ТРУДЫ МАТЕМАТИЧЕСКОГО ИНСТИТУТА ИМ. В.А. СТЕКЛОВА, 2007, т. 259, с. 86–105

УДК 512.62+512.12

Вариации на тему разрешимости в радикалах[1]

©2007 г. А. Г. Хованский[2]

Поступило в декабре 2006 г.

Владимиру Игоревичу Арнольду,
математическому кумиру моего поколения

Обсуждается задача о представимости и непредставимости алгебраических функций в радикалах. Показано, что римановы поверхности функций, обратных к полиномам Чебышева, определяются своим локальным поведением около точек ветвления. Оценены снизу степени уравнений, к которым сводятся при помощи радикалов достаточно общие алгебраические функции. Начата классификация рациональных функций простой степени, обращения которых представимы в радикалах.

Сорок один год назад, весной 1966 г., Владимир Игоревич согласился стать моим научным руководителем. Мне было девятнадцать лет, Арнольду — двадцать девять. Он начал читать свою "классическую механику" осенью 1966 г. Студенты нашего курса были первыми слушателями. Первые впечатления: Владимир Игоревич — необычайно широкий математик со своим собственным взглядом на предмет. Вся математика для него едина и пронизана множеством одному ему известных связей.

Его семинар по теории особенностей занимался буквально всем. Например, где-то в эти годы там интенсивно обсуждалась "проблема резольвент" — вариант 13-й проблемы Гильберта о суперпозициях, в котором речь идет не о непрерывных, а об алгебраических функциях. Владимир Игоревич инициировал топологический подход к этой проблеме. Он предложил рассматривать алгебраическую функцию как многозначную аналитическую функцию многих комплексных переменных и искать топологические препятствия к представимости таких функций в виде суперпозиции алгебраических функций от меньшего числа переменных.

За несколько лет до этого, занимаясь с одаренными школьниками в Колмогоровском интернате, Владимир Игоревич с помощью топологических рассуждений доказал, что достаточно общая алгебраическая функция степени ≥ 5 от одной переменной непредставима в радикалах. Дело здесь в следующем. Как было известно еще Фробениусу, группа монодромии алгебраической функции изоморфна группе Галуа расширения поля рациональных функций, полученного присоединением к этому полю всех ветвей алгебраической функции. Согласно теории Галуа алгебраическое уравнение решается в радикалах, если и только если его группа Галуа разрешима.

Владимир Игоревич отметил, что раз группа монодромии — топологический инвариант, то только топология может быть ответственна за представимость алгебраических функций в радикалах. Он нашел чисто топологическое доказательство, не апеллирующее к теории Галуа, непредставимости в радикалах алгебраических функций с неразрешимой группой монодромии. Арнольд прочел курс лекций о своем доказательстве в Колмогоровском интернате. Позднее этот курс был переработан и опубликован В.Б. Алексеевым [1].

[1]Работа выполнена при частичной финансовой поддержке Канадского гранта (проект 156833-2).

[2]University of Toronto, Canada; Независимый московский университет, Москва, Россия; Институт системного анализа РАН, Москва, Россия.
E-mail: askold@math.toronto.edu

Согласно Владимиру Игоревичу топологические доказательства неразрешимости каких-либо аналитических задач, как правило, сильнее доказательств неразрешимости, полученных классическими средствами [2–9].

Развивая подход Арнольда, я построил топологический вариант теории Галуа, который дает новые более сильные результаты о неразрешимости алгебраических и дифференциальных уравнений в явном виде [10, 11].

В этой работе приводятся новые теоремы о разрешимости и неразрешимости алгебраических уравнений в радикалах. Эти теоремы я нашел осенью 2006 г., читая курс лекций о теории Галуа в университете Торонто.

Более подробно о содержании статьи и расположении материала. В разд. 1 приводятся явные формулы для обращения полинома Чебышева степени n, использующие только арифметические операции и радикалы. В разд. 2, следуя Эйлеру, мы решаем кубическое уравнение, используя формулу для обращения полинома Чебышева степени 3. В разд. 3 мы напоминаем, как сводить уравнение четвертой степени к кубическому уравнению.

В разд. 4–6 вычислены группы монодромии функций F_n и $F_n \circ \sigma$, обратных к полиному Чебышева T_n степени n и к полиному $-T_n$. Показано, что римановы поверхности этих функций целиком определяются по их локальному поведению около точек ветвления.

В разд. 7 обсуждаются транзитивные группы перестановок. Показывается, что транзитивная группа перестановок множества из n элементов, содержащая хотя бы одну транспозицию, не менее сложна, чем симметрическая группа из p элементов, где p — наименьший простой делитель числа n. Формулируются теоремы Галуа о разрешимой транзитивной группе, действующей на множестве, содержащем простое число элементов. Эти факты применяются в следующих разделах.

В разд. 8 показано, что алгебраическая функция степени n, дискриминант которой имеет хотя бы один простой корень, не может быть сведена при помощи радикалов и арифметических операций к алгебраическим функциям степени $p-1$, где p — наименьший простой делитель числа n (здесь предполагается, что $p \geq 5$).

Из теорем Галуа о транзитивной разрешимой группе, действующей на множестве, содержащем простое число p элементов, вытекают очень сильные ограничения на локальное поведение представимых в радикалах алгебраических функций степени p. Они сказываются на глобальных инвариантах. Эти ограничения обсуждаются в разд. 9. Например, там показано, что все алгебраические функции степени 23, у которых риманова поверхность имеет род $g = 1$, непредставимы в радикалах.

В разд. 10 показано, что обращение полинома простой степени p представимо в радикалах, если и только если полином аффинными заменами координат в образе и прообразе приводится либо к полиному Чебышева T_p, либо к функции x^p.

В разд. 11 начата топологическая классификация рациональных функций простой степени p, обращение которых представимо в радикалах. В разд. 12 в случае $p \equiv -1 \bmod 12$ эта классификация доведена до конца.

1. ПОЛИНОМЫ ЧЕБЫШЕВА И ИХ ОБРАЩЕНИЯ

Следующие утверждения были, вероятно, известны уже Муавру[3]:

1) $\cos nx$ *полиномиально выражается через* $\cos x$;

2) $\cos x$ *выражается при помощи арифметических операций и радикалов через* $\cos nx$.

Остановимся на этих утверждениях подробнее.

[3]Муавр Абрахам (de Moivre, Abraham) (1667–1754) — английский математик, друг Ньютона и Галлея. Среди его открытий — правило возведения в степень и извлечения корня n-й степени из комплексных чисел.

Из формулы Муавра $\cos nx + i\sin nx = (\cos x + i\sin x)^n$ вытекает, что

$$\cos nx = \sum (-1)^k C_n^{2k} \cos^{n-2k} x \cdot \sin^{2k} x. \qquad (*)$$

Определение. *Нормированным полиномом Чебышева степени n* назовем полином T_n, определенный формулой $T_n(u) = \sum (-1)^k C_n^{2k} u^{n-2k}(1-u^2)^k$.

На интервале $-1 < u < 1$ полином T_n имеет $n-1$ критических точек с критическими значениями 1 и -1. Справедливы равенства $T_n(1) = 1$ и $T_n(-1) = (-1)^n$. Эти свойства определяют полином T_n. Он отличается от классического полинома Чебышева степени n множителем 2^{n-1}. В дальнейшем мы будем называть полином T_n *полиномом Чебышева степени n*, опуская слово "нормированный". Из формулы $(*)$ вытекает следующее

Утверждение 1. *Справедливо равенство* $\cos nx = T_n(\cos x)$.

Определение. *Обращением полинома Чебышева степени n* назовем многозначную алгебраическую функцию F_n, определенную формулой

$$F_n(v) = \frac{\left(v + i\sqrt{1-v^2}\,\right)^{1/n} + \left(v - i\sqrt{1-v^2}\,\right)^{1/n}}{2}. \qquad (**)$$

Из определения функции F_n видно, что она *представима в радикалах.*

Утверждение 2. *Для каждой точки x существует такая ветвь функции F_n, что выполняется равенство* $\cos x = F_n(\cos nx)$.

Доказательство. Пусть $v = \cos nx$, $u = \cos x$. По формуле Муавра

$$\left(v + i\sqrt{1-v^2}\,\right)^{1/n} = u + i\sqrt{1-u^2}, \qquad \left(v - i\sqrt{1-v^2}\,\right)^{1/n} = u - i\sqrt{1-u^2},$$

откуда $u = F_n(v)$.

Следствие 3. *Функция F_n задает обращение полинома T_n: если $v = T_n(u)$, то для каждой точки v для некоторой ветви функции F_n выполняется равенство $u = F_n(v)$.*

2. ФУНКЦИЯ F_3 И РЕШЕНИЕ КУБИЧЕСКОГО УРАВНЕНИЯ

Эйлер использовал функцию F_3 для решения общего кубического уравнения в радикалах. Приведем (в модифицированном виде) его рассуждения.

Полином Чебышева $T_3 = 4u^3 - 3u$ имеет две критические точки $u_{1,2} = \pm 1/2$, в которых производная $T_3'(u) = 12(u^2 - 1/4)$ обращается в нуль.

Утверждение 4. *Аффинными заменами переменных полином T_3 переводится в любой полином третьей степени Q, имеющий две критические точки. Точнее, выполняется тождество $Q(x) \equiv AT_3(B(x + x_0)) + C$, параметры A, B, C, x_0 которого явно выражаются через коэффициенты полинома Q при помощи арифметических операций и извлечения квадратных корней.*

Доказательство. Если $Q(x) = ax^3 + bx^2 + cx + d$, то $Q' = 3a(x^2 + px + q)$, где $p = 2b/3a$ и $q = c/3a$. По условию дискриминант D полинома $x^2 + px + q$ не равен нулю. Полином $T_3(B(x + x_0))$, где $B = 1/\sqrt{D}$ и $x_0 = p/2$, имеет те же критические точки, что и полином Q. Поэтому производные этих полиномов различаются постоянным множителем. Сравнивая старшие коэффициенты и свободные члены этих полиномов, убеждаемся, что $Q(x) \equiv AT_3(B(x + x_0)) + C$, где $A = a/4B^3$, $C = d - AT_3(B(x_0))$.

