widetilde{R}$ не может меняться при линейных преобразованиях пространства V, натянутого на $y_1,\dots,y_n$. Любая невырожденная $(n\times n)$-матрица может быть получена как образ фундаментальной матрицы Y при некотором линейном преобразовании пространства V. Рациональная функция $\widetilde{R}$ должна быть постоянна на множестве невырожденных матриц, поэтому она постоянна на множестве всех матриц, не зависит от матрицы Y, а зависит лишь от дифференциальных инвариантов и их производных.

Следствие 4.2. *Всякая рациональная функция от независимых решений $y_1,\dots,y_n$ линейного дифференциального уравнения и от их производных, которая не меняется при выборе другого базиса $z_1,\dots,z_n$ в пространстве решений, является рациональной функцией от коэффициентов дифференциального уравнения и от их производных.*

4.2. Группа Галуа линейного дифференциального уравнения. Рассмотрим линейное дифференциальное уравнение

$$y^{(n)}+p_1y^{(n-1)}+\dots+p_ny=0 \tag{8}$$

с коэффициентами в некотором функциональном дифференциальном поле K. (Напомним, что мы всегда предполагаем, что поле K содержит все комплексные константы.)

Дифференциальным полиномом над K от функций $u_1,\dots,u_n$ называется полином с коэффициентами из K от функции $u_1,\dots,u_n$ и от их производных. *Дифференциальным соотношением* над K между решениями $y_1,\dots,y_n$ уравнения (8) называется дифференциальный полином над полем K от функций $u_1,\dots,u_n$, который обращается в нуль при подстановке $u_1=y_1,\dots,u_n=y_n$.

Определение. *Группой Галуа дифференциального уравнения* (8) *над дифференциальным полем* K называется подгруппа G группы $GL(V)$ всех линейных преобразований пространства решений V уравнения (8), сохраняющих все дифференциальные соотношения над K между решениями уравнения (т.е. если $A\in G$ и Q – любое соотношение над K между некоторыми решениями $y_1,\dots,y_n$, то решения $Ay_1,\dots,Ay_n$ должны быть связаны тем же соотношением Q).

Утверждение 4.3. *Группа Галуа линейного дифференциального уравнения является алгебраической подгруппой в* $GL(V)$.

Доказательство. Очевидно, что для каждого дифференциального соотношения Q между решениями $y_1, \dots, y_n$ множество линейных преобразований A, для которых соотношение Q выполняется для $Ay_1, \dots, Ay_n$, является алгебраическим. Пересечение любого числа алгебраических многообразий является алгебраическим многообразием.

Определение. Функциональное дифференциальное поле P называется *расширением Пикара–Вессио* функционального дифференциального поля K, если существует линейное дифференциальное уравнение (8) с коэффициентами в дифференциальном поле K такое, что P получается присоединением к K всех решений уравнения (8). *Группой Галуа расширения Пикара–Вессио* над полем K называется группа всех автоморфизмов дифференциального поля P, оставляющих на месте все элементы поля K.

Каждый элемент τ из группы Галуа дифференциального поля P над дифференциальным полем K задает линейное преобразование пространства решений и сохраняет все дифференциальные соотношения, определенные над полем K между решениями. Таким образом, группа Галуа дифференциального поля P над K имеет представление в группе Галуа G уравнения (8), определяющее расширение Пикара–Вессио P. Очевидно, что это представление является изоморфизмом групп, т.е. группа Галуа уравнения и группа Галуа заданного им расширения Пикара–Вессио изоморфны. Используя этот изоморфизм, можно определить на группе Галуа расширения Пикара–Вессио структуру алгебраической группы. Если два различных линейных дифференциальных уравнения над полем K задают одно и то же расширение Пикара–Вессио, то группы Галуа этих уравнений изоморфны не только как абстрактные группы, но и как алгебраические группы. Поэтому структура алгебраической группы на группе расширения Пикара–Вессио определена корректно.

4.3. Основная теорема теории Пикара–Вессио. Пусть P – расширение Пикара–Вессио дифференциального поля K и G – его группа Галуа.

Определены следующие отображения между множеством промежуточных дифференциальных полей F, $K \subseteq F \subseteq P$, и множеством подгрупп группы Галуа G.

1) *Отображение* Fd, сопоставляющее каждой подгруппе Γ группы G дифференциальное поле $Fd(\Gamma)$, состоящее из элементов поля P, остающихся неподвижными при действии подгруппы Γ (ясно, что $K \subseteq Fd(\Gamma)$).

2) *Отображение* Gp, сопоставляющее каждому промежуточному дифференциальному полю $F, K \subseteq F \subseteq P$, подгруппу $Gp(F) \subseteq G$, являющуюся группой Галуа расширения Пикара–Вессио P поля F (P является расширением Пикара–Вессио поля K, и поэтому оно автоматически является расширением Пикара–Вессио промежуточного поля $F, K \subset F \subset P$).

Отображения Fd и Gp устанавливают *соответствие Галуа* между подгруппами группы Галуа и промежуточными дифференциальными полями расширения Пикара–Вессио. Приведем без доказательства следующую теорему.

Основная теорема 4.4 (теории Пикара–Вессио). *Для всякого расширения* P *Пикара–Вессио дифференциального поля* K *с группой Галуа* G

1) *композиция отображений Fd и Gp является тождественным отображением множества промежуточных полей в себя: если F – дифференциальное поле и $K \subseteq F \subseteq P$, то $Fd(Gp(F)) = F$;*

2) *композиция отображений Gp и Fd сопоставляет каждой подгруппе Γ в группе Галуа G ее алгебраическое замыкание $\overline{\Gamma}$ в группе G: если Γ – подгруппа группы Галуа, $\Gamma \subset G$, то $Gp(Fd(\Gamma)) = \overline{\Gamma}$;*

3) *промежуточное дифференциальное поле F, $K \subseteq F \subseteq P$, является расширением Пикара–Вессио поля K, если и только если группа $Gp(F)$ является нормальным делителем группы G. При этом группа Галуа расширения Пикара–Вессио F поля K является фактор-группой группы G по нормальному делителю $Gp(F)$.*

Докажем полезное характеристическое свойство расширений Пикара–Вессио, непосредственно вытекающее из основной теоремы.

Следствие 4.5. *Дифференциальное поле P является расширением Пикара–Вессио дифференциального поля K, $K \subseteq P$, если и только если существует группа Γ автоморфизмов дифференциального поля P такая, что* 1) *она оставляет неподвижными все элементы поля K и только их*; 2) *существует лежащее в P конечномерное линейное пространство V над полем констант, инвариантное относительно группы Γ и такое, что поле P является наименьшим дифференциальным полем, содержащим V и K.*

Доказательство. Расширения Пикара–Вессио указанными свойствами обладают. Это вытекает из п. 1) основной теоремы, примененной к полю $F = K$. Обратно, пусть $y_1, \ldots, y_n$ – базис линейного пространства V, о котором идет речь в п. 2) следствия. Коэффициенты линейного дифференциального уравнения n-го порядка, которому удовлетворяют функции $y_1, \ldots, y_n$, инвариантны относительно всех линейных преобразований пространства V. Поэтому они инвариантны относительно группы Γ и лежат в K. Следовательно, P получается из K присоединением всех решений указанного уравнения и P является расширением Пикара–Вессио поля K.

Что произойдет с группой Галуа линейного дифференциального уравнения, если дифференциальное поле коэффициентов K расширить, заменив его бо́льшим дифференциальным полем K_1? Этот вопрос особенно интересен в том случае, когда поле K_1 является расширением Пикара–Вессио поля K. Обозначим через G_1 группу Галуа расширения K_1 дифференциального поля K. Результаты о неразрешимости линейных дифференциальных уравнений основаны на следующей теореме из теории Пикара–Вессио, которую мы приводим без доказательства и которая формулируется вполне аналогично теореме 3.4.

Теорема 4.6 (об изменении группы Галуа уравнения при расширении Пикара–Вессио поля коэффициентов). *При замене дифференциального поля коэффициентов K его расширением Пикара–Вессио K_1 группа Галуа G уравнения заменяется некоторым своим алгебраическим нормальным делителем H. Фактор-группа G/H группы G относительно этого нормального делителя изоморфна некоторой алгебраической фактор-группе группы Галуа G_1 нового дифференциального поля K_1 над старым дифференциальным полем K.*

4.4. Простейшие расширения Пикара–Вессио. В этом пункте рассматривается следующие простейшие расширения Пикара–Вессио: алгебраическое расширение, присоединение интеграла и присоединение экспоненты интеграла.

4.4.1. Алгебраическое расширение. Рассмотрим алгебраическое уравнение

$$Q(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0 \tag{9}$$

над функциональным дифференциальным полем K и расширение Галуа P, получающееся присоединением к полю K всех решений уравнения (9).

Лемма 4.7. *Поле P является дифференциальным полем. Каждый автоморфизм поля P над полем K, который сохраняет лишь арифметические операции в поле P, автоматически сохраняет и операцию дифференцирования.*

Доказательство. Изменив, если нужно, алгебраическое уравнение (9), можно считать, что оно неприводимо над полем K и что каждый корень x_i уравнения (9) порождает поле P над полем K. Дифференцируя тождество $Q(x_i) = 0$, получим $\dfrac{\partial Q}{\partial x}(x_i)x_i' + \dfrac{\partial Q}{\partial t}(x_i) = 0$, где $\dfrac{\partial Q}{\partial t} = \sum_{i=1}^{n-1} a_i' x^i$. Полином $\dfrac{\partial Q}{\partial t}$ не может обращаться в нуль в точке x_i, так как уравнение $Q = 0$ неприводимо. Получаем алгебраическое выражение производной $x_i' = -\dfrac{\partial Q}{\partial x}(x_i)\Big/\dfrac{\partial Q}{\partial t}(x_i)$ корня x_i, которое одинаково для всех корней x_i полинома Q. Отсюда и вытекают оба утверждения леммы.

Группа Галуа Γ расширения Галуа P над полем K оставляет неподвижными лишь элементы поля K. Линейное пространство V над полем констант, натянутое на корни $x_1, \dots, x_n$ уравнения (9), инвариантно относительно действия группы Γ. Согласно следствию 4.5, дифференциальное поле P является расширением Пикара–Вессио. Группа Галуа расширения Пикара–Вессио P поля K совпадает с группой Галуа алгебраического уравнения (9). *Основная теорема теории Пикара–Вессио для расширения Пикара–Вессио P дифференциального поля K совпадает с основной теоремой теории Галуа расширения Галуа P поля K.*

4.4.2. Присоединение интеграла. Пусть y_1 – интеграл над функциональным дифференциальным полем K и $y_1' = a$, $a \in K$, $a \neq 0$.

Однородное дифференциальное уравнение $ay'' - a'y' = 0$ имеет своими независимыми решениями y_1 и единицу. Расширение дифференциального поля K, полученное из K присоединением элемента y_1, является поэтому расширением Пикара–Вессио (напомним, что мы всегда предполагаем, что поле K содержит все комплексные постоянные).

Лемма 4.8. *Интеграл y_1 либо принадлежит полю K, либо трансцендентен над полем K.*

Доказательство. Допустим, что интеграл y_1 алгебраичен над полем K. Пусть $Q(y) = a_n y^n + \dots + a_0 = 0$ – неприводимое над K уравнение, которому удовлетворяет y_1. Можно считать, что $n > 1$ и что $a_n = 1$. Продифференцировав тождество $Q(y) = 0$, получим уравнение меньшей степени $nay^{n-1} + \dots + a_0' = 0$, которому удовлетворяет y_1. Это противоречит неприводимости полинома Q.

Пусть элемент y_1 трансцендентен над K. Покажем, что единственное независимое дифференциальное соотношение над K, которому удовлетворяет y_1, есть $y_1' = a$. Действительно, используя это соотношение, каждый дифференциальный полином над K от y_1 можно переписать как полином от y_1 с коэффициентами из K. Но ни один такой нетривиальный полином не может обратиться в нуль, так как элемент y_1 трансцендентен над K. Поэтому группа Галуа уравнения $ay'' - a'y' = 0$ состоит из линейных преобразований вида $Ay_1 = y_1 + C$, $A(1) = 1$, где C – любое комплексное число. Итак, *группа Галуа нетривиального интегрального расширения изоморфна аддитивной группе комплексных чисел.*

В терминологии Колчина [26] алгебраическая группа называется антикомпактной, если она не содержит элементов конечного порядка, отличных от единицы. Очевидно, что *группа Галуа нетривиального интегрального расширения антикомпактна.*

Утверждение 4.9. *Не существует дифференциальных полей между полем K и $K\langle y\rangle$, где y – интеграл над K, не лежащий в K.*

Доказательство. Действительно, пусть F – дифференциальное поле такое, что $K \subset F \subseteq K\langle y\rangle$. Пусть $b \in F$ и $b \notin K$. Тогда элемент b представим в виде нетривиальной рациональной функции от y с коэффициентами из K. Существование такой функции означает, что элемент y алгебраичен над F. Но элемент y является интегралом над F, так как $y' = a \in K$. Интеграл алгебраичен над дифференциальным полем, если и только если он лежит в этом поле (см. лемму 4.8), т.е. $F = K\langle y\rangle$.

Утверждение доказывает основную теорему теории Пикара–Вессио для присоединения интеграла. Действительно, группа Галуа C поля $K\langle y\rangle$ над полем K не имеет алгебраических подгрупп, а пара дифференциальных полей $K \subset K\langle y\rangle$ не содержит промежуточных дифференциальных полей.

4.4.3. Присоединение экспоненты интеграла. Пусть y_1 – экспонента интеграла над функциональным дифференциальным полем K, т.е. $y_1' = ay_1$, где $a \in K$. Расширение поля K элементом y_1 является по определению расширением Пикара–Вессио.

Лемма 4.10. *Пусть экспонента интеграла y_1 является алгебраичным над полем K элементом. Тогда y_1 – радикал над полем K.*

Доказательство. Пусть $Q(y) = a_n y^n + \dots + a_0 = 0$ – неприводимое над K уравнение, которому удовлетворяет элемент y_1. Можно считать, что $n > 1$, $a_n \neq 0$ и $a_0 = 1$. Продифференцировав тождество $Q(y_1) = 0$, получим уравнение $\sum(a_k' + k a_k a)y^k = 0$, которому удовлетворяет y_1. Это уравнение имеет степень $\leqslant n$, но не содержит свободного члена. Все коэффициенты этого уравнения должны тождественно обратиться в нуль, так как в противном случае мы получим противоречие с неприводимостью полинома Q. Равенство $a_n' + n a_n a = 0$ означает, что частное $a_n/y_1^n = c$ является константой. Действительно, из соотношения $y_1' = ay_1$ вытекает, что $(y_1^{-n})' + na(y_1^{-n}) = 0$, т.е. что y_1^{-n} и a_n удовлетворяют одному и тому же уравнению. Поэтому $y^n = a_n/c$. Лемма доказана.

Допустим, что элемент y_1 трансцендентен над K. Покажем, что в этом случае единственное независимое дифференциальное соотношение над K, которому удовлетворяет y_1, есть $y_1' = ay_1$. Действительно, используя это соотношение, каждый дифференциальный полином над K от y_1 можно переписать как полином от y_1 с коэффициентами из K. Но ни один такой нетривиальный полином не может обратиться в нуль, так как y_1 трансцендентен над K. Поэтому группа Галуа уравнения $y' = ay$ состоит из линейных преобразований вида $Ay_1 = Cy_1$, где $C \neq 0$ – любое ненулевое комплексное число. Итак, *группа Галуа неалгебраического расширения, являющегося присоединением экспоненты интеграла, совпадает с мультипликативной группой* $\mathbb{C}^*$ *ненулевых комплексных чисел.*

Экспонента интеграла над K является алгебраическим элементом y над K, если и только если y – радикал над K. Поэтому *если присоединение экспоненты интеграла является алгебраическим расширением, то его группа Галуа является конечной мультипликативной подгруппой в* $\mathbb{C}^*$.

В терминологии Колчина [26] алгебраическая группа называется квазикомпактной, если каждая ее нееденичная подгруппа содержит элементы конечного порядка, отличные от единицы. Очевидно, что группа Галуа неалгебраического расширения, полученного присоединением экспоненты интеграла, квазикомпактна.

Утверждение 4.11. *Пусть y – экспонента интеграла над K и элемент y трансцендентен над K. Тогда каждому неотрицательному целому числу n можно поставить в соответствие дифференциальное поле между полями K и $K\langle y\rangle$. Именно, это дифференциальное поле K_n, состоящее из рациональных функций от элемента y^n с коэффициентами из поля K. Для разных n поля K_n различны. Всякое промежуточное дифференциальное поле совпадает с некоторым полем K_n.*

Доказательство. Пусть F – дифференциальное поле, строго содержащее поле K и лежащее в поле $K\langle y\rangle$. Повторяя рассуждения утверждения 4.9, получаем, что элемент y алгебраичен над F. Элемент y является экспонентой интеграла над F. Поэтому неприводимое над полем F алгебраическое уравнение, которому удовлетворяет y, имеет вид $y^n - a = 0$, где $a \in F$ (см. лемму 4.10), и, значит, $K_n \subseteq F$. Поле K_n должно совпадать с F. Действительно, в противном случае существует элемент $b \in F$, $b \notin K_n$. Элемент b является некоторой рациональной функцией R от y, и соотношение $R(y)$ не является следствием уравнения $y^n = a$. Это противоречит неприводимости уравнения $y^n = a$. Противоречие доказывает, что $K_n = F$. Поля K_n при разных n различны в силу трансцендентности y над K.

Утверждение доказывает основную теорему теории Пикара–Вессио для присоединения экспоненты интеграла. Действительно, каждая собственная алгебраическая подгруппа группы $\mathbb{C}^*$ является группой корней n-й степени из единицы для некоторого n. Промежуточное между K и $K\langle y\rangle$ дифференциальное поле состоит в точности из элементов поля $K\langle y\rangle$, которые остаются на месте при действии группы корней n-й степени из единицы на $K\langle y\rangle$.

4.5. Разрешимость дифференциальных уравнений. Скажем, что *алгебраическая группа G является разрешимой, k-разрешимой* или *почти разрешимой в категории алгебраических групп*, если у нее существует нормальная башня алгебраических подгрупп $G = G_0 \supset \dots \supset G_m = e$ со следующими свойствами

а) для разрешимых групп: для каждого $i = 1, \dots, m$ фактор-группа на G_{i-1}/G_i коммутативна (т.е. группа G разрешима);

б) для k-разрешимых групп: для каждого $i = 1, \dots, m$ либо глубина группы G_i в группе G_{i-1} не превосходит k, либо группа G_{i-1}/G_i коммутативна;

в) для почти разрешимых групп: для каждого $i = 1, \dots, m$ либо индекс группы G_i в группе G_{i-1} конечен, либо группа G_{i-1}/G_i коммутативна.

Теорема 4.12 (Пикара–Вессио). *Линейное дифференциальное уравнение над дифференциальным полем K решается в квадратурах, в k-квадратурах или обобщенных квадратурах, если и только если группа Галуа уравнения над полем K является соответственно разрешимой, k-разрешимой или почти разрешимой группой в категории алгебраических групп.*

Замечание. В классической теореме Пикара–Вессио не обсуждается вопрос о разрешимости уравнений в k-квадратурах. Мы включили этот вопрос в теорему, потому что, во-первых, ответ на него аналогичен и, во-вторых, он переносится в топологический вариант теории Галуа.

В этом пункте мы докажем лишь необходимость условий на группу Галуа для разрешимости уравнения. Доказательство достаточности отложим до п. 4.7. Итак, справедлива следующая теорема.

Теорема 4.13. *Если линейное дифференциальное уравнение решается в квадратурах, в k-квадратурах или в обобщенных квадратурах, то группа Галуа G этого уравнения является разрешимой, k-разрешимой или почти разрешимой группой в категории алгебраических групп.*

Доказательство. Разрешимость уравнений в обобщенных квадратурах над полем K означает существование цепочки дифференциальных полей $K = K_0 \subset \dots \subset K_N$, в которой первое поле совпадает с исходным полем K, последнее поле K_N содержит все решения дифференциального уравнения и для каждого $i = 1, \dots, N$ поле K_i получается из поля K_{i-1} либо присоединением интеграла, либо присоединением экспоненты интеграла, либо присоединением всех решений алгебраического уравнения. (В случае разрешимости в квадратурах последний из этих типов расширений запрещен. В случае разрешимости в k-квадратурах допускается лишь присоединение корней алгебраических уравнений степени не выше k.)

Пусть $G = G_0 \supset \dots \supset G_m = e$ – убывающая цепочка групп, в которой группа G_i – группа Галуа исходного уравнения над полем K_i. Согласно основной теореме 4.4, фактор-группа G_{i-1}/G_i является фактор-группой группы Галуа расширения Пикара–Вессио K_i поля K_{i-1}. Если это расширение является присоединением интеграла или экспоненты интеграла, то группа G_{i-1}/G_i коммутативна как фактор-группа коммутативной группы (см. п. 4.4.2 и п. 4.4.3). Если расширение K_i поля K_{i-1} получено присоединением всех корней алгебраического уравнения, то фактор-группа G_{i-1}/G_i конечна. Если это алгебраическое уравнение имеет степень $\leqslant k$, то между группами $G_i \supset G_{i-1}$ можно вставить цепочку нормальных делителей $G_i = G_{i1} \supset \dots \supset G_{ip} = G_{i-1}$ такую, что глубина группы G_{ij} в группе $G_{i,j-1}$ не превосходит k (см. п. 3.4.2). Доказательство теоремы закончено.

Только что доказанную теорему можно сформулировать следующим образом.

Если расширение Пикара–Вессио является расширением Лиувилля, k-расширением Лиувилля или обобщенным расширением Лиувилля, то его группа Галуа является соответственно разрешимой, k-разрешимой или почти разрешимой группой в категории алгебраических групп.

В такой переформулировке теорема становится применимой и к алгебраическим уравнениям над дифференциальными полями. Она дает более сильные результаты о неразрешимости алгебраических уравнений.

