

О группах автоморфизмов кривых рода $p > 1$

М. Д. Малых

15 августа 2015 г.

1. Введение

Изыскания относительно устройства группа бирациональных автоморфизмов алгебраических кривых рода $p > 1$ были начаты еще во второй половине XIX века, тогда было установлено, что

- эта группа — конечная и ее порядок не превосходит $82(p - 1)$ (Hurwitz, 1893),
- порядок каждого автоморфизма не превосходит $2(2p + 1)$ (Wiman, 1895).

Первый пример кривой, группа автоморфизмов которой имеет максимально допустимый порядок $82(p - 1)$, был указан Клейном, это кватрика

$$x^3y + y^3 + x = 0$$

рода $p = 3$. Позже было установлено, что среди кривых рода $p = 2m^6 + 1$ можно указать и такие, которые имеют максимально возможный порядок $82(p - 1)$ (Macbeath, 1960). С другой стороны, среди кривых рода 3 имеются и такие, которые не допускают нетривиальных автоморфизмов (Walter L. Baily, 1961). Наконец, автоморфизм максимально возможно порядка имеет гиперэллиптическая кривая

$$y^2 = x(x^{2p+1} - 1).$$

Задача о вычислении группы бирациональных автоморфизмов заданной алгебраической кривой средствами компьютерной алгебры была поставлена еще в 1990-х годах, однако оказалась на удивление сложной:

However, it is not an easy task to compute the automorphism group of a given algebraic curve. Even compiling a list of possible candidates for a small genus g is quite difficult. In *Magaard et al.*, 2003 we provide an algorithm which computes such lists. We give a complete list for $g = 3$ and list «large» groups for $g \leq 10$. This work is based on previous work of Breuer, among many others. — Tanush Shaska, 2003.

Трудность задачи заставила авторов обратиться к простейшим случаям, в особенности к гиперэллиптическим кривым. Хотя вычислительные трудности постоянно подталкивали этих исследователей к привлечению систем компьютерной алгебры, в нашем распоряжении нет свободного пакета, позволяющего вычислить группу авторфизмов заданной кривой, а, вероятно, и алгоритма, годного для всех кривых. Последнее особенно удивительно, поскольку в редко цитируемой работе Гурвица (Hurwitz, 1887), предшествующей всеми поминаемой работе 1893 года, имеются размышления, которые можно превратить в таковой. Перескажем эту работу современным языком.

2. Гомоморфизм Гурвица

Пусть F — произвольная плоская алгебраическая кривая рода $p > 1$, заданная в некоторой декартовой системе координат уравнением

$$F(x, y) = 0$$

с рациональными коэффициентами, и пусть $\text{Bir}(F)$ — группа бирациональных автоморфизмов этой кривой. Обозначим как

$$H_1(x, y)dx, \dots, H_p(x, y)dx$$

базис линейного пространства L дифференциалов, всюду конечных на F . Для любого автоморфизма T из $\text{Vir}(F)$ абелевы интегралы

$$\int_0^{T(x,y)} H_i(\xi, \eta) d\xi$$

как функции точки (x, y) на F является всюду конечным, поэтому

$$\int_0^{T(x,y)} H_i(\xi, \eta) d\xi = \sum_{j=1}^p \pi_{ij} \int_0^{(x,y)} H_j(\xi, \eta) d\xi + \pi_i \quad (i = 1, \dots, p),$$

где матрица π_{ij} и столбец π_i зависят от T , но не от x и y . Сопоставление автоморфизму T матрицы $\pi(T)$ задает гомоморфизм

$$\text{Vir}(F) \rightarrow \text{Gl}(p, \mathbb{C}).$$

В работе Гурвица исследуются свойства этого гомоморфизма, который мы далее будем называть гомоморфизмом Гурвица.

Теорема 1 (Hurwitz, 1887). Если род p кривой F больше единицы, то гомоморфизм Гурвица является мономорфизмом, то есть

$$0 \rightarrow \text{Vir}(F) \rightarrow \text{Gl}(p, \mathbb{C}),$$

причем матрица, служащая образом любого автоморфизма, приводится к диагональной матрице, на главной диагонали которой стоят корни из единицы, то есть

$$T \sim \text{diag}(\varepsilon_1, \dots, \varepsilon_p), \quad \varepsilon_j = \sqrt[p]{1}.$$

Мы приведем здесь ее доказательство, поскольку используемая в нем конструкция и позволит вычислить группу автоморфизмов.