Следствие 5. *Кубическое уравнение $Q(x) = ax^3 + bx^2 + cx + d = 0$, где Q — полином, имеющий две критические точки, решается при помощи арифметических операций, операции извлечения квадратного корня и суперпозиции с функцией F_3.*

Доказательство. По утверждению 4, используя лишь арифметические операции и операцию извлечения квадратного корня, можно подобрать параметры A, B, C, x_0 так, чтобы выполнялось тождество $Q(x) \equiv AT_3(B(x+x_0))+C$. В силу этого тождества корни уравнения $Q(x)=0$ представимы в виде $x = B^{-1}F_3(-C/A) - x_0$.

Утверждение 6. *Аффинными заменами переменных полином x^3 переводится в любой полином третьей степени Q, имеющий одну кратную критическую точку. Точнее, выполняется тождество $Q(x) \equiv A(x+x_0)^3+B$, параметры A, B, x_0 которого явно выражаются через коэффициенты полинома Q с помощью арифметических операций.*

Доказательство. По условию производная полинома $Q(x) = ax^3+bx^2+cx+d$ имеет кратный корень. Этот корень равен $-b/3a$. Полиномы Q и $(x+x_0)^3$, где $x_0 = -b/3a$, имеют пропорциональные производные. Сравнивая старшие коэффициенты и свободные члены этих полиномов, убеждаемся, что $Q(x) \equiv A(x+x_0)^3+B$ при $A=a$ и $B = d - ax_0^3$.

Следствие 7. *Кубическое уравнение $Q(x) = ax^3+bx^2+cx+d=0$, где Q — полином, имеющий одну кратную критическую точку, решается при помощи арифметических операций и суперпозиции с функцией $v^{1/3}$.*

Доказательство. По утверждению 6, используя лишь арифметические операции, можно подобрать параметры A, B, x_0 так, чтобы выполнялось тождество $Q(x) \equiv A(x+x_0)^3+B$. В силу этого тождества корни уравнения $Q(x)=0$ представимы в виде $x = (-B/A)^{1/3} - x_0$.

Итак, общее кубическое уравнение явно сводится либо к уравнению $T_3(x) = C$, либо к уравнению $x^3 = C$ и решается в радикалах. Известно, что общее уравнение четвертой степени сводится к кубическому уравнению. Напомним, как это делается.

3. СВЕДЕНИЕ УРАВНЕНИЯ ЧЕТВЕРТОЙ СТЕПЕНИ К УРАВНЕНИЮ ТРЕТЬЕЙ СТЕПЕНИ

Уравнение четвертой степени можно свести к уравнению третьей степени, рассматривая пучок плоских квадрик [12].

Утверждение 8. *Координаты точек пересечения двух плоских квадрик $P=0$ и $Q=0$, где P и Q — заданные полиномы второй степени от x и y, можно найти, решая одно кубическое и несколько квадратных уравнений.*

Доказательство. Каждая квадрика пучка $P+\lambda Q = 0$, где λ — произвольный параметр, проходит через искомые точки. При некотором значении λ_0 параметра λ квадрика $P+\lambda Q = 0$ распадается на пару прямых. Это значение удовлетворяет кубическому уравнению $\det(\widetilde{P}+\lambda\widetilde{Q}) = 0$, где $\widetilde{P}$ и $\widetilde{Q}$ — (3×3)-матрицы квадратичных форм, соответствующих уравнениям квадрик в однородных координатах. Уравнения каждой из двух прямых, составляющих квадрику $P+\lambda_0 Q = 0$, можно найти, решая квадратное уравнение: каждая такая прямая проходит через центр симметрии квадрики, координаты которого выражаются через коэффициенты квадрики при помощи арифметических операций, и через одну из точек пересечения квадрики с любой фиксированной прямой. Для нахождения координат этой точки нужно решить квадратное уравнение. Уравнение прямой, проходящей через две заданные точки, находится с помощью арифметических операций. Если известны уравнения прямых, на которые распадается квадрика $P+\lambda_0 Q = 0$, то для нахождения искомых точек остается лишь решить квадратные уравнения для точек пересечения квадрики $P=0$ и каждой из двух прямых, составляющих квадрику.

Следствие 9. *Общее уравнение четвертой степени с помощью арифметических операций и извлечения квадратных корней сводится к кубическому уравнению.*

Доказательство. Корни уравнения $a_0x^4+a_1x^3+a_2x^2+a_3x+a_4=0$ являются проекциями на ось x точек пересечения квадрик $y=x^2$ и $a_0y^2+a_1xy+a_2y+a_3x+a_4=0$.

4. ГРУППА ПЕРЕСТАНОВОК, ПОРОЖДЕННАЯ ДВУМЯ ИНВОЛЮЦИЯМИ, ПРОИЗВЕДЕНИЕ КОТОРЫХ — ЦИКЛИЧЕСКИЙ ЭЛЕМЕНТ

Представим группу $S(n)$ как группу перестановок множества A, содержащего n элементов. В этом разделе описываются всевозможные тройки a, b, c элементов группы $S(n)$ такие, что

1) $a^2 = b^2 = e$,

2) $c = ab$,

3) элемент c задает преобразование множества A, имеющее единственную орбиту длины n.

Рассмотрим два примера, в которых множество A является кольцом $\mathbb{Z}/n\mathbb{Z}$ остатков по модулю n.

Пример 1. Пусть a_1, b_1 — перестановки множества $\mathbb{Z}/n\mathbb{Z}$, переводящие элемент $x \in \mathbb{Z}/n\mathbb{Z}$ соответственно в элементы $a_1(x) \equiv -x \bmod n$ и $b_1(x) \equiv -x - 1 \bmod n$. Легко видеть, что перестановки a_1^2 и b_1^2 тождественны, а перестановка $c_1(x) = a_1(b_1(x))$ задается формулой $c_1(x) \equiv x + 1 \bmod n$ и является циклической.

Если в примере 1 перестановки a_1 и b_1 поменять местами, то их произведение по-прежнему будет циклической перестановкой. Действительно, $b_1 a_1 = (a_1 b_1)^{-1}$. Пример 2 получается из примера 1 переменой порядка перестановок и сменой циклического порядка в множестве A на противоположный.

Пример 2. Пусть a_2, b_2 — перестановки множества $\mathbb{Z}/n\mathbb{Z}$, переводящие элемент $x \in \mathbb{Z}/n\mathbb{Z}$ соответственно в элементы $a_2(x) \equiv -x + 1 \bmod n$ и $b_2(x) \equiv -x \bmod n$. Легко видеть, что перестановки a_2^2 и b_2^2 тождественны, а перестановка $c_2(x) = a_2(b_2(x))$ задается формулой $c_2(x) \equiv x + 1 \bmod n$ и является циклической.

Разумеется, пример 1 также получается из примера 2 переменой порядка перестановок и сменой циклического порядка на противоположный. При нечетном n каждая инволюция из примеров 1, 2 имеет в точности одну неподвижную точку. Несложно показать (см. доказательство теоремы 10), что при нечетном n существует взаимно однозначное преобразование кольца $\mathbb{Z}/n\mathbb{Z}$ в себя, переводящее инволюции a_1, b_1 из примера 1 в инволюции a_2, b_2 из примера 2. При четном n это не так: инволюция a_1 имеет две неподвижные точки, а инволюция a_2 не имеет ни одной.

Теорема 10. *Пусть перестановки a, b, c из группы $S(n)$ удовлетворяют условиям, перечисленным в начале этого раздела. Тогда*

1) *если n нечетно, то A можно отождествить с $\mathbb{Z}/n\mathbb{Z}$ так, чтобы перестановки a, b, c перешли в элементы a_1, b_1, c_1 из примера* 1, *и так, чтобы они переходили в элементы a_2, b_2, c_2 из примера* 2;

2) *если n четно, то либо a имеет две неподвижные точки, а b — ни одной, либо b имеет две неподвижные точки, а a — ни одной. В первом случае A можно отождествить с $\mathbb{Z}/n\mathbb{Z}$ так, чтобы перестановки a, b, c перешли в элементы a_1, b_1, c_1 из примера* 1. *Во втором случае — так, чтобы перестановки a, b, c переходили в элементы a_2, b_2, c_2 из примера* 2.

Доказательство. По условию элемент c задает циклическое преобразование множества A. Поэтому множество A можно отождествить с кольцом $\mathbb{Z}/n\mathbb{Z}$ так, чтобы $c(x) \equiv x + 1 \bmod n$. Тогда $cb(x) \equiv b(x) + 1 \bmod n$ и $(cb)^2(x) \equiv b(b(x) + 1) + 1 \bmod n$. Но по условию $cb = a$ и $a^2 = e$, следовательно, $(cb)^2(x) \equiv x \bmod n$. Учитывая, что $c(x) \equiv x + 1 \bmod n$, получаем $b(b(x)+1) \equiv x-1 \bmod n$. Так как $b^2 = e$, то $b(x)+1 \equiv b(x-1)$, или $b(x)+x \equiv b(x-1)+(x-1) \bmod n$. Последнее равенство означает, что величина $b(x)+x \bmod n$ не зависит от x. Обозначим $b(x)+x$ через l. Имеем $b(x) \equiv -x+l \bmod n$. Для всякого $q \in \mathbb{Z}/n\mathbb{Z}$ сделаем замену переменной $x = u + q \bmod n$, $u = x - q \bmod n$. В терминах переменной u отображение c по-прежнему

задается формулой $c(u) \equiv u+1 \bmod n$. Отображение b запишется в виде $b(u) \equiv -u-2q+l \bmod n$. При нечетном n вычет 2 обратим в кольце $\mathbb{Z}/n\mathbb{Z}$, поэтому можно выбрать q так, что $2q \equiv l+1 \bmod n$ или что $2q \equiv l \bmod n$. Отображение b будет задаваться соответственно формулой $b(u) \equiv -u-1 \bmod n$ или формулой $b(u) \equiv -u \bmod n$. Формулы для преобразований b и c идентичны соответственно формулам для b_1, c_1 из примера 1 и формулам для b_2, c_2 из примера 2. Поэтому при нечетном n можно установить взаимно однозначное соответствие множества A с кольцом $\mathbb{Z}/n\mathbb{Z}$ так, чтобы элементы a, b, c переходили в элементы a_1, b_1, c_1 из примера 1, и так, чтобы они переходили в элементы a_2, b_2, c_2 из примера 2.

Если n четно, то при нечетном l можно выбрать q так, что $2q \equiv l+1 \bmod n$, и при четном l — так, что $2q \equiv l \bmod n$. При замене переменной $x = u+q \bmod n$, $u = x-q \bmod n$ формулы для преобразований b и c станут идентичны соответственно формулам для b_1, c_1 из примера 1 и формулам для b_2, c_2 из примера 2.