Теорема 4.14. *Если группа Галуа алгебраического уравнения над дифференциальным полем K неразрешима, то это алгебраическое уравнение не только не решается в радикалах, но не решается и в квадратурах. Если группа Галуа не является k-разрешимой, то алгебраическое уравнение не решается в k-квадратурах над K.*

4.6. Алгебраические матричные группы и необходимые условия разрешимости. Группа Галуа линейного дифференциального уравнения является алгебраической матричной группой. Такие группы обладают общими свойствами, которые помогают переформулировать условия разрешимости, k-разрешимости и почти разрешимости группы Галуа и доказать, что эти условия являются достаточными (см. п. 4.7) для разрешимости уравнения.

Отметим прежде всего, что *всякая алгебраическая матричная группа является группой Ли.* Действительно, множество особых точек всякого алгебраического многообразия имеет коразмерность $\geqslant 1$. Но групповым преобразованием любая точка группы переводится в любую другую точку. Поэтому около каждой точки группа устроена одинаково, и, следовательно, множество ее особых точек пусто. *Компонента связности единицы алгебраической группы является нормальным делителем конечного индекса в этой группе.* Действительно, компонента связности единицы является нормальным делителем во всякой группе Ли, и каждое алгебраическое многообразие имеет лишь конечное число компонент связности.

Для дальнейшего ключевую роль играет следующая знаменитая теорема Ли, которую мы приведем без доказательства.

Теорема 4.15 (Ли). *Связная разрешимая матричная группа Ли в некотором базисе приводится к треугольному виду.*

Утверждение 4.16. *Алгебраическая матричная группа является почти разрешимой группой в категории алгебраических групп, если и только если все матрицы ее компоненты связности единицы в некотором базисе одновременно приводятся к треугольному виду.*

Доказательство. Всякая группа, состоящая из треугольных матриц, разрешима. Это доказывает утверждение в одну сторону. Пусть $G = G_0 \supset \cdots \supset G_n = e$ – нормальная башня алгебраических подгрупп группы G, для которой каждая фактор-группа G_i/G_{i-1} либо коммутативна, либо конечна. Рассмотрим компоненты связности единицы этих групп. Они образуют нормальную башню $G^0 = G_0^0 \supset \cdots \supset G_n^0 = e$ алгебраических подгрупп компоненты связности единицы G^0 группы G. При этом если фактор-группа G_{i-1}/G_i коммутативна, то фактор-группа G_{i-1}^0/G_i^0 тоже коммутативна. Если фактор-группа G_{i-1}/G_i конечна, то группы G_{i-1}^0 и G_i^0 совпадают. Утверждение доказано.

Утверждение 4.17. *Алгебраическая матричная группа G является разрешимой или k-разрешимой группой в категории алгебраических групп, если и только* *если все матрицы ее компоненты связности единицы G^0 в некотором базисе приводятся к треугольному виду и конечная фактор-группа G/G_0 соответственно разрешима или k-разрешима.*

Доказательство. Согласно утверждению 4.16, группа G^0 является треугольной. Кроме того, группа G^0 является нормальным делителем конечного индекса в группе G. Конечная фактор-группа G/G_0 является соответственно разрешимой или k-разрешимой группой. В обратную сторону утверждение очевидно.

В группах матриц есть замечательная топология Зарисского, сопоставляющая каждой группе $\Gamma \subset GL(V)$ ее алгебраическое замыкание $\overline{\Gamma}$. Эта операция позволяет обобщить утверждения 4.16 и 4.17 на произвольные матричные группы.

Утверждение 4.18. 1) *Матричная группа является обобщенно разрешимой группой, если и только если у нее существует треугольный нормальный делитель H конечного индекса. Матричная группа является k-разрешимой или разрешимой, если и только если конечная фактор-группа G/H группы G по некоторому треугольному нормальному делителю H конечного индекса является соответственно k-разрешимой или разрешимой группой.*

2) *Алгебраическая матричная группа G является обобщенно разрешимой, k-разрешимой или разрешимой группой в категории алгебраических групп, если и только если она является соответственно обобщенно разрешимой, k-разрешимой или разрешимой группой.*

Доказательство. Пусть $G = G_0 \supset \cdots \supset G_n = e$ – нормальная башня группы G, тогда замыкания в топологии Зарисского групп из этой башни образуют нормальную башню алгебраических групп $\overline{G} = \overline{G}_0 \supset \cdots \supset \overline{G}_n = e$. При этом если группа G_{i-1}/G_i коммутативна, конечна или если группа G_i имеет в G_{i-1} глубину $\leqslant k$, то группа $\overline{G}_{i-1}/\overline{G}_i$ будет соответственно коммутативной, конечной или группа $\overline{G}_i$ будет иметь в группе $\overline{G}_{i-1}$ глубину $\leqslant k$. Это доказывает все пункты утверждения в одну сторону. В другую сторону все утверждения очевидны.

4.7. Достаточное условие разрешимости дифференциальных уравнений. Группу автоморфизмов Γ дифференциального поля F с дифференциальным полем неподвижных элементов K назовем *допустимой группой автоморфизмов*, если существует конечномерное пространство V над полем констант, инвариантное относительно группы Γ и такое, что $K\langle V\rangle = F$. Согласно теории Пикара–Вессио (см. следствие 4.5), дифференциальное поле F является расширением Пикара–Вессио дифференциального поля K, если и только если существует допустимая группа автоморфизмов дифференциального поля F с дифференциальным полем неподвижных элементов K. В общем случае существование допустимой группы преобразований для расширения Пикара–Вессио совсем неочевидно и является частью основной теоремы этой теории. Однако для обширного класса случаев существование допустимой группы автоморфизмов известно априори. Такой класс случаев доставляют расширения поля рациональных функций всеми решениями любого линейного дифференциального уравнения типа Фукса (см. п. 6.1.1). В этих случаях группа монодромии уравнения играет роль группы Γ.

Если группа Γ разрешима, то элементы поля F представляются в квадратурах через элементы поля K. Конструкция такого представления, по существу, относится к линейной алгебре и не использует основных теорем Пикара–Вессио. Допустимая группа автоморфизмов Γ изоморфна индуцированной группе линейных преобразований пространства V, и ее можно рассматривать как матричную группу.

ЛЕММА 4.19 (Лиувилль). *Если все преобразования допустимой группы Γ приводятся в некотором базисе к треугольному виду, то дифференциальное поле F является расширением Лиувилля дифференциального поля K.*

ДОКАЗАТЕЛЬСТВО. Пусть $e_1,\dots,e_n$ – базис пространства V, в котором каждое преобразование $\mu\in\Gamma$ имеет вид $\mu(e_i)=\sum_{j\leqslant i}a_{ij}e_j$. Рассмотрим векторное пространство $\widetilde V$, натянутое на векторы $\widetilde e_i=\left(\dfrac{e_i}{e_1}\right)'$, где $i=2,\dots,n$. Пространство $\widetilde V$ инвариантно относительно группы Γ, причем каждое преобразование μ группы Γ в базисе $\widetilde e_i$ имеет треугольный вид. Действительно,

$$\mu(\widetilde e_i)=\mu\left(\left[\frac{e_i}{e_1}\right]'\right)=\left(\frac{a_{i1}}{a_{11}}+\sum_{2\leqslant j\leqslant i}\frac{a_{ij}}{a_{11}}\frac{e_j}{e_1}\right)'=\sum_{2\leqslant j\leqslant i}\frac{a_{ij}}{a_{11}}\widetilde e_j.$$

Пространство $\widetilde V$ имеет меньшую размерность, чем пространство V, поэтому можно считать, что дифференциальное поле $K\langle\widetilde V\rangle$ есть расширение Лиувилля дифференциального поля K. Для всякого $\mu\in\Gamma$ имеем $\mu\left(\dfrac{e_1'}{e_1}\right)=\dfrac{a_{11}e_1'}{a_{11}e_1}=\dfrac{e_1'}{e_1}$, следовательно, элемент $\dfrac{e_1'}{e_1}=a$ лежит в дифференциальном поле инвариантов K. Дифференциальное поле F получается из дифференциального поля K присоединением экспоненты интеграла e_1 от элемента a и интегралов $\dfrac{e_i}{e_1}$ от элементов $\widetilde e_i$, где $i=2,\dots,n$.

УТВЕРЖДЕНИЕ 4.20. *Если группа Γ допустимых автоморфизмов поля F с полем неподвижных элементов K почти разрешима, то существует инвариантное относительно группы Γ поле K_0 такое, что* 1) *поле F является расширением Лиувилля поля K_0,* 2) *индуцированная группа автоморфизмов поля K_0 конечна, при этом каждый элемент поля K_0 является алгебраическим над полем K,* 3) *если группа Γ разрешима, то каждый элемент поля K_0 представим в радикалах над полем K.*

ДОКАЗАТЕЛЬСТВО. Пусть V – инвариантное пространство относительно группы Γ такое, что $K\langle V\rangle=F$.

Из утверждения 4.16 вытекает, что группа Γ обладает нормальным делителем Γ_0 конечного индекса, приводящимся в некотором базисе пространства V к треугольному виду. Пусть K_0 – дифференциальное поле инвариантов группы Γ. Согласно лемме 4.19, дифференциальное поле F есть расширение Лиувилля дифференциального поля K_0.

Очевидно (см. утверждение 3.9), что поле K_0 инвариантно относительно действия группы Γ, и индуцированная группа автоморфизмов этого поля $\widetilde\Gamma_0$ является конечной фактор-группой группы Γ. Поэтому каждый элемент поля K_0 алгебраичен над K (см. лемму 3.17). Если исходная группа Γ разрешима, то ее конечная фактор-группа $\widetilde\Gamma_0$ тоже разрешима. В этом случае любой элемент поля K_0 выражается в радикалах через элемент поля K (см. п. 3.3.1).

Доказательство следующего утверждения опирается на теорию Галуа.

Утверждение 4.21. *Если в условиях утверждения 4.20 группа Γ k-разрешима, то каждый элемент поля K_0 выражается через элементы поля K при помощи радикалов и решений алгебраических уравнений степени не выше k.*

Доказательство. Так как группа $\widetilde{\Gamma}_0$ конечна, то расширение K_0 поля K является расширением Галуа поля K. Если группа Γ_0 k-разрешима, то ее конечная фактор-группа тоже k-разрешима. Утверждение 4.21 теперь вытекает из теоремы 3.16.

Закончим теперь доказательство теоремы Пикара–Вессио (см. п. 4.5).

Согласно основной теореме 4.4, для всякого линейного дифференциального уравнения над дифференциальным полем K его группа Галуа оставляет неподвижными лишь элементы поля K. Поэтому применимы только что доказанные утверждения 4.20 и 4.21, что и доказывает достаточность условий на группу Галуа в теореме Пикара–Вессио.

Теорема Пикара–Вессио не только доказывает критерий Лиувилля–Мордухай-Болтовского (см. п. 2.3.2), но позволяет его обобщить на случай разрешимости в квадратурах и k-квадратурах. Именно, справедливы следующие утверждения.

Линейное дифференциальное уравнение n-го порядка решается в обобщенных квадратурах над дифференциальным полем K, если и только если, во-первых, у него существует решение y_1, удовлетворяющее уравнению $y_1' = ay_1$, где a – элемент, принадлежащий некоторому алгебраическому расширению K_1, и, во-вторых, если дифференциальное уравнение $(n-1)$-го порядка на функцию $z = y' - ay$ с коэффициентами из поля K_1, полученное из исходного уравнения процедурой понижения порядка (см. п. 4.1.2), решается в обобщенных квадратурах. Аналогичные утверждения справедливы и для разрешимости линейного дифференциального уравнения в квадратурах и в k-квадратурах. Для разрешимости в квадратурах надо дополнительно требовать, чтобы алгебраическое расширение K_1 получилось из K присоединением радикалов, а для разрешимости в k-квадратурах – чтобы расширение K_1 получалось из K присоединением радикалов и корней алгебраических уравнений степени $\leqslant k$. Для доказательства этих утверждений достаточно посмотреть на конструкцию решений дифференциальных уравнений.

Дифференциальная алгебра позволяет существенно уточнить этот критерий. *Для линейных дифференциальных уравнений, коэффициентами которых являются рациональные функции с рациональными коэффициентами, удается получить конечный алгоритм, позволяющий определить, решается ли уравнение в обобщенных квадратурах, и в случае существования решения найти его* [37]. Алгоритм использует: 1) оценку степени расширения K_1 поля K, зависящую лишь от порядка уравнения и вытекающую из общих соображений теории групп (см. п. 6.2.2); 2) теорию нормальных форм линейных дифференциальных уравнений в окрестности особой точки; 3) теорию исключения для дифференциальных уравнений и неравенств от нескольких функций (найденную Зайденбергом и обобщающую теорему Тарского–Зайденберга на случай дифференциальных полей).

4.8. Другие виды разрешимости. Колчин дополнил теорему Пикара–Вессио [26]. Он рассмотрел задачи о разрешимости линейных уравнений отдельно в интегралах и отдельно в экспонентах интегралов и варианты этих задач, в которых допускаются алгебраические расширения.

При определении расширений Лиувилля использовались три вида расширений: алгебраические расширения, присоединения интегралов и присоединения экспонент интегралов. Можно определить более частные виды разрешимости, используя в качестве “строительных кирпичиков” только некоторые из этих расширений (и используя лишь специальные алгебраические расширения). Перечислим основные варианты.

1) Разрешимость в интегралах.
2) Разрешимость в интегралах и радикалах.
3) Разрешимость в интегралах и алгебраических функциях.
4) Разрешимость в экспонентах интегралов.
5) Разрешимость в экспонентах интегралов и алгебраических функциях.

Расшифруем третье из этих определений.

Рассмотрим произвольную цепочку дифференциальных полей $K = K_0 \subseteq \cdots \subseteq K_n$, в которой каждое следующее поле K_i, $i = 1, \dots, n$, либо получается из предыдущего поля K_{i-1} присоединением интеграла над K_{i-1}, либо является алгебраическим расширением поля K_{i-1}. Каждый элемент дифференциального поля K_n по определению *представим в интегралах и алгебраических функциях* над полем K. Уравнение решается над полем K в интегралах и алгебраических функциях, если каждое его решение представлено в интегралах и алгебраических функциях.

Аналогично расшифровываются и другие виды разрешимости 1)–5).

Замечания. 1) Отдельно рассматривать разрешимость в радикалах и экспонентах интегралов не надо, так как каждый радикал является экспонентой интеграла.

2) Выше мы рассматривали специальные алгебраические расширения, полученные присоединением корней алгебраических уравнений степени не выше k. Можно было бы, скажем, определить k-разрешимость в интегралах, комбинируя подобные алгебраические расширения с присоединениями интегралов. Мы этого не делаем, чтобы не загромождать текст и из-за отсутствия интересных примеров.

Определение 1. Скажем, что матричная группа G является *специальной треугольной группой*, если существует базис, в котором все матрицы группы G одновременно приводятся к треугольному виду и все собственные числа каждой матрицы из группы G равны единице.

Определение 2. Скажем, что матричная группа *диагональна*, если существует базис, в котором все матрицы группы диагональны.

Теорема 4.22 (Колчина о разрешимости в интегралах). *Линейное дифференциальное уравнение над дифференциальным полем K решается в интегралах, в интегралах и радикалах, в интегралах и алгебраических функциях, если и только если группа Галуа уравнения над K соответственно является специальной треугольной группой, разрешима и содержит специальный треугольный нормальный делитель конечного индекса, содержит специальный треугольный нормальный делитель конечного индекса.*

Теорема 4.23 (Колчина о разрешимости в экспонентах интегралов). *Линейное дифференциальное уравнение над дифференциальным полем K решается в экспонентах интегралов и в экспонентах интегралов и алгебраических функциях,* *если и только если его группа Галуа над K соответственно разрешима и содержит диагональный нормальный делитель конечного индекса, содержит диагональный нормальный делитель конечного индекса.*

Несколько слов о доказательстве этих теорем. Группа Галуа присоединения интеграла антикомпактна (см. п. 4.4.2). Группа Галуа присоединения экспоненты интеграла квазикомпактна (см. п. 4.4.3). Колчин развил теорию антикомпактных и квазикомпактных алгебраических матричных групп. Вот одно несложное утверждение из этой теории.

Утверждение 4.24 [26]. 1) *Алгебраическая матричная группа квазикомпактна, если и только если каждая матрица группы приводится к диагональному виду.* 2) *Алгебраическая матричная группа антикомпактна, если и только если все собственные числа каждой матрицы группы равны единице.*

Теория квазикомпактных и антикомпактных групп вместе с основной теоремой теории Пикара–Вессио позволили Колчину доказать его теоремы о разрешимости в интегралах и о разрешимости в экспонентах интегралов.

Разумеется, теоремы Колчина, так же как и теорема Пикара–Вессио, справедливы не только для линейных дифференциальных уравнений, но и для расширений Пикара–Вессио (каждое такое расширение порождено решениями линейного дифференциального уравнения). Сформулируем критерий для различных видов представимости всех элементов расширения Пикара–Вессио с треугольной группой Галуа. Этот критерий легко вытекает из теорем Колчина и теоремы Пикара–Вессио. Мы применим этот критерий в п. 6.2.3 при обсуждении различных видов разрешимости систем уравнений типа Фукса с малыми коэффициентами.

Расширение с треугольной группой Галуа (ср. с [26]). *Пусть расширение Пикара–Вессио F дифференциального поля K имеет треугольную группу Галуа. Тогда каждый элемент поля F:*

1) *представим в квадратурах над полем K;*
2) *представим в интегралах и алгебраических функциях или в интегралах и радикалах*[1] *над полем K, если и только если собственные числа всех матриц группы Галуа – корни из единицы;*
3) *представим в интегралах над полем K, если и только если все собственные числа всех матриц группы Галуа равны единице;*
4) *представим в экспонентах интегралов и алгебраических функциях или в экспонентах интегралов*[1] *над полем K, если и только если группа Галуа диагональна;*
5) *представим в алгебраических функциях или в радикалах*[1] *над полем K, если и только если группа Галуа диагональна, а все собственные числа всех матриц группы Галуа – корни из единицы;*
6) *лежит в поле K, если и только если группа Галуа тривиальна.*

[1] Эти виды разрешимости различаются, если не требовать треугольности группы Галуа.

§ 5. Одномерный топологический вариант теории Галуа

5.1. Предварительные замечания. В п. 5.1.1 рассказывается о теории Галуа для полей мероморфных функций на алгебраических кривых, которая имеет прозрачную геометрическую интерпретацию и тесно связана с одномерным топологическим вариантом теории Галуа. В п. 5.1.2 обсуждаются топологическая непредставимость функций в радикалах и топологическая неэлементарность эллиптических функций, доказанные В.И. Арнольдом. В п. 5.1.3 обсуждается идея топологического варианта теории Галуа и трудности в ее реализации.

5.1.1. Теория Галуа полей мероморфных функций на алгебраических кривых. С алгебраической точки зрения в этом пункте идет речь о полях, являющихся расширениями степени трансцендентности один поля комплексных чисел $\mathbb{C}$, которые конечно-порождены над $\mathbb{C}$. Теория Галуа для таких полей имеет простой геометрический смысл.

Прежде всего, такое поле изоморфно полю P_M мероморфных функций на некоторой связной компактной римановой поверхности M, определенной с точностью до аналитического диффеоморфизма. Простейший пример такого поля доставляет поле рациональных функций одной комплексной переменной, т.е. поле мероморфных функций на сфере Римана.

Гомоморфизму таких полей $\tau\colon P_{M_1} \to P_{M_2}$, тождественному на подполях комплексных чисел, отвечает регулярное отображение $\rho\colon M_2 \to M_1$ соответствующих римановых поверхностей такое, что $\rho^* f = \tau(f)$, где f и $\tau(f)$ – мероморфные функции на M_1 и M_2. Если отображение ρ непостоянно, то образ $\tau(P_{M_1}) = \rho^*(P_{M_1})$ поля P_{M_1} изоморфен полю P_{M_1}, а поле P_{M_2} является конечным алгебраическим расширением своего подполя $\tau(P_{M_1}) = \rho^*(P_{M_1})$.

Непостоянное аналитическое отображение $\rho\colon M_2 \to M_1$ связной компактной римановой поверхности M_2 в связную компактную риманову поверхность M_1 задает конечное разветвленное накрытие над поверхностью M_1. Разветвленные накрытия $\rho_1\colon M_2 \to M_1$ и $\rho_2\colon M_3 \to M_1$ задают изоморфные расширения поля P_{M_1}, если и только если соответствующие разветвленные накрытия изоморфны, т.е. если существует обратимое аналитическое отображение $\rho\colon M_2 \to M_3$, коммутирующее с проекциями, т.е. $\rho_1 = \rho_2 \circ \rho$. Таким образом, теория конечных алгебраических расширений полей рассматриваемого типа эквивалентна теории конечных разветвленных накрытий над компактными римановыми поверхностями. В частности, теория конечных алгебраических расширений поля мероморфных функций эквивалентна теории конечнолистных разветвлений накрытий над сферой Римана.