Доказательство. Первое утверждение сразу получается из теоремы Абеля. В самом деле, пусть T переходит в единичную матрицу, тогда

$$\int_{(x,y)}^{T(x,y)} H_i(\xi, \eta) d\xi = \pi_i \quad (i = 1, \dots, p).$$

Тогда для любых двух точек (x_1, y_1) и (x_2, y_2) справедливо равенство

$$\int_{(x_1, y_1)}^{T(x_1, y_1)} H_i(\xi, \eta) d\xi + \int_{(x_2, y_2)}^{T^{-1}(x_2, y_2)} H_i(\xi, \eta) d\xi = 0 \quad (i = 1, \dots, p),$$

которое в силу теоремы Абелея означает, что существует рациональная функция 2-ой степени, полюсами которой служат эти две точки. Но это означает, что род кривой против предположения строго меньше 2.

Для доказательства второго, приведем матрицу π к Жордановой форме. Для краткости обозначим штрихом образ элемента под действием преобразования T . При надлежащем выборе базиса пространства L , можно принять, что

$$\begin{cases} H'_1 dx' = \varepsilon_1 H_1 dx \\ H'_2 dx' = \varepsilon_2 H_2 dx + \eta H_1 dx \\ \dots \end{cases}$$

Здесь ε_1, \dots — собственные значения матрицы π , а число η равно нулю, если $\varepsilon_2 \neq \varepsilon_1$. Зная базис, можно подобрать две рациональные функции, которые при преобразовании T испытывают линейную подстановку. Именно, возьмем

$$z = \frac{H_2 dx}{H_1 dx}, \quad s = \frac{H_1 dx}{dz},$$

тогда

$$z' = \frac{H'_2 dx'}{H'_1 dx'} = \frac{\varepsilon_2 H_2 dx + \eta H_1 dx}{\varepsilon_1 H_1 dx} = \alpha z + \beta$$

и

$$s' = \frac{H'_1 dx'}{dz'} = \frac{\varepsilon_1 H_1 dx}{adz} = \gamma s',$$

где

$$\alpha = \frac{\varepsilon_2}{\varepsilon_1}, \quad \beta = \frac{\eta}{\varepsilon_1}, \quad \gamma = \frac{\varepsilon_1^2}{\varepsilon_2}.$$

Эти две функции на кривой связаны некоторым неприводимым соотношением

$$G(s, z) = 0,$$

род которого строго больше нуля, поскольку

$$\int sdz = \int H_1 dx$$

является интегралом 1-го рода на G . Под действием преобразования T , нуль переходит в нуль, поэтому

$$0 = TG(s, z) = G(\gamma s, \alpha z + \beta).$$

Это означает, что равенство

$$G(\gamma s, \alpha z + \beta) = 0$$

справедливо во всех комплексных точках кривой $G(s, z) = 0$, и поэтому

$$G(\gamma s, \alpha z + \beta) = \text{const.}G(s, z)$$

как полиномы двух переменных.

Если $\beta \neq 0$, то $a = \frac{\varepsilon_2}{\varepsilon_1} = 1$, поэтому

$$G(\gamma s, z + 1) = \text{const.}G(s, z).$$

Коэффициент при i -ой степени s тогда удовлетворяет тождеству

$$\varphi_i(z + 1) = \text{const.}\varphi_i(z).$$

Если i -ый коэффициент зависит от z , то $\varphi_i(z) = 0$ имеет хотя бы один корень, а следовательно и бесконечно много, что невозможно. Поэтому коэффициенты G при всех степенях s не зависят от z и уравнение сводится к $G(s) = 0$, что невозможно. Поэтому всегда $\beta = 0$, то есть матрицу преобразования всегда можно привести к диагональному виду.