Из теоремы вытекает следующее

Следствие 11. *В условиях теоремы* 10 *группа преобразований множества A, порожденная элементами a, b, c, изоморфна группе отображений кольца $\mathbb{Z}/n\mathbb{Z}$ в себя, имеющих вид $x \to ax+b \bmod n$, где $a = \pm 1$ и b — любой элемент кольца $\mathbb{Z}/n\mathbb{Z}$.*

Перепишем примеры 1 и 2 в виде, в котором они встретятся ниже.

Пример 3. Рассмотрим множество $A = \{V_0, \dots, V_{n-1}\}$ и следующие две его инволюции a и b, произведение ab которых задает циклическую перестановку множества A:

1) при инволюции a точка V_0 неподвижна; точки V_{2m-1} и V_{2m}, где $0 < 2m < n$, меняются местами; при четном n последняя точка V_{n-1} неподвижна;
2) при инволюции b точки V_{2m} и V_{2m+1}, где $0 \le 2m < n-1$, меняются местами; при нечетном n последняя точка V_{n-1} неподвижна.

Следствие 12. *Существует отождествление множества A из примера* 3 *с кольцом $\mathbb{Z}/n\mathbb{Z}$, переводящее инволюции a, b в инволюции a_1, b_1 из примера* 1. *При нечетном n существует также отождествление, переводящее инволюции a, b в инволюции a_2, b_2 из примера* 2.

Следующий пример 4 получается из примера 3 перестановкой инволюций a и b.

Пример 4. Рассмотрим множество $\widetilde{A} = \{\widetilde{V}_0, \dots, \widetilde{V}_{n-1}\}$ и следующие две его инволюции $\widetilde{a}$ и $\widetilde{b}$, произведение $\widetilde{a}\widetilde{b}$ которых задает циклическую перестановку множества $\widetilde{A}$:

1) при инволюции $\widetilde{a}$ точки $\widetilde{V}_{2m}$ и $\widetilde{V}_{2m+1}$, где $0 \le 2m < n-1$, меняются местами; при нечетном n последняя точка $\widetilde{V}_{n-1}$ неподвижна;
2) при инволюции $\widetilde{b}$ точка $\widetilde{V}_0$ неподвижна, точки $\widetilde{V}_{2m-1}$ и V_{2m}, где $0 < 2m < n$, меняются местами, при четном n последняя точка $\widetilde{V}_{n-1}$ неподвижна.

Следствие 13. *Существует отождествление множества $\widetilde{A}$ из примера* 3 *с кольцом $\mathbb{Z}/n\mathbb{Z}$, переводящее инволюции $\widetilde{a}$, $\widetilde{b}$ в инволюции a_2, b_2 из примера* 1. *При нечетном n существует также отождествление, переводящее инволюции $\widetilde{a}$, $\widetilde{b}$ в инволюции a_1, b_1 из примера* 1.

5. ПРЕДСТАВЛЕНИЯ МОНОДРОМИИ ФУНКЦИЙ F_n И $F_n \circ \sigma$

Рассмотрим алгебраическую функцию F_n, обратную к полиному Чебышева T_n степени n (см. разд. 1). Полином T_n имеет два критических значения: 1 и -1. Поэтому алгебраическая функция F_n имеет на сфере Римана $\overline{\mathbb{C}}$ три точки ветвления: $+1$, -1 и ∞. Пусть $\sigma\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ — инволюция, определенная формулой $\sigma(x) = -x$. Алгебраическая функция $F_n \circ \sigma$ имеет те же точки ветвления, что функция F_n. При нечетном n полином Чебышева является нечетной функцией. Поэтому при нечетном n функции F_n и $F_n \circ \sigma$ различаются лишь знаком $F_n \circ \sigma = -F_n$.

Пусть U — дополнение $\overline{\mathbb{C}} \setminus \{1, -1, \infty\}$ сферы Римана к точкам ветвления функций F_n и $F_n \circ \sigma$. Рассмотрим фундаментальную группу $\pi_1(U, 0)$ области U с отмеченной точкой 0. Выберем в качестве образующих в группе $\pi_1(U, 0)$ описанные ниже петли γ_1 и γ_2.

Петля $\gamma_1 \colon [0, 1] \to U$ соответствует следующему движению точки $\gamma_1(t)$: сначала точка движется по вещественному отрезку $I_1 = [0, 1 - \varepsilon]$, где $\varepsilon > 0$ — малое положительное число, от точки нуль до точки $1-\varepsilon$, затем обходит вокруг точки 1 в направлении против часовой стрелки по окружности радиуса ε и затем возвращается в точку нуль по отрезку I_1.

Петля $\gamma_2 \colon [0, 1] \to U$ определяется формулой $\gamma_2(t) = -\gamma_1(t)$.

Из определения петель γ_1 и γ_2 видно, что в фундаментальной группе $\pi_1(U, 0)$ петля $\gamma_3 = \gamma_2\gamma_1$ равна петле, обходящей вокруг точки ∞ в направлении по часовой стрелке.

Утверждение 14. *При обходе по петле $\gamma_2\gamma_1$ циклически переставляются*

1) *ветви функции F_n,*

2) *ветви функции $F_n \circ \sigma$.*

Доказательство. Функции F_n и $F_n \circ \sigma$ обратны к полиномам T_n и $-T_n$, а петля $\gamma_2\gamma_1$ в области U гомотопна петле, один раз обходящей вокруг точки ∞.

Ограничение полинома T_n на отрезок $-1 \le u \le 1$ имеет две граничные и $n-1$ внутренних точек экстремума u_i, где $-1 = u_0 < \ldots < u_n = 1$. Если $n - i \equiv 0 \bmod 2$, то $T_n(u_i) = 1$. Если $n - i \equiv 1 \bmod 2$, то $T_n(u_i) = -1$. Точки u_i разбивают отрезок $[-1, 1]$ на n сегментов с общими концами. На сегментах $I_{2m} = [u_{n-2m-1}, u_{n-2m}]$, где $0 \le 2m < n$, функция T_n монотонно возрастает от -1 до $+1$. На сегментах $I_{2m-1} = [u_{n-2m}, u_{n-2m+1}]$, где $0 < 2m \le n$, она монотонно убывает от $+1$ до -1.

Поскольку на определенных выше сегментах $I_0, \ldots, I_{n-1}$ функция T_n монотонна и принимает значения от -1 до 1, на отрезке $-1 \le v \le 1$ определено n вещественных ветвей обратной функции F_n. Будем называть *j-й ветвью* и обозначать через V_j ветвь функции F_n, принимающую значения на отрезке I_j. Приводимые ниже теоремы 15 и 16 описывают группу монодромии функции F_n при нечетном и четном n соответственно.

Теорема 15. *Обходам по петлям γ_1 и γ_2 соответствуют описанные в примере 3 инволюции a и b множества $V_0, \ldots, V_{n-1}$ ветвей функции F_n.*

Доказательство. Опишем преобразование монодромии ветвей функции F_n, соответствующее обходу по петле γ_1. При движении по отрезку $[0, 1]$ ветвь V_{2m} возрастает до u_{n-2m}, а ветвь V_{2m-1} убывает до u_{n-2m}. При $0 < 2m < n$ точка u_{n-2m} является точкой невырожденного локального максимума функции T_n и две ветви V_{2m}, V_{2m-1} обратной функции F_n, принимающие значение u_{n-2m} в точке 1, переставляются друг с другом при обходе точки 1 (так же как переставляются друг с другом две ветви функции $\sqrt{z}$ при обходе вокруг точки 0). В точке $u_n = 1$ производная $T_n'(1)$ не равна нулю, поэтому ветвь V_0 функции F_n аналитически продолжается на окрестность точки 1. Поэтому при обходе вокруг точки 1 ветвь V_0 возвращается к своему прежнему значению. Аналогично при четном n ветвь V_{n-1} равна 1 в точке 1, регулярна в этой точке и при ее обходе возвращается к своему прежнему значению.

Утверждение теоремы о преобразовании монодромии, соответствующем петле γ_2, доказывается аналогично.

Обозначим через $\widetilde{V}_j$ ветвь функции $F_n \circ \sigma$ на отрезке $[-1, 1]$, определенную формулой $\widetilde{V}_j = V_j \circ \sigma$, где $j = 0, \ldots, n-1$.

Теорема 16. *Обходам по петлям γ_1 и γ_2 соответствуют описанные в примере 4 инволюции $\widetilde{a}$ и $\widetilde{b}$ множества $\widetilde{V}_0, \ldots, \widetilde{V}_{n-1}$ ветвей функции $F_n \circ \sigma$.*

Теорема 16 является прямым следствием теоремы 15.

Следствие 17. *Группы монодромии функций F_n и $F_n \circ \sigma$ изоморфны группе всех преобразований вида $x \to \pm x + b \bmod n$ кольца $\mathbb{Z}/n\mathbb{Z}$.*

6. РИМАНОВЫ ПОВЕРХНОСТИ ФУНКЦИЙ F_n И $F_n \circ \sigma$ ОПРЕДЕЛЯЮТСЯ ЛОКАЛЬНЫМИ ДАННЫМИ

В этом разделе описываются римановы поверхности алгебраических функций F_n и $F_n \circ \sigma$ в терминах их локального поведения в окрестностях точек ветвления.

Рассмотрим тройку $(\pi, R, \overline{\mathbb{C}})$, состоящую из связной римановой поверхности R некоторой n-значной алгебраической функции и ее естественной проекции $\pi\colon R \to \overline{\mathbb{C}}$ на сферу Римана $\overline{\mathbb{C}}$. Пусть разветвленное n-листное накрытие $\pi\colon R \to \overline{\mathbb{C}}$ имеет три точки ветвления -1, 1, ∞. Допустим, что

1) в группе монодромии накрытия обходы вокруг точек 1 и -1 задают инволюции множества листов алгебраической функции;
2) обход вокруг ∞ задает циклическую перестановку множества листов алгебраической функции.

Теорема 18. *При выполнении условий* 1), 2) *тройка* $(\pi, R, \overline{\mathbb{C}})$ *является или римановой поверхностью функции* F_n, *или римановой поверхностью функции* $F_n \circ \sigma$.