Теперь подробнее о приведенных выше фактах и о связанной с ними геометрии. Каждое конечное алгебраическое расширение всякого поля порождается над этим полем одним элементом y, удовлетворяющим некоторому неприводимому алгебраическому уравнению над исходным полем. Пусть расширение поля P_M порождено элементом y, удовлетворяющим неприводимому уравнению

$$y^n + r_1 y^{n-1} + \dots + r_n = 0, \tag{10}$$

в котором r_i – мероморфные функции на M. В малой окрестности точки a определены n аналитических ростков $y_{1a}, \dots, y_{na}$, удовлетворяющих уравнению (10). Уравнение (10) неприводимо, если и только если каждый из этих ростков y_{ia} получается из любого другого ростка y_{ja} аналитическим продолжением вдоль некоторой кривой, лежащей на поверхности M (см. [14]). Рассмотрим риманову поверхность M_i ростка y_{ia} над поверхностью M, $\rho_i\colon M_i \to M$. Поверхность M_i является связным компактным многообразием. Поле мероморфных функций на M_i порождено над полем $\rho_i^* P_M$ элементом y_i (см. [14]). Неприводимость уравнения означает также, что разветвленные накрытия $\rho_i\colon M_i \to M$ и $\rho_j\colon M_j \to M$, соответствующие римановым поверхностям различных решений y_{ia} и y_{ja} уравнения (10), изоморфны как накрытия. Итак, *каждому конечному алгебраическому расширению поля P_M, заданному с точностью до изоморфизма, мы сопоставили класс эквивалентных конечных разветвленных покрытий над M.*

Построение обратного отображения, сопоставляющего каждому конечному разветвленному накрытию $\rho\colon M_1 \to M$ над M конечное расширение поля M, основано на теореме существования Римана. Согласно этой теореме, на всяком одномерном комплексном многообразии для любого конечного множества существует мероморфная функция, которая принимает разные значения в точках множества. Рассмотрим мероморфную функцию на M_1, принимающую различные значения в различных прообразах какого-либо регулярного значения $a \in M$ отображения ρ. Такая функция y является многозначной алгебраической функцией на M и порождает все поле мероморфных функций на M_1 над подполем $\rho^*(P_M)$.

Перейдем к геометрическому описанию разветвленных накрытий над компактной римановой поверхностью M. Для задания такого накрытия достаточно фиксировать конечное множество $A \subset M$ и подгруппу F конечного индекса в фундаментальной группе $\pi_1(M \setminus A)$ дополнения к множеству A. По этим данным разветвленное накрытие над M строится так. Сначала по подгруппе F строится накрытие над множеством $M \setminus A$, образ фундаментальной группы которого при проекции в $M \setminus A$ совпадает с подгруппой F (см., например, [12]). Число прообразов любой точки в $M \setminus A$ при этом накрытии совпадает с индексом подгруппы F в группе $\pi_1(M \setminus A)$. Полученное накрытие однозначно компактифицируется добавлением некоторых точек, лежащих над множеством A (множество добавленных точек над $a \in A$ находится в соответствии с множеством циклов в перестановке листов накрытия, соответствующих обходу вокруг точки a).

Два разветвленных накрытия, построенных по множествам $A_1 \subset M$ и $A_2 \subset M$ и по группам $F_1 \subset \pi_1(M \setminus A_1)$ и $F_2 \subset \pi_1(M \setminus A_2)$, изоморфны, если и только если для конечного множества B, содержащего множества A_1 и A_2, подгруппы $\widetilde{F}_1, \widetilde{F}_2$ группы $\pi_1(M \setminus B)$ сопряжены в этой группе $\pi_1(M \setminus B)$, где $\widetilde{F}_1$ и $\widetilde{F}_2$ – прообразы групп F_1 и F_2 при индуцированных вложениями гомоморфизмах группы $\pi_1(M \setminus B)$ в группы $\pi_1(M \setminus A_1)$ и $\pi_1(M \setminus A_2)$. Легко видеть, что выписанное условие не зависит от выбора конечного множества B, содержащего множества A_1 и A_2.

Разветвленное накрытие $\rho\colon M_1 \to M$ соответствует расширению Галуа поля P_M, если и только если определяющая это накрытие подгруппа H конечного индекса в $\pi_1(M \setminus A)$ является нормальной подгруппой в $\pi_1(M \setminus A)$ (здесь A – любое конечное множество, содержащее все критические значения отображения ρ; выписанное условие не зависит от конкретного выбора множества A). *Группа Галуа этого расширения Галуа совпадает с фактор-группой $\pi_1(M \setminus A)/H$, изоморфной группе взаимно однозначных преобразований поверхности M_1 в себя, коммутирующих с проекцией ρ.*

Промежуточному расширению поля P_M соответствует промежуточное разветвленное накрытие, т.е. такое накрытие $\rho_2 \colon M_2 \to M$, что существует отображение $\rho_1 \colon M_1 \to M_2$, для которого $\rho_2 \circ \rho_1 = \rho$. Промежуточное накрытие соответствует промежуточной подгруппе F в $\pi_1(M \setminus A)$, т.е. такой подгруппе F, что $H \subseteq F$.

Промежуточное поле является расширением Галуа, если и только если F – нормальный делитель в $\pi_1(M \setminus A)$. Группа Галуа промежуточного расширения Галуа является фактор-группой группы Галуа исходного расширения, так как фактор-группа $\pi_1(M \setminus A)/H$ естественно отображается на фактор-группу $\pi_1(M \setminus A)/F$.

Выше мы привели геометрическую интерпретацию основной теоремы теории Галуа для полей мероморфных функций на алгебраических кривых. Нам осталось лишь описать геометрически поведение группы Галуа алгебраического уравнения при расширении основного поля. Итак, пусть $\rho_1 \colon M_1 \to M$ – разветвленное накрытие, соответствующее расширению Галуа поля P_M, и пусть $\rho_2 \colon M_2 \to M$ – другое накрытие, соответствующее другому расширению Галуа того же поля P_M. Пусть B – любое конечное множество на M, содержащее критические точки отображений ρ_1 и ρ_2, и $G = \pi_1(M \setminus B)$ – фундаментальная группа дополнения к множеству B. Накрытия $\rho_1 \colon M_1 \setminus B_1 \to M \setminus B$ и $\rho_2 \colon M_2 \setminus B_2 \to M \setminus B$, где $B_1 = \rho_1^{-1}(B)$ и $B_2 = \rho_2^{-1}(B)$, соответствуют нормальным подгруппам H_1 и H_2 группы G, изоморфным фундаментальным группам многообразий $M_1 \setminus B_1$ и $M_2 \setminus B_2$. Проекция $\rho_2 \colon M_2 \setminus B_2 \to M \setminus B$ отображает многообразие $M_2 \setminus B_2$ в базу накрытия $\rho_1 \colon M_1 \setminus B_1 \to M \setminus B$. При помощи отображения ρ_2 из накрытия $\rho_1 \colon M_1 \setminus B_1 \to S \setminus B$ индуцируется накрытие $\rho \colon U \to M_2 \setminus B_2$ над $M_2 \setminus B_2$. Многообразие U, вообще говоря, несвязно. Каждая компонента связности $U_i \subset U$ определяет накрытие $\rho \colon U_i \to M_2 \setminus B_2$. Легко видеть, что все накрытия, связанные с различными компонентами U_i, эквивалентны как накрытия, и каждое из них соответствует нормальному делителю $H_1 \cap H_2$ в группе H_2. Рассмотрим любую из компонент $U_i = V$. Накрытие $\rho \colon V \to M_2 \setminus B_2$ допускает компактификацию $\rho \colon M_3 \to M_2$, где $V = M_3 \setminus B_3$ и $B_3 = \rho^{-1}(B_2)$, соответствующую исходному расширению Галуа над полем P_{M_2}. Группа Галуа этого накрытия есть фактор-группа $H_3/H_1 \cap H_2$. Именно это и утверждается в теореме 3.4.

Итак, все утверждения теории Галуа для полей мероморфных функций на кривых имеют прозрачное геометрическое объяснение. Более того, *геометрическая конструкция разветвленных накрытий, соединенная с теоремой существования Римана, доставляет полное описание всех конечных расширений рассматриваемого класса полей.* Например, она моментально решает для таких полей обратную задачу теории Галуа (т.е. задачу построения расширения Галуа с заданной группой Галуа). Отметим, что для поля рациональных чисел обратная задача теории Галуа до сих пор не решена.

5.1.2. Топологическая непредставимость функций в радикалах. Прежде чем переходить к топологическому варианту теории Галуа, остановимся еще на одной топологической интерпретации группы Галуа алгебраического уравнения над полем рациональных функций.

Пусть

$$y^n + r_1 y^{n-1} + \cdots + r_n = 0 \tag{11}$$

– неприводимое уравнение над полем рациональных функций P_S, $r_i \in P_S$.

Хорошо известно следующее утверждение.

Утверждение 5.1. *Группа Галуа уравнения* (11) *над полем рациональных функций изоморфна группе монодромии* (*многозначной*) *алгебраической функции* y, *определенной уравнением* (11).

Доказательство. Пусть D – дискриминант уравнения (11). Обозначим через $[D]$ множество нулей и полюсов дискриминанта D. В малой связной окрестности U точки a, $a \notin [D]$, на сфере Римана определены n голоморфных решений $y_{1a}, \dots, y_{na}$ уравнения (11). Обозначим через Q поле мероморфных функций в области U, полученное присоединением к полю P_S всех этих решений. Пусть γ – кривая на сфере Римана, начинающаяся и заканчивающаяся в точке a и не пересекающая множество $[D]$. Вдоль кривой γ регулярно продолжается каждое решение $y_{1a}, \dots, y_{na}$ уравнения (11), поэтому вдоль γ мероморфно продолжается любой элемент z поля Q. Отображение $z \to z(\gamma)$, сопоставляющее элементу z его мероморфное продолжение вдоль γ, является, очевидно, изоморфизмом поля Q. Этот изоморфизм однозначно определяется перестановкой $y_{ia} \to y_{ia}(\gamma)$ элементов $y_{1a}, \dots, y_{na}$, зависит лишь от класса $[\gamma]$ кривой γ в $\pi_1(S \setminus [D], a)$ и оставляет тождественно на месте все рациональные функции. Обратно, элементы поля Q, остающиеся на месте при всех изоморфизмах $z \to z(\gamma)$, являются однозначными алгебраическими функциями, т.е. являются рациональными функциями. Следовательно, группа изоморфизмов вида $z \to z(\gamma)$ поля Q совпадает с его группой Галуа над полем P_S. С другой стороны, эта группа изоморфна группе перестановок листов $y_{1a}, \dots, y_{na}$ алгебраической функции y, соответствующих аналитическим продолжениям $y_{ia} \to y_{ia}(\gamma)$ вдоль путей γ, $\gamma \in \pi_1(S \setminus D, a)$, т.е. изоморфна группе монодромии функции y. Утверждение доказано.

Из теории Галуа и только что доказанного утверждения вытекает следующее следствие.

Следствие 5.2. 1) *Алгебраическая функция представима в радикалах, если и только если ее группа монодромии разрешима.* 2) *Алгебраическая функция представима в k-радикалах, если и только если ее группа монодромии k-разрешима.*

В. И. Арнольд доказал топологическую неразрешимость ряда классических задач [2]–[9]. Приведем принадлежащее Арнольду определение.

Определение (Арнольд). $f\colon X \to Y$ называется *топологически нехорошим отображением* (например, топологически неэлементарной функцией), если среди (лево-право) топологически эквивалентных ему нет хороших (элементарных, например).

С каждой многозначной аналитической функцией f комплексного переменного связаны ее риманова поверхность M_f и проекция $\pi_f\colon M_f \to S^2$ этой поверхности на сферу Римана S^2.

Следствие 5.3. *Пусть проекции π_f и π_g римановых поверхностей M_f и M_g функций f и g на сферу Римана топологически эквивалентны. Тогда функции f и g представимы или непредставимы в радикалах* (*k-радикалах*) *одновременно* (т.е. топологический тип проекции римановой поверхности функции на сферу Римана отвечает за представимость функции в радикалах и в k-радикалах).

Доказательство. Следствие 5.3 немедленно вытекает из следствия 5.2. Действительно, алгебраичность функции связана с компактностью ее римановой поверхности, ее представимость в радикалах связана с разрешимостью ее группы монодромии, а ее представимость в k-радикалах связана с k-разрешимостью ее группы монодромии. Все эти свойства топологические.

Арнольд в 60-е годы доказал топологическую непредставимость в радикалах общих алгебраических функций (см. следствие 5.3) непосредственно топологически, не опираясь на теорию Галуа, и прочел курс на эту тему в Колмогоровском интернате. В. А. Алексеев значительно переработал этот курс и опубликовал его в виде книги [1]. Согласно Арнольду, топологическое доказательство неразрешимости какой-либо задачи, как правило, влечет за собой новые следствия. Например, из топологического доказательства непредставимости в радикалах функции с неразрешимой группой монодромии легко вытекает непредставимость такой функции формулой, включающей в себя не только радикалы, но и любые целые функции [19].

В 60-е годы Арнольд нашел также результаты о топологической неэлементарности эллиптических функций и интегралов (и других близких вещей), но ничего не опубликовал на эту тему. В декабре 2003 года Владимир Игоревич написал мне письмо об этом. Следующая теорема, так же как и приведенное выше определение, заимствованы из этого письма.

Теорема 5.4 (Арнольд). *Если мероморфная функция* $g\colon U \to \mathbb{C}P^1$, *определенная в комплексной области* $U \subset \mathbb{C}$, *топологически эквивалентна эллиптической функции* $f\colon \mathbb{C} \to \mathbb{C}P^1$, *то* g *– эллиптическая функция* (*возможно, с иными, нежели у функции* f, *периодами*).

Доказательство. Эллиптическая функция f инвариантна относительно группы сдвигов $\mathbb{Z}^2$ $(z \to z + k_1w_1 + k_2w_2,\ (k_1,k_2) \in \mathbb{Z}^2)$. Поэтому функция g инвариантна относительно группы гомеоморфизмов $\mathbb{Z}^2$ области U. Каждый гомеоморфизм h этой группы, на самом деле, является биголоморфным отображением области U в себя. Действительно, по теореме об обратной функции из тождества $g(z) \equiv g(h(z))$ вытекает голоморфность отображения h в окрестности каждой точки, не принадлежащей прообразу при отображении h множества критических точек функции g. В точках этого прообраза отображение h голоморфно по теореме об устранимой особенности. По условию область U гомеоморфна $\mathbb{C}$. Следовательно, по теореме Римана область U либо совпадает с $\mathbb{C}$, либо биголоморфно эквивалентна внутренности единичного круга. Область U совпадает с $\mathbb{C}$, так как группа биголоморфных преобразований единичного круга не содержит подгруппы $\mathbb{Z}^2$. Подгруппа $\mathbb{Z}^2$ группы биголоморфных преобразований $\mathbb{C}$, действующая на $\mathbb{C}$ без неподвижных точек, является группой сдвигов $(z \to k_1\tau_1 + k_2\tau_2,\ (k_1,k_2) \in \mathbb{Z}^2)$. Поэтому g – эллиптическая функция.

Как известно, эллиптические функции неэлементарны[2]. Из этого классического

[2] Неэлементарность эллиптических функций вытекает из обобщения теории Пикара–Вессио, принадлежащего Колчину [27]. Это обобщение применимо не только к линейным, но и к некоторым нелинейным дифференциальным уравнениям, например к уравнению на γ-функцию Вейерштрасса. Группа Галуа дифференциального поля эллиптических функций над полем констант $\mathbb{C}$, очевидно, содержит группу $\mathbb{C}/\mathbb{Z}^2$, состоящую из фактор-группы группы сдвигов $f(z) \to f(z+a)$ по подгруппе $\mathbb{Z}^2$ периодов эллиптических функций. (Несложно показать, что группа Галуа сов-

результата и доказанной выше теоремы вытекает топологическая неэлементарность эллиптических функций.

Ниже приводится цитата из письма Владимира Игоревича.

"Эти соображения доказывали, мне помнится, топологическую неэлементарность как эллиптических функций, f, так и эллиптических интегралов, f^{-1}, да и многого другого. Причем все это обобщается и на кривые других родов (с другими накрытиями, или хотя бы с универсальными накрытиями). Не помню, доказал ли я аккуратно, но думаю, что у меня были соображения, почему аналогичные приведенной теореме многомерные высказывания должны быть *неверны*: помнится, что *сохранение топологического типа в многомерном случае не гарантирует сохранение алгебраичности.* Само по себе это не препятствует топологической неэлементарности (нехорошести), но препятствует моему доказательству его, доказательству путем сведения к неэлементарности классического (алгебраического) объекта вроде эллиптической функции".

5.1.3. Об одномерном топологическом варианте теории Галуа. На классе алгебраических функций группа монодромии совпадает с группой Галуа и отвечает за представимость функции в радикалах (см. п. 5.1.2). Но группа монодромии определена не только для алгебраических функций, она определена для логарифма, арктангенса и для многих других функций, для которых группа Галуа не определена. Естественно попытаться для таких функций использовать группу монодромии вместо группы Галуа для доказательства непринадлежности функции тому или иному классическому классу. Именно этот подход и реализует топологический вариант теории Галуа [18]–[22].

Приведем пример, который показывает, какие трудности приходится преодолевать на этом пути.

Рассмотрим элементарную функцию f, определенную следующей формулой:

$$f(z) = \ln\left(\sum_{j=1}^{n} \lambda_j \ln(z - a_j)\right),$$

где a_j, $j = 1, \dots, n$, – различные точки на комплексной прямой и λ_j, $j = 1, \dots, n$, – комплексные константы. Обозначим через Λ аддитивную группу комплексных чисел, порожденную константами $\lambda_1, \dots, \lambda_n$. Ясно, что если $n > 2$, то почти для всякого набора констант $\lambda_1, \dots, \lambda_n$ группа Λ всюду плотна на комплексной прямой.

УТВЕРЖДЕНИЕ 5.5. *Если группа Λ всюду плотна на комплексной прямой, то элементарная функция f имеет всюду плотное множество точек логарифмического ветвления.*

ДОКАЗАТЕЛЬСТВО. Пусть g_a – один из ростков функции g, определенной формулой $g(z) = \sum_{j=1}^{n} \lambda_j \ln(z - a_j)$ в точке a, $a \neq a_j$, $j = 1, \dots, n$. После обхода точек $a_1, \dots, a_n$ к ростку g_a прибавится число $2\pi i\lambda$, где λ – элемент группы Λ. Обратно,

падает с этой группой.) Непредставимость эллиптических функций в обобщенных квадратурах, согласно Колчину, вытекает из несуществования у группы $\mathbb{C}/\mathbb{Z}^2$ нормальной башни подгрупп, каждая фактор-группа относительно которой является или конечной группой, или аддитивной, или мультипликативной группой комплексных чисел.

всякий росток $g_a + 2\pi i\lambda$, где $\lambda \in \Lambda$, получается из ростка g_a в результате аналитического продолжения вдоль некоторой кривой. Пусть U – малая окрестность точки a и $G\colon U \to C$ – аналитическая функция, росток которой в точке a есть g_a. Образ V области U при отображении $G\colon U \to \mathbb{C}$ открыт. Поэтому в области V найдется точка вида $2\pi i\lambda$, где $\lambda \in \Lambda$. Функция $G - 2\pi i\lambda$ является одной из ветвей функции g над областью U, причем множество нулей этой ветви в области U непусто. Поэтому одна из ветвей функции $f = \ln g$ имеет в U точку логарифмического ветвления.

Несложно проверить, что в условиях утверждения группа монодромии функции f континуальна (это неудивительно: фундаментальная группа $\pi_1(S \setminus A)$, где A – счетное всюду плотное множество на сфере Римана, очевидно, содержит континуум элементов).

Можно показать также, что образ фундаментальной группы $\pi_1(S^2 \setminus \{A \cup b\})$, где $b \notin A$ – любая точка на комплексной прямой, в группе перестановок листов функции f является собственной подгруппой группы монодромии функции f. (То обстоятельство, что удаление одной лишней точки может изменить группу монодромии, несколько усложняет все доказательства.)

Итак, уже простейшие элементарные функции могут иметь всюду плотное множество особых точек и континуальную группу монодромии.

В топологическом варианте теории Галуа мы рассматриваем функции, представимые в квадратурах, как многозначные аналитические функции одного комплексного переменного. Оказывается, что существуют топологические ограничения на характер расположения над комплексной плоскостью римановой поверхности функции, представимой в квадратурах. Если функция не удовлетворяет этим ограничениям, то ее нельзя выразить в квадратурах.

Этот подход, кроме геометрической наглядности, имеет следующее преимущество. Топологические запреты относятся к характеру многозначности функции. Они сохраняются не только для функций, представимых в квадратурах, но и для значительно более широкого класса функций. Этот более широкий класс получится, если к функциям, представимым в квадратурах, добавить все мероморфные функции и разрешить им участвовать во всех формулах. Из-за этого топологические результаты о непредставимости в квадратурах оказываются более сильными, чем алгебраические. Дело в том, что суперпозиция функций – не алгебраическая операция. В дифференциальной алгебре вместо суперпозиции функций рассматривается дифференциальное уравнение, которому она удовлетворяет. Но, например, Г-функция Эйлера не удовлетворяет никакому алгебраическому дифференциальному уравнению. Поэтому безнадежно искать уравнение, которому удовлетворяет, скажем, функция $\Gamma(\exp x)$. Единственные известные результаты о непредставимости функций в квадратурах и, скажем, в Г-функциях Эйлера получены только нашим методом.

С другой стороны, этим методом невозможно доказать непредставимость в квадратурах какой-либо однозначной мероморфной функции.

Используя дифференциальную теорию Галуа (а точнее, ее линейно-алгебраическую часть, имеющую дело с алгебраическими матричными группами и их дифференциальными инвариантами), можно показать, что единственные причины неразрешимости в квадратурах линейных дифференциальных уравнений типа Фукса – топологические (ср. с § 6). Другими словами, если к разрешимости в квадратурах дифференциального уравнения типа Фукса не существует топологических препятствий, то оно решается в квадратурах.

Существуют следующие топологические препятствия к представимости функций в квадратурах, в обобщенных квадратурах и в k-квадратурах.

Во-первых, функции, представимые в обобщенных квадратурах, и, в частности, функции, представимые в квадратурах и в k-квадратурах, могут иметь не более чем счетное число особых точек на комплексной прямой (см. п. 5.2). (Хотя уже для простейших функций, представимых в квадратурах, множество особых точек может быть всюду плотным.)

Во-вторых, группа монодромии функции, представимой в квадратурах, обязательно разрешима (см. п. 5.5.2). (Хотя уже для простейших функций, представимых в квадратурах, группа монодромии может содержать континуум элементов.)