Обратимся теперь к соотношению

$$G(\gamma s, \alpha z) = \text{const.}G(s, z).$$

Подстановка увеличивает коэффициент при $s^\nu z^\mu$ на $\gamma^\nu \alpha^\mu$, поэтому

$$\gamma^\nu \alpha^\mu = \gamma^{\nu'} \alpha^{\mu'}$$

для всех степеней, входящих в G с ненулевыми коэффициентами. Отсюда

$$\gamma^{\nu-\nu'} = \alpha^{\mu-\mu'}.$$

Поэтому можно подобрать такое комплексное число t , что

$$\gamma = t^q, \quad \alpha = t^r,$$

где q и r обозначают некоторые целые числа. Если t не является корнем из единицы, то

$$t^{q\nu+r\mu} = t^{q\nu'+r\mu'}$$

влечет

$$q\nu + r\mu = q\nu' + r\mu'.$$

В этом случае, все решения уравнения $G(s, z) = 0$ можно выразить через одно (s_0, z_0) , положив

$$\begin{cases} s = s_0\lambda^q, \\ z = z_0\lambda^r, \end{cases}$$

где λ — параметр. Таким образом кривая G допускает рациональную параметризацию, и поэтому ее род равен нулю, что невозможно. Таким образом, t — обязательно корень из единицы. Остается заметить, что в таком случае

$$\varepsilon_1 = \alpha\gamma = t^{q+r}, \quad \varepsilon_2 = \alpha\varepsilon_1$$

тоже являются корнями из единицы. Итак,

$$\pi \sim \text{diag}(\varepsilon_1, \dots, \varepsilon_p),$$

где ε_i — корни из единицы. □

Гурвиц далее употребляет эту теорему как вспомогательное средство для получения оценок на порядки элементов. Однако сама теорема много интереснее этих приложений, которые теперь получают иначе и проще.

3. Уравнение Гурвиуп

Пусть нам задана кривая

$$F(x, y) = 0$$

с рациональными коэффициентами. Мы можем вычислить ее род и некоторый базис пространства дифференциалов, всюду конечных на F , напр., в пакете **Algcurves** в системе Maple.

Введем два набора a_1, \dots, a_p и b_1, \dots, b_p новых переменных и положим, как и в доказательстве теоремы Гурвица

$$z = \frac{\beta_1 H_1 + \dots + \beta_p H_p}{\alpha_1 H_1 + \dots + \alpha_p H_p}, \quad s = \frac{(\alpha_1 H_1 + \dots + \alpha_p H_p) dx}{dz}.$$

Как известно, базис составляют элементы вида

$$H_i dx = \frac{Q_i}{\frac{\partial F}{\partial y}} dx, \quad (i = 1, \dots, p)$$

где Q_i — многочлен относительно x и y , задающий сопряженную кривую к F . Поэтому, воспользовавшись формулой

$$\frac{dz}{dx} = \frac{\partial z}{\partial x} - \frac{\partial z}{\partial y} \frac{\partial F}{\partial x} : \frac{\partial F}{\partial y},$$

эти формулы можно существенно упростить:

$$z = \frac{\beta_1 Q_1 + \dots + \beta_p Q_p}{\alpha_1 Q_1 + \dots + \alpha_p Q_p}, \quad s = \frac{\alpha_1 Q_1 + \dots + \alpha_p Q_p}{\frac{\partial z}{\partial x} \frac{\partial F}{\partial y} - \frac{\partial z}{\partial y} \frac{\partial F}{\partial x}}. \quad (1)$$

Исключая x, y из системы

$$\begin{cases} (\alpha_1 Q_1 + \dots + \alpha_p Q_p) z = \beta_1 Q_1 + \dots + \beta_p Q_p, \\ \left(\frac{\partial z}{\partial x} \frac{\partial F}{\partial y} - \frac{\partial z}{\partial y} \frac{\partial F}{\partial x} \right) s = \alpha_1 Q_1 + \dots + \alpha_p Q_p, \\ F(x, y) = 0, \end{cases}$$

получим уравнение

$$G(s, z; \alpha_1, \dots, \beta_p) = 0,$$

которое дальше будем называть общим уравнением Гурвица. В некоторых особых случаях, числители и знаменатели функций z и s имеют общие

нули, и поэтому система совместна при всех значениях s и z . Во избежании этих трудностей, примем след.:

Определение 1. Уравнением Гурвица будем называть неприводимое уравнение, которому удовлетворяют функции s и z , заданные формулами (1), на открытом в топологии Зарисского подмножестве кривой F .