Точнее, либо существует биголоморфное отображение $h_1\colon \mathbb{C} \to R$ *такое, что* $\pi \circ h_1 = T_n$, *либо существует биголоморфное отображение* $h_2\colon \mathbb{C} \to R$ *такое, что* $\pi \circ h_2 = -T_n$. *При нечетном* n *реализуются обе возможности, при четном — одна.*

Доказательство. Пусть U — дополнение сферы Римана к множеству точек ветвления разветвленного накрытия $\pi\colon R \to \overline{\mathbb{C}}$ и $M\colon \pi_1(U, 0) \to S(n)$ — гомоморфизм монодромии. Согласно теореме 10 с точностью до сопряжения группы $S(n)$ при нечетном n существует лишь единственный гомоморфизм M, удовлетворяющий условиям теоремы 18. По теоремам 15, 16 именно такой гомоморфизм монодромии имеют функции F_n и $F_n \circ \sigma$. При четном n согласно теореме 10 таких гомоморфизмов два. По теоремам 15, 16 гомоморфизмы монодромии функций F_n и $F_n \circ \sigma$ соответствуют именно этим двум гомоморфизмам. (Они имеют следующее различие: преобразование монодромии, соответствующее обходу по петле γ_1, для функции F_n имеет две неподвижные точки, а для функции $F_n \circ \sigma$ не имеет ни одной.)

Известна следующая классическая теорема (см., например, [12]): если у двух n-листных разветвленных накрытий $\pi_1\colon R_1 \to \overline{\mathbb{C}}$ и $\pi_2\colon R_2 \to \overline{\mathbb{C}}$ с одинаковыми множествами точек ветвления гомоморфизмы монодромии с точностью до сопряжения группы $S(n)$ совпадают, то существует биголоморфное отображение $h\colon R_1 \to R_2$ такое, что $\pi_1 = \pi_2 \circ h$. Накрытия $T_n\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ и $-T_n\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ представляют римановы поверхности функций F_n и $F_n \circ \sigma$ соответственно. Теорема 18 доказана.

Нам понадобится одно (очевидное) утверждение того же характера, что и теорема 18. Рассмотрим тройку $(\pi, R, \overline{\mathbb{C}})$, состоящую из связной римановой поверхности R некоторой n-значной алгебраической функции и ее естественной проекции $\pi\colon R \to \overline{\mathbb{C}}$ на сферу Римана $\overline{\mathbb{C}}$. Пусть разветвленное n-листное накрытие $\pi\colon R \to \overline{\mathbb{C}}$ имеет две точки ветвления 0 и ∞.

Утверждение 19. *При выполнении перечисленных выше условий тройка* $(\pi, R, \overline{\mathbb{C}})$ *является римановой поверхностью функции* $v^{1/n}$. *Точнее, существует биголоморфное отображение* $h_1\colon \mathbb{C} \to R$ *такое, что* $\pi \circ h_1 = u^n$.

Доказательство. Фундаментальная группа области $U = \overline{\mathbb{C}} \setminus \{0, \infty\}$ изоморфна аддитивной группе целых чисел $\mathbb{Z}$. С точностью до сопряжения группы $S(n)$ существует единственный гомоморфизм группы $\mathbb{Z}$ в группу $S(n)$ такой, что образ группы $\mathbb{Z}$ транзитивен. Поэтому любые два разветвленные n-листные накрытия с точками ветвления 0 и ∞ эквивалентны между собой и, следовательно, эквивалентны римановой поверхности функции $v^{1/n}$.

7. ТРАНЗИТИВНЫЕ ГРУППЫ ПЕРЕСТАНОВОК КОНЕЧНЫХ МНОЖЕСТВ

Здесь мы обсудим несколько утверждений о транзитивных группах перестановок, которые нам понадобятся в дальнейшем.

Пусть группа G транзитивно действует на множестве A. Фиксируем точку x в множестве A и обозначим через G_x стационарную подгруппу точки x. Действие G на A восстанавливается по паре групп $G_x \subset G$: точки множества A можно отождествить с правыми классами смежности группы G по подгруппе G_x (правый класс смежности элемента h — совокупность элементов группы, представимых в виде hg, где $g \in G_x$). Действие группы G на X при этом отождествлении переходит в действие группы на множестве правых классов смежности группы G по подгруппе G_x при помощи умножения слева.

Пусть в A введено некоторое соотношение эквивалентности. Скажем, что это соотношение *G-инвариантно*, если для любого элемента g группы G и любой пары эквивалентных точек $a \approx b$ множества A справедливо соотношение $g(a) \approx g(b)$. Опишем все возможные G-инвариантные соотношения эквивалентности на множестве A.

Пусть F — любая подгруппа в группе G, содержащая подгруппу G_x. С подгруппой F связано следующее отношение эквивалентности на множестве A: скажем, что точки a и b *F-эквивалентны*, если $a = g_1(x)$, $b = g_2(x)$ и элементы g_1, g_2 принадлежат одному правому классу смежности по подгруппе F. Легко проверяется следующее

Утверждение 20. *F-эквивалентность корректно определена и G-инвариантна. Для разных подгрупп F соотношения F-эквивалентности различны. Каждое G-инвариантное соотношение эквивалентности является F-эквивалентностью для некоторой подгруппы $F \supseteq G_x$.*

Следствие 21. *Пусть на конечном множестве A транзитивно действует группа G и введено некоторое G-инвариантное соотношение эквивалентности. Тогда каждый класс эквивалентности содержит одно и то же число точек.*

Пусть транзитивная группа G преобразований множества A содержит транспозицию. По множеству A и группе G построим следующий граф A_G: вершины графа — точки множества A; две вершины $a, b \in A$ соединяются ребром, если и только если в группе G есть транспозиция, меняющая местами точки a и b.

Утверждение 22. *Пусть вершины a, b графа A_G соединены ребром. Тогда для любого элемента g группы G вершины $g(a)$, $g(b)$ тоже соединены ребром.*

Доказательство. Пусть транспозиция $\sigma \in G$ меняет местами точки a и b. Тогда $g\sigma g^{-1}$ — инволюция, меняющая местами точки $g(a)$ и $g(b)$.

Пусть на множестве A транзитивно действует группа, содержащая транспозицию. Введем на множестве A следующее соотношение эквивалентности: *две точки $a, b \in A$ эквивалентны, если вершины a, b графа A_G принадлежат одной компоненте связности этого графа.*

Следствие 23. *Введенное соотношение эквивалентности G-инвариантно. В частности, все классы эквивалентности содержат одно и то же число точек.*

Доказательство. Первое утверждение следствия вытекает из утверждения 22, второе — из следствия 21.

Утверждение 24. *Транзитивная группа перестановок конечного множества A, порожденная транспозициями, совпадает с группой всех перестановок множества A.*

Доказательство этого несложного утверждения можно найти, например, в [10].

Пусть группа G транзитивно действует на множестве A и содержит хотя бы одну транспозицию. Тогда выполняется следующая

Теорема 25. *На A существует G-инвариантное соотношение эквивалентности такое, что*

1) *каждый класс эквивалентности содержит не менее двух точек*;

2) *у группы G есть нормальный делитель H, состоящий из всех перестановок множества A, сохраняющих соотношение эквивалентности.*

Доказательство. Введем в множестве A соотношение эквивалентности, о котором идет речь в следствии 23. Из утверждения 24 видно, что группа G содержит все перестановки множества A, сохраняющие это соотношение эквивалентности. Эти перестановки образуют нормальный делитель H, о котором идет речь в теореме.

Следствие 26. *Пусть в условиях теоремы* 25 *множество A содержит n элементов. Тогда у числа n есть делитель $k > 1$, $n = km$, такой, что группа G содержит нормальный делитель H, изоморфный прямой сумме m экземпляров симметрической группы $S(k)$. Поэтому, в частности, у группы G существует подгруппа, изоморфная симметрической группе $S(p)$, где p — наименьший простой делитель числа n.*

Галуа нашел замечательные результаты о разрешимых группах, транзитивно действующих на множествах, содержащих простое число элементов. Ниже мы формулируем его результаты (называя их первой и второй теоремами Галуа о разрешимых группах) и обсуждаем их следствия.

Введем нужные обозначения. Пусть $m \in \mathbb{Z}$ — натуральное число, $\mathbb{Z}/m\mathbb{Z}$ — кольцо вычетов по модулю m, $(\mathbb{Z}/m\mathbb{Z})^*$ — мультипликативная группа обратимых относительно умножения элементов кольца $(\mathbb{Z}/m\mathbb{Z})^*$. *Метациклической группой* M_m называется группа всех перестановок g множества $\mathbb{Z}/m\mathbb{Z}$ вида $g(x) \equiv ax+b \bmod m$, где $a \in (\mathbb{Z}/m\mathbb{Z})^*$ и $b \in \mathbb{Z}/m\mathbb{Z}$. Отображение $\pi\colon M_m \to \mathbb{Z}/m\mathbb{Z}$, сопоставляющее элементу $g \in M_m$, где $g(x) \equiv ax + b$, элемент $a \in (\mathbb{Z}/m\mathbb{Z})^*$, является гомоморфизмом группы M_m на группу $(\mathbb{Z}/m\mathbb{Z})^*$. Обозначим через $H(m)$ циклическую группу порядка m, состоящую из всех перестановок g множества $\mathbb{Z}/m\mathbb{Z}$ вида $g(x) \equiv x+b \bmod m$, где $b \in \mathbb{Z}/m\mathbb{Z}$. Ядром этого гомоморфизма является группа $H(m)$. Группы H_m и $(\mathbb{Z}/m\mathbb{Z})^*$ коммутативны. Поэтому *метациклическая группа M_m разрешима.*

Первая теорема Галуа о разрешимых группах. *Пусть G — транзитивная группа перестановок конечного множества A, содержащего простое число p элементов. Тогда группа G разрешима, если и только если существует отождествление $\phi\colon A \to (\mathbb{Z}/p\mathbb{Z})^*$ множества A с полем вычетов по модулю p, при котором группа G переходит в подгруппу метациклической группы M_p, содержащую нормальный делитель H_p.*

Вторая теорема Галуа о разрешимых группах. *Транзитивная группа преобразований конечного множества, содержащего простое число элементов, разрешима, если и только если преобразование из группы, имеющее более чем одну неподвижную точку, тождественно.*

Красивые и простые теоремы Галуа о разрешимых группах тесно связаны между собой. В немного других формулировках их можно найти, например, в книге [14]. Вторая теорема Галуа накладывает сильные ограничения на циклический тип каждой перестановки g группы G. Именно справедливо следующее

Следствие 27. *Транзитивная группа преобразований множества A, содержащего простое число p элементов, разрешима, если и только если под действием нетождественного преобразования $g \in G$ множество A распадается на орбиты следующих длин*:

1) *или на одну орбиту длины p*;

2) *или на одну орбиту длины* 1 *и на $(p-1)/l$ орбит длины l, где $l > 1$ — любой натуральный делитель числа $p-1$.*

Доказательство. Согласно второй теореме Галуа группа G, удовлетворяющая условиям следствия, разрешима. Пусть преобразование $g \in G$ разрешимой группы G имеет две орбиты различных длин k и m, содержащих больше одной точки. Можно считать, что $k > m > 1$.

