УДК 512.7, 519.688

О вычислении группы автоморфизмов гиперэллиптических кривых

М. Д. Малых, Л. А. Севастьянов

29 сентября 2019 г.

Аннотация

Предложен алгоритм отыскания группы бирациональных автоморфизмов гиперэллиптической кривой $y^2 = p(x)$, $p \in \mathbb{Q}[x]$, над полем комплексных чисел, основанный на разложения в степенные ряды. Представлена реализация этого алгоритма в системе компьютерной алгебры Sage, приведены примеры. Проделанные численные эксперименты свидетельствуют о том, что этот алгоритм не приводит к неожиданно чрезмерно сложным вычислениям. Формат представления группы позволяет применять для ее исследования инструменты для работы с конечными группами малого порядка, встроенные в Sage.

Ключевые слова: hyperelliptic curve, group of birational autimorphisms, sage, sagemath.

1. Введение

Алгебраическая геометрия изучает свойства кривых, инвариантные относительно бирациональных преобразований [1]. Ни порядок, ни класс таковыми не являются, поэтому важнейшим инвариантным целочисленным параметром, характеризующим кривую, является ее род. Если кривая неприводима и имеет не очень сложные особые точки, то род вычисляется по явной формуле [2]. Современные системы компьютерной алгебры, в том числе Maple и Sage, содержат алгоритм вычисления рода любой плоской кривой. Намереваясь исследовать кривую с точностью до бирациональных

преобразований, прежде всего следует описать группу всех бирациональных автоморфизмов этой кривой.

Задача 1. На плоскости x, y дана неприводимая алгебраическая кривая C

$$f(x, y) = 0, \quad f \in \mathbb{Q}[x, y],$$

требуется отыскать группу $\mathfrak{G}(C)$, образованную всеми бирациональными автоморфизмами этой кривой над полем $\mathbb{C}$.

Кривые рода нуль бирационально эквивалентны прямой, поэтому их группа автоморфизмов изоморфна группе дробно-линейных подстановок. Кривые рода 1 бирационально эквивалентны эллиптической кривой, поэтому их группа тоже бесконечна. Ее однопараметрическая подгруппа было описана в середине XIX веке при помощи эллиптического интеграла первого типа [3]. Если же род кривой больше 1, то, как доказали еще в 1860-х годах Пикар и Шварц, группа бирациональных автоморфизмов конечна. Чуть позже Гурвиц получил оценки сверху на порядок группы и порядок элементов [1], затем было показано, что эти оценки достигаются на некоторых кривых [4, 5]. Тем не менее, задача 1 не была решена для казалось бы самого простого случая, когда искомая группа заведомо является конечной и даже известны оценки на порядок этой группы.

Спустя сто лет, к этой проблеме вернулись, когда в системах компьютерной алгебры стали появляться пакеты для работы с алгебраическими кривыми [6, 7, 8]. Для гиперэллиптических кривых рода 2 эта задача была решена в системе Magma, однако уже случай гиперэллиптических кривых рода 3 оказался слишком трудным [6]. Существующие на данный момент пакеты для работы с алгебраическими кривыми в Maple [9] и Sage [10], созданные в начале 2000-х годов, способны вычислить род и базис пространства абелевых дифференциалов 1-го типа, однако выйти за этот круг проблем пока не удалось. Это и заставляет думать, что задача 1 или алгоритмически неразрешима или, во всяком случае, слишком сложная.

С другой стороны задача 1 — простейшая из задач алгебраической геометрии в том смысле, что решение практически любой задачи алгебраической геометрии (построение алгебраического соответствия между кривыми, классификация подполей поля рациональных функций на кривой и проч.), в которой требуется найти объект, инвариантный относительно бирациональнальных преобразований, неизбежно приведет к решению и этой задачи. Поэтому алгоритмическая неразрешимость задачи 1 приведет к алгебраической неразрешимости значительного числа задач алгебраической геометрии, подобно тому, как алгоритмическая неразрешимость диафантовой задачи приводит к неразрешимости целого ряда задач в теории линейных дифференциальных уравнений [11, 12]. Если же задача 1 разрешима, то ее сложность дает оценку снизу для сложности этих задач. Если эта задача слишком сложна, то возможности по применению методов алгебраической геометрии, напр., в теории интегрирования дифференциальных уравнений [13] окажутся чрезвычайно ограничены. Поэтому для дальнейшего представляется крайне важным отыскать решение задачи 1.