Теоретически, используя технику исключаящих идеалов, можно составить уравнения Гурвица для любой заданной кривой. С этой целью мы зададим в Sage функцию `hurwitz_equation(F,V1,V2)`, аргументами которой служит левая часть уравнения нашей кривой, $V_1 = \sum a_i Q_i$ и $V_2 = \sum b_i Q_i$:

```
def hurwitz_equation(F,V1,V2):
    Z=V2/V1
    S=V1/(diff(Z,x)*diff(F,y)-diff(Z,y)*diff(F,x))
    Gz=(A*[z*denominator(Z)-numerator(Z),F]).elimination_ideal(y).gen(0)
    Gs=(A*[s*denominator(S)-numerator(S),F]).elimination_ideal(y).gen(0)
    if gcd(Gz,Gs) in CC:
        I=A*[z*denominator(Z)-numerator(Z),s*denominator(S)-numerator(S),F]
        G=I.elimination_ideal([x,y]).gen(0)
    else:
        I=(A*[Gz/gcd(Gz,Gs),Gs/gcd(Gz,Gs)]).elimination_ideal(x)
        G=I.gen(0)
    GG=list(factor(G))[len(list(factor(G)))-1][0]
    return GG
```

Пример 1. Воспользовавшись пакетом `Algcurves`, легко видеть, что кривая

$$x^3y + x^2 + y^2 + 1 = 0 \quad (2)$$

имеет род 2, а базисом пространства дифференциалов 1-го типа служат

$$\frac{dx}{x^3 + 2y}, \quad \frac{xdx}{x^3 + 2y},$$

в их числителе которых стоят многочлены

$$Q_1 = 1, \quad Q_2 = x.$$


```

sage: A.<x,y,z,s,a1,a2,b1,b2>=PolynomialRing(QQ,4+4) 1
sage: F=x^3*y+x^2+y^2+1 2
sage: hurwitz_equation(F,a1+a2*x,b1+b2*x) 3
-z^6*s^2*a1^6 + 4*z^6*s^2*a1^2*a2^4 + 4*z^6*s^2*a2^6 4
+ 6*z^5*s^2*a1^5*b1 - 8*z^5*s^2*a1*a2^4*b1 - 16*z
^5*s^2*a1^2*a2^3*b2 - 24*z^5*s^2*a2^5*b2 - 15*z^4*s
^2*a1^4*b1^2 + 4*z^4*s^2*a2^4*b1^2 + 32*z^4*s^2*
a1*a2^3*b1*b2 + 24*z^4*s^2*a1^2*a2^2*b2^2 + 60*z
^4*s^2*a2^4*b2^2 + 20*z^3*s^2*a1^3*b1^3 - 16*z^3*s
^2*a2^3*b1^2*b2 - 48*z^3*s^2*a1*a2^2*b1*b2^2 - 16*
z^3*s^2*a1^2*a2*b2^3 - 80*z^3*s^2*a2^3*b2^3 - 15*z
^2*s^2*a1^2*b1^4 + 24*z^2*s^2*a2^2*b1^2*b2^2 + 32*
z^2*s^2*a1*a2*b1*b2^3 + 4*z^2*s^2*a1^2*b2^4 + 60*z
^2*s^2*a2^2*b2^4 + 6*z*s^2*a1*b1^5 - 16*z*s^2*a2*
b1^2*b2^3 - 8*z*s^2*a1*b1*b2^4 - 24*z*s^2*a2*b2^5
+ a2^4*b1^4 - s^2*b1^6 - 4*a1*a2^3*b1^3*b2 + 6*a1
^2*a2^2*b1^2*b2^2 - 4*a1^3*a2*b1*b2^3 + a1^4*b2^4
+ 4*s^2*b1^2*b2^4 + 4*s^2*b2^6