Преобразование g^m будет иметь по крайней мере $m > 1$ неподвижных точек, но не будет тождественным. По второй теореме Галуа группа G неразрешима. Отсюда и вытекает следствие.

8. ЛОКАЛЬНАЯ МОНОДРОМИЯ И НЕРАЗРЕШИМОСТЬ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ В ЯВНОМ ВИДЕ

Рассмотрим неприводимое алгебраическое уравнение

$$y^n + R_1 y^{n-1} + \ldots + R_n = 0, \qquad (***)$$

коэффициенты которого принадлежат полю $\mathbb{C}\langle x\rangle$ рациональных функций одного переменного x. Как было известно еще Фробениусу, *группа Галуа уравнения* $(***)$ *над полем* $\mathbb{C}\langle x\rangle$ *изоморфна группе монодромии алгебраической функции* y *переменной* x, *определенной уравнением* $(***)$ (см., например, [11–13]).

Алгебраическое уравнение над некоторым полем K *разрешимо в* k*-радикалах*, если существует цепочка расширений $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m$ такая, что поле K_{j+1} получается из поля K_j присоединением либо радикала, либо алгебраического элемента степени $\leq k$ над полем K_j и поле K_m содержит все решения уравнения $(***)$. Алгебраическая функция переменной x *представима в* k*-радикалах*, если неприводимое алгебраическое уравнение, задающее эту функцию, разрешимо в k-радикалах над полем $\mathbb{C}\langle x\rangle$. За разрешимость уравнения в k-радикалах отвечает его группа Галуа. Группа G называется k-разрешимой, если у нее существует нормальная башня подгрупп $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = e$ такая, что каждая фактор-группа G_i/G_{i+1} либо коммутативна, либо изоморфна некоторой подгруппе группы $S(k)$. Справедлив следующий

Критерий разрешимости в k-радикалах (см. [11, 13]). *Алгебраическое уравнение над полем нулевой характеристики разрешимо в* k*-радикалах, если и только если его группа Галуа* k*-разрешима.*

Легко видеть, что *подгруппа и фактор-группа* k*-разрешимой группы* k*-разрешимы*. Поэтому *при* $m > k \geq 4$ *группа* $S(m)$ *не-*k*-разрешима*: группа $S(m)$ содержит простую подгруппу $A(m)$, которая некоммутативна и неизоморфна подгруппе группы $S(k)$.

Теорема 28. *Пусть группа Галуа неприводимого алгебраического уравнения степени* n *над полем нулевой характеристики* K, *рассматриваемая как группа перестановок корней уравнения, содержит хотя бы одну транспозицию. Пусть наименьший простой делитель* p *числа* n *больше* 3. *Тогда уравнение неразрешимо в* $(p-1)$*-радикалах над полем* K.

Доказательство. По теореме 25 группа Галуа содержит подгруппу, изоморфную $S(p)$. Так как по условию $p \geq 5$, отсюда вытекает, что группа Галуа не является $(p-1)$-разрешимой. Теперь теорема 28 вытекает из критерия разрешимости уравнений в k-радикалах.

Следствие 29. *Пусть группа монодромии* n*-значной алгебраической функции* y *содержит хотя бы одну транспозицию, и пусть наименьший простой делитель* p *числа* n *больше* 3. *Тогда функция* y *непредставима в* $(p-1)$*-радикалах.*

Следствие 30. *Пусть* n*-значная алгебраическая функция* y *определена неприводимым уравнением* $P_0 y^n + \ldots + P_{n-1} y + P_n = 0$ *с полиномиальными коэффициентами. Пусть дискриминант этого уравнения имеет хотя бы один простой корень, в котором полином* P_0 *не обращается в нуль, и пусть наименьший простой делитель* p *числа* n *больше* 3. *Тогда функция* y *непредставима в* $(p-1)$*-радикалах.*

Доказательство. Действительно, обход вокруг простого корня дискриминанта, не являющегося корнем старшего коэффициента, задает транспозицию ветвей алгебраической функции.

Утверждение 31. *Оценка из следствия* 29 *точна, т.е. существует алгебраическая функция y, удовлетворяющая условиям теоремы* 28 *и представимая в p-радикалах.*

Доказательство. Пусть $p \geq 5$ — наименьший простой делитель числа n и $n = pk$. Рассмотрим любую общую алгебраическую функцию w степени k, все точки ветвления которой некратны (обходы вокруг таких точек задают транспозиции ветвей алгебраической функции w) и множество точек ветвления которой не содержит точек 0 и ∞. Алгебраическая функция y, заданная формулой $y(x) = w(x^{1/k})$, имеет степень n, все ее точки ветвления, кроме точек 0 и ∞, некратны. По построению функция y представима в p-радикалах. По теореме 28 она непредставима в $(p-1)$-радикалах.

Следствие 29 можно усилить. Справедлива следующая

Теорема 28′. *Если y удовлетворяет условиям следствия* 29 (*и, в частности, если она удовлетворяет условиям следствия* 30), *то y нельзя выразить через мероморфные функции при помощи суперпозиций, арифметических операций, решения алгебраических уравнений степени $< p$, извлечения корней и при помощи операции неопределенного интегрирования.*

Доказательство. Теорема 28′ вытекает из следствия 29 и из необходимого условия представимости функций в $(p-1)$-квадратурах, доказанного в топологическом варианте теории Галуа (см. [11]).

9. ОБ АЛГЕБРАИЧЕСКИХ ФУНКЦИЯХ ПРОСТОЙ СТЕПЕНИ, ПРЕДСТАВИМЫХ В РАДИКАЛАХ

Галуа нашел следующий

Критерий разрешимости в радикалах (см. [13, 14])**.** *Алгебраическое уравнение над полем нулевой характеристики разрешимо в радикалах, если и только если его группа Галуа разрешима.*

В силу второй теоремы Галуа о разрешимых группах (см. разд. 7) для неприводимых уравнений простой степени этот критерий принимает следующий вид.

Теорема Галуа. *Неприводимое алгебраическое уравнение простой степени над полем нулевой характеристики разрешимо в радикалах над этим полем, если и только если каждое нетождественное преобразование его группы Галуа оставляет неподвижным не более одного корня уравнения.*

Так как группа монодромии алгебраической функции изоморфна группе Галуа ее уравнения над полем рациональных функций, критерий Галуа дает необходимые и достаточные условия представимости алгебраической функции в радикалах в терминах ее группы монодромии (см. [11, 12]). В частности, критерий Галуа накладывает очень сильные ограничения на поведение представимой в радикалах алгебраической функции простой степени около своих точек ветвления.

Теорема 32. *Если алгебраическая функция y простой степени p представима в радикалах, то обходу вокруг любой из ее точек ветвления соответствует перестановка листов функции y, которая либо является циклической перестановкой, либо раскладывается на циклы, один из которых имеет единичную длину, а все остальные имеют одинаковые длины.*

Доказательство. Теорема 32 вытекает из теоремы Галуа и следствия 27.

Пусть $\pi\colon R \to \overline{\mathbb{C}}$ — естественная проекция римановой поверхности алгебраической функции на сферу Римана $\overline{\mathbb{C}}$ и $a \in \overline{\mathbb{C}}$ — ее точка ветвления. Назовем *дефектом* $\mu(a)$ точки ветвления $a \in \overline{\mathbb{C}}$ сумму по всем прообразам точки a кратностей нулей дифференциала отображения π.

Сопоставим простому числу p *множество дефектов* A_p — конечное множество натуральных чисел, элементами которого являются

1) число $p-1$,

2) число $(p-1)(1-1/l)$, где $l>1$ — делитель числа $p-1$.

Пример 5. Пусть p и $q=(p-1)/2$ — простые числа. Тогда множество A_p равно $\{q, 2q-2, 2q-1, 2q\}$. Действительно, разложение числа $p-1$ на простые множители имеет вид $p-1=2q$, поэтому делители числа $p-1$, большие единицы, — это числа 2, q, $2q$. В частности, 23 и $11=(23-1)/2$ — простые числа. Поэтому $A_{23}=\{11,20,21,22\}$.

Утверждение 33. *Дефект каждой точки ветвления представимой в радикалах алгебраической функции простой степени p принадлежит множеству A_p.*

Доказательство. Утверждение вытекает из теоремы 32. Действительно, если обходу вокруг точки ветвления соответствует циклическая перестановка листов алгебраической функции, то дефект точки ветвления равен $p-1$. Пусть при обходе точки ветвления один лист алгебраической функции неподвижен, а остальные листы разбиваются на циклы равной длины l. Тогда число $p-1$ делится на l. Над такой точкой ветвления находится $(p-1)/l$ критических точек, в каждой из которых дифференциал проекции имеет нуль кратности $l-1$. Дефект такой точки ветвления равен $(l-1)(p-1)/l=(p-1)(1-1/l)$.

С понятием дефекта связана следующая классическая

Формула Римана–Гурвица. *Род g римановой поверхности R удовлетворяет следующему соотношению*:

$$2-2g=2p-\sum\mu(a),$$

где суммирование ведется по точкам ветвления функции a.

Для каждого простого p определим *полугруппу* P_p, порожденную множеством дефектов A_p. По определению $m\in P_p$, если существуют целые неотрицательные числа m_i такие, что $m=\sum m_ik_i$, где $k_i\in A_p$. Нам понадобится *множество* B_p, *состоящее из натуральных чисел q, не принадлежащих полугруппе P_p, и удовлетворяющее следующему условию*: q — *четное число, большее или равное* $2p-2$.

Множество B_p для любого простого p конечно (см. ниже следствие 35), для многих простых чисел p оно пусто.

Теорема 34. *Алгебраическая функция простой степени p, род g которой равен $[N-(2p-2)]/2$, где N — четное число из множества B_p, непредставима в радикалах.*

Доказательство. Согласно формуле Римана–Гурвица род g алгебраической функции y степени p удовлетворяет соотношению $2-2g=2p-\sum\mu(a)$. Согласно утверждению 33 если функция y представима в радикалах, то дефект $\mu(a)$ каждой ее точки ветвления a лежит в множестве A_p. Пусть $\sum\mu(a)=D$. Тогда $D\in P_p$ и род g представим в виде $[D-(2p-2)]/2$, где D — четное число из полугруппы P_p. Отсюда и вытекает теорема.