С целью отыскания такового мы просмотрели работы Гурвица и отыскали в первой, редко цитируемой работе [14] конструкцию, пригодную для конструктивного решения задачи 1. Результаты были представлены на совещании по компьютерной алгебре в Дубне в 2015. Оказалось, что задача 1 все же алгоритмически разрешима, однако предложенный алгоритм даже для гиперэллиптических кривых приводил к вычислениям, неподъемным на современном компьютере.

Тем не менее, в классе гиперэллиптических кривых задача 1 имеет очень простое решение, основанное на технике разложения в степенные ряды, лежащей в основе вейерштрассовской теории абелевых интегралов [15]. В настоящей статье мы дадим описание этого решения и представим его реализацию в системе Sage. Вероятно, это решение должно было казаться ученикам Вейерштрасса, и в первую очередь самому Гурвицу, тривиальным и потому не было описано. Современные же авторы, желают отыскать

решение, пригодное и для кривых над полями с произвольными характеристиками, поэтому этот подход оказывается в стороне от магистральной линии исследований.

2. Группа автоморфизмов гиперэллиптической кривой

Напомним, что кривая, заданная уравнением вида

$$y^2 = p(x)$$

на проективной плоскости xy называется гиперэллиптической, если p — многочлен из $\mathbb{C}[x]$ степени $n > 4$, все комплексные корни которого простые. Эти корни будем далее обозначать как $e_1, \ldots, e_n$. Эта кривая — неприводимая, а ее род ρ равен

$$\frac{n-2}{2} \quad \text{или} \quad \frac{n-1}{2}$$

для четных и нечетных n соответственно.

При описании искомой группы старые авторы [17] начинали с понятия рационального преобразования на кривой. Оно представляет собой отображение вида

$$\hat{x} = X(x, y), \quad \hat{y} = Y(x, y),$$

где X, Y — рациональные функции, которые подобраны таким образом, что из $f(x, y) = 0$ следует $f(\hat{x}, \hat{y}) = 0$. Это преобразование называют бирациональным, если для любой точки $(\hat{x}, \hat{y})$ на кривой можно отыскать единственный прообраз. При этом из системы

$$\hat{x} = X(x, y), \quad \hat{y} = Y(x, y), \quad f(\hat{x}, \hat{y}) = 0$$

переменные x, y можно выразить как рациональные функции $\hat{x}, \hat{y}$.

Современные авторы исходят из представления о поле рациональных функций на кривой [1]. Дело в том, что сопоставление рациональной функции $R(x, y)$ функции $R(\hat{x}, \hat{y})$ как сложной функции от x, y задает автоморфизм поля рациональных функций на кривой. Более того, между автоморфизмами этого поля и бирациональными преобразованиями тем самым

устанавливается взаимно однозначное соответствие [1]. По этой причине в современном изложении группу $\mathfrak{G}$ рассматривают как группу автоморфизмов полей, что позволяет вписать вопрос в круг идей теории Галуа.

Лемма 1. Пусть T — бирациональный автоморфизм на гиперэллиптической кривой. Тогда найдутся такие комплексные числа $\alpha, \ldots, \delta$, что

$$Tx = \frac{\alpha + \beta x}{\gamma + \delta x}.$$

Доказательство. Доказательство в существенном повторяет аргументы доказательства конечности группы автоморфизмов, указанное Пикаром. Линейное пространство дифференциалов 1-го типа имеет базис

$$\frac{dx}{y}, \quad \frac{xdx}{y}, \ldots, \frac{x^{\rho-1}dx}{y}.$$

Интеграл

$$\int^{(Tx,Ty)} \frac{x^m dx}{y}, \quad m = 0, 1, \ldots, \rho - 1$$

остается всюду конечным при любом выборе точки (x, y), следовательно, он является интегралом первого типа. Это означает, что найдутся такие числа $c_{m,k}$, что

$$\frac{Tx^m dTx}{Ty} = \sum_{k=0}^{\rho-1} c_{m,k} \frac{x^k dx}{y}. \tag{1}$$

В частности при $m = 0$

$$\frac{dTx}{Ty} = \sum_{k=0}^{\rho-1} c_{0,k} \frac{x^k dx}{y}. \tag{2}$$

Как следствие соотношений (1) и (2), имеем

$$(Tx)^m = \frac{c_{m,0} + c_{m,1}x + \cdots + c_{m,\rho-1}x^{\rho-1}}{c_{0,0} + c_{0,1}x + \cdots + c_{0,\rho-1}x^{\rho-1}}, \quad m = 1, \ldots, \rho - 1.$$