Аналогичные ограничения на расположение римановой поверхности существуют и для функций, представимых в обобщенных квадратурах и в k-квадратурах. Однако эти ограничения формулируются сложнее. В них группа монодромии фигурирует не как абстрактная группа, а как группа перестановок множества листов функции. Или, другими словами, в этих ограничениях фигурирует не только группа монодромии, но и *монодромная пара* функции, состоящая из ее группы монодромии и стационарной подгруппы некоторого ростка (см. п. 5.3.3).

Переходим к подробному описанию этого геометрического подхода к проблеме разрешимости.

5.2. Функции с не более чем счетным множеством особых точек. В этом пункте определяется обширный класс функций одной комплексной переменной, нужный для построения топологического варианта теории Галуа.

5.2.1. Запрещенные множества. Определим класс функций, внутри которого будут проводиться дальнейшие рассмотрения. Многозначная аналитическая функция одного комплексного переменного называется *$\mathcal{S}$-функцией*, если множество ее особых точек не более чем счетно. Уточним это определение.

Два регулярных ростка f_a и g_b, заданных в точках a и b сферы Римана S^2, называются эквивалентными, если росток g_b получается из ростка f_a регулярным продолжением вдоль некоторой кривой. Каждый росток g_b, эквивалентный ростку f_a, называется также регулярным ростком многозначной аналитической функции f, порожденной ростком f_a.

Точка $b \in S^2$ называется особой для ростка f_a, если существует кривая $\gamma\colon [0,1] \to S^2$, $\gamma(0) = a$, $\gamma(1) = b$, такая, что росток не может быть регулярно продолжен вдоль этой кривой, но для любого t, $0 \leqslant t < 1$, росток регулярно продолжается вдоль укороченной кривой $\gamma\colon [0,t] \to S^2$. Легко видеть, что у эквивалентных ростков множества особых точек совпадают.

Регулярный росток называется *$\mathcal{S}$-ростком*, если множество его особых точек не более чем счетно. Многозначная аналитическая функция называется $\mathcal{S}$-функцией, если каждый ее регулярный росток является $\mathcal{S}$-ростком.

В дальнейшем нам понадобится лемма, согласно которой малым шевелением кривую на плоскости можно снять со счетного множества.

Лемма 5.6 (о снятии кривой со счетного множества). *Пусть A – не более чем счетное множество на плоскости $\mathbb{C}$, $\gamma\colon [0,1] \to \mathbb{C}$ – кривая и φ – непрерывная* *положительная функция на интервале* $0 < t < 1$. *Тогда существует кривая* $\widehat{\gamma}\colon [0,1] \to \mathbb{C}$ *такая, что при* $0 < t < 1$ $\widehat{\gamma}(t) \notin A$ *и* $|\gamma(t) - \widehat{\gamma}(t)| < \varphi(t)$.

"Научное" доказательство леммы заключается в следующем. В функциональном пространстве кривых $\overline{\gamma}$, близких к кривой γ, $|\gamma(t) - \overline{\gamma}(t)| < \varphi(t)$, кривые, не пересекающие одной из точек множества A, образуют открытое плотное множество. Пересечение счетного числа открытых плотных множеств в таких функциональных пространствах непусто.

Приведем элементарное доказательство леммы (оно почти дословно переносится на более общий случай, когда множество A несчетно, но имеет нулевую длину по Хаусдорфу, ср. с п. 5.5.3). Сначала построим бесконечнозвенную ломаную $\overline{\gamma}$ с вершинами, не принадлежащими A, такую, что $|\gamma(t) - \overline{\gamma}(t)| < \frac{1}{2}\varphi(t)$. Такую ломаную можно построить, так как дополнение к множеству A всюду плотно. Покажем, как изменить каждое звено $[p,q]$ ломаной $\overline{\gamma}$, чтобы она не пересекала множества A. Возьмем отрезок $[p,q]$. Пусть m – перпендикуляр к его середине. Рассмотрим двузвенные ломаные $[p,b]$, $[b,q]$, где $b \in m$ и точка b достаточно близка к отрезку. Они пересекаются только по концам p, q, и их число континуально. Значит, среди них есть ломаная, не пересекающая множества A. Заменив таким образом каждое звено бесконечнозвенной ломаной, получим искомую кривую.

Кроме множества особых точек удобно рассматривать и другие множества, вне которых функция неограниченно продолжается. Не более чем счетное множество A называется *запрещенным множеством* для регулярного ростка f_a, если росток f_a регулярно продолжается вдоль кривой $\gamma(t)$, $\gamma(0) = a$, пересекающей множество A лишь, может быть, в начальный момент.

Теорема 5.7 (о запрещенном множестве). *Не более чем счетное множество является запрещенным множеством ростка, если и только если оно содержит множество его особых точек. В частности, росток обладает некоторым запрещенным множеством, если и только если он является ростком $\mathcal{S}$-функции.*

Доказательство. Предположим, что существует особая точка b ростка f_a, не лежащая в некотором запрещенном множестве A этого ростка. По определению должна существовать кривая $\gamma\colon [0,1] \to S^2$, $\gamma(0) = a$, $\gamma(1) = b$, вдоль которой не существует регулярного продолжения ростка f_a, но вдоль которой росток продолжается до любой точки $t < 1$. Не ограничивая общности, можно считать, что точки a, b и кривая $\gamma(t)$ лежат в конечной части сферы Римана, т.е. $\gamma(t) \neq \infty$ при $0 \leqslant t \leqslant 1$. Обозначим через $R(t)$ радиус сходимости рядов $f_{\gamma(t)}$, получающихся при продолжении ростка f_a вдоль кривой $\gamma(t)$. Функция $R(t)$ непрерывна на полуинтервале $[0,1)$. Согласно лемме 5.6, существует кривая $\widehat{\gamma}(t)$, $\widehat{\gamma}(0) = a$, $\widehat{\gamma}(1) = b$, такая, что $|\gamma(t) - \widehat{\gamma}(t)| < \frac{1}{3}R(t)$ и $\widehat{\gamma}(t) \notin A$ при $t > 0$. Росток f_a по условию должен продолжаться вдоль кривой $\widehat{\gamma}$ до точки 1. Но отсюда легко следует, что росток f_a продолжается вдоль кривой γ. Полученное противоречие доказывает, что множество особых точек ростка f_a содержится во всяком запрещенном множестве этого ростка. Обратное утверждение (счетное множество, содержащее множество особенностей ростка, является запрещенным для ростка) очевидно.

5.2.2. Замкнутость класса $\mathcal{S}$-функций. Докажем замкнутость введенного класса функций относительно всех естественных операций.

Теорема 5.8 (о замкнутости класса $\mathcal{S}$-функций). *Класс $\mathcal{S}$ всех $\mathcal{S}$-функций замкнут относительно следующих операций:*

1) *дифференцирования, т.е. если $f \in S$, то $f' \in \mathcal{S}$;*
2) *интегрирования, т.е. если $f \in \mathcal{S}$ и $g' = f$, то $g \in \mathcal{S}$;*
3) *суперпозиции, т.е. если $g, f \in \mathcal{S}$, то $g \circ f \in \mathcal{S}$;*
4) *мероморфных операций, т.е. если $f_i \in \mathcal{S}$, $i = 1, \dots, n$, $F(x_1, \dots, x_n)$ – мероморфная функция n-переменных и $f = F(f_1, \dots, f_n)$, то $f \in \mathcal{S}$;*
5) *решения алгебраических уравнений, т.е. если $f_i \in \mathcal{S}$, $i = 1, \dots, n$, и $f^n + f_1 f^{n-1} + \dots + f_n = 0$, то $f \in \mathcal{S}$;*
6) *решения линейных дифференциальных уравнений, т.е. если $f_i \in \mathcal{S}$, $i = 1, \dots, n$, и $f^{(n)} + f_1 f^{(n-1)} + \dots + f_n = 0$, то $f \in \mathcal{S}$.*

Доказательство. 1)–2). Пусть f_a, $a \neq \infty$, – росток $\mathcal{S}$-функции с множеством особых точек A. Если росток f_a регулярно продолжается вдоль некоторой кривой γ, лежащей в конечной части сферы Римана, то интеграл и производная этого ростка регулярно продолжаются вдоль кривой γ. Поэтому в качестве запрещенного множества для интеграла и производной ростка f_a достаточно взять множество $A \cup \{\infty\}$.

3) Пусть f_a и g_b – ростки $\mathcal{S}$-функций с множествами особых точек A и B и $f_a(a) = b$. Обозначим через $f^{-1}(B)$ полный прообраз множества B при многозначном соответствии, порожденном ростком f_a. Иными словами, $x \in f^{-1}(B)$, если и только если существует росток ψ_x, эквивалентный ростку f_a и такой, что $\psi(x) \in B$. Множество $f^{-1}(B)$ не более чем счетно. В качестве запрещенного множества ростка $g_b \circ f_a$ достаточно взять множество $A \cup f^{-1}(B)$.

4) Пусть f_{ia} – ростки $\mathcal{S}$-функций, A_i – множества их особых точек и F – мероморфная функция n переменных. Мы предполагаем, что ростки f_{ia} и функция F таковы, что росток $f_a = F(f_{1a}, \dots, f_{na})$ является вполне определенным мероморфным ростком. Заменив, если надо, точку a близкой точкой, можно считать, что росток f_a регулярен. Если кривая $\gamma(t)$ не пересекает множество $A = \bigcup A_i$ при $t > 0$, то росток f_a мероморфно продолжается вдоль этой кривой. Пусть B – проекция на сферу Римана множества полюсов функции f, порожденной ростком f_a. В качестве запрещенного множества ростка достаточно взять множество $A \cup B$.

5) Пусть f_{ia} – ростки $\mathcal{S}$-функций, A_i – множества их особых точек и f_a – регулярный росток, удовлетворяющий равенству

$$f_a^n + f_{1a} f_a^{n-1} + \dots + f_{na} = 0.$$

Если кривая $\gamma(t)$ не пересекает множество $A = \bigcup A_i$ при $t > 0$, то существует продолжение ростка f_a вдоль этой кривой, содержащее, вообще говоря, мероморфные и алгебраические элементы. Пусть B – проекция множества полюсов функции f и точек разветвления ее римановой поверхности на сферу Римана S^2. В качестве запрещенного множества для ростка f_a достаточно взять множество $A \cup B$.

6) Если коэффициенты уравнения

$$f_a^{(n)} + f_{1a} f_a^{(n-1)} + \dots + f_{na} = 0$$

регулярно продолжаются вдоль некоторой кривой γ, лежащей в конечной части сферы Римана, то любое решение f_a этого уравнения также регулярно продолжается вдоль кривой γ. Поэтому в качестве запрещенного множества ростка f_a достаточно взять множество $A = \bigcup A_i \cup \{\infty\}$, где A_i – множества особых точек ростков f_{a_i}.

Замечание. Арифметические операции и потенцирование являются примерами мероморфных операций, поэтому *класс $\mathcal{S}$-функций замкнут относительно арифметических операций и потенцирования.*

Следствие 5.9. *Если многозначную функцию f можно получить из однозначных $\mathcal{S}$-функций с помощью интегрирования, дифференцирования, мероморфных операций, суперпозиций, решения алгебраических уравнений и линейных дифференциальных уравнений, то функция f имеет не более чем счетное число особых точек. В частности, функцию, имеющую несчетное число особых точек, нельзя представить в обобщенных квадратурах.*

5.3. Группа монодромии. В этом пункте обсуждаются различные понятия, связанные с группой монодромии.

5.3.1. Группа монодромии с запрещенным множеством. Группа монодромии $\mathcal{S}$-функции f с запрещенным множеством A – это группа всех перестановок листов функции f, которые происходят при обходе точек множества A. Дадим теперь точное определение.

Пусть F_a – множество всех ростков $\mathcal{S}$-функции f в точке a, не лежащей в некотором запрещенном множестве A. Возьмем замкнутую кривую γ в $S^2 \setminus A$ с началом в точке a. Продолжение каждого ростка из множества F_a вдоль кривой γ приводит к ростку из множества F_a.

Итак, каждой кривой γ соответствует отображение множества F_a в себя, причем гомотопным в $S^2 \setminus A$ кривым отвечают одинаковые отображения. Произведению кривых отвечает произведение отображений. Возникает гомоморфизм τ фундаментальной группы множества $S^2 \setminus A$ в группу $S(F_a)$ взаимно однозначных преобразований множества F_a. Этот гомоморфизм будем называть *гомоморфизмом A-монодромии.* Группой монодромии $\mathcal{S}$-функции f с запрещенным множеством A или, короче, *группой A-монодромии* называется образ фундаментальной группы $\pi_1(S^2 \setminus A, a)$ в группе $S(F_a)$ при гомоморфизме τ.

Утверждение 5.10. 1) *Группа A-монодромии $\mathcal{S}$-функции не зависит от выбора точки a.*

2) *Группа A-монодромии $\mathcal{S}$-функции f транзитивно действует на листах функции f.*

Оба утверждения просто доказываются при помощи леммы 5.6. Остановимся, например, на доказательстве второго из них.

Доказательство. Пусть f_{1a} и f_{2a} – некоторые ростки функции f в точке a. Так как ростки f_{1a} и f_{2a} эквивалентны, то существует кривая γ, при продолжении вдоль которой ростка f_{1a} получается росток f_{2a}. Согласно лемме 5.6, существует сколь угодно близкая кривая $\widehat{\gamma}$, не пересекающая множества A. Если кривая $\widehat{\gamma}$ достаточно близка к кривой γ, то соответствующая ей перестановка листов переводит росток f_{1a} в росток f_{2a}.

5.3.2. Замкнутая группа монодромии. Зависимость группы A-монодромии от выбора множества A (см. п. 5.1.3) заставляет ввести тихоновскую топологию в группе перестановок листов. Оказывается, что замыкание группы A-монодромии уже не зависит от множества A.

Группу $S(M)$ взаимно однозначных преобразований множества M мы будем рассматривать вместе со следующей топологией. Для каждого конечного множества $L \subset M$ определим окрестность U_L тождественного преобразования как совокупность преобразований p таких, что $p(l) = l$ при $l \in L$. Базис окрестностей тождественного преобразования определяется как множество окрестностей вида U_L, где L пробегает все конечные подмножества M.

Лемма 5.11 (о замыкании группы монодромии). *Замыкание группы монодромии $\mathcal{S}$-функции f с запрещенным множеством A в группе $S(F)$ всех перестановок листов функции f не зависит от выбора запрещенного множества A.*

Доказательство. Пусть A_1 и A_2 – два запрещенных множества функции f и F_a – совокупность листов функции f в точке a, $a \notin A_1 \cup A_2$. Пусть $\Gamma_1, \Gamma_2 \subseteq S(F_a)$ – группы монодромии функции f с этими запрещенными множествами. Достаточно показать, что для каждой перестановки $\mu_1 \in \Gamma_1$ и для каждого конечного множества $L \subseteq F_a$ существует перестановка $\mu_2 \in \Gamma_2$ такая, что $\mu_1|_L = \mu_2|_L$. Пусть кривая $\gamma \in \pi_1(S^2 \setminus A_1, a)$ задает перестановку μ_1. Так как множество L конечно, всякая кривая $\widehat{\gamma} \in \pi_1(S^2 \setminus A_1, a)$, достаточно близкая к кривой γ, задает перестановку $\widehat{\mu}_1$, совпадающую с перестановкой μ_1 на множестве L, $\mu_1|_L = \widehat{\mu}_1|_L$. По лемме 5.6 такую кривую $\widehat{\gamma}$ можно выбрать так, чтобы она не пересекала множества A_2. Перестановка $\widehat{\mu}_1$ в этом случае будет лежать в группе Γ_2.

Лемма делает корректным следующее определение: *замкнутой группой монодромии* $\mathcal{S}$-функции f называется замыкание в группе $S(F)$ группы монодромии функции с некоторым запрещенным множеством A.

5.3.3. Транзитивное действие группы на множестве и монодромная пара $\mathcal{S}$-функции. Группа монодромии функции f – это не просто абстрактная группа, но транзитивная группа перестановок листов этой функции. В этом пункте напоминается алгебраическое описание транзитивных действий группы на множествах.

Действием группы Γ на множестве M называется гомоморфизм τ группы Γ в группу $S(M)$. Два действия $\tau_1 : \Gamma \to S(M_1)$ и $\tau_2 : \Gamma \to S(M_2)$ называются эквивалентными, если существует такое взаимно однозначное отображение $q : M_1 \to M_2$, что $\overline{q} \circ \tau_1 = \tau_2$, где $\overline{q} : S(M_1) \to S(M_2)$ – изоморфизм, индуцированный отображением q.

Стационарной подгруппой Γ_a точки $a \in M$ при действии τ называется подгруппа, состоящая из всех элементов $\mu \in \Gamma$ таких, что $\tau\mu(a) = a$. Действие τ называется *транзитивным*, если для любых точек $a, b \in M$ существует $\mu \in \Gamma$ такое, что $\tau\mu(a) = b$. Очевидно следующее утверждение.

Утверждение 5.12. 1) *Действие τ группы Γ транзитивно, если и только если стационарные подгруппы любых двух точек $a, b \in M$ сопряжены. Образ группы Γ при транзитивном действии τ изоморфен фактор-группе $\Gamma / \bigcap_{\mu \in \Gamma} \mu\Gamma_a\mu^{-1}$.*

2) *Существует и при этом единственное с точностью до эквивалентности транзитивное действие группы Γ с фиксированной стационарной подгруппой некоторой точки.*

Итак, транзитивные действия группы Γ описываются парами групп. Пару групп $[\Gamma, \Gamma_a]$, где Γ_a – стационарная подгруппа некоторой точки a при транзитивном действии τ группы Γ, будем называть *монодромной парой точки a* относительно действия τ. Группу $\tau(\Gamma) \sim \Gamma/\bigcap_{\mu\in\Gamma}\mu\Gamma_a\mu^{-1}$ будем называть группой монодромии пары $[\Gamma,\Gamma_a]$.

Гомоморфизм A-монодромии τ задает транзитивное действие фундаментальной группы $\pi_1(S^2\setminus A)$ в множестве F_a листов функции f в точке a.

Монодромную пару ростка f_a относительно действия τ будем называть *монодромной парой ростка f_a с запрещенным множеством A*. Монодромную пару ростка f_a при действии замкнутой группой монодромии будем называть *замкнутой монодромной парой ростка f_a*. У разных ростков $\mathcal{S}$-функции f монодромные пары с запрещенным множеством A изоморфны, поэтому имеет смысл говорить о монодромной паре с запрещенным множеством A и замкнутой монодромной паре $\mathcal{S}$-функции f. Замкнутую монодромную пару $\mathcal{S}$-функции f будем обозначать $[f]$.

5.3.4. Почти нормальные функции. Пару групп $[\Gamma,\Gamma_0]$, $\Gamma_0\subseteq\Gamma$, будем называть *почти нормальной парой*, если существует конечное множество $P\subset\Gamma$ такое, что

$$\bigcap_{\mu\in\Gamma}\mu\Gamma_0\mu^{-1}=\bigcap_{\mu\in P}\mu\Gamma_0\mu^{-1}.$$

Лемма 5.13 (о дискретном действии). *Образ $\tau(\Gamma)$ группы Γ при транзитивном действии $\tau\colon\Gamma\to S(M)$ является дискретной подгруппой в $S(M)$, если и только если монодромная пара $[\Gamma,\Gamma_0]$ некоторого элемента $x_0\in M$ почти нормальна.*

Доказательство. Пусть группа $\tau(\Gamma)$ дискретна. Обозначим через $\overline{P}$ такое конечное подмножество множества M, что окрестность тождественного преобразования $U_{\overline{P}}$ не содержит преобразований группы $\tau(\Gamma)$, отличных от тождественного. Это означает, что пересечению $\bigcap_{x\in\overline{P}}\Gamma_x$ стационарных подгрупп точек $x\in\overline{P}$ отвечает тривиальное действие на множестве M, т.е. $\bigcap_{x\in\overline{P}}\Gamma_x\subseteq\bigcap_{\mu\in\Gamma}\mu\Gamma_0\mu^{-1}$. Группы Γ_x сопряжены группе Γ_0, поэтому можно выбрать такое конечное множество $P\subset\Gamma$, что $\bigcap_{\mu\in P}\mu\Gamma_0\mu^{-1}=\bigcap_{\mu\in\Gamma}\mu\Gamma_0\mu^{-1}$. Обратное утверждение доказывается аналогично.

$\mathcal{S}$-функцию f будем называть *почти нормальной*, если ее группа монодромии дискретна. Из леммы вытекает, что функция f почти нормальна, если и только если почти нормальна ее замкнутая монодромная пара $[f]$.

Дифференциальной рациональной функцией от нескольких функций называется рациональная функция от этих функций и их производных.

Лемма 5.14 (о конечно-порожденных функциях). *Пусть каждый росток $\mathcal{S}$-функции f в точке a является дифференциальной рациональной функцией от конечного числа фиксированных ростков функции f в точке a. Тогда функция f почти нормальна.*

Действительно, если при продолжении вдоль замкнутой кривой не изменяются фиксированные ростки функции, то не меняются и дифференциальные рациональные функции от них.

Из леммы о конечно-порожденных функциях вытекает, что любое решение линейного дифференциального уравнения с рациональными коэффициентами является почти нормальной функцией. То же самое верно и для многих других функций, естественно встречающихся в дифференциальной алгебре.

5.3.5. Классы пар групп. В следующем пункте мы опишем, как изменяются замкнутые монодромные пары функций при суперпозициях, интегрированиях, дифференцированиях и т. д. Для этого нам понадобятся некоторые понятия, связанные с парами групп.

Парой групп мы всегда будем называть пару, состоящую из группы и некоторой ее подгруппы. Будем отождествлять группу с парой групп, состоящей из этой группы и ее единичной подгруппы.