```

Для наглядности составим для него диаграмму Ньютона, которую будем называть диаграммой Гурвица для кривой (1), см. рис. 3. Процесс исключения переменных — трудоемкий, поэтому предусмотрена возможность составить частное уравнение Гурвица, минуя составление общего. Напр.,

```

sage: A.<x,y,z,s,a1,a2,b1,b2>=PolynomialRing(QQ,4+4) 5
sage: F=x^3*y+x^2+y^2+1 6
sage: hurwitz_equation(F,1,x) 7
z^6*s^2 - 4*z^2*s^2 - 4*s^2 - 1 8

```

Среди уравнений небольших степеней, к сожалению, имеются и такие, для которых составить общее уравнение Гурвица не удастся.

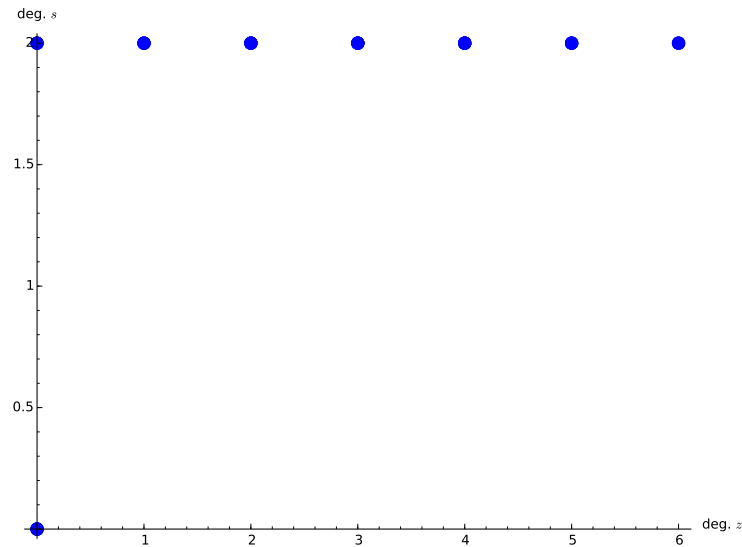


Рис. 1. Диаграмма Гурвица для кривой (2).

Пример 2. Вероятно простейшим из них является

$$y^3 + x^4 + x^2 = 0.$$

Это уравнение задает кривую рода 2,

$$Q_1 = x, \quad Q_2 = y;$$

упоминается в справке к пакету `Algsurves` как пример кривой с явно вычисляемой матрицей Римана. Для этой кривой составить общее уравнение Гурвица не удастся, а в частных уравнения получаются на удивление большие числовые коэффициенты:

```

sage: A.<x,y,z,s>=PolynomialRing(QQ,4)          9
sage: F=y^3+x^4+x^2                             10
sage: hurwitz_equation(F,x+2*y,63*x+y).coefficient({ 11
    s:0,z:0})
16796099217572151063328729                       12
sage: hurwitz_equation(F,x+2*y,63*x+y).coefficient({ 13
    s:2,z:0})
-8000756592040586027514531250                   14

```

4. Отыскание автоморфизмов заданной кривой при помощи общего уравнения Гурвица

Если кривая F допускает автоморфизм $T \sim \text{diag}(\varepsilon_1, \varepsilon_2, \dots)$, то в некотором базисе пространства всюду конечных дифференциалов образ T будет диагональной матрицей, то есть

$$H'_i(x', y')dx' = \varepsilon_i H'_i(x, y)dx \quad (i = 1, \dots, p)$$

Приняв в качестве значения параметров a_1, \dots, b_p такие числа, что

$$H'_1(x, y)dx = a_1 H_1(x, y)dx + \dots + a_p H_p(x, y)dx$$

$$H'_2(x, y)dx = b_1 H_1(x, y)dx + \dots + b_p H_p(x, y)dx$$

мы получим частное уравнение Гурвица, которое, как видно из доказательства теоремы 1, должно удовлетворять соотношению

$$G(\gamma s, \alpha z) = \text{const.} G(s, z).$$

Отсюда:

Теорема 2. Если кривая F допускает автоморфизм $T \sim \text{diag}(\varepsilon_1, \varepsilon_2, \dots)$, то параметры α_1, \dots, β_p можно подобрать таким образом, чтобы частное уравнение Гурвица удовлетворяло тождеству

$$G(\gamma s, \alpha z) = \delta G(s, z), \tag{3}$$

где

$$\alpha = \frac{\varepsilon_2}{\varepsilon_1}, \quad \gamma = \frac{\varepsilon_1^2}{\varepsilon_2},$$

а δ — произведение некоторых степеней ε_1 и ε_2 .