При $\rho = 2$ это означает, что Tx — дробно-линейная функция x. При $\rho > 2$ мы получаем, что Tx — рациональная функция x, $(\rho - 1)$-ая степень которой является рациональной функцией порядка не выше $\rho - 1$. Такая функция является функцией порядка 1, то есть дробно-линейной функцией. $\square$

Обозначим как $\mathfrak{G}$ группу всех автоморфизмов этой кривой. Доказанная лемма означает, что закон преобразования x-овой координаты точки кривой не зависит от y, то есть определена проекция π группы $\mathfrak{G}$ в группу дробно-линейных преобразований оси x. Эта проекция согласована с композицией преобразований и поэтому является гомоморфизмом.

Лемма 2. Пусть T — бирациональный автоморфизм на гиперэллиптической кривой. Если порядок многочлена p — четный, то проекция $\pi(T)$ переставляет корни многочлена p. Если же порядок многочлена p — нечетный, то проекция $\pi(T)$ переставляет корни многочлена p и бесконечно удаленную точку ∞.

Доказательство. Всякая алгебраическая кривая допускает локальную униформизацию [15, 18]. Это означает следующее. В окрестности любой точки (a, b) общего положения на кривой саму кривую можно описать параметрически при помощи двух степенных рядов

$$x = a + a_1 t + a_2 t^2 + \dots, \quad y = b + b_1 t + b_2 t^2 + \dots,$$

причем локально соответствие между малыми значениями t и точками (x, y) взаимно-однозначное. Если точка (a, b) — особая, то она может быть точкой пересечения нескольких дуг, допускающих такое представление. Если же эта точка бесконечно удаленная, то в разложении появляются отрицательные степени t.

В случае гиперэллиптической кривой в окрестности любой точки (a, b) с $b \neq 0$ можно представить дугу как

$$x = a + t, \quad y = \sqrt{p(a + t)} = b + b_1 t + \dots,$$

а в окрестности точки $(e_m, 0)$ — как

$$x = e_m + t^2, \quad y = \sqrt{p(e_m + t)} = \sqrt{\prod_{k \neq m} (e_k - e_m)}\, t + \dots.$$

В последней формуле не следует писать $\pm$, поскольку при любом выборе знака у корня эта формула дает параметризацию всей окрестности. Наконец, окрестность бесконечно удаленной точки при четном n дается двумя

дугами

$$x = \frac{1}{t}, \quad y = \pm\sqrt{p\left(\frac{1}{t}\right)} = \pm\sqrt{p_n}t^{\frac{n}{2}} + \ldots,$$

а при нечетном — одной дугой

$$x = \frac{1}{t^2}, \quad y = \pm\sqrt{p\left(\frac{1}{t}\right)} = \pm\sqrt{p_n}t^{n} + \ldots,$$

Пусть бирациональное преобразование

$$T: \quad \hat{x} = X(x, y), \quad \hat{y} = Y(x, y),$$

переводит точку (a, b) в точку $(\hat{a}, \hat{b})$ и пусть дугу кривой в окрестности точки (a, b) можно представить как

$$x = a + a_1 t + a_2 t^2 + \ldots, \quad y = b + b_1 t + b_2 t^2 + \ldots,$$

а дугу в окрестности точки $(\hat{a}, \hat{b})$ — как

$$\hat{x} = \hat{a} + \hat{a}_1 \tau + \hat{a}_2 \tau^2 + \ldots, \quad \hat{y} = \hat{b} + \hat{b}_1 \tau + \hat{b}_2 \tau^2 + \ldots.$$

Бирациональное соответствие устанавливает взаимно однозначное соответствие между этими дугами, поэтому и между значениями параметров t и τ. В силу известной теоремы из теории конформных преобразований это означает, что

$$\tau = c_1 t + c_2 t^2 + \ldots, \quad c_1 \neq 0.$$

Пусть теперь T — автоморфизм гиперэллиптической кривой. Допустим, что обычная точка (a, b) кривой переходит в точку $(e_m, 0)$. Тогда

$$\hat{x} = \frac{\alpha + \beta x}{\gamma + \delta x}$$

дает

$$e_m + \tau^2 = \frac{\alpha + \beta(a + t)}{\gamma + \delta(a + t)}.$$

Это означает, что взаимно однозначное соответствие имеется между t и τ^2, что невозможно. По тем же причинам точка $(e_m, 0)$ не может переходит в обычную.