Теорема Сильвестра дает информацию о полугруппе $P(m,n)$, порожденной взаимно простыми числами n, m. Определим число $N(m,n)$ формулой $N(m,n)=(m-1)(n-1)-1$.

Теорема Сильвестра. *Каждое целое число, большее чем $N(m,n)$, принадлежит полугруппе $P(m,n)$. Для любой пары неотрицательных чисел, сумма которых равна $N(m,n)$, одно из чисел принадлежит полугруппе $P(m,n)$, а второе не принадлежит. В частности, существует ровно $(m-1)(n-1)/2$ целых неотрицательных чисел, не принадлежащих полугруппе $P(m,n)$.*

Следствие 35. *Для всякого простого $p>2$ множество B_p конечно.*

Доказательство. Множество A_p содержит два взаимно простых числа: число $p-1$ и число $p-2=(p-1)(1-1/(p-1))$. По теореме Сильвестра дополнение множества натуральных чисел к полугруппе P_p конечно.

Опишем полугруппу P_p в случае, когда $q=(p-1)/2$ — простое число. Согласно примеру 5 для этого достаточно описать полугруппу P, порожденную числами q, $2q-2$, $2q-1$ и $2q$.

Утверждение 36. *Полугруппа P, порожденная числами q, $2q-2$, $2q-1$ и $2q$, является объединением следующих множеств натуральных чисел*:

1) *для каждого четного числа $2l\geq 0$ множества решений неравенств $2l(q-1)\leq x\leq 2lq$;*
2) *для нечетного числа $2l+1>0$ множества решений неравенств $2l(q-1)+q\leq x\leq (2l+1)q$.*

Доказательство. Числа из полугруппы представимы в виде $k_0q+k_1(2q-2)+k_2(2q-1)+k_3(2q)$, где $k_0,k_1,k_2,k_3\geq 0$. Рассмотрим следующие два случая.

1. Число k_0 четно. Тогда, взяв вместо k_3 число $k_3+k_0/2$, можно считать, что $k_0=0$. Итак, нас интересуют числа вида $(k_1+k_2+k_3)2q-(k_2+2k_1)$. Положим $k_1+k_2+k_3=l$. Имеем ограничения $k_1,k_2,k_3\geq 0$ и $k_1+k_2+k_3=l$. При этих ограничениях выражение k_2+2k_1 принимает любое значение от нуля до $2l$. Поэтому при четном k_0 мы получаем объединение по $0\leq l$ отрезков натурального ряда $2lq-2l\leq x\leq 2lq$.

2. Число k_0 нечетно. Тогда, взяв вместо k_3 число $k_3+(k_0-1)/2$, можно считать, что $k_0=1$. Итак, нас интересуют числа вида $(k_1+k_2+k_3)2q-(k_2+2k_1)+q$. Положим $k_1+k_2+k_3=l$. Имеем ограничения $k_1,k_2,k_3\geq 0$ и $k_1+k_2+k_3=l$. При этих ограничениях выражение k_2+2k_1 принимает любое значение от нуля до $2l$. Поэтому при нечетном k_0 мы получаем объединение по $0\leq l$ отрезков натурального ряда $2l(q-1)+q\leq x\leq (2l+1)q$. Утверждение доказано.

Пример 6. Для числа $p=23$ число $q=11$. Имеем $A_{23}=\{11,20,21,22\}$. Применяя утверждение 36, получим, что полугруппа P_{23} содержит следующие числа: 0, 11, 20–22, 31–33, 40–44, 51–55, 60–66, 71–77, 80–88, 91–99, 100–110, далее все натуральные числа. Итак, четные числа ≥ 44, не попавшие в P_{23}, суть $46,48,50,56,58,68,70,78,90$.

Теорема 37. *Алгебраическая функция степени* 23, *имеющая один из следующих родов*: $g=1,2,3,6,7,12,13,17,23$, *непредставима в радикалах.*

Доказательство. Теорема 37 вытекает из теоремы 34 и вычислений примера 6.

Олег Иврий, студент университета Торонто, посещавший мои лекции по теории Галуа, составил программу для перечисления всех пар p,g, где $p<60$ — простое число и $g\leq 2$ — четное число, для которых согласно теореме 34 алгебраическая функция степени p и рода g непредставима в радикалах. Чисел $p<60$, для которых такие пары существуют, оказалось шесть. Вот их список: $23,29,43,47,53,59$. Для простых чисел $p=23,47,59$ из этого списка числа $(p-1)/2$ простые. Для таких p соответствующих родов g много (соответственно 9, 81, 144), но их все можно вычислить без компьютера, пользуясь утверждением 36. Воспроизведу ответ Олега для оставшихся трех простых чисел. Для $p=29$ подходят роды $g=1,2$. Для $p=43$ — роды $g=1,5$. Для $p=53$ — роды $g=1,2,3,4,5,7,8,14,15,16,27,28,29,40,53$.

В этих вычислениях мы пользовались теоремой 34. По-видимому, существует больше пар p,g, для которых алгебраическая функция степени p и рода g непредставима в радикалах, чем множество пар p,g из теоремы 34. В оставшейся части это раздела мы обсудим, почему теорема 34 скорее всего неточна.

Дело в том, что преобразования монодромии, соответствующие обходам вокруг точек ветвления алгебраической функции, не произвольны: их произведение должно быть тождественным преобразованием и они должны порождать транзитивную группу монодромии.

Группа монодромии представимой в радикалах алгебраической функции степени p является подгруппой метациклической группы. Метациклическая группа M_p имеет гомоморфизм

$\pi\colon M_p \to (\mathbb{Z}/p\mathbb{Z})^*$ в мультипликативную группу $(\mathbb{Z}/p\mathbb{Z})^*$ кольца $\mathbb{Z}/p\mathbb{Z}$. Допустим, что среди преобразований монодромии, соответствующих обходам вокруг точек ветвления алгебраической функции, нет циклических перестановок. В этом случае образ $\pi(g)$ преобразования монодромии g определяет длины циклов, на которые распадается преобразование g. Элемент $g(x) = ax + b \bmod p$ при $a = \pi(g) \neq 1 \bmod p$ разбивается на циклы равных длин l и на один цикл длины 1, где l — порядок элемента $a = \pi(g)$. Произведение обходов вокруг точек ветвления равно единичному элементу монодромии. Занумеруем точки ветвления. Пусть g_j — преобразование монодромии, соответствующее обходу вокруг j-й точки ветвления, $a_j = \pi(g_j)$ и порядок элемента a_j равен l_j. Имеем $a_1 \cdot \ldots \cdot a_k = 1$, где k — число точек ветвления. Из этого тождества вытекают некоторые ограничения на порядки l_j. Вот пример: разложим l_j на простые множители. Пусть $p_1, \ldots, p_m$ — совокупность простых чисел, встречающихся в разложениях порядков l_j. Пусть μ_q — наибольшая кратность, с которой простое число p_q входит в числа $l_1, \ldots, l_k$.

Утверждение 38. *Для каждого q имеется не менее двух чисел l_i, l_j, в разложения которых простое число p_q входит с максимальной кратностью μ_q.*

Доказательство. Рассмотрим число $N = p_1^{\mu_1} \cdot \ldots \cdot p_m^{\mu_m}$. Положим $N_q = N/p_q$. Пусть максимальная кратность μ_q встречается ровно в одном числе $l_{j(q)}$. Тогда $(a_1 \cdot \ldots \cdot a_m)^{N_q} \neq 1$, что невозможно. Действительно, при возведении в степень N_q все элементы a_i, кроме элемента $a_{j(q)}$, станут единицами. Противоречие доказывает утверждение.

10. КЛАССИФИКАЦИЯ ПОЛИНОМОВ ПРОСТОЙ СТЕПЕНИ, ОБРАЩЕНИЯ КОТОРЫХ ПРЕДСТАВИМЫ В РАДИКАЛАХ

Начнем со следующего очевидного утверждения.

Утверждение 39. *Если функция обратна к полиному степени n, то сумма дефектов ее конечных точек ветвления равна $n - 1$.*

Доказательство. Дефект конечной точки ветвления a функции, обратной к полиному P, по определению равен сумме кратностей нулей производной P' по точкам множества $P^{-1}(a)$. Но сумма кратностей всех нулей функции P' равна $n - 1$.

Утверждение 40. *Если обратная к полиному простой степени функция представима в радикалах, то функция имеет*

1) *либо одну конечную точку ветвления, обход вокруг которой задает циклическую перестановку ее листов*;
2) *либо две конечные точки ветвления, обход вокруг каждой из которых задает инволюцию множества ее листов.*

Доказательство. Пусть алгебраическая функция y, обратная к полиному степени p, представима в радикалах. Согласно утверждению 33 дефект каждой конечной точки ветвления функции y либо равен $p-1$, либо равен $(p-1)(1-1/l)$, где $l > 1$ — делитель числа $p-1$. По утверждению 39 сумма всех дефектов равна $p-1$. При $l > 2$ число $(p-1)(1-1/l)$ больше половины числа $p-1$. Следовательно, дефект точки ветвления может равняться только $p-1$ и $(p-1)(1-1/2)$. Представляются лишь две возможности: имеется лишь одна точка ветвления с дефектом $p-1$ либо две точки ветвления с дефектом $(p-1)(1-1/2)$. По теореме 32 в первом случае обход вокруг конечной точки ветвления задает циклическую перестановку листов функции y. По той же теореме 32 во втором случае обход вокруг каждой конечной точки ветвления задает инволюцию множества ее листов.

Теорема 41. *Полином простой степени p имеет представимую в радикалах обратную функцию, если и только если аффинными заменами переменных в образе и прообразе полином*

можно привести к одному из следующих двух видов:

1) *к степенной функции* x^p;

2) *к полиному Чебышева* T_p.

Доказательство. Воспользуемся предыдущим утверждением. Пусть полином имеет два критических значения. Рассмотрим композицию полинома с аффинным преобразованием, переводящим два критических значения в точки 1, -1. Согласно теореме 18 полученный полином аффинной заменой переменной переводится в полином Чебышева T_p.

Пусть полином имеет одно критическое значение. Рассмотрим композицию полинома с аффинным преобразованием, переводящим критическое значение в точку 0. Согласно утверждению 19 полученный полином аффинной заменой переменной переводится в степенную функцию x^p.