Эту теорему нетрудно превратить в алгоритм отыскания автоморфизмов заданного порядка.

Алгоритм 1. Чтобы получить список автоморфизмов заданного порядка N заданной кривой $F(x, y) = 0$, следует:

- 1) вычислить ее род p и базис пространства дифференциалов Q_1, \dots, Q_p ;
- 2) составить общее уравнение Гурвица $G(s, z; a_1, \dots, b_p) = 0$;
- 3) приравнять коэффициенты при одинаковых степенях s и z в левой и правой частях равенства (3) и получить систему (S) для отыскания параметров;
- 4) перебрать все возможные комбинации значений $\varepsilon_1, \varepsilon_2$ и δ среди корней N -го порядка и выписать все случаи, когда система (S) совместна и дает линейно независимые $\sum a_i Q_i(x, y)$ и $\sum b_i Q_i(x, y)$;
- 5) для каждого из указанных случаев проверить, задает ли система

$$\begin{cases} \frac{\sum a_i Q_i(x', y') dx'}{F_y(x', y')} = \varepsilon_1 \frac{\sum a_i Q_i(x, y) dx}{F_y(x, y)}, \\ \frac{\sum b_i Q_i(x', y') dx'}{F_y(x', y')} = \varepsilon_2 \frac{\sum b_i Q_i(x, y) dx}{F_y(x, y)}, \end{cases}$$

автоморфизм порядка N . Неподходящие случаи исключить из составленного списка.

Чтобы вычислить всю группу автоморфизмов заданной кривой, достаточно по заданному алгоритму отыскать все автоморфизмы до $2(2p + 1)$ порядка включительно.

Дабы не испытывать известные трудности при манипулировании с однородными идеалами, заметим следующее. Поскольку базис пространства всюду конечных дифференциалов, в котором матрица $\pi(T)$ имеет диагональный вид, определен с точностью до перестановки элементов и умножения их на число, не ограничивая общности рассмотрения, можно взять $\alpha_1 = \beta_2 = 1$ и тем самым перейти от однородных координат к аффинным.

При $p = 2$ это означает, что мы ограничимся дифференциалами

$$(Q_1 + \alpha Q_2) \frac{dx}{F_y}, \quad (\beta Q_1 + Q_2) \frac{dx}{F_y}.$$

При этом замена $\alpha = \frac{1}{\beta'}$ и $\beta = \frac{1}{\alpha'}$ дает дифференциалы, отличающиеся на постоянный множитель, поэтому под действием T они испытывают тоже умножение на ε_i . Наконец, случай, когда $\alpha\beta = 1$ следует исключить

из рассмотрения, поскольку тогда получаются линейно зависимые дифференциалы. Поскольку во всех рассматриваемых ниже примерах равенство $\delta = 1$ было очевидно, мы не стали реализовать перебор по этой переменной и описали 3-ий пункт алгоритма так:

```
def hurwitz_untrivial2(l):
    ll=[]
    for n in range(0,len(l)):
        if a.subs(l[n][0])*b.subs(l[n][1])!=1:
            ll.append(l[n])
    return ll

def hurwitz_solution(G,e1,e2,e3):
    a,b=var('a,b')
    alpha=e2/e1
    gamma=e1^2/e2
    l=G.exponents()
    eq=[G.coefficient({z:l[n][2],s:l[n][3]})*(alpha^(l[n][2])*gamma^(l[n][3])-e3) for n in l]
    return hurwitz_untrivial2(solve(eq,[a,b]))

def hurwitz_transformation(G,N):
    n,m=var('n,m')
    eps=exp(2*pi*i/N)
    l=[]
    for n in range(N):
        for m in range(N):
            solution=hurwitz_solution(G,eps^n,eps^m,1)
            if solution != []:
                l.append([eps^n,eps^m,solution])
    return l
```

Рассмотрим подробно один простой пример.