Если порядок n — четный, то точка $(e_m, 0)$ не может переходит в бесконечно удаленную и наоборот. В противном случае из

$$\hat{x} = \frac{\alpha + \beta x}{\gamma + \delta x}$$

следует

$$\frac{1}{\tau} = \frac{\alpha + \beta(e_m + t^2)}{\gamma + \delta(e_m + t^2)},$$

то есть между τ и t^2, а не между τ и t имеется взаимно-однозначное соответствие. В случае, когда порядок n нечетный получается

$$\frac{1}{\tau^2} = \frac{\alpha + \beta(e_m + t^2)}{\gamma + \delta(e_m + t^2)},$$

в чем нет никакого противоречия. □

Лемма 2 означает, что группа $\pi(\mathfrak{G})$ является подгруппой группы всех дробно-линейных преобразований, которая оставляет инвариантным конченое множество точек оси Ox. Если степень многочлена p — четная, то это множество образовано $n = 2\rho + 2$ нулями этого многочлена; если же степень p нечетная, то это множество образовано $n = 2\rho + 1$ нулями многочлена и бесконечно удаленной точкой. Таким образом, в любом случае инвариантное множество состоит из $2\rho + 2$ точек оси Ox.

Доказанное допускает обращение.

Лемма 3. Всякое дробно-линейное преобразование оси Ox, которое оставляет инвариантным множество из $2\rho+2$ точек, образованных нулями многочлена p или нулями и бесконечно удаленной точкой, продолжается до автоморфизма кривой $y^2 = p(x)$ ровно двумя способами.

Доказательство. Рассмотрим для простоты случай, когда степень многочлена p — четная. Пусть дробно-линейное преобразование

$$\hat{x} = \frac{\alpha + \beta x}{\gamma + \delta x}$$

переставляет нули p. Тогда

$$p(\hat{x}) = \prod_m \left(e_m - \frac{\alpha + \beta x}{\gamma + \delta x} \right) = \frac{q(x)}{(\gamma + \delta x)^n}$$

где q — многочлен степени n. Если x совпадает с одном из корней многочлена p, то $\hat{x}$ обладает тем же свойством, поэтому левая часть этого равенства обращается в нуль. Это означает, что q имеет те же нули, что и p, то есть найдется такое число A, что

$$q = Ap$$

Но в таком случае, для любой точке (x, y), лежащей на рассматриваемой кривой, верно

$$p(\hat{x}) = \frac{Ap(x)}{(\gamma + \delta x)^n} = \frac{Ay^2}{(\gamma + \delta x)^n}$$

Это означает, что $p(\hat{x})$ можно представить как квадрат рациональной функции

$$\frac{\sqrt{A}y}{(\gamma + \delta x)^{\frac{n}{2}}};$$

в скобках напомним, что n — четное число.

Рассмотрим теперь преобразование

$$\hat{x} = \frac{\alpha + \beta x}{\gamma + \delta x}, \quad \hat{y} = \frac{\sqrt{A}y}{(\gamma + \delta x)^{\frac{n}{2}}}.$$

Если (x, y) лежит на кривой, то по построению

$$\hat{y}^2 = \frac{Ay^2}{(\gamma + \delta x)^n} = p(\hat{x}),$$

то есть эти формулы задают рациональное отображение рассматриваемой кривой на эту же кривую. Это преобразование является бирациональным, поскольку по заданной точке $(\hat{x}, \hat{y})$ на рассматриваемой кривой мы однозначно определим x из

$$\hat{x} = \frac{\alpha + \beta x}{\gamma + \delta x},$$

а затем, по известным $x, \hat{x}, \hat{y}$, из линейного уравнения

$$\hat{y} = \frac{\sqrt{A}y}{(\gamma + \delta x)^{\frac{n}{2}}}$$

определением и y. Таким образом, мы продолжили заданное дробно-линейное преобразование до бирационального преобразования гиперэллиптической кривой.