Итак, мы показали, что с точностью до аффинных замен переменной среди полиномов простой степени только для полинома Чебышева и степенной функции обратные функции представимы в радикалах. Напомним, что общее кубическое уравнение решается в радикалах именно потому, что всякий кубический полином аффинными заменами координат переводится либо в полином T_3, либо в функцию x^3.

11. О РАЦИОНАЛЬНЫХ ФУНКЦИЯХ ПРОСТОЙ СТЕПЕНИ, ОБРАЩЕНИЯ КОТОРЫХ ПРЕДСТАВИМЫ В РАДИКАЛАХ

Начнем со следующего очевидного утверждения.

Утверждение 42. *Если степень алгебраической функции равна* n, *а род ее римановой поверхности равен нулю, то сумма дефектов ее точек ветвления равна* $2(n-1)$.

Доказательство. Согласно формуле Римана–Гурвица $2 = 2n - \sum \mu(a)$, или $\sum \mu(a) = 2(n-1)$.

Назовем *приведенным дефектом* точки ветвления a n-значной алгебраической функции, род римановой поверхности которой равен нулю, число $\mu(a)/(n-1)$, где $\mu(a)$ — дефект этой точки. По формуле Римана–Гурвица *сумма приведенных дефектов равна* 2.

Пусть алгебраическая функция y простой степени p, род римановой поверхности которой равен 0, представима в радикалах. *Каким может быть множество приведенных дефектов ее точек ветвления*?

Для каждого простого p дефекты точек ветвления функции y — элементы множества A_p, содержащего число $p-1$ и числа $(p-1)(1-1/l)$, где $l > 1$ — делитель числа $p-1$. Обозначим через $\overline{A}_\infty = \{1, 1/2, 3/4, 4/5, \dots\}$ объединение двух множеств, одно из которых состоит из числа 1, другое — из всех чисел последовательности $k/(k+1)$, где $k = 1, 2, \dots$ Видно, что *приведенный дефект каждой точки ветвления функции* y *содержится в множестве* $\overline{A}_\infty$.

Задача. Перечислить все неупорядоченные наборы чисел, каждое число в которых принадлежит множеству $\overline{A}_\infty$, а сумма всех чисел в наборе равна 2.

Утверждение 43. *Имеются лишь следующие шесть наборов чисел, удовлетворяющих условиям задачи*:

1) 1, 1;

2) 1, 1/2, 1/2;

3) 1/2, 1/2, 1/2, 1/2;

4) 1/2, 2/3, 5/6;

5) 1/2, 3/4, 3/4;

6) 2/3, 2/3, 2/3.

Доказательство. 1. Пусть набор или содержит число 1, или содержит поднабор $\{1/2,1/2\}$. Сумма остальных чисел набора должна равняться 1. Остальные числа могут быть лишь единицами и половинами. Действительно, если число $x \in \overline{A}_\infty \setminus \{1,1/2\}$ есть в наборе, то, так как $x<1$, должно присутствовать еще одно число множества $\overline{A}_\infty$, что невозможно, так как $x>1/2$, а все числа множества $\overline{A}_\infty$ не меньше чем $1/2$. Оставшиеся возможности легко перебираются и соответствуют наборам 1)–3).

2. Пусть набор не содержит единицы и содержит одну половину. Сумма остальных чисел набора должна равняться $3/2$. Кроме $1/2$, в наборе должно присутствовать ровно два числа. Действительно, все числа в множестве $\overline{A}_\infty \setminus \{1/2\}$ больше чем $(3/2)/3$. Среди оставшихся чисел есть числа $\le (3/2)/2 = 3/4$ — это числа $2/3$ и $3/4$. Значит, среди оставшихся чисел есть либо $2/3$, либо $3/4$. Эти возможности реализуются и соответствуют наборам 4) и 5).

3. Пусть набор не содержит чисел 1 и $1/2$. Все числа x множества $\overline{A}_\infty \setminus \{1,1/2\}$ удовлетворяют неравенствам $2/3 \le x < 1$. Здесь есть единственная возможность — в наборе есть три числа и все они равны $2/3$. Эта возможность соответствует набору 6).

Следствие 44. *Для простого числа $p>2$ представимые в радикалах функции, обратные к рациональным функциям степени p, могут иметь лишь следующие наборы приведенных дефектов*: *наборы* 1) *и* 2) *— эти наборы реализуются, если и только если рациональные функции дробно-линейными заменами в образе и прообразе приводятся к степенной функции x^p или к полиному Чебышева T_p*; *набор* 3); *наборы* 4) *и* 6) *— эти наборы могут встретиться при $p \equiv 1 \bmod 3$*; *набор* 5) *— этот набор может встретиться при $p \equiv 1 \bmod 4$.*

Я планирую вернуться к топологической классификации представимых в радикалах функций, обратных к рациональным. Остановимся на топологической классификации таких функций с набором приведенных дефектов типа 3).

12. КЛАССИФИКАЦИЯ РАЦИОНАЛЬНЫХ ФУНКЦИЙ ПРОСТОЙ СТЕПЕНИ p, $p \equiv -1 \bmod 12$, ОБРАЩЕНИЯ КОТОРЫХ ПРЕДСТАВИМЫ В РАДИКАЛАХ

Напомним общие факты о топологической классификации аналитических отображений $\varphi\colon R \to \overline{\mathbb{C}}$ степени n связных компактных римановых поверхностей в сферу Римана $\overline{\mathbb{C}}$. Каждому такому отображению соответствует гомоморфизм монодромии $M\colon \pi_1(\overline{\mathbb{C}} \setminus A, *) \to S(n)$, где A — множество критических значений отображения φ и $\pi_1(\overline{\mathbb{C}} \setminus A, *)$ — фундаментальная группа дополнения $\overline{\mathbb{C}} \setminus A$ с отмеченной точкой $*$. Гомоморфизм M определен с точностью до сопряжения группы $S(n)$. Образ фундаментальной группы при гомоморфизме монодромии транзитивен.

Отображения $\varphi_1\colon R_1 \to \overline{\mathbb{C}}$ и $\varphi_2\colon R_2 \to \overline{\mathbb{C}}$ называются *эквивалентными как разветвленные накрытия*, если существует гомеоморфизм $h\colon R_1 \to R_2$ такой, что $\varphi_2 \circ h = \varphi_1$. *Отображения эквивалентны как разветвленные накрытия, если и только если множества A_1, A_2 их критических значений совпадают и гомоморфизмы монодромии $M_1\colon \pi_1(\overline{\mathbb{C}} \setminus A, *) \to S(n)$ и $M_2\colon \pi_1(\overline{\mathbb{C}} \setminus A, *) \to S(n)$, где $A = A_1 = A_2$, этих разветвленных накрытий одинаковы с точностью до сопряжения в группе $S(n)$.*

Занумеруем точки множества критических значений $A = \{v_1, \dots, v_{m+1}\}$ и фиксируем образующие $\gamma_1, \dots, \gamma_{m+1}$ в группе $\pi_1(\overline{\mathbb{C}} \setminus A, *)$, состоящие из непересекающихся петель,"обегающих против часовой стрелки" вокруг точек $v_1, \dots, v_{m+1}$ и связанных соотношением $\gamma_1 \dots \gamma_{m+1} = e$. После фиксации образующих задание гомоморфизма $q\colon \pi_1(\overline{\mathbb{C}} \setminus A, *) \to S(n)$ эквивалентно заданию упорядоченного набора элементов $g_1 = q(\gamma_1), \dots, g_{m+1} = q(\gamma_{m+1})$ в группе $S(n)$ таких, что $g_1 \dots g_{m+1} = e$.

Так как гомоморфизм монодромии определен с точностью до сопряжения в группе $S(n)$ и его образ транзитивен, то нас интересуют заданные с точностью до сопряжения упорядоченные

наборы $g_1, \dots, g_{m+1}$ элементов группы $S(n)$, которые порождают транзитивную группу. На таких наборах действует группа кос $B(m+1)$ из $m+1$ нитей с образующими $p_1, \dots, p_m$. Действие задается следующим правилом: при действии на набор $g_1, \dots, g_{m+1}$ образующая p_i оставляет неподвижными все элементы, кроме элементов g_i и g_{i+1}, а $p_i(g_i) = g_{i+1}$ и $p_i(g_{i+1}) = g_{i+1}^{-1} g_i g_{i+1}$.

Отображения $\varphi_1 \colon R_1 \to \overline{\mathbb{C}}$ и $\varphi_2 \colon R_2 \to \overline{\mathbb{C}}$ называются *топологически эквивалентными*, если существуют сохраняющие ориентацию гомеоморфизмы $h \colon R_1 \to R_2$ и $\rho \colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ такие, что $\varphi_2 \circ h = \rho \circ \varphi_1$. Разветвленные накрытия с множеством ветвления A *топологически эквивалентны, если и только если упорядоченный набор элементов* $g_1, \dots, g_{m+1} \in S(n)$, *соответствующий гомоморфизму монодромии первого накрытия, с точностью до сопряжения в группе* $S(n)$ *и описанного выше действия группы кос равен набору элементов* $l_1, \dots, l_{m+1} \in S(n)$, *соответствующих гомоморфизму монодромии второго накрытия* [15].

Обозначим через SM_p подгруппу метациклической группы M_p, порожденной всеми элементами второго порядка. Группа SM_p состоит из преобразований g кольца $\mathbb{Z}/p\mathbb{Z}$ вида $g(x) \equiv -x + a \bmod p$ (каждое такое преобразование имеет порядок 2) и из преобразований вида $g(x) \equiv x + b \bmod p$. Введем следующие обозначения: для всякого элемента a кольца $\mathbb{Z}/p\mathbb{Z}$ обозначим через σ_a преобразование $g(x) \equiv x + a \bmod p$ и через $\widetilde{\sigma}_a$ преобразование $g(x) \equiv -x + a \bmod p$. Напишем таблицу умножения в группе SM_p. Легко проверить следующее

Утверждение 45. *Для любых* $a, b \in \mathbb{Z}/p\mathbb{Z}$ *справедливы соотношения*

$$\sigma_a \sigma_b = \sigma_{a+b}, \qquad \sigma_a \widetilde{\sigma}_b = \widetilde{\sigma}_{a+b}, \qquad \widetilde{\sigma}_a \widetilde{\sigma}_b = \sigma_{a-b}, \qquad \widetilde{\sigma}_a \sigma_b = \widetilde{\sigma}_{a-b}.$$

Теорема 46. *Пусть* $\widetilde{\sigma}_a$, $\widetilde{\sigma}_b$, $\widetilde{\sigma}_c$, $\widetilde{\sigma}_d$ — *четыре элемента второго порядка в группе* SM_p, *связанные соотношением* $\widetilde{\sigma}_a \widetilde{\sigma}_b \widetilde{\sigma}_c \widetilde{\sigma}_b = e$ *и порождающие транзитивную группу. Каждая такая четверка при помощи сопряжения в группе* SM_p *и действия группы кос* $B(4)$ *переводится в четверку, в которой* $\widetilde{\sigma}_a(x) \equiv \widetilde{\sigma}_c(x) \equiv -x + 1 \bmod p$ *и* $\widetilde{\sigma}_b(x) \equiv \widetilde{\sigma}_d(x) \equiv -x - 1 \bmod p$.