Определение. Совокупность $\mathscr{L}$ пар будем называть *почти полным классом пар групп*, если

1) для каждой пары групп $[\Gamma, \Gamma_0] \in \mathscr{L}$, $\Gamma_0 \subseteq \Gamma$, и любого гомоморфизма $\tau\colon \Gamma \to G$, где G – некоторая группа, пара групп $[\tau\Gamma, \tau\Gamma_0]$ также содержится в $\mathscr{L}$,
2) для каждой пары групп $[\Gamma, \Gamma_0] \in \mathscr{L}$, $\Gamma_0 \subseteq \Gamma$, и любого гомоморфизма $\tau\colon G \to \Gamma$, где G – некоторая группа, пара групп $[\tau^{-1}\Gamma, \tau^{-1}\Gamma_0]$ также содержится в $\mathscr{L}$,
3) для каждой пары групп $[\Gamma, \Gamma_0] \in \mathscr{L}$, $\Gamma_0 \subseteq \Gamma$, и группы G, наделенной T_2-топологией и содержащей группу Γ, $\Gamma \subseteq G$, пара групп $[\overline{\Gamma}, \overline{\Gamma}_0]$ также содержится в $\mathscr{L}$, где $\overline{\Gamma}$, $\overline{\Gamma}_0$ – замыкания групп Γ, Γ_0 в группе G.

Определение. Почти полный класс пар групп будем называть *полным классом пар групп* $\mathscr{M}$, если

1) для каждой пары групп $[\Gamma, \Gamma_0] \in \mathscr{M}$ и группы $\Gamma_1, \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma$, пара групп $[\Gamma, \Gamma_1]$ также содержится в $\mathscr{M}$,
2) для каждых двух пар групп $[\Gamma, \Gamma_1], [\Gamma_1, \Gamma_2] \in \mathscr{M}$ пара групп $[\Gamma, \Gamma_2]$ также содержится в $\mathscr{M}$.

Минимальные почти полный и полный классы пар групп, содержащие фиксированное множество пар групп $\mathscr{B}$, будем обозначать соответственно $\mathscr{L}\langle\mathscr{B}\rangle$ и $\mathscr{M}\langle\mathscr{B}\rangle$.

Лемма 5.15. 1) *Если группа монодромии пары $[\Gamma, \Gamma_0]$ содержится в некотором полном классе пар $\mathscr{M}$, то пара $[\Gamma, \Gamma_0]$ также содержится в $\mathscr{M}$.*

2) *Если почти нормальная пара $[\Gamma, \Gamma_0]$ содержится в некотором полном классе пар $\mathscr{M}$, то ее группа монодромии также содержится в $\mathscr{M}$.*

Остановимся на доказательстве второго утверждения. Пусть Γ_i, $i = 1, \ldots, n$, – конечное число подгрупп, сопряженных с Γ_0, таких, что $\bigcap_{i=1}^n \Gamma_i = \bigcap_{\mu \in \Gamma} \mu\Gamma_0\mu^{-1}$. Пары $[\Gamma, \Gamma_i]$ изоморфны паре $[\Gamma, \Gamma_0]$, поэтому $[\Gamma, \Gamma_i] \in \mathscr{M}$. Пусть $\tau\colon \Gamma_2 \to \Gamma$ – гомоморфизм вложения, тогда $\tau^{-1}(\Gamma_1) = \Gamma_2 \cap \Gamma_1$, поэтому $[\Gamma_2, \Gamma_2 \cap \Gamma_1] \in \mathscr{M}$. Класс $\mathscr{M}$ содержит пары $[\Gamma, \Gamma_2]$ и $[\Gamma_2, \Gamma_2 \cap \Gamma_1]$, следовательно, $[\Gamma, \Gamma_1 \cap \Gamma_2] \in \mathscr{M}$. Продолжая это рассуждение, получим, что класс $\mathscr{M}$ содержит пару $[\Gamma, \bigcap_{i=1}^n \Gamma_i]$ и вместе с ней группу $\Gamma / \bigcap_{\mu \in \Gamma} \mu\Gamma_0\mu^{-1}$.

Утверждение 5.16 (о классе $\mathscr{L}\langle[f]\rangle$). *Почти полный класс пар $\mathscr{L}$ содержит замкнутую монодромную пару $[f]$ $\mathcal{S}$-функции f, если и только если этот класс содержит монодромную пару функции f с запрещенным множеством A.*

Доказательство. Пусть $[\Gamma, \Gamma_0]$ – монодромная пара функции f с запрещенным множеством A. Тогда $[f] = [\overline{\Gamma}, \overline{\Gamma}_0]$. Поэтому всякий почти полный класс $\mathscr{L}$, содержащий пару $[\Gamma, \Gamma_0]$, содержит и пару $[f]$. Обратно, если $[\overline{\Gamma}, \overline{\Gamma}_0]$ содержится в классе $\mathscr{L}$, то и $[\Gamma, \Gamma_0] \in \mathscr{L}$. Действительно, топология в группе перестановок устроена таким образом, что $\Gamma_0 = \Gamma \cap \overline{\Gamma}_0$. Поэтому пара $[\Gamma, \Gamma_0]$ является прообразом пары $[\overline{\Gamma}, \overline{\Gamma}_0]$ при вложении группы Γ в ее замыкание.

5.4. Основная теорема. Здесь формулируется и доказывается основная теорема топологического варианта теории Галуа.

Основная теорема 5.17. *Класс $\mathcal{S}$-функций $\widehat{\mathscr{M}}$, состоящий из $\mathcal{S}$-функций, замкнутая монодромная пара которых лежит в некотором полном классе пар $\mathscr{M}$, замкнут относительно дифференцирования, суперпозиций и мероморфных операций.*

Если, кроме того, класс $\mathscr{M}$ содержит группу $\mathbb{C}$ комплексных чисел по сложению, то класс $\widehat{\mathscr{M}}$ замкнут относительно интегрирования. Если же класс $\mathscr{M}$ содержит группу $S(k)$ перестановок k элементов, то класс $\widehat{\mathscr{M}}$ замкнут относительно решения алгебраических уравнений степени не выше k.

Доказательство основной теоремы состоит из следующих лемм.

Лемма 5.18 (о производной). *Для всякой $\mathcal{S}$-функции f справедливо включение $[f'] \in \mathscr{M}\langle[f]\rangle$.*

Доказательство. Пусть A – множество особых точек $\mathcal{S}$-функции f и f_a – росток функции f в неособой точке a. Обозначим через Γ фундаментальную группу $\pi_1(S^2 \setminus A, a)$, через Γ_1 и Γ_2 – стационарные группы ростков f_a и f'_a. Группа Γ_1 содержится в группе Γ_2. Действительно, при продолжении вдоль кривой $\gamma \in \Gamma_1$ не изменяется росток f_a, а значит, не меняется и его производная. Из определения полного класса пар следует, что $[\Gamma, \Gamma_2] \in \mathscr{M}\langle[\Gamma, \Gamma_1]\rangle$. Воспользовавшись утверждением 5.16, получим, что $[f'] \in \mathscr{M}\langle[f]\rangle$.

Лемма 5.19 (о суперпозиции). *Для всяких $\mathcal{S}$-функций f и g справедливо включение $[g \circ f] \in \mathscr{M}\langle[f], [g]\rangle$.*

Доказательство. Пусть A и B – множества особых точек функций f и g. Пусть $f^{-1}(B)$ – прообраз множества B при многозначном соответствии, порожденном многозначной функцией f. Положим $Q = A \cup f^{-1}(B)$. Пусть f_a – некоторый росток функции f в точке $a \notin Q$ и g_b – некоторый росток функции g в точке $b = f(a)$. Множество Q будет запрещенным для ростка $g_b \circ f_a$. Обозначим через Γ фундаментальную группу $\pi_1(S^2 \setminus Q, a)$, через Γ_1 и Γ_2 – стационарные подгруппы ростков f_a и $g_b \circ f_a$. Обозначим через G фундаментальную группу $\pi_1(S^2 \setminus B, b)$ и через G_0 – стационарную группу ростка g_b.

Определим гомоморфизм $\tau : \Gamma_1 \to G$. Каждой кривой $\gamma \in \Gamma_1$ поставим в соответствие кривую $\tau \circ \gamma(t) = f(\gamma(t))$, где $f_{\gamma(t)}$ – росток, полученный при продолжении ростка f_a вдоль кривой γ до точки t. Кривые $\tau \circ \gamma$ будут замкнуты, так как при продолжении вдоль кривых из Γ_1 росток f_a не изменяется. При гомотопии кривой γ в множестве $S^2 \setminus Q$ будет происходить гомотопия кривой $\tau \circ \gamma$ в множестве $S^2 \setminus B$, так как $f^{-1}(B) \subseteq Q$. Следовательно, гомоморфизм определен корректно.

Росток $g_b \circ f_a$ не будет меняться при продолжении вдоль кривых из группы $\tau^{-1}(G_0)$, или, другими словами, $\tau^{-1}(G_0) \subseteq \Gamma_2$. Откуда и вытекает лемма. Действительно, мы получаем включения $\Gamma \supseteq \Gamma_2 \supseteq \tau^{-1}(G_0) \subseteq \tau^{-1}(G) = \Gamma_1 \subseteq \Gamma$, из которых следует, что $[\Gamma, \Gamma_2] \in \mathscr{M}\langle[G, G_0], [\Gamma, \Gamma_1]\rangle$. Воспользовавшись утверждением 5.16, получим, что $[g \circ f] \in \mathscr{M}\langle[f], [g]\rangle$.

Лемма 5.20 (об интеграле). *Для всякой $\mathcal{S}$-функции f справедливо включение $[\int f(x)\,dx] \in \mathscr{M}\langle [f], \mathbb{C}\rangle$, где $\mathbb{C}$ – группа комплексных чисел по сложению.*

Доказательство. Пусть A – множество особых точек функции f и $Q = A \cup \{\infty\}$. Пусть f_a – некоторый росток функции f в точке $a \notin Q$ и g_a – росток $\int f(x)\,dx$ в этой точке, $g_a' = f_a$. В качестве запрещенного множества для ростков f_a и g_a можно взять множество Q. Обозначим через Γ фундаментальную группу $\pi_1(S^2 \setminus Q, a)$, через Γ_1 и Γ_2 – стационарные подгруппы ростков f_a и g_a.

Определим гомоморфизм $\tau\colon \Gamma_1 \to \mathbb{C}$. Каждой кривой $\gamma \in \Gamma_1$ поставим в соответствие число $\int_\gamma f(\gamma(t))\,dx$, где $f_{\gamma(t)}$ – росток, полученный продолжением ростка f_a вдоль кривой γ до точки t, и $x = \gamma(t)$. Стационарная подгруппа Γ_2 ростка g_a совпадает с ядром гомоморфизма τ, откуда следует, что $[\Gamma, \Gamma_2] \in \mathscr{M}\langle [\Gamma, \Gamma_1], \mathbb{C}\rangle$. Воспользовавшись утверждением 5.16, получим, что $[\int f(x)\,dx] \in \mathscr{M}\langle [f], \mathbb{C}\rangle$.

В дальнейшем будет удобно пользоваться векторными функциями. На векторные функции непосредственно переносятся определения запрещенного множества, $\mathcal{S}$-функции, группы монодромии.

Лемма 5.21 (о векторной функции). *Для всякой векторной $\mathcal{S}$-функции $\mathbf{f} = (f_1, \dots, f_n)$ справедливо равенство*:

$$\mathscr{M}\langle [\mathbf{f}]\rangle = \mathscr{M}\langle [f_1], \dots, [f_n]\rangle.$$

Доказательство. Пусть A_i – множества особых точек функций f_i. Множеством особых точек векторной функции $\mathbf{f}$ является множество $Q = \bigcup A_i$. Пусть $\mathbf{f}_a = (f_{1a}, \dots, f_{na})$ – некоторый росток векторной функции $\mathbf{f}$ в точке $a \notin Q$. Обозначим через Γ фундаментальную группу $\pi_1(S^2 \setminus Q, a)$, через Γ_i – стационарные группы ростков f_{ia} и через Γ_0 – стационарную группу векторного ростка $\mathbf{f}_a$. Стационарная подгруппа Γ_0 есть в точности $\bigcap_{i=1}^n \Gamma_i$, откуда следует, что

$$\mathscr{M}\langle [\Gamma, \Gamma_0]\rangle = \mathscr{M}\langle [\Gamma, \Gamma_1], \dots, [\Gamma, \Gamma_n]\rangle.$$

Воспользовавшись утверждением 5.16, получим, что

$$\mathscr{M}\langle [\mathbf{f}]\rangle = \mathscr{M}\langle [f_1], \dots, [f_n]\rangle.$$

Лемма 5.22 (о мероморфной операции). *Для всякой векторной $\mathcal{S}$-функции $\mathbf{f} = (f_1, \dots, f_n)$ и мероморфной функции $F(x_1, \dots, x_n)$ такой, что функция $F \circ \mathbf{f}$ определена, справедливо включение $[F \circ \mathbf{f}] \in \mathscr{M}\langle [\mathbf{f}]\rangle$.*

Доказательство. Пусть A – множество особых точек функции $\mathbf{f}$ и B – проекция множества полюсов функции $F \circ \mathbf{f}$ на сферу Римана. В качестве запрещенного множества функций $F \circ \mathbf{f}$ и $\mathbf{f}$ можно взять множество $Q = A \cup B$. Пусть $\mathbf{f}_a$ – некоторый росток функции $\mathbf{f}$ в точке a, $a \notin Q$. Обозначим через Γ фундаментальную группу $\pi_1(S^2 \setminus Q, a)$, через Γ_1 и Γ_2 – стационарные группы ростков $\mathbf{f}_a$ и $F \circ \mathbf{f}_a$. Группа Γ_2 содержится в группе Γ_1. Действительно, при продолжении вдоль кривой $\gamma \in \Gamma_1$ не изменяется векторная функция, а значит, не меняется мероморфная функция от нее. Из включения $\Gamma_2 \subseteq \Gamma_1$ следует, что $[\Gamma, \Gamma_2] \in \mathscr{M}\langle [\Gamma, \Gamma_1]\rangle$. Воспользовавшись утверждением 5.16, получим, что

$$[F \circ \mathbf{f}] \in \mathscr{M}\langle [\mathbf{f}]\rangle.$$

Лемма 5.23 (об алгебраической функции). *Для всякой векторной $\mathcal{S}$-функции $\mathbf{f} = (f_1, \dots, f_n)$ и алгебраической функции y от нее, определенной равенством*

$$y^k + f_1 y^{k-1} + \dots + f_k = 0, \tag{12}$$

справедливо включение $[y] \in \mathscr{M}\langle [f], S(k)\rangle$, где $S(k)$ – группа перестановок k элементов.

Доказательство. Пусть A – множество особых точек функции $\mathbf{f}$ и B – проекция множества алгебраических точек ветвления функции y на сферу Римана. В качестве запрещенного множества функций y и $\mathbf{f}$ можно взять множество $Q = A \cup B$. Пусть y_a и $\mathbf{f}_a$ – некоторые ростки функций y и $\mathbf{f}$ в точке $a \notin Q$, связанные равенством

$$y_a^k + f_{1a} y_a^{k-1} + \dots + f_{ka} = 0.$$

Обозначим через Γ фундаментальную группу $\pi_1(S^2 \setminus Q, a)$ и через Γ_1 и Γ_2 – стационарные подгруппы ростков $\mathbf{f}_a$ и y_a. При продолжении вдоль кривой $\gamma \in \Gamma_1$ коэффициенты уравнения (12) не меняются, следовательно, при продолжении вдоль кривой γ корни уравнения (12) переставляются. Возникает гомоморфизм τ группы Γ_1 в группу $S(k)$, $\tau\colon \Gamma_1 \to S(k)$. Группа Γ_2 содержится в ядре гомоморфизма τ, откуда следует, что $[\Gamma, \Gamma_2] \in \mathscr{M}\langle [\Gamma, \Gamma_1], S(k)\rangle$. Воспользовавшись утверждением 5.16, получим, что

$$[y] \in \mathscr{M}\langle [f], S(k)\rangle.$$

Доказательство основной теоремы закончено.

5.5. Групповые препятствия к представимости в квадратурах. В этом пункте вычисляются классы пар групп, встречающиеся в основной теореме, и формулируются необходимые условия представимости функций в квадратурах, k-квадратурах и обобщенных квадратурах.

5.5.1. Вычисление некоторых классов пар групп. Основная теорема делает актуальной задачу описания наименьшего класса пар групп, содержащего группу $\mathbb{C}$ комплексных чисел по сложению, а также наименьших пар классов пар групп, содержащих соответственно группу $\mathbb{C}$ и все конечные группы, а также группу $\mathbb{C}$ и группу $S(k)$. В настоящем пункте мы приводим решение этих задач.

Утверждение 5.24. *Наименьший полный класс пар $\mathscr{M}\langle \mathscr{L}_\alpha\rangle$, содержащий заданные почти полные классы пар $\mathscr{L}_\alpha$, состоит из пар групп $[\Gamma, \Gamma_0]$, для которых существует цепочка подгрупп $\Gamma = \Gamma_1 \supseteq \dots \supseteq \Gamma_m \subseteq \Gamma_0$ такая, что для любого i, $1 \leqslant i \leqslant m-1$, пара групп $[\Gamma_i, \Gamma_{i+1}]$ содержится в некотором почти полном классе $\mathscr{L}_{\alpha(i)}$.*

Для доказательства достаточно проверить, что пары групп $[\Gamma, \Gamma_0]$, удовлетворяющие условию утверждения, во-первых, содержатся в полном классе $\mathscr{M}\langle \mathscr{L}_\alpha\rangle$ и, во-вторых, образуют полный класс пар. И то и другое непосредственно выводится из определений.

Просто проверить также следующие утверждения.

УТВЕРЖДЕНИЕ 5.25. *Совокупность пар групп* $[\Gamma, \Gamma_0]$ *таких, что* Γ_0 *есть нормальный делитель группы* Γ *и группа* Γ/Γ_0 *коммутативна, образует наименьший почти полный класс пар* $\mathscr{L}\langle\mathscr{A}\rangle$, *содержащий класс* $\mathscr{A}$ *всех абелевых групп.*

УТВЕРЖДЕНИЕ 5.26. *Совокупность пар групп* $[\Gamma, \Gamma_0]$ *таких, что* Γ_0 *есть нормальный делитель группы* Γ *и группа* Γ/Γ_0 *конечна, образует наименьший почти полный класс пар* $\mathscr{L}\langle\mathscr{K}\rangle$, *содержащий класс* $\mathscr{K}$ *всех конечных групп.*

УТВЕРЖДЕНИЕ 5.27. *Совокупность пар групп* $[\Gamma, \Gamma_0]$ *таких, что* $\operatorname{ind}(\Gamma, \Gamma_0) \leqslant k$, *образует почти полный класс групп.*

Класс пар групп из утверждения 5.27 будем обозначать через $\mathscr{L}\langle\operatorname{ind} \leqslant k\rangle$. Утверждение 5.27 интересно для нас в связи с характеристическим свойством подгрупп группы $S(k)$ из леммы 3.13. Цепочка подгрупп Γ_i, $i = 1, \dots, m$, $\Gamma = \Gamma_1 \supseteq \dots \supseteq \Gamma_m \subseteq \Gamma_0$ называется *нормальной башней пары групп* $[\Gamma, \Gamma_0]$, если группа Γ_{i+1} является нормальным делителем группы Γ_i при каждом $i = 1, \dots, m-1$. Совокупность фактор-групп Γ_i/Γ_{i+1} называется совокупностью делителей относительно нормальной башни.

ТЕОРЕМА 5.28 (о классах пар $\mathscr{M}\langle\mathscr{A}, \mathscr{K}\rangle$, $\mathscr{M}\langle\mathscr{A}, S(k)\rangle$ и $\mathscr{M}\langle\mathscr{A}\rangle$). 1) *Пара групп* $[\Gamma, \Gamma_0]$ *принадлежит наименьшему полному классу* $\mathscr{M}\langle\mathscr{A}, \mathscr{K}\rangle$, *содержащему все конечные и коммутативные группы, если и только если она обладает нормальной башней, каждый делитель относительно которой является или конечной, или коммутативной группой.*

2) *Пара групп* $[\Gamma, \Gamma_0]$ *принадлежит наименьшему полному классу* $\mathscr{M}\langle\mathscr{A}, S(k)\rangle$, *содержащему группу* $S(k)$ *и все коммутативные группы, если и только если она обладает нормальной башней, каждый делитель относительно которой является или подгруппой группы* $S(k)$, *или коммутативной группой.*

3) *Пара групп* $[\Gamma, \Gamma_0]$ *принадлежит наименьшему классу* $\mathscr{M}\langle\mathscr{A}\rangle$, *если и только если группа монодромии этой пары разрешима.*

ДОКАЗАТЕЛЬСТВО. Первый пункт теоремы вытекает из описания классов $\mathscr{L}\langle\mathscr{A}\rangle$ и $\mathscr{L}\langle\mathscr{K}\rangle$ в утверждениях 5.25 и 5.26 и из утверждения 5.24.

Для доказательства второго пункта рассмотрим наименьший полный класс пар групп, содержащий классы $\mathscr{L}\langle\mathscr{A}\rangle$ и $\mathscr{L}\langle\operatorname{ind} \leqslant k\rangle$. Этот класс состоит из пар групп $[\Gamma, \Gamma_0]$, для которых существует цепочка подгрупп $\Gamma = \Gamma_1 \supseteq \dots \supseteq \Gamma_m \subseteq \Gamma_0$ такая, что для любого i, $1 \leqslant i \leqslant m-1$, либо группа Γ_i/Γ_{i+1} коммутативна, либо $\operatorname{ind}(\Gamma_i, \Gamma_{i+1}) \leqslant k$ (см. утверждения 5.26, 5.27 и утверждение 5.24). Описанный класс пар групп содержит группу $S(k)$ (см. лемму 3.13) и все коммутативные группы и является, очевидно, наименьшим полным классом пар, обладающим этими свойствами. Нам осталось переформулировать ответ. Цепочку подгрупп $\Gamma = \Gamma_1 \supseteq \dots \supseteq \Gamma_m \subseteq \Gamma_0$ последовательно преобразуем в нормальную башню пары $[\Gamma, \Gamma_0]$. Пусть при $j < i$ группа Γ_{j+1} является нормальным делителем группы Γ_j и $\operatorname{ind}(\Gamma_i, \Gamma_{i+1}) \leqslant k$. Обозначим через $\overline{\Gamma}_{i+1}$ наибольший нормальный делитель группы Γ_i, содержащийся в Γ_{i+1}. Ясно, что фактор-группа $\Gamma_i/\overline{\Gamma}_{i+1}$ является подгруппой группы $S(k)$. Вместо исходной цепочки подгрупп рассмотрим цепочку $\Gamma = G_1 \supseteq \dots \supseteq G_m = \Gamma_0$, в которой $G_j = \Gamma_j$ при $j \leqslant i$ и $G_j = \Gamma_j \cap \overline{\Gamma}_{i+1}$ при $j > i$. Продолжая этот процесс (не более чем m раз), мы перейдем от исходной цепочки подгрупп к нормальной башне и получим описание класса $\mathscr{M}\langle\mathscr{A}, S(k)\rangle$ в нужных терминах.