Описанный способ оставляет неопределенность в выборе значения корня из A, поэтому всегда имеется два таких автоморфизма. Если бы имелся третий, от них отличный, то все равно выполнялось бы равенство

$$\hat{y}^2 = p(\hat{x}),$$

поэтому число автоморфизмов совпадает с числом способов, которым $p(\hat{x})$ можно представить как квадрат рациональной функции на кривой $y^2 = p(x)$. Нули такой функции определены однозначно, а ее значение в какой либо точки — с точностью до знака, поэтому таких функций не может быть более двух. □

Теперь соберем все леммы вместе.

Теорема 1. Пусть $\mathfrak{G}$ — группа всех бирациональных автоморфизмов гиперэллиптической кривой

$$y^2 = p(x), \quad p \in \mathbb{C}[x]$$

рода ρ. Тогда существует гомоморфизм π группы $\mathfrak{G}$ на группу всех дробно-линейных преобразований оси Ox, оставляющих инвариантным множество Z из $2\rho + 2$ точек оси Ox, обладающий следующими свойствами:

1) если $T \in \mathfrak{G}$ сопоставляет точке (x, y) на кривой точку $(\hat{x}, \hat{y})$ на этой же кривой, то $\pi(T) = Tx$ сопоставляет точке x на проективной прямой точку $\hat{x}$,

2) если $T \in \pi(\mathfrak{G})$, то $\pi^{-1}(T)$ состоит ровно из двух элементов;

3) $\ker \pi$ — циклическая группа $\mathfrak{C}_2$, порожденная преобразованием

$$\hat{x} = x, \quad \hat{y} = -y.$$

При этом инвариантное множество Z образовано или нулями многочлена p, если степень его четная, или нулями этого многочлена и бесконечно удаленной точкой, если его степень нечетная.

Если задана гиперэллиптическая кривая с целыми коэффициентами, то нули многочлена p нетрудно найти как элементы алгебраического замыкания $\mathbb{Q}$, а следовательно, и составить инвариантное множество Z. Группа всех перестановок этого множества $\mathfrak{P}(Z)$ — конечная и за конечное число действий можно проверить, имеется ли дробно-линейное преобразование, осуществляющее перестановку $P \in \mathfrak{P}(Z)$.

В самом деле, пусть дана перестановка

$$P = \begin{pmatrix} e_1 & e_2 & \cdots & e_{2\rho+2} \\ \hat{e}_1 & \hat{e}_2 & \cdots & \hat{e}_{2\rho+2} \end{pmatrix}.$$

Всякое дробно-линейное преобразование проективной прямой сохраняет ангармоническое отношение четырех точек. Поэтому всякое дробно-линейное преобразование однозначно определяется заданием трех пар соответствующих точек, это преобразование дается формулой

$$(e_1, e_2, e_3, x) = (\hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{x}).$$

Выполнение равенств

$$(e_1, e_2, e_3, e_m) = (\hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{e}_m), \quad m = 4, \ldots, 2\rho + 2,$$

является необходимым и достаточным условием инвариантности множества Z. Проверив выполнение этих равенств, мы выясним, существует ли дробно-линейное преобразование, осуществляющее перестановку P.

Алгоритм 1 (построения группы $\mathfrak{G}$)**.** Дано: многочлен $p \in \mathbb{Q}[x]$ степени n с простыми корнями в $\mathbb{C}$. Требуется найти π-проекцию группы бирациональных автоморфизмов кривой $y^2 = p(x)$. Решение:

1) найти корни $e_1, \ldots, e_n \in \overline{\mathbb{Q}}$ уравнения $p(x) = 0$ и составить множество $Z = [e_1, \ldots, e_n]$;

2) если степень p нечетная добавить к множеству Z бесконечно удаленную точку;

3) перебором по всем перестановкам из группы перестановок $\mathfrak{P}(Z)$ найти такие перестановки, для которых верно

$$(e_1, e_2, e_3, e) = (\hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{e}), \quad e \in Z;$$

образовать из них подгруппу $\mathfrak{P}$ в группе $\mathfrak{P}(Z)$, изоморфную группе $\pi(\mathfrak{G})$

4) перестановкам из $\mathfrak{P}$ сопоставить дробно-линейные соответствия по формулам

$$(e_1, e_2, e_3, x) = (\hat{e}_1, \hat{e}_2, \hat{e}_3, \hat{x}),$$

группу всех этих перестановок выдать как $\pi(\mathfrak{G})$;

5) перебором по подстановкам

$$\hat{x} = \frac{\alpha + \beta x}{\gamma + \delta x},$$

из $\pi(\mathfrak{G})$ восстановить

$$\hat{y} = \pm\sqrt{\frac{p(\hat{x})}{p(x)}}y,$$

собрать из этих преобразований $\mathfrak{G}$.