Пример 3. Гиперэллиптическая кривая

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

имеет род 2, а базисом пространства дифференциалов 1-го типа служит

$$\frac{dx}{y}, \quad \frac{x dx}{y};$$

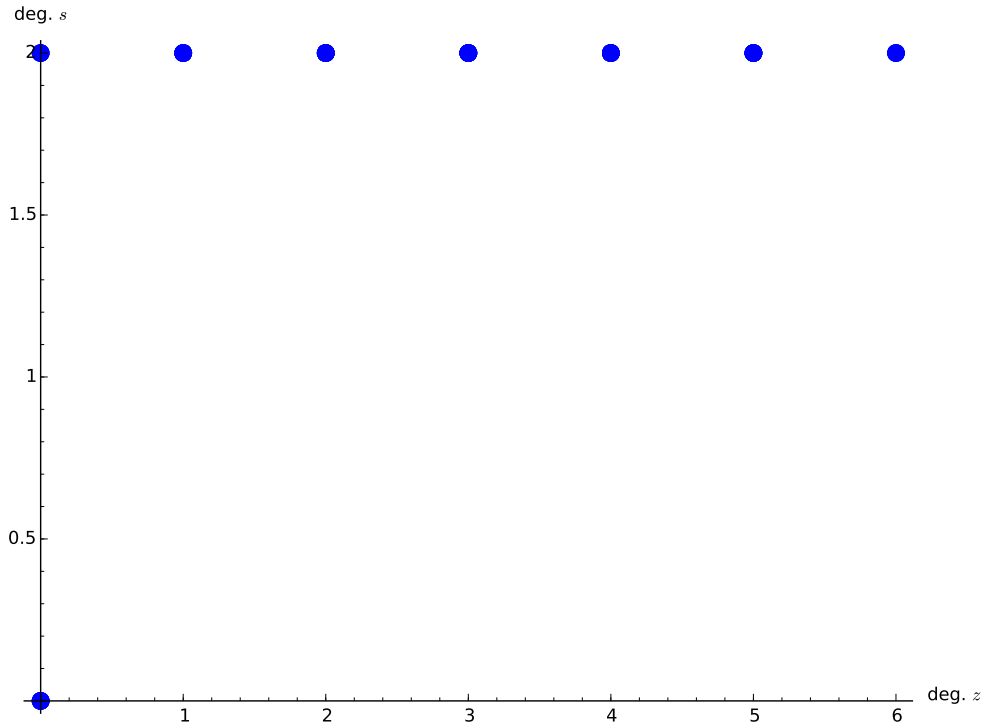


Рис. 2. Диаграмма Гурвица для кривой $y^2 = x(x^2 - 1)(x^2 - 4)$.

в их числителе стоят многочлены

$$Q_1 = 1, \quad Q_2 = x.$$

Составим для этой кривой общее уравнение Гурвица:

```
sage: A.<x,y,z,s,a,b>=PolynomialRing(QQ,4+2) 15
```

```
sage: F=y^2-x*(x^2-1)*(x^2-4) 16
```

```
sage: G=hurwitz_equation(F,1+a*x,b+x) 17
```

Мы не стали выводить на печать это весьма длинное уравнение, структуру которого проще понять, взглянув на диаграмму 3.

Свободный член уравнения Гурвица равен

```
sage: G.coefficient({z:0,s:0}).factor() 18
```

```
(-1) * (a*b - 1)^4 19
```

и потому он обратится в нуль лишь тогда, когда $ab = 1$. Этот случай мы должны исключить из рассмотрения, поэтому равенство

$$G(\gamma s, \alpha z; a, b) = \delta G(s, z; a, b)$$

может выполняться тождественно по s и z лишь в том случае, когда $\delta = 1$.