Докажем пункт 3). Согласно утверждениям 5.25 и 5.26, пара групп $[\Gamma, \Gamma_0]$ принадлежит классу $\mathscr{M}\langle\mathscr{A}\rangle$, если и только если существует такая цепочка $\Gamma = \Gamma_1 \supseteq \dots \supseteq \Gamma_m \subseteq \Gamma_0$, что Γ_i/Γ_{i+1} – коммутативная группа. Рассмотрим цепочку групп $\Gamma = G^1 \supseteq \dots \supseteq G^m$, в которой группа G^{i+1} при $i = 1, \dots, m-1$ есть коммутант группы G^i. Всякий автоморфизм группы Γ переводит цепочку групп G^i в себя, поэтому каждая группа G^i является нормальным делителем группы Γ. Индукция по i показывает, что $G^i \subseteq \Gamma_i$ и, в частности, $G^m \subseteq \Gamma_m \subseteq \Gamma_0$. Группа G^m является нормальным делителем группы Γ, и так как $G^m \subseteq \Gamma_0$, то $G^m \subseteq \bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1}$. В силу определения цепочки G^i группа Γ/G^m разрешима. Группа $\Gamma/\bigcap_{\mu\in\Gamma} \mu\Gamma_0\mu^{-1}$ разрешима как фактор-группа группы Γ/G^m. Обратное утверждение (пара групп с разрешимой группой монодромии лежит в классе $\mathscr{M}\langle\mathscr{A}\rangle$) очевидно.

Утверждение 5.29. *Каждая не более чем континуальная коммутативная группа Γ принадлежит классу $\mathscr{L}\langle\mathbb{C}\rangle$.*

Доказательство. Комплексные числа $\mathbb{C}$ образуют векторное пространство над рациональными числами континуальной размерности. Пусть $\{e_\alpha\}$ – некоторый базис этого пространства. Подгруппа $\widetilde{\mathbb{C}}$ группы $\mathbb{C}$, натянутая на числа $\{e_\alpha\}$, является свободной абелевой группой с континуальным числом образующих. Всякая не более чем континуальная коммутативная группа Γ есть фактор-группа группы $\widetilde{\mathbb{C}}$ и, следовательно, $\Gamma \in \mathscr{L}\langle\mathbb{C}\rangle$.

Из утверждения 5.29 и результатов вычисления классов $\mathscr{M}\langle\mathscr{A},\mathscr{K}\rangle$, $\mathscr{M}\langle S(n)\rangle$ и $\mathscr{M}\langle\mathscr{A}\rangle$ следует, что пара групп $[\Gamma, \Gamma_0]$ с не более чем континуальной группой Γ принадлежит классу $\mathscr{M}\langle\mathbb{C},\mathscr{K}\rangle$, $\mathscr{M}\langle\mathbb{C}, S(n)\rangle$ или $\mathscr{M}\langle\mathbb{C}\rangle$, если и только если она принадлежит классу $\mathscr{M}\langle\mathscr{A},\mathscr{K}\rangle$, $\mathscr{M}\langle\mathscr{A}, S(n)\rangle$ или $\mathscr{M}\langle\mathscr{A}\rangle$.

Мы вправе ограничиться этим результатом, так как группа перестановок листов функции не более чем континуальна.

Лемма 5.30. *Свободная некоммутативная группа Λ не лежит в классе $\mathscr{M}\langle\mathscr{A},\mathscr{K}\rangle$.*

Доказательство. Предположим, что $\Lambda \in \mathscr{M}\langle\mathscr{A},\mathscr{K}\rangle$, т.е. Λ обладает нормальной башней $\Lambda = \Gamma_1 \supseteq \dots \supseteq \Gamma_m = e$, каждый делитель относительно которой есть конечная или коммутативная группа. Каждая группа Γ_i свободна как подгруппа свободной группы (см. [28]). Группа $\Gamma_m = e$ коммутативна. Пусть Γ_{i+1} – первая по номеру коммутативная группа. Для любых элементов $a, b \in \Gamma_i$ существует нетривиальное соотношение: если Γ_i/Γ_{i+1} коммутативна, то коммутируют, например, элементы $aba^{-1}b^{-1}$ и $ab^2a^{-1}b^{-2}$, если Γ_i/Γ_{i+1} конечна, то коммутируют некоторые степени a^p, b^p элементов a, b. Следовательно, группа Γ_i имеет не более одной образующей и поэтому коммутативна. Противоречие доказывает, что $\Lambda \notin \mathscr{M}\langle\mathscr{A},\mathscr{K}\rangle$.

Лемма 5.31. *При $k > 4$ симметрическая группа $S(k)$ не лежит в классе $\mathscr{M}\langle\mathbb{C}, S(k-1)\rangle$.*

Доказательство. При $k > 4$ знакопеременная группа $A(n)$ проста и некоммутативна. Для этой группы, очевидно, не выполняется критерий принадлежности классу $\mathscr{M}\langle\mathbb{C}, S(k-1)\rangle$. Следовательно, и симметрическая группа $S(n)$ при $k > 4$ не лежит в классе $\mathscr{M}\langle\mathbb{C}, S(k-1)\rangle$.

Лемма 5.32. *Единственной транзитивной группой перестановок k элементов, натянутой на транспозиции, является симметрическая группа $S(k)$.*

Доказательство. Пусть группа Γ есть транзитивная группа перестановок множества M из n элементов, натянутая на транспозиции. Подмножество $M_0 \subseteq M$ назовем полным, если всякая перестановка множества M_0 продолжается до некоторой перестановки множества M из группы Γ. Полные подмножества существуют. Например, два элемента множества M, переставляемые базисной транспозицией, образуют полное подмножество. Возьмем наибольшее по числу элементов полное подмножество M_0. Предположим, что $M_0 \neq M$. Так как группа Γ транзитивна, то существует базисная транспозиция μ, переставляющая некоторый элемент $a \notin M_0$ с некоторым элементом $b \in M_0$. Группа перестановок, порожденная транспозицией μ и группой $S(M_0)$, есть группа $S(M_0 \cup \{a\})$. Множество $M_0 \cup \{a\}$ является полным и содержит множество M_0. Полученное противоречие доказывает, что группа Γ есть группа $S(M)$.

5.5.2. Необходимые условия представимости функций в квадратурах, в k-квадратурах и в обобщенных квадратурах. Основная теорема (см. п. 5.4) и вычисление классов пар групп доставляют топологические препятствия к представимости функций в обобщенных квадратурах, в k-квадратурах и в квадратурах. В этом пункте мы соберем вместе полученную информацию. Начнем с определения класса функций, представимых при помощи однозначных $\mathcal{S}$-функций и квадратур (k-квадратур, обобщенных квадратур). Как и в п. 1.2, мы определим эти классы, задав списки основных функций и допустимых операций.

Функции, представимые при помощи однозначных $\mathcal{S}$-функций и квадратур.

Список основных функций: однозначные $\mathcal{S}$-функции.

Список допустимых операций: суперпозиции, мероморфные операции, дифференцирование, интегрирование.

Функции, представимые при помощи однозначных $\mathcal{S}$-функций и k-квадратур. Этот класс функций определяется в точности так же. Нужно лишь к списку допустимых операций добавить операцию решения алгебраических уравнений степени $\leqslant k$.

Функции, представимые при помощи однозначных $\mathcal{S}$-функций и обобщенных квадратур. Этот класс функций определяется в точности так же. Нужно лишь к списку допустимых операций добавить операцию решения алгебраических уравнений.

Из определения видно, что класс функций, представимых с помощью однозначных $\mathcal{S}$-функций и квадратур (k-квадратур, обобщенных квадратур), содержит класс функций, представимых в квадратурах (k-квадратурах, обобщенных квадратурах). Ясно, что только что определенные классы функций несравненно шире, чем их классические аналоги. Поэтому, скажем, утверждение о непринадлежности функции f классу функций, представимых с помощью однозначных $\mathcal{S}$-функций и квадратур, значительно сильнее, чем утверждение о непредставимости f в квадратурах.

Утверждение 5.33. *Класс функций, представимых с помощью однозначных*

$\mathcal{S}$-функций и квадратур (k-квадратур, обобщенных квадратур), лежит в классе $\mathcal{S}$-функций.

Это утверждение немедленно вытекает из теоремы о замкнутости класса $\mathcal{S}$-функций (см. п. 5.2.2).

Результат об обобщенных квадратурах. *Замкнутая монодромная пара $[f]$ функции f, представимой в обобщенных квадратурах, обладает нормальной башней, каждый делитель относительно которой есть или конечная, или коммутативная группа. Более того, этому условию удовлетворяет замкнутая монодромная пара $[f]$ всякой функции f, представимой при помощи однозначных $\mathcal{S}$-функций и обобщенных квадратур. Если дополнительно известно, что функция f почти нормальна, то указанному условию удовлетворяет и группа монодромии функции $[f]$.*

Результат о k-квадратурах. *Замкнутая монодромная пара $[f]$ функции f, представимой в k-квадратурах, обладает нормальной башней, каждый делитель относительно которой есть или подгруппа группы $S(k)$, или коммутативная группа. Более того, этому условию удовлетворяет замкнутая монодромная пара $[f]$ всякой функции f, представимой при помощи однозначных $\mathcal{S}$-функций и k-квадратур. Если дополнительно известно, что функция f почти нормальна, то указанному условию удовлетворяет и группа монодромии функции $[f]$.*

Результат о квадратурах. *Замкнутая группа монодромии функции f, представимой в квадратурах, разрешима. Более того, разрешима замкнутая группа монодромии всякой функции f, представимой при помощи однозначных $\mathcal{S}$-функций и квадратур.*

Для доказательства этих результатов достаточно применить основную теорему к классам $\mathcal{S}$-функций $\widehat{\mathscr{M}\langle\mathbb{C},\mathscr{K}\rangle}$, $\widehat{\mathscr{M}\langle\mathbb{C},S(k)\rangle}$ и $\widehat{\mathscr{M}\langle\mathbb{C}\rangle}$ и воспользоваться вычислением классов $\mathscr{M}\langle\mathbb{C},\mathscr{K}\rangle$, $\mathscr{M}\langle\mathbb{C},S(k)\rangle$ и $\mathscr{M}\langle\mathbb{C}\rangle$.

Приведем теперь примеры функций, не представимых в обобщенных квадратурах. Пусть риманова поверхность функции f является универсальной накрывающей над областью $S^2\setminus A$, где S^2 – сфера Римана и A – конечное множество, содержащее не меньше трех точек. Тогда *функция f не выражается при помощи однозначных $\mathcal{S}$-функций и обобщенных квадратур.* Действительно, функция f является почти нормальной функцией. Замкнутая группа монодромии функции f свободна и некоммутативна, так как свободна и некоммутативна фундаментальная группа области $S^2\setminus A$.

Пример 1. Рассмотрим функцию f, конформно отображающую верхнюю полуплоскость на треугольник с нулевыми углами, ограниченный дугами окружностей. Функция f обратна к модулярной функции Пикара. Риманова поверхность функции f является универсальной накрывающей над сферой без трех точек, поэтому функция f не выражается при помощи однозначных $\mathcal{S}$-функций и обобщенных квадратур.

Отметим, что функция f тесно связана с эллиптическими интегралами

$$K_1(k)=\int_0^1\frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}\quad\text{и}\quad K_2(k)=\int_0^{\frac{1}{k}}\frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}\,.$$

Каждые две из функций K_1, K_2 и f выражаются друг через друга при помощи квадратур (см. [13]). Поэтому *каждый из интегралов K_1 и K_2 не выражается при помощи однозначных $\mathcal{S}$-функций и обобщенных квадратур.*

Пример 1 допускает существенное обобщение: в работе [21] (см. также [22]) перечислены все многоугольники, ограниченные дугами окружностей, на которые можно отобразить верхнюю полуплоскость функцией, представимой в обобщенных квадратурах.

Пример 2. Пусть f – k-значная алгебраическая функция с некратными точками ветвления, расположенными в разных точках сферы Римана. *При $k > 4$ функция f не выражается при помощи однозначных $\mathcal{S}$-функций и $(k-1)$-квадратур, суперпозиций и мероморфных операций. В частности, функция f не представима в $(k-1)$-квадратурах.*

Действительно, при обходе некратной точки ветвления функции f происходит транспозиция в множестве листов этой функции. Группа монодромии функции f является транзитивной группой перестановок, натянутой на транспозиции, т.е. группой $S(k)$. При $k > 4$ группа $S(k)$ не лежит в классе $\mathscr{M}\langle\mathbb{C}, S(k-1)\rangle$.

В статьях [23]–[25] топологические результаты о непредставимости функций в квадратурах (k-квадратурах и обобщенных квадратурах) обобщены на случай функций многих комплексных переменных.

5.5.3. Классы особых множеств и обобщение основной теоремы. В § 5 рассматривались $\mathcal{S}$-функции, т.е. многозначные аналитические функции комплексного переменного, множества особых точек которых не более чем счетны. Пусть $\mathcal{S}$ – класс всех не более чем счетных подмножеств сферы Римана S^2. Перечислим свойства класса $\mathcal{S}$, которыми мы существенно пользовались:

1) если $A \in S$, то множество $S^2 \setminus A$ всюду плотно и локально линейно связно,
2) существует непустое множество A такое, что $A \in \mathcal{S}$,
3) если $A \in \mathcal{S}$ и $B \subseteq A$, то $B \in \mathcal{S}$,
4) если $A_i \in \mathcal{S}$, $i = 1, 2, \dots$, то $\bigcup_{i=1}^{\infty} A_i \in \mathcal{S}$,
5) пусть U_1 и U_2 – открытые подмножества сферы и $f\colon U_1 \to U_2$ – обратимое аналитическое отображение, тогда если $A \subseteq U_1$ и $A \in \mathcal{S}$, то $f(A) \in \mathcal{S}$.

Полным классом множеств будем называть всякое множество подмножеств сферы Римана, удовлетворяющее свойствам 1)–5). Многозначную аналитическую функцию будем называть Q-функцией, если множество ее особых точек лежит в некотором полном классе множеств Q. На Q-функции переносятся все определения и теоремы из § 5. Так, например, справедлив следующий вариант основной теоремы.

Вариант основной теоремы. *Для всякого полного класса множеств Q и полного класса пар $\mathscr{M}$ класс $\widehat{\mathscr{M}}$, состоящий из всех Q-функций f, для которых $[f] \in \mathscr{M}$, замкнут относительно дифференцирования, суперпозиций и мероморфных операций.*

Если дополнительно $\mathbb{C} \in \mathscr{M}$, то класс Q-функций $\widehat{\mathscr{M}}$ замкнут относительно интегрирования.

Если же $S(k) \in \mathscr{M}$, то класс Q-функций $\widehat{\mathscr{M}}$ замкнут относительно решения алгебраических уравнений степени не выше k.

Приведем пример полных классов множеств. Пусть X_α – множество всех подмножеств сферы Римана, имеющих нулевую хаусдорфову меру веса α. Несложно показать, что при $\alpha \leqslant 1$ множество X_α образует полный класс подмножеств сферы.

Отметим, что новая формулировка основной теоремы позволяет усилить все отрицательные результаты. Остановимся, например, на результате о непредставимости функций в квадратурах. (Результаты о непредставимости в k-квадратурах и в обобщенных квадратурах обобщаются точно так же.) Определим следующий класс функций.

Функции, представимые при помощи однозначных X_1-функций и квадратур.

Список основных функций: однозначные X_1-функции.

Список допустимых операций: суперпозиции, мероморфные операции, дифференцирование, интегрирование.

Согласно новой формулировке основной теоремы, $\mathcal{S}$-функция, имеющая неразрешимую группу монодромии, не только непредставима в квадратурах, но непредставима и при помощи однозначных X_1-функций и квадратур.

§ 6. Разрешимость в квадратурах линейных дифференциальных уравнений типа Фукса и топологический вариант теории Галуа

6.1. Теория Пикара–Вессио для уравнений типа Фукса. В этом пункте показывается, что топология расположения над комплексной плоскостью римановой поверхности общего решения линейного дифференциального уравнения типа Фукса целиком отвечает за разрешимость уравнения в явном виде.

6.1.1. Группа монодромии линейного дифференциального уравнения, ее связь с группой Галуа. Рассмотрим линейное дифференциальное уравнение

$$y^{(n)} + r_1 y^{(n-1)} + \cdots + r_n y = 0, \tag{13}$$

где r_i – рациональные функции комплексного переменного x. Полюсы рациональных функций r_i и точка ∞ называются особыми точками уравнения (13).

В окрестности неособой точки x_0 решения уравнения образуют n-мерное пространство V^n. Возьмем теперь произвольную кривую $\gamma(t)$ на комплексной плоскости, ведущую из точки x_0 в точку x_1 и не проходящую через особые точки a_i. Решения уравнения будут аналитически продолжаться вдоль кривой, оставаясь при этом решениями уравнения. Поэтому каждой кривой γ отвечает линейное отображение M_γ пространства решений $V^n_{x_0}$ в точке x_0 в пространство решений $V^n_{x_1}$ в точке x_1.

Если пошевелить кривую γ, не задевая при этом особых точек и оставляя закрепленными концы, то отображение M_γ меняться не будет. Замкнутым кривым будет отвечать линейное преобразование пространства V^n в себя. Совокупность всех таких линейных преобразований пространства V^n образует группу, которая и называется *группой монодромии уравнения* (13). Итак, группа монодромии уравнения – это группа линейных преобразований решений, которые возникают при обходе особых точек. Группа монодромии уравнения характеризует многозначность его решений.

Лемма 6.1. 1) *Группа монодромии почти каждого решения уравнения* (13) *изоморфна группе монодромии этого уравнения.*

2) *Монодромная пара каждого решения уравнения* (13) *почти нормальна.*

Доказательство. Второе утверждение леммы вытекает из леммы 5.14. Остановимся на доказательстве первого утверждения. Группа монодромии уравнения (13) – это матричная группа, содержащая не более чем счетное число элементов. Для каждого нетождественного элемента этой группы множество его неподвижных точек является собственным подпространством конечномерного пространства решений уравнения (13). Множество решений, остающихся неподвижными, хотя бы для одного нетождественного преобразования из группы монодромии имеет нулевую меру в пространстве решений (так как объединение не более чем счетного числа собственных подпространств конечномерного пространства имеет в этом пространстве нулевую меру). Группа монодромии всех остальных решений уравнения (13) изоморфна группе монодромии уравнения.

В окрестности неособой точки x_0 существуют n линейно независимых решений $y_1, \dots, y_n$ уравнения (13). В этой окрестности можно рассмотреть поле функций $\mathscr{R}\langle y_1, \dots, y_n\rangle$, полученное присоединением к полю рациональных функций $\mathscr{R}$ всех решений y_i и всех их производных.

Каждое преобразование M_γ пространства решений из группы монодромии можно продолжить до автоморфизма всего поля $\mathscr{R}\langle y_1, \dots, y_n\rangle$. Действительно, вместе с функциями $y_1, \dots, y_n$ вдоль кривой γ будет мероморфно продолжаться каждый элемент поля $\mathscr{R}\langle y_1, \dots, y_n\rangle$. Это продолжение и дает требуемый автоморфизм, так как при продолжении сохраняются арифметические операции и дифференцирование, а рациональные функции возвращаются к своему прежнему значению из-за однозначности.

Итак, *группа монодромии уравнения* (13) *лежит в группе Галуа этого уравнения над полем рациональных функций.*

Поле инвариантов группы монодромии – это подполе поля $\mathscr{R}\langle y_1, \dots, y_n\rangle$, состоящее из однозначных функций. В отличие от алгебраических уравнений, для дифференциальных уравнений поле инвариантов относительно действия группы монодромии может быть больше, чем поле рациональных функций.

Например, для дифференциального уравнения (13), у которого все коэффициенты $r_i(x)$ являются полиномами, все решения – целые функции. Но, конечно, решения таких уравнений далеко не всегда полиномиальны. Дело здесь в том, что решения дифференциальных уравнений могут расти при подходе к особым точкам экспоненциальным образом. Известен широкий класс линейных дифференциальных уравнений, для которых такого осложнения нет, т.е. для которых решения при подходе к каждой особой точке (вдоль любого сектора с вершиной в этой точке) растут не быстрее чем степенным образом. Дифференциальные уравнения, обладающие этим свойством, называются дифференциальными уравнениями типа Фукса (см. [11], [16]). Для дифференциальных уравнений типа Фукса справедлива следующая теорема Фробениуса.

Теорема 6.2 (Фробениуса). *Подполе дифференциального поля $\mathscr{R}\langle y_1, \dots, y_n\rangle$, состоящее из однозначных функций, для дифференциальных уравнений типа Фукса совпадает с полем рациональных функций.*

Прежде чем доказывать теорему Фробениуса, остановимся на ее непосредственных следствиях.

Следствие 6.3. *Алгебраическое замыкание группы монодромии M (т.е. наименьшая алгебраическая группа, содержащая M) уравнения типа Фукса совпадает с группой Галуа этого уравнения над полем рациональных функций.*

Доказательство. Следствие вытекает из теоремы Фробениуса и основной теоремы дифференциальной теории Галуа (см. п. 4.3).