3. Реализация алгоритма в системе Sage

Мы реализовали этот алгоритм в системе компьютерной алгебры Sage в виде пакета Hyperelliptic curves for Sage [19]. Прежде, чем перейти к примерам, сделаем несколько замечаний о реализации алгоритма 1.

Прежде всего, в системе Sage имеется реализация поля $\overline{\mathbb{Q}}$ (QQbar), поэтому 1-ый шаг реализуется дословно так, как написано в алгоритме 1.

На 3-ом шаге мы получаем подгруппы в группе перестановок $2\rho+2$ элементов, изоморфную $\pi(\mathfrak{G})$. В системе Sage имеется хорошо разработанный инструментарий для работы с конечными группами малого порядка [16].

Поэтому у нас в пакете имеется особая функция, которая позволяет вычислить эту группу, дабы открыть доступ к ее исследованию методами, уже встроенными в Sage.

При реализации 5-го шага не возникает никаких затруднений, поскольку система допускает извлечение корня из элементов поля $\overline{\mathbb{Q}}(x)$. На последнем шаге для извлечения корня достаточно указать, что выражение $p(\hat{x})/p(x)$ рассматривается как элемент поля $\overline{\mathbb{Q}}(x)$.

4. Примеры применения пакета Hyperelliptic curves for Sage

Для применения пакета Hyperelliptic curves for Sage [19] следует ввести символьные переменные, которые будут использовать в дальнейшем, и загрузить сам пакет.

```
sage: var('x,y,xx,yy')
(x, y, xx, yy)
sage: load("hyperelliptic-curves.sage")
None
```

В качестве первого примера рассмотрим кривую

$$y^2 = x(x^2 - 1)(x^2 - 4)$$

рода 2. Чтобы описать ее группу автоморфизмов с точностью до изоморфизма, достаточно выполнить первые 3 шага алгоритма. Функция `pi_group_of_automorphisms` возвращает подгруппу в группе перестановок $2\rho + 2$ элементов, изморенную $\pi(\mathfrak{G})$.

```
sage: p=x*(x^2-1)*(x^2-4)
sage: G=pi_group_of_automorphisms(p)
sage: G
Permutation Group with generators [(1,2)(3,6)(4,5),
  (1,4)(2,5)(3,6), (1,5)(2,4)]
```

Стандартные средства Sage/PARI позволяют найти id-код этой группы в таблице групп малого порядка [20]

```
sage: G.group_id()
[4, 2]
```

Следовательно, $\pi(\mathfrak{G})$ — четверная группа Клейна $\mathfrak{C}_2 \times \mathfrak{C}_2$. Ее можно исследовать стандартным средствами Sage:

```
sage: G.is_abelian()
True
sage: G.is_cyclic()
False
sage: order(G)
4
sage: G.list()
[(), (1,5)(2,4), (1,4)(2,5)(3,6), (1,2)(3,6)(4,5)]
```

Список подстановок группы $\pi(\mathfrak{G})$ возвращает другая функция `list_of_substitutions`.

```
sage: list_of_substitutions(p)
[[xx == x, yy == y], [xx == x, yy == -y], [xx == 2/x
  , yy == 2.828427124746190?*y/x^3], [xx == 2/x, yy
  == -2.828427124746190?*y/x^3], [xx == -2/x, yy ==
  2.828427124746190?*I*y/x^3], [xx == -2/x, yy ==
  -2.828427124746190?*I*y/x^3], [xx == -x, yy == I*y
  ], [xx == -x, yy == -I*y]]
```

В качестве второго примера рассмотрим кривую

$$y^2 = x(x^2-1)(x^2-4)(x^2-9)$$

рода 3.

```
sage: p=x*(x^2-1)*(x^2-4)*(x^2-9)
```

```
sage: G=pi_group_of_automorphisms(p)
sage: G.group_id()
[2, 1]
sage: G.is_cyclic()
True
```

Таким образом, $\pi(\mathfrak{G})$ изоморфна циклической группе $\mathfrak{C}_4$.