Доказательство. Соотношение $\widetilde{\sigma}_a \widetilde{\sigma}_b \widetilde{\sigma}_c \widetilde{\sigma}_d = e$ означает, что $(\widetilde{\sigma}_a \widetilde{\sigma}_b)(\widetilde{\sigma}_c \widetilde{\sigma}_d) = \sigma_{(a-b)} \sigma_{(c-d)} = \sigma_{(a-b+c-d)} = e$, т.е. что $a + c = b + d$.

При действии образующей p_1 группы кос $B(4)$ четверка g_1, g_2, g_3, g_4 переходит в четверку $g_2, g_2^{-1} g_1 g_2, g_3, g_4$. Для $g_1 = \widetilde{\sigma}_a$, $g_2 = \widetilde{\sigma}_b$ имеем $g_2^{-1} g_1 g_2 = \widetilde{\sigma}_b \circ \widetilde{\sigma}_a \circ \widetilde{\sigma}_b = \widetilde{\sigma}_{2b-a}$. Итак, образующая p_1 пару $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ переводит в пару $\widetilde{\sigma}_b, \widetilde{\sigma}_{2b-a}$ и не меняет два последних элемента в четверке. Обозначим $a - b$ через q. В этих обозначениях пара элементов $\widetilde{\sigma}_a, \widetilde{\sigma}_b$, равная паре $\widetilde{\sigma}_a, \widetilde{\sigma}_{a-q}$, переходит в пару $\widetilde{\sigma}_{a-q}, \widetilde{\sigma}_{a-2q}$. Поэтому элемент $p_1^m \in B(4)$ переводит пару $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ в пару $\widetilde{\sigma}_{a-mq}, \widetilde{\sigma}_{a-(m+1)q}$.

Допустим, что $q \neq 0 \bmod p$. В этом случае, не меняя элементов $\widetilde{\sigma}_c$, $\widetilde{\sigma}_d$, пару $\widetilde{\sigma}_a, \widetilde{\sigma}_b$ можно перевести в пару $\widetilde{\sigma}_l, \widetilde{\sigma}_{-l}$, где $2l \equiv q \bmod p$. Действительно, при $q \neq 0 \bmod p$ уравнение $a + mq = l$ в поле $\mathbb{Z}/p\mathbb{Z}$ разрешимо относительно m. Для m, равного решению этого уравнения, пара a, b под действием элемента p_1^m переходит в пару $l, -l$, где $2l \equiv a - b \bmod p$.

По условию элементы a, b, c, d связаны соотношением $a + c = b + d$. Поэтому если $a - b = 2l \neq 0$, то $c - d = -2l \neq 0$. Повторяя предыдущие вычисления, получаем, что пара $\widetilde{\sigma}_c, \widetilde{\sigma}_d$ под действием степеней образующей p_3 группы кос $B(4)$ переводится в пару $\widetilde{\sigma}_{-l}, \widetilde{\sigma}_l$. Итак, под действием степеней образующих p_1 и p_3 четверка $\widetilde{\sigma}_a, \widetilde{\sigma}_b, \widetilde{\sigma}_c, \widetilde{\sigma}_d$ переводится в четверку $\widetilde{\sigma}_l, \widetilde{\sigma}_{-l}, \widetilde{\sigma}_{-l}, \widetilde{\sigma}_l$.

Рассмотрим теперь случай $q \equiv 0 \bmod p$. Если $q = 0$, то $c = d$, так как по условию $a - b = c - d$, т.е. четверка имеет вид $\widetilde{\sigma}_a, \widetilde{\sigma}_a, \widetilde{\sigma}_b, \widetilde{\sigma}_b$. Элементы a и b не могут быть равными: в противном случае все четыре преобразования имеют точку 0 общей неподвижной точкой, что противоречит транзитивности группы. При $a \neq b$ под действием образующей p_2 группы кос $B(4)$ исходная четверка перейдет в четверку $\widetilde{\sigma}_a, \widetilde{\sigma}_b, \widetilde{\sigma}_{2b-a}, \widetilde{\sigma}_b$. К этой четверке применимы уже проведенные вычисления, так как $a \neq b$ и $b \neq 2b - a$.

Значит, действием группы кос $B(4)$ исходную четверку можно привести к виду $\widetilde{\sigma}_l, \widetilde{\sigma}_{-l}$, $\widetilde{\sigma}_{-l}, \widetilde{\sigma}_l$, где $l \neq 0$. Теперь, делая в поле $\mathbb{Z}/p\mathbb{Z}$ аффинную замену $g(x) \equiv lx \bmod p$, можно добиться, чтобы l стало равным 1. Действительно, $g^{-1}\widetilde{\sigma}_l g = \widetilde{\sigma}_1$ и $g^{-1}\widetilde{\sigma}_{-l} g = \widetilde{\sigma}_{-1}$.

Следствие 47. *С точностью до топологической эквивалентности существует единственное рациональное отображение $\pi\colon \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ простой степени $p > 2$ такое, что обратное отображение представимо в радикалах и преобразование монодромии, соответствующее обходу вокруг каждой точки ветвления, является инволюцией. Такое рациональное отображение имеет четыре критических значения. Гомоморфизм монодромии обратной функции описан в теореме* 46.

Согласно следствию 44 если простое число p удовлетворяет условиям $p \neq 1 \bmod 3$ и $p \neq 1 \bmod 4$, то представимая в радикалах функция, обратная к рациональной функции степени p, может иметь набор приведенных дефектов лишь типов 1)–3). Простое число $p > 3$ удовлетворяет соотношениям $p \neq 1 \bmod 3$ и $p \neq 1 \bmod 4$, если и только если $p \equiv -1 \bmod 12$.

Следствие 48. *Пусть $p > 3$ — простое число такое, что $p \equiv -1 \bmod 12$. Тогда существуют три топологических типа рациональных функций степени p, обратные к которым представимы в радикалах. Это функция x^p, полином Чебышева T_p и функция, описанная в теореме* 46. *Функции первых двух типов приводятся к своим нормальным формам дробно-линейными преобразованиями в образе и прообразе. Функции третьего типа относительно такой группы преобразований зависят от одного модуля — двойного отношения четырех критических значений.*

Замечание. После того как статья была принята к печати, я обнаружил следующую замечательную работу: *Ritt J.F.* On algebraic functions which can be expressed in terms of radicals // Trans. Amer. Math. Soc. 1922. V. 24, N 1. P. 21–30. Во многом Ритт продвинулся дальше меня. Он показал, что полином (не обязательно простой степени), обращение которого представимо в радикалах, является композицией полиномов первой и четвертой степеней, функций вида z^p и полиномов Чебышева. Он также классифицировал рациональные функции простой степени, обращения которых представимы в радикалах. Но некоторых моих результатов в работе Ритта нет. Вот примеры: 1) риманова поверхность функции, обратной к полиному Чебышева, определяется своим локальным поведением около точек ветвления; 2) алгебраическая функция степени n, имеющая хотя бы одну некратную точку ветвления, не может быть сведена при помощи радикалов к алгебраическим функциям степени $< p$, где p — наименьший простой делитель числа n (здесь предполагается, что $p \geq 5$).

СПИСОК ЛИТЕРАТУРЫ

1. *Алексеев В.Б.* Теорема Абеля в задачах и решениях. М.: МЦНМО, 2001.
2. *Арнольд В.И.* 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. *Арнольд В.И., Олейник О.А.* Топология действительных алгебраических многообразий // Вестн. Моск. ун-та. Математика. Механика. 1979. № 6. С. 7–17.
4. *Арнольд В.И.* Суперпозиции // Колмогоров А.Н. Избр. тр.: Математика и механика. М.: Наука, 1985. С. 444–451.
5. *Арнольд В.И.* Топологическое доказательство трансцендентности абелевых интегралов в "Математических началах натуральной философии" Ньютона // Ист.-мат. исслед. 1989. Т. 31. С. 7–17.
6. *Arnold V.I., Vassiliev V.A.* Newton's "Principia" read 300 years later // Not. Amer. Math. Soc. 1989. V. 36, N 9. P. 1148–1154; Addendum: V. 37, N 2. P. 144.
7. *Arnold V.I.* Problèmes résolubles et problèmes irrésolubles analytiques et géométriques // Passion des formes. Dynamique qualitative, sémiophysique et intelligibilité. Á René Thom. Fontenay–St.-Cloud: ENS Éditions, 1994. P. 411–417.

8. *Arnold V.I.* Sur quelques problèmes de la théorie des systèmes dynamiques // Topol. Meth. Nonlin. Anal. 1994. V. 4, N 2. P. 209–225. Рус. пер.: *Арнольд В.И.* О некоторых задачах теории динамических систем // Избранное–60. М.: Фазис, 1997. С. 533–551.
9. *Арнольд В.И.* И.Г. Петровский, топологические проблемы Гильберта и современная математика // УМН. 2002. Т. 57, № 4. С. 197–207.
10. *Khovanskii A.G.* Topological obstructions to the representability of functions by quadratures // J. Dyn. and Control Syst. 1995. V. 1, N 1. P. 91–123.
11. *Хованский А.Г.* О разрешимости и неразрешимости уравнений в явном виде // УМН. 2004. Т. 59, № 4. С. 69–146.
12. *Бержe М.* Геометрия. М.: Мир, 1984. Т. 1, 2.
13. *Хованский А.Г.* Теория Галуа, накрытия и римановы поверхности. М.: МЦНМО, 2006.
14. *Чеботарев Н.Г.* Основы теории Галуа. М.: Едиториал УРСС, 2004. Ч. 1.
15. *Khovanskii A.G., Zdravkovska S.* Branched covers of S^2 and braid groups // J. Knot Theory and Ramif. 1996. V. 5, N 1. P. 55–75.