Отыщем преобразования второго порядка:

```
sage: hurwitz_transformation(G,2) 20
[[1, 1, [[a == r2, b == r1]]], [1, -1, [[a == 1/2* 21
sqrt(2), b == -sqrt(2)], [a == -1/2*sqrt(2), b ==
sqrt(2)], [a == -1/2*I*sqrt(2), b == -I*sqrt(2)],
[a == 1/2*I*sqrt(2), b == I*sqrt(2)]]], [-1, 1, [[
a == 1/2*sqrt(2), b == -sqrt(2)], [a == -1/2*sqrt
(2), b == sqrt(2)], [a == -1/2*I*sqrt(2), b == -I*
sqrt(2)], [a == 1/2*I*sqrt(2), b == I*sqrt(2)]]],
[-1, -1, [[a == r4, b == r3]]]]
```

Первое из названных преобразований, эквивалентно E , а потому является тождественным преобразованием, исключаем его из списка. Последнее преобразование эквивалентно $-E$, эта матрица в любом базисе будет диагональной, поэтому и получилось, что a и b могут быть любыми. Взяв $a = b = 0$, имеем

$$\begin{cases} \frac{dx'}{y'} = -\frac{dx}{y}, \\ \frac{x'dx'}{y'} = -\frac{xdx}{y}, \end{cases}$$

откуда

$$x' = x, \quad y' = -y.$$

Это преобразование действительно является автоморфизмом кривой (4) порядка 2.

Обратимся теперь к преобразованиям, эквивалентным $\text{diag}(1, -1)$. Первое из них дает

$$\begin{cases} \left(1 + \frac{x'}{\sqrt{2}}\right) \frac{dx'}{y'} = \left(1 + \frac{x}{\sqrt{2}}\right) \frac{dx}{y} \\ \left(x' - \sqrt{2}\right) \frac{dx'}{y'} = -\left(x - \sqrt{2}\right) \frac{dx}{y} \end{cases}$$

Поделив первое уравнение на второе, получим

$$\frac{x' + \sqrt{2}}{x' - \sqrt{2}} = \frac{x + \sqrt{2}}{x - \sqrt{2}}$$

или

$$x' = \frac{2}{x}.$$

Это преобразование оси Ox можно продолжить до двух автоморфизмов кривой. В самом деле, подставляя это выражение вместо x' в соотношение

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

получим

$$y'^2 = \frac{8(4 - x^2)(1 - x^2)}{x^5} = \frac{8y^2}{x^6}.$$

Поэтому два преобразования

$$\begin{cases} x' = \frac{2}{x}, \\ y' = \pm \frac{2\sqrt{2}y}{x^3} \end{cases}$$

действительно задают автоморфизмы кривой порядка 2, эквивалентные $\text{diag}(1, -1)$ и $\text{diag}(-1, 1)$.

Второй набор значений отличается от первого знаком и не дает ничего нового, исключаем его из списка.

Третий набор дает

$$\begin{cases} \left(1 - \frac{ix'}{\sqrt{2}}\right) \frac{dx'}{y'} = \left(1 - \frac{ix}{\sqrt{2}}\right) \frac{dx}{y} \\ (x' - i\sqrt{2}) \frac{dx'}{y'} = -(x - i\sqrt{2}) \frac{dx}{y} \end{cases}$$

У нас действительно имеются такие преобразования:

$$\begin{cases} x' = -\frac{2}{x}, \\ y' = \pm \frac{2\sqrt{2}iy}{x^3}, \end{cases}$$

эквивалентные $\text{diag}(1, -1)$ и $\text{diag}(-1, 1)$.

Четвертый набор опять не дает нового преобразования.

Преобразования, эквивалентные $\text{diag}(1, -1)^2$, мы уже получили как квадраты двух найденных преобразований.

Преобразований третьего порядка нет:


```
sage: hurwitz_transformation(G,3) 22
[[1, 1, [[a == r6, b == r5]]]] 23
```

В списке возможных преобразований 4-го порядка:

```
sage: hurwitz_transformation(G,4) 24
[[1, 1, [[a == r8, b == r7]]], [1, -1, [[a == 1/2* 25
sqrt(2), b == -sqrt(2)], [a == -1/2*sqrt(2), b ==
sqrt(2)], [a == -1/