В качестве 3-го примера рассмотрим многочлен с комплексными корнями.

```
sage: p=x*(x^5-1)
sage: G=pi_group_of_automorphisms(p)
sage: G
Permutation Group with generators [(2,3,6,5,4),
  (2,4,5,6,3), (2,5,3,4,6), (2,6,4,3,5)]
sage: G.group_id()
[5, 1]
sage: G.is_cyclic()
True
```

Таким образом, $\pi(\mathfrak{G})$ — циклическая группа 5-го порядка $\mathfrak{C}_5$.

5. Заключение

В настоящей работе предложен алгоритм 1 решения задачи 1 для класса гиперэллиптических кривых и представлена его реализация в системе компьютерной алгебры Sage. Проделанные эксперименты свидетельствуют о том, что этот алгоритм, даже без распараллеливания, не приводит к чрезмерно сложным вычислениям.

Простота алгоритма и его реализации позволяют с оптимизмом смотреть на перспективы реализации методов алгебраической геометрии в системах компьютерной алгебры и их использовании при конструктивном

решении дифференциальных уравнений.

Список литературы

[1] Hartshorne, R.: Algebraic Geometry. Springer (1977).

[2] Severi, F.: Lezioni di geometria algebrica. Padova, Angelo Graghi, (1908).

[3] Painlevé, P.: Leçons sur la théorie analytique des équations différentielles, professées à Stockholm (septembre, octobre, novembre 1895) sur l'invitation de S. M. le roi de Suède et de Norwège. In: Œuvres de Painlevé, 1, Paris, CNRS (1971)

[4] A. Broughton, T. Shaska, A. Wootton. On automorphisms of algebraic curves // Contemp. Math., 724, pg. 175–212, Amer. Math. Soc., Providence, RI, 2019

[5] Eslam E. Badr and Mohammed A. Saleem: Cyclic Automorphisms groups of genus 10 non-hyperelliptic curves // `https://arxiv.org/abs/1307.1254`. (2013).

[6] Tanush Shaska: Determining the Automorphism Group of a Hyperelliptic Curve // Proceedings of the 2003 international symposium on Symbolic and algebraic computation. P. 248-254 (2003).

[7] Tanush Shaska: SOME SPECIAL FAMILIES OF HYPERELLIPTIC CURVES // Journal of Algebra and Its ApplicationsVol. 03, No. 01, pp. 75-89 (2004) doi: 10.1142/S0219498804000745.

[8] Sevilla, D. and Shaska, T. Hyperelliptic curves with reduced automorphism group A_5 // Applicable Algebra in Engineering, Communication and Computing, 18: 3 (2007). doi: 10.1007/s00200-006-0030-9

[9] Overview of Algcurves package. At: www.maplesoft.com

[10] Stein W. et al. Affine curves. In: Sage Reference Manual (url: doc.sagemath.org), 2019.

[11] Abramov S.A., Petkovšek M. On polynomial solutions of linear partial differential and (q-)difference equations. // Computer Algebra in Scientific Computing. CASC 2012. Lecture Notes in Computer Science. Vol 7442. P.1-11. (2012) doi: 10.1007/978-3-642-32973-9_1

[12] Paramonov S. V. Undecidability of existence of certain solutions of partial differential and difference equations // Computer Algebra in Scientific Computing, Lecture Notes in Computer Science. Vol. 8660. P. 350–356. (2014)

[13] Ayryan E. A., Malykh M. D., Sevastianov L. A., and Yu Ying. On explicit difference schemes for autonomous systems of differential equations on manifolds // Computer Algebra in Scientific Computing, Lecture Notes in Computer Science. Vol. 11520. (2019)

[14] Hurwitz, A.: Über diejenigen algebraischen Gebilde, welche eindeutige Transformationen in sich zulassen // Math. Ann. 32. (1887).

[15] Weierstrass, K.: Mathematische Werke, 4. Berlin, Mayer&Müller (1902).

[16] David Joyner et al. Permutation groups. In: Sage Reference Manual (url: `doc.sagemath.org`)

[17] Zeuthen, H.G.: Lehrbuch der abzählenden Methoden der Geometrie. Leipzig und Berlin, Teubner (1914).

[18] Неванлинна, Р. Униформизация. М. : ИЛ, 1955.

[19] Сайт М.Д. Малых. URL: `https://malykhmd.neocities.org`

[20] Datebase GroupNames.com. URL: `https://people.maths.bris.ac.uk/~matyd/GroupNames`