Теорема 6.4. *Линейное дифференциальное уравнение типа Фукса решается в квадратурах, в k-квадратурах или в обобщенных квадратурах, если и только если его группа монодромии соответственно разрешима, k-разрешима или почти разрешима.*

Доказательство вытекает из теоремы Пикара–Вессио (см. п. 4.5) и предыдущего следствия.

Дифференциальная теория Галуа доказывает тем самым два результата.

1) *Если группа монодромии дифференциального уравнения типа Фукса разрешима (k-разрешима, почти разрешима), то это уравнение решается в квадратурах (в k-квадратурах, в обобщенных квадратурах).*

2) *Если группа монодромии дифференциального уравнения типа Фукса неразрешима (не k-разрешима, не почти разрешима), то это уравнение не решается в квадратурах (в k-квадратурах и в обобщенных квадратурах).*

Первый из этих результатов не требует основной теоремы теории Галуа и, по существу, относится к линейной алгебре. Дело в том, что группу автоморфизмов дифференциального поля $R\langle y_1, \dots, y_n\rangle$, оставляющих на месте только поле рациональных функций, не нужно специально конструировать. Такой группой является группа монодромии. Поэтому для доказательства разрешимости в квадратурах и в обобщенных квадратурах уравнений типа Фукса с разрешимой или с почти разрешимой группой монодромии достаточно воспользоваться линейно-алгебраическими рассуждениями из п. 4.7. Для доказательства разрешимости в k-квадратурах уравнение типа Фукса с k-разрешимой группой монодромии этих линейно-алгебраических рассуждений недостаточно. Нужно еще воспользоваться теорией Галуа алгебраических расширений поля рациональных функций (см. утверждение 4.21). Впрочем, теория Галуа алгебраических расширений поля R весьма наглядна и геометрична (см. п. 5.1.1).

Наша теорема позволяет усилить отрицательный результат 2). Об этом – в п. 6.2.4. А сейчас перейдем к доказательству теоремы Фробениуса.

6.1.2. Доказательство теоремы Фробениуса. Мы покажем, что каждая однозначная функция из дифференциального поля $\mathscr{R}\langle y_1, \dots, y_n\rangle$ мероморфна на сфере Римана и, следовательно, рациональна. Пусть $p \in S$ – особая точка уравнения типа Фукса и x – локальный параметр около этой точки такой, что $x(p) = 0$. Согласно теории Фукса, около точки p каждое решение y представляется в виде конечной суммы $y = \sum f_{\alpha k} x^\alpha \ln^k x$, где $f_{\alpha k}$ – мероморфные функции около точки p. Ясно, что функции, представимые в виде $\sum f_{\alpha k} x^\alpha \ln^k x$, где функции $f_{\alpha k}$ мероморфны около точки p, образуют дифференциальное кольцо, содержащее поле функций, мероморфных около точки p. Нам нужно показать, что частное двух функций из этого дифференциального кольца является однозначной функцией около точки p, если и только если эта функция мероморфна. Доказательство этого факта основано на формулируемом ниже утверждении 6.5. Нам понадобятся следующие обозначения: $U(0,\varepsilon)$ – ε-окрестность точки 0 на комплексной плоскости; $\widehat{U}(0,\varepsilon)$ – проколотая ε-окрестность точки 0, $\widehat{U}(0,\varepsilon) = U(0,\varepsilon) \setminus \{0\}$; $M(0,\varepsilon)$ и $\widehat{M}(0,\varepsilon)$ – поля мероморфных функций в областях $U(0,\varepsilon)$ и $\widehat{U}(0,\varepsilon)$.

Два мероморфных ростка f_a и g_b называются *эквивалентными над областью* U, $a, b \in U$, если росток g_b получается из ростка f_a при продолжении вдоль некоторой кривой, лежащей в области U.

Определим теперь кольцо $K_a(0,\varepsilon)$. Мероморфный росток f_a, заданный в точке $a \in \widehat{U}(0,\varepsilon)$, принадлежит *кольцу* $K_a(0,\varepsilon)$, если:

1) росток f_a мероморфно продолжается вдоль всех кривых, лежащих в $\widehat{U}(0,\varepsilon)$,
2) комплексное векторное пространство, натянутое на все мероморфные ростки в точке a, эквивалентные над окрестностью $\widehat{U}(0,\varepsilon)$ ростку f_a, конечномерно.

Кольцо $K_a(0,\varepsilon)$ содержит поле $\widehat{M}(0,\varepsilon)$ и является векторным пространством над ним.

Утверждение 6.5 (о базисе). *При любом выборе ветвей функций* $\ln x$ *и* x^α, $[\operatorname{Re}\alpha] = 0$, *ростки* $x_a^\alpha \ln_a^k x$, $k = 0, 1, 2, \ldots$, *образуют базис пространства* $K_a(0,\varepsilon)$ *над полем* $\widehat{M}(0,\varepsilon)$.

Сначала докажем лемму.

Лемма 6.6. *Ростки* $1, \ln_a x, \ldots, \ln_a^k x, \ldots$ *линейно независимы над полем* $\widehat{M}(0,\varepsilon)$.

Доказательство. Действительно, существование нетривиального соотношения $\sum a_k \ln_a^k x = 0$, $a_k \in \widehat{M}(0,\varepsilon)$, влечет за собой конечнозначность функции $\ln x$ в окрестности нуля.

Доказательство утверждения основывается на рассмотрении оператора монодромии $A\colon K_a(0,\varepsilon) \to K_a(0,\varepsilon)$, который сопоставляет каждому ростку его продолжение вдоль замкнутой кривой, обходящей точку 0.

Лемма 6.7. *Ростки* $x_a^\alpha \ln_a^k x$, $[\operatorname{Re}\alpha] = 0$, $k = 0, 1, \ldots, n-1$, *образуют базис в пространстве* $\ker(A - \lambda E)^n$, *где* λ *и* α *связаны соотношением* $\lambda = e^{2\pi i\alpha}$.

Доказательство. Заметим, что пространство $\ker(A - \lambda E)$ не более чем одномерно. Действительно, если $Af_a = \lambda f_a$ и $Ag_a = \lambda g_a$, то $A(f_a/g_a) = f_a/g_a$. Следовательно, росток $\psi_a = f_a/g_a$ является ростком некоторой функции ψ из поля $\widehat{M}(0,\varepsilon)$ и $f_a = \psi g_a$. Поэтому пространство $\ker(A - \lambda E)^n$ имеет размерность не выше n. С другой стороны, легко проверить, что в этом пространстве лежат ростки $x_a^\alpha \ln_a^k x$, $[\operatorname{Re}\alpha] = 0$, $k = 0, 1, \ldots, n-1$. Согласно лемме 6.6, эти ростки линейно независимы и поэтому образуют базис пространства $\ker(A - \lambda E)^n$.

Пространства $\ker(A - \lambda E)^n$ при разных λ имеют нулевое пересечение. Поэтому все ростки $x_a^\alpha \ln_a^k x$ линейно независимы. Покажем, что всякий росток f_a из пространства $K_a(0,\varepsilon)$ можно разложить по этим функциям. По определению росток f_a лежит в некотором конечномерном пространстве V, инвариантном относительно оператора монодромии. Пусть $\widetilde{A}$ – ограничение оператора A на пространстве V. Согласно линейной алгебре, пространство V раскладывается в прямую сумму подпространств $\ker(\widetilde{A} - \lambda E)^{n_\lambda}$, где λ – собственное значение оператора $\widetilde{A}$ и n_λ – его кратность. Из леммы 6.7 вытекает, что всякий элемент пространства V раскладывается по векторам $x_a^\alpha \ln_a^k x$.

Замечание. Выбор разных ветвей функций $\ln x$ и x^α приводит к разным базисам пространства $K_a(0,\varepsilon)$. Коэффициенты разложения векторов из таких базисов по другому базису являются комплексными числами.

Определение. 1) Мероморфный росток f_a, $a \in \widehat{U}(0,\varepsilon)$, имеет над окрестностью $\widehat{U}(0,\varepsilon)$ *целую фуксову особенность*, если $f_a \in K_a(0,\varepsilon)$ и коэффициенты разложения ростка f_a по базису $x_a^\alpha \ln_a^k x$ мероморфны, т.е. если

$$f_a = \sum f_{\alpha,k} \ln_a^k x \cdot x_a^\alpha, \quad \text{где} \quad f_{\alpha,k} \in M(0,\varepsilon).$$

2) Мероморфный росток f_a, $a \in \widehat{U}(0,\varepsilon)$, имеет над окрестностью $\widehat{U}(0,\varepsilon)$ *фуксову особенность*, если он представим в виде частного двух ростков ψ_a, g_a, имеющих над $\widehat{U}(0,\varepsilon)$ целую фуксову особенность, $f_a = \psi_a/g_a$.

Следствие 6.8. *Росток $f_a \in K_a(0,\varepsilon)$ имеет фуксову особенность над окрестностью $\widehat{U}(0,\varepsilon)$, если и только если он имеет целую фуксову особенность над этой окрестностью.*

Доказательство. Росток $f_a \in K_a(0,\varepsilon)$, следовательно, $f_a = \sum r_{\alpha,k} x_a^\alpha \ln_a^k x$, где $r_{\alpha,k} \in \widehat{M}(0,\varepsilon)$ – коэффициенты разложения ростка f_a по базису. Росток f_a имеет также фуксову особенность, поэтому справедливо равенство

$$\frac{\sum p_{\alpha,k} x_a^\alpha \ln_a^k x}{\sum q_{\alpha,k} x_a^\alpha \ln_a^k x} - \sum r_{\alpha,k} x_a^\alpha \ln_a^k x = 0,$$

где $p_{\alpha,k}$, $q_{\alpha,k}$ – некоторые элементы поля $M(0,\varepsilon)$. Умножим последнее равенство на $\sum q_{\alpha,k} x_a^\alpha \ln_a^k x$, раскроем скобки и приведем, если надо, ростки $x_a^\beta \ln_a^k x$ к виду $x^n \cdot x_a^\alpha \ln_a^k x$, где n – целое и $[\operatorname{Re}\alpha] = 0$. Так как ростки $x_a^\alpha \ln_a^k x$ линейно независимы над полем $\widehat{M}(0,\varepsilon)$, то равенство эквивалентно системе уравнений, полученной приравниванием к нулю коэффициентов при этих функциях. Полученная система представляет собой систему линейных уравнений относительно функций $r_{\alpha,k}$ с коэффициентами из поля $M(0,\varepsilon)$. Система имеет единственное решение, так как функции $r_{\alpha,k}$ определены однозначно. Следовательно, функции $r_{\alpha,k}$ лежат в поле $M(0,\varepsilon)$.

Следствие 6.9. *Если росток f_a мероморфной в окрестности $\widehat{U}(0,\varepsilon)$ функции f имеет над этой окрестностью фуксову особенность, то функция f мероморфна в окрестности $\widehat{U}(0,\varepsilon)$.*

Доказательство. Росток $f_a \in K_a(0,\varepsilon)$ и его разложение по базису имеет вид $f_a = f \cdot 1$. Согласно следствию 6.8, росток f_a имеет целую фуксову особенность и поэтому $f \in M(0,\varepsilon)$.

Следствие 6.9 завершает доказательство теоремы Фробениуса.

6.1.3. Группа монодромии систем линейных дифференциальных уравнений, ее связь с группой Галуа. Результаты из п. 6.1.1 автоматически переносятся на системы линейных дифференциальных уравнений с регулярными особыми точками.

Рассмотрим линейное дифференциальное уравнение

$$\mathbf{y}' = \mathbf{A}(x)\mathbf{y}, \tag{14}$$

где $\mathbf{y} = (y_1(x), \dots, y_n(x))$, $\mathbf{A}(x) = (a_{i,j}(x),\ 1 \leqslant i, j \leqslant n)$ – матрица рациональных функций и x – комплексная переменная. Пусть $a_1, \dots, a_k$ – полюсы матрицы $\mathbf{A}(x)$. В окрестности неособой точки x_0, $x_0 \neq \infty$, $x_0 \neq a_i$, $i = 1, \dots, k$, решения уравнения (14) образуют n-мерное пространство V^n. Возьмем теперь произвольную кривую $\gamma(t)$ на комплексной плоскости, ведущую из точки x_0 в точку x_1 и не проходящую через особые точки a_i, $\gamma(0) = x_0$, $\gamma(1) = x_1$, $\gamma(t) \neq a_i$. Решения уравнения будут аналитически продолжаться вдоль кривой, оставаясь при этом решениями уравнения. Поэтому каждой кривой γ отвечает линейное отображение M_γ пространства решений $V^n_{x_0}$ в точке x_0 в пространство решений V_{x_1} в точке x_1.

Если пошевелить кривую γ, не задевая при этом особых точек и оставляя закрепленными концы, то отображение M_γ меняться не будет. Замкнутым кривым будет отвечать линейное преобразование пространства V^n в себя. Совокупность всех таких линейных преобразований пространства V^n образует группу, которая и называется *группой монодромии уравнения* (14). Итак, группа монодромии уравнения – это группа линейных преобразований решений, которые возникают при обходе особых точек. Группа монодромии уравнения характеризует многозначность его решений.

Лемма 6.10. 1) *Группа монодромии почти каждого решения системы* (14) *совпадает с группой монодромии системы* (14). 2) *Монодромная пара каждой компоненты каждого решения системы* (14) *почти нормальна.* 3) *Если группа монодромии системы* (14) *не лежит в некотором полном классе пар групп* $\mathscr{M}$, *то монодромная пара одной из компонент почти каждого решения этой системы не лежит в* $\mathscr{M}$.

Доказательство. Первые два утверждения леммы доказываются так же, как лемма 6.1. Утверждение 3) вытекает из 1) и леммы 5.21.

В окрестности неособой точки x_0 существуют все решения $\mathbf{y}_1, \dots, \mathbf{y}_n$ уравнения (14). В этой окрестности можно рассмотреть дифференциальное поле функций $R\langle \mathbf{y}_1, \dots, \mathbf{y}_n\rangle$, полученное присоединением к полю рациональных функций R всех компонент $y_{i1}, \dots, y_{in}$ всех решений $\mathbf{y}_i$ и всех их производных $y_{ij}^{(p)}$.

Каждое преобразование M_γ пространства решений из группы монодромии можно продолжить до автоморфизма всего дифференциального поля $\mathscr{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n\rangle$ над полем R. Действительно, вместе с вектор-функциями $\mathbf{y}_1, \dots, \mathbf{y}_n$ вдоль кривой γ будет мероморфно продолжаться каждый элемент поля $\mathscr{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n\rangle$. Это продолжение и дает требуемый автоморфизм, так как при продолжении сохраняются арифметические операции и дифференцирование, а рациональные функции возвращаются к своему прежнему значению из-за однозначности.

Особая точка уравнения (14) называется *регулярной*, если в любом секторе с вершиной в особой точке все решения при подходе к этой точке растут не быстрее чем степенным образом (см. [16], [11]). Известно, что около регулярной особой точки каждая компонента каждого решения имеет целую фуксову особенность (см. определение из п. 6.1.2). *Уравнение* (14) называется *регулярным*, если все его особые точки (включая ∞) регулярны. Для регулярного уравнения (14) все однозначные функции из поля $\mathscr{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ являются рациональными функциями.

Теорема 6.11. *Для регулярной системы линейных дифференциальных уравнений* (14) *дифференциальное поле $\mathscr{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ является расширением Пикара–Вессио поля R. Группа Галуа этого расширения является алгебраическим замыканием группы монодромии системы уравнений* (14).

Доказательство. На дифференциальном поле $\mathscr{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ группа монодромии действует как группа изоморфизмов с полем инвариантов R. Поле $\mathscr{R}\langle \mathbf{y}_1, \dots, \mathbf{y}_n \rangle$ порождено над R конечномерным $\mathbb{C}$-линейным пространством, инвариантным относительно действия монодромии, а именно линейным пространством, натянутым на все компоненты всех решений уравнения (14). Теперь теорема вытекает из следствия 4.5.

Теорема 6.12. *Каждая компонента каждого решения регулярной системы линейных дифференциальных уравнений выражается в квадратурах, в k-квадратурах и в обобщенных квадратурах, если и только если группа монодромии системы соответственно разрешима, k-разрешима или почти разрешима.*

Доказательство вытекает из теоремы 4.12 (Пикара–Вессио) и из предыдущей теоремы. Как и в случае уравнения типа Фукса, "положительная" часть теоремы, относящаяся к разрешимости системы, доказывается, в основном, при помощи линейной алгебры (см. п. 4.7). А отрицательную часть теоремы значительно усиливает топологический вариант теории Галуа (см. п. 6.2.4).

6.2. Теория Галуа систем линейных дифференциальных уравнений типа Фукса с малыми коэффициентами. Оказывается, для систем уравнений типа Фукса с достаточно малыми коэффициентами условия разрешимости становятся абсолютно явными [15].

6.2.1. Системы уравнений типа Фукса. Среди систем регулярных линейных дифференциальных уравнений выделяются системы линейных дифференциальных уравнений типа Фукса. Это уравнение вида $\mathbf{y}' = \mathbf{A}(x)\mathbf{y}$, где матрица $\mathbf{A}(x)$ не имеет кратных полюсов и обращается в нуль на бесконечности. Другими словами, это уравнения вида

$$\mathbf{y}' = \sum_{p=1}^{k} \frac{A_p}{x - a_p}\mathbf{y},$$

где A_p – комплексная $(n \times n)$-матрица, а $\mathbf{y} = (y_1, \dots, y_n)$ – вектор в $\mathbb{C}^n$. Точки a_p называются полюсами, а матрицы A_p – матрицами-вычетами системы уравнений типа Фукса.

Для систем уравнений типа Фукса, как и для других регулярных систем дифференциальных уравнений, *алгебраическое замыкание группы монодромии совпадает с группой Галуа порожденного системой уравнений расширения Пикара–Вессио поля рациональных функций* (см. п. 6.1.3).

Лаппо-Данилевский развил теорию аналитических функций от матриц и применил ее к дифференциальным уравнениям [29]. Нам понадобятся результаты Лаппо-Данилевского относительно систем уравнений типа Фукса, которые мы будем использовать в виде следствия, приведенного в конце этого пункта.

Возьмем неособую точку $x_0 \neq a_p$. Зафиксируем k кривых $\gamma_1, \dots, \gamma_k$ так, чтобы кривая γ_p начиналась в точке x_0, подходила к полюсу a_p, обходила его и возвращалась назад в точку x_0. Кривым $\gamma_1, \dots, \gamma_k$ отвечают матрицы монодромии $M_1, \dots, M_k$. Очевидно, что матрицы $M_1, \dots, M_k$ порождают группу монодромии. При фиксации кривых матрицы монодромии зависят лишь от матриц-вычетов. Эта зависимость изучалась Лаппо-Данилевским.

Во-первых, он показал, что матрицы монодромии M_p – целые функции матриц-вычетов A_j. Точнее, *существуют специальные ряды с комплексными коэффициентами*

$$M_p = E + 2\pi i A_p + \sum_{1 \leqslant i,j \leqslant k} c_{i,j} A_i A_j + \cdots \tag{15}$$

от матриц $A_1, \dots, A_k$, выражающие матрицы монодромии M_p и сходящиеся при любых матрицах $A_1, \dots, A_k$.

Хотя матрица монодромии M_p зависит от всех матриц-вычетов A_j, ее собственные числа определяются только по собственным числам матрицы-вычета A_p.

Теорема 6.13 [16], [11]. *Пусть $\{\mu_m\}$ – набор собственных чисел матрицы A_p. Тогда $\{e^{2\pi i \mu_m}\}$ – набор собственных чисел матрицы M_p.*

Знаменитая проблема Римана–Гильберта – это вопрос о разрешимости обратной задачи, т.е. вопрос о существовании уравнений типа Фукса с заданным набором матриц монодромии. Для почти всякого набора матриц монодромии задача Римана–Гильберта разрешима. Традиционно считалось, что этот классический результат переносится на любые наборы матриц монодромии. Однако, как обнаружил А. А. Болибрух [10], [11], это не так. Он предъявил пример набора матриц монодромии, для которых проблема Римана–Гильберта неразрешима.

Лаппо-Данилевский показал, что в предположении малости матриц-вычетов A_j матрицы-вычеты A_j – однозначные аналитические функции матриц монодромии M_p. А именно, он показал, что если ограничиться уравнениями типа Фукса с достаточно малыми матрицами-вычетами $\|A_j\| < \varepsilon$, $\varepsilon = \varepsilon(n, a_1, \dots, a_k)$, то для достаточно близких к E матриц монодромии M_p, $\|M_p - E\| < \varepsilon$, задача Римана–Гильберта имеет единственное решение. Более того, *существуют специальные ряды с комплексными коэффициентами*

$$A_p = -\frac{1}{2\pi i} E + \frac{1}{2\pi i} M_p + \sum_{1 \leqslant i,j \leqslant k} b_{ij} M_i M_j + \cdots \tag{16}$$

от матриц $M_1, \dots, M_k$, выражающие матрицы-вычеты A_p и сходящиеся при $\|M_p - E\| < \varepsilon$.

Ряды (16) получаются обращением рядов (15). Этот результат является своеобразной теоремой о неявной функции (для аналитических отображений с некоммутативными переменными).

Теорию Лаппо-Данилевского мы будем использовать в форме следующего утверждения.

Следствие 6.14. *Матрицы монодромии лежат в алгебре с единицей, натянутой на матрицы-вычеты. Обратно, если матрицы-вычеты достаточно малы и матрицы монодромии достаточно близки к E, то матрицы-вычеты лежат в алгебре с единицей, натянутой на матрицы монодромии.*

6.2.2. Группы, порожденные матрицами, близкими к единичной. В этом пункте доказывается аналог теоремы Ли для матричных групп, порожденных матрицами, близкими к единичным. Напомним формулировку теоремы Жордана.

Теорема 6.15 (Жордан). *Конечная группа G линейных преобразований n-мерного пространства обладает диагональным нормальным делителем G_d ограниченного индекса,* $\operatorname{ind}(G, G_d) \leqslant J(n)$.

Известны различные явные оценки сверху чисел $J(n)$. (Например, Шур показал, что $J(n) \leqslant (\sqrt{8n}+1)^{2n^2} - \sqrt{8n}-1)^{2n^2}$, см. [37].)

Утверждение 6.16. *Существует целое число $T(n)$ такое, что подгруппа G в $GL(n)$ обладает разрешимым нормальным делителем конечного индекса, если и только если она обладает треугольным нормальным делителем индекса $\leqslant T(n)$.*

Доказательство. Теорема Ли гарантирует существование у группы G треугольного нормального делителя G_l конечного индекса. Действительно, достаточно положить $G_l = G \cap \overline{G}_0$, где $\overline{G}_0$ – компонента связности единицы алгебраического замыкания $\overline{G}$ группы G. Однако индекс G_l может быть как угодно велик. Так, например, для группы $\mathbb{Z}_k$ корней k-й степени из единицы этот индекс равен k при $n = 1$. Мы будем увеличивать нормальный делитель G_l, оставляя его треугольным. Отметим, что нам достаточно доказать существование треугольной подгруппы ограниченного индекса, так как подгруппа индекса k содержит нормальный делитель индекса $\leqslant k!$. Доказательство будем вести индукцией по размерности n. Если группа G обладает инвариантным пространством V^k размерности k, $0 < k < n$, мы сможем сделать индукционный шаг. Действительно, группа G в этом случае действует и на пространстве V^k размерности k, и на фактор-пространстве V^n/V^k размерности $(n-k)$. По индукции можно считать, что группа G обладает нормальным делителем индекса $\leqslant T(k)T(n-k)$, который треуголен как в V^k, так и в V^n/V^k, т.е. треуголен в V^n.

Нормальный делитель G_l приводится к треугольному виду и поэтому обладает ненулевым максимальным собственным подпространством V^k. Возникают два случая: $V^k \subset V^n$ и $V^k = V^n$. Рассмотрим первый случай: $V^k \subset V^n$. Обозначим через $\widetilde{G}_l$ подгруппу G, состоящую из всех преобразований, для которых V^k инвариантно (в этом месте и происходит увеличение нормального делителя G_l). Докажем, что $\operatorname{ind}(G, \widetilde{G}_l) \leqslant n$. Действительно, группа перестановок G переставляет максимальные собственные пространства всякого своего нормального делителя и, в частности, G_l. Однако максимальных собственных пространств не может быть больше n. Отсюда и вытекает нужное соотношение $\operatorname{ind}(G, \widetilde{G}_l) \leqslant n$. Для окончания доказательства достаточно применить к группе $\widetilde{G}_l$ индукционный шаг. Рассмотрим второй случай: $V^k = V^n$, т.е. G_l состоит из матриц λE. Можно считать, что группа G состоит из матриц с единичным детерминантом. Действительно, в противном случае можно рассмотреть группу, составленную из матриц $(\det A)^{-1}A$. Нормальный делитель D_l при этом предположении конечен (поскольку $\lambda^n = 1$). Группа G тоже конечна, так как

$\mathrm{ind}(G, G_l) < \infty$. Для окончания доказательства достаточно воспользоваться теоремой Жордана.

Утверждение 6.16$'$. *Существует целое число $D(n)$ такое, что подгруппа G в $GL(n)$ обладает диагональным нормальным делителем конечного индекса, если и только если она обладает диагональным нормальным делителем индекса $\leqslant D(n)$.*

Утверждение 6.16$'$ доказывается точно так же, как утверждение 6.16, и мы не будем останавливаться на его доказательстве. Числа $T(n)$ и $D(n)$ также допускают явную оценку сверху (ср. [37]).

Лемма 6.17. *Уравнение $X^N = A$, $\|A - E\| < \varepsilon$, $\|X - E\| < \varepsilon$, в котором X и A – комплексные $(n \times n)$-матрицы, близкие к E, имеет единственное решение, если $\varepsilon = \varepsilon(n, N)$ достаточно мало. При этом каждое инвариантное пространство V матрицы A будет инвариантно и для матрицы X.*

Доказательство. Положим $B = A - E$ и

$$X = E + \frac{1}{N}B + \frac{1}{2}\frac{1}{N}\left(\frac{1}{N} - 1\right)B^2 + \cdots .$$

При $\|B\| < 1$ ряд сходится и $X^N = A$. Выберем теперь $\varepsilon = \varepsilon(n, N)$ столь малым, чтобы теорема о неявной функции гарантировала бы единственность решения. Пространство V будет инвариантно относительно $B = A - E$ и, следовательно, относительно X.

Лемма 6.18. *Пусть N-е степени всех матриц из группы G лежат в некоторой алгебраической группе L, тогда группа $G \cap L$ имеет в группе G конечный индекс.*

Доказательство. Рассмотрим алгебраическое замыкание $\overline{G}$ группы G. Легко видеть, что если $X \in \overline{G}$, то $X^N \in L$. Обозначим через $\overline{G}_0$ и L_0 компоненты связности единицы групп $\overline{G}$ и L. Если A лежит в группе L_0, $A = e^M$, то уравнение $X^N = A$ имеет решение в этой же группе. Действительно, достаточно положить $X = e^{\frac{M}{N}}$. Но уравнение $X^N = A$ имеет единственное решение при матрицах A и X, близких к E. Отсюда следует, что $\overline{G}_0 \subseteq L_0 \subseteq L$. Лемма теперь вытекает из того, что $\mathrm{ind}(\overline{G}, \overline{G}_0) < \infty$.

Замечание. При $L = e$ лемма 6.18 превращается в теорему Бернсайда: *матричная группа с тождеством $X^N = e$ конечна.*

Утверждение 6.19. *Существует целое число $N(n)$ такое, что подгруппа G в $GL(n)$ обладает разрешимым нормальным делителем конечного индекса, если и только если все матрицы $A^{N(n)}$, $A \in G$, одновременно приводятся к треугольному виду.*

Доказательство. В одну сторону утверждение 6.19 вытекает из утверждения 6.16, если положить $N(n) = T(n)!$. Для доказательства в другую сторону нужно применить лемму 6.18 для группы G и группы треугольных матриц L.

Аналогично доказывается следующее утверждение.

Утверждение 6.19$'$. *Существует целое число $N(n)$ такое, что подгруппа G в $GL(n)$ обладает диагональным нормальным делителем конечного индекса, если и только если все матрицы $A^{N(n)}$, $A \in G$, одновременно приводятся к диагональному виду.*

Теорема 6.20. *Существует положительное число $\varepsilon(n) > 0$, такое, что подгруппа G в $GL(n)$, порожденная матрицами A_α, близкими к единичной, $\|E - A_\alpha\| < \varepsilon(n)$, обладает разрешимым нормальным делителем конечного индекса, если и только если все матрицы A_α одновременно приводятся к треугольному виду.*

Доказательство. Выберем $\varepsilon(n) > 0$ столь малым, что для уравнения

$$X^{N(n)} = A,$$

$\|E - X\| < \varepsilon(n)$, выполнены условия леммы 6.17. По утверждению 6.19 все матрицы $A_\alpha^{N(n)}$ должны приводиться к треугольному виду. Но по лемме 6.17 инвариантные пространства матриц $A_\alpha^{N(n)}$ и A_α совпадают. Поэтому матрицы A_α тоже приводятся к треугольному виду.

Аналогично доказывается следующее утверждение.

Утверждение 6.21. *Существует положительное число $\varepsilon(n) > 0$ такое, что подгруппа G в $GL(n)$, порожденная матрицами A_α, близкими к единичной, $\|E - A_\alpha\| < \varepsilon(n)$, обладает диагональным нормальным делителем конечного индекса, если и только если все матрицы A_α одновременно приводятся к диагональному виду.*

Замечание. В теореме 6.20 и в утверждении 6.21 можно ослабить требование близости матриц A_α к единичной. Достаточно ограничиться близостью в топологии Зарисского. Скажем, что матрица A k-резонансна, если у нее найдутся разные собственные числа λ_1 и λ_2, связанные соотношением $\lambda_1 = \varepsilon_k \lambda_2$, $\varepsilon_k^k = 1$, $\varepsilon_k \neq 1$. Все k-резонансные матрицы образуют алгебраическое множество, не содержащее единицы. Достаточно требовать, чтобы матрицы A_α не были $N(n)$-резонансными.

6.2.3. Явные критерии разрешимости. Перейдем к явному критерию разрешимости. Начнем с двух простых лемм.

Лемма 6.22. *Система типа Фукса n-го порядка*

$$\dot{\mathbf{y}} = \sum_{i=1}^{k} \frac{A_i}{x - a_i} \mathbf{y}$$

с достаточно малыми коэффициентами $\|A_i\| < \varepsilon = \varepsilon(n, a_1, \ldots, a_k)$ решается в обобщенных квадратурах, если и только если ее матрицы монодромии M_i треугольны.

Доказательство. Группа монодромии системы порождена матрицами монодромии M_i. Если матрицы-вычеты A_i малы, $\|A_i\| < \varepsilon$, то матрицы M_i будут близки к E. Выберем $\varepsilon = \varepsilon(n, a_1, \ldots, a_k)$ столь малым, чтобы для матриц монодромии $M_1, \ldots, M_k$ выполнялись условия теоремы 6.20. В силу этой теоремы у группы монодромии существует разрешимый нормальный делитель конечного индекса, если и только если матрицы $M_1, \ldots, M_k$ треугольны. Теперь осталось воспользоваться теоремой 6.12.

ЛЕММА 6.23. *Для системы типа Фукса треугольность и диагональность группы Галуа эквивалентны тому же условию на матрицы монодромии* $M_1, \ldots, M_k$.

ДОКАЗАТЕЛЬСТВО. Группа монодромии порождена матрицами монодромии $M_1, \ldots, M_k$ и треугольна или диагональна вместе с ними. Теперь лемма вытекает из того, что для уравнения типа Фукса группа Галуа совпадает с алгебраическим замыканием группы монодромии (см. п. 6.1.3).

КРИТЕРИЙ РАЗРЕШИМОСТИ. *По набору полюсов* $a_1, \ldots, a_k$ *и порядку* n *можно указать число* $\varepsilon(n, a_1, \ldots, a_k)$ *такое, что условия разрешимости для систем* n*-го порядка типа Фукса*

$$\dot{\mathbf{y}} = \sum_{i=1}^{k} \frac{A_i}{x - a_i}\mathbf{y}$$

с малыми коэффициентами, $\|A_i\| < \varepsilon(n, a_1, \ldots, a_k)$, *принимают явный вид.*

Именно, система решается:

1) *в квадратурах или в обобщенных квадратурах*[3], *если и только если матрицы* A_i *(в некотором базисе) треугольны;*
2) *в интегралах и алгебраических функциях или в интегралах и радикалах*[3], *если и только если матрицы* A_i *треугольны и их собственные числа рациональны;*
3) *в интегралах, если и только если матицы* A_i *треугольны и их собственные числа равны нулю;*
4) *в экспонентах интегралов и в алгебраических функциях или в экспонентах интегралов*[3], *если и только если матрицы* A_i *диагональны;*
5) *в алгебраических функциях или в радикалах*[3], *если и только если матрицы* A_i *диагональны и их собственные числа рациональны;*
6) *в рациональных функциях, если и только если все матрицы* A_i *равны нулю.*

ДОКАЗАТЕЛЬСТВО. Выберем $\varepsilon(n, a_1, \ldots, a_k)$ столь малым, чтобы выполнялись условия леммы 6.23 и чтобы матрицы-вычеты выражались через матрицы монодромии (см. п. 6.2.1).

Каждый из видов разрешимости влечет за собой разрешимость в обобщенных квадратурах. Разрешимость в обобщенных квадратурах при наших предположениях влечет треугольность матриц монодромии (лемма 6.22) и, следовательно, треугольность группы Галуа (лемма 6.23). Поэтому мы находимся в рамках применимости критерия, приведенного в конце п. 4.8. Нам нужно превратить условия на группу Галуа из этого критерия в условия на матрицы-вычеты A_i.

Условия на группу Галуа из критерия п. 4.8 эквивалентны тем же условиям на матрицы монодромии $M_1, \ldots, M_k$. Частично мы это проверили в лемме 6.23. Остальная проверка столь же несложна.

В предположениях нашей теоремы условие принадлежности матриц монодромии $M_1, \ldots, M_k$ некоторой алгебре с единицей, например алгебре треугольных или диагональных матриц, эквивалентно тому же условию на матрицы-вычеты $A_1, \ldots, A_k$ (следствие 6.14).

[3]Эти виды разрешимости различаются, если не ограничивать величины коэффициентов.

Собственные числа матрицы M_i будут корнями из единицы или единицами, если и только если собственные числа матрицы A_i – рациональные или целые числа (см. п. 6.2.1).

Теперь наш критерий вытекает из критерия п. 4.8.

Замечание. На конференции, посвященной 100-летию А.Н. Колмогорова, А.А. Болибрух сказал мне, что в условиях критерия разрешимости требование малости матриц A_i можно ослабить. *Достаточно лишь требовать, чтобы собственные числа этих матриц были малы.* Это был наш последний разговор с Андреем.

6.2.4. Сильная неразрешимость уравнений. Топологический вариант теории Галуа позволяет усилить классические результаты о неразрешимости уравнений в явном виде.

Группа монодромии алгебраической функции совпадает с группой Галуа соответствующего расширения Галуа поля рациональных функций (см. п. 5.1.2). Поэтому, согласно теории Галуа, 1) *алгебраическая функция представима в радикалах, если и только если ее группа монодромии разрешима*; 2) *алгебраическая функция выражается через рациональные функции при помощи радикалов и решения алгебраических уравнений степени k, если и только если ее группа монодромии k-разрешима.*

Из наших результатов (см. п. 5.5.2) вытекает следующее утверждение.

Следствие 6.24. 1) *Если группа монодромии алгебраического уравнения над полем рациональных функций неразрешима, то его решение не принадлежит классу функций, представимых при помощи однозначных $\mathcal{S}$-функций и квадратур.*

2) *Если группа монодромии алгебраического уравнения не k-разрешима, то его решение не принадлежит классу функций, представимых при помощи однозначных $\mathcal{S}$-функций и k-квадратур.*

Аналогичным образом усиливаются результаты о неразрешимости в явном виде из пп. 6.1.1, 6.1.3 и 6.2.3.

Следствие 6.25. *Если группа монодромии линейного дифференциального уравнения над полем рациональных функций неразрешима (не k-разрешима, не почти разрешима), то общее решение уравнения не принадлежит классу функций, представимых при помощи однозначных $\mathcal{S}$-функций и квадратур (k-квадратур, обобщенных квадратур).*

Следствие 6.26. *Если группа монодромии системы линейных дифференциальных уравнений над полем рациональных функций неразрешима (не k-разрешима, не почти разрешима), то по крайней мере одна из компонент почти каждого решения не лежит в классе функций, представимых с помощью однозначных $\mathcal{S}$-функций и квадратур (k-квадратур, обобщенных квадратур).*

Следствие 6.27. *Если система дифференциальных уравнений типа Фукса с маленькими коэффициентами не является треугольной, то по крайней мере одна из компонент почти каждого решения не лежит в классе функций, представимых с помощью однозначных $\mathcal{S}$-функций и квадратур (k-квадратур, обобщенных квадратур).*

СПИСОК ЛИТЕРАТУРЫ

[1] В. Б. Алексеев. Теорема Абеля в задачах и решениях. М.: Изд-во МЦНМО, 2001.

[2] В. И. Арнольд. Алгебраическая неразрешимость проблемы устойчивости по Ляпунову и проблемы топологической классификации особых точек аналитической системы дифференциальных уравнений // Функц. анализ и его прил. 1970. Т. 4. №3. С. 1–9.

[3] В. И. Арнольд. Суперпозиции // А. Н. Колмогоров. Избранные труды. Математика и механика. М.: Наука, 1985. С. 444–451.

[4] В. И. Арнольд. Топологическое доказательство трансцендентности абелевых интегралов в "Математических началах натуральной философии" Ньютона // Историко-математические исследования. 1989. №31. С. 7–17.

[5] V. I. Arnol'd. Problèmes résolubles et problèmes irrésolubles analytiques et géométriques // Passion des Formes. Dynamique Qualitative Sémiophysique et Intelligibilité. Dédié à R. Thom. Fontenay–St Cloud: ENS Éditions, 1994. P. 411–417.

[6] V. I. Arnol'd. Sur quelques problèmes de la théorie des systèmes dynamiques // Topol. Methods Nonlinear Anal. 1994. V. 4. №2. P. 209–225. Рус. пер.: В. И. Арнольд. О некоторых задачах теории динамических систем // Владимир Игоревич Арнольд. Избранное-60. М.: Фазис, 1997. С. 533–551.

[7] В. И. Арнольд. И. Г. Петровский, топологические проблемы Гильберта и современная математика // УМН. 2002. Т. 57. №4. С. 197–207.

[8] В. И. Арнольд, О. А. Олейник. Топология действительных алгебраических многообразий // Вестник МГУ. Сер. 1. Матем., мех. 1979. Т. 6. С. 7–17.

[9] V. I. Arnol'd, V. A. Vassill'ev. Newton's *Principia* read 300 years later // Notices Amer. Math. Soc. 1989. V. 36. №9. P. 1148–1154. Addendum: ibid. 1990. V. 37. № 2. P. 144.

[10] А. А. Болибрух. Обратные задачи монодромии аналитической теории дифференциальных уравнений // Математические события XX века. М.: Фазис, 2003. С. 53–79.

[11] А. А. Болибрух. Фуксовы дифференциальные уравнения и голоморфные расслоения. М.: Изд-во МЦНМО, 2000.

[12] Д. Б. Фукс, А. Т. Фоменко, В. Л. Гутенмахер. Гомотопическая топология. М.: Изд-во Моск. ун-та, 1969.

[13] В. В. Голубев. Лекции по аналитической теории дифференциальных уравнений. М.–Л.: Гостехиздат, 1950.

[14] А. Гурвиц, Р. Курант. Теория функций. М.: Наука, 1968.

[15] Ю. С. Ильяшенко, А. Г. Хованский. Теория Галуа систем дифференциальных уравнений типа Фукса с малыми коэффициентами // Препринт ИПМ АН СССР № 117. М., 1974.

[16] Э. Л. Айнс. Обыкновенные дифференциальные уравнения. Харьков: Гос. научно-техн. изд-во, 1939.

[17] И. Капланский. Введение в дифференциальную алгебру. М.: Мир, 1959.

[18] А. Г. Хованский. О представимости алгеброидных функций суперпозициями аналитических функций и алгеброидных функций одной переменной // Функц. анализ и его прил. 1970. Т. 4. №2. С. 74–79.

[19] А. Г. Хованский. О суперпозициях голоморфных функций с радикалами // УМН. 1971. Т. 26. №2. С. 213–214.

[20] А. Г. Хованский. О представимости функций в квадратурах // УМН. 1971. Т. 26. №4. С. 251–252.

[21] А. Г. Хованский. О представимости функций в квадратурах // Дисс. ... канд. физ.-матем. наук. М.: МИАН, 1973.

[22] A. Khovanskij. Topological obstructions for representability of functions by quadratures // J. Dynam. Control Systems. 1995. V. 1. №1. P. 91–123.

[23] А. Г. Хованский. О продолжаемости многозначных аналитических функций на аналитическое подмножество // Функц. анализ и его прил. 2001. Т. 35. №1. С. 62–73.

[24] А. Г. Хованский. О монодромии многозначной функции на ее множестве ветвления // Функц. анализ и его прил. 2003. Т. 37. №2. С. 65–74.

[25] А. Г. Хованский. Многомерные результаты о непредставимости функций в квадратурах // Функц. анализ и его прил. 2003. Т. 37. №4. С. 74–85.

[26] E.R. Kolchin. Algebraic matric groups and the Picard–Vessiot theory of homogeneous linear ordinary differential equations // Ann. of Math. (2). 1948. V. 49. P. 1–42.
[27] E.R. Kolchin. Galois theory of differential fields // Amer. J. Math. 1953. V. 75. P. 753–824.
[28] А.Г. Курош. Лекции по общей алгебре. М.: Физматгиз, 1962.
[29] И.А. Лаппо-Данилевский. Применение функций от матриц к теории линейных систем обыкновенных дифференциальных уравнений. М.: ГИТТЛ, 1957.
[30] J. Liouville. Sur la détermination des intégrales dont la valeur est algébrique // J. Ecole Polytech. Paris. 1833. V. 14. P. 124–193.
[31] J. Liouville. Mémoire sur l'intégration d'une classe de fonctions transcendentes // J. Reine Angew. Math. 1835. V. 13. №2. P. 93–118.
[32] J. Liouville. Mémoire sur l'intégration d'une classe d'équations différentielles du second ordre en quantités finies explicites // J. Math. Pures Appl. Sér. I. 1839. V. 4. P. 423–456.
[33] J.F. Ritt. Integration in Finite Terms. Liouville's Theory of Elementary Methods. New York: Columbia Univ. Press, 1948.
[34] M. Rosenlicht. Liouville's theorem on functions with elementary integrals // Pacific J. Math. 1968. V. 24. P. 153–161.
[35] M. Rosenlicht. On Liouville's theory of elementary functions // Pacific J. Math. 1976. V. 65. №2. P. 485–492.
[36] M.F. Singer. Formal solutions of differential equations // J. Symbolic Comput. 1990. V. 10. №1. P. 59–94.
[37] M.F. Singer. Liouvillian solutions of nth order homogeneous linear differential equations // Amer. J. Math. 1981. V. 103. №4. P. 661–682.

University of Toronto, Canada,
Московский независимый университет, Россия,
Институт системного анализа РАН, Россия
E-mail: `askold@math.toronto.edu`

Поступила в редакцию
30.03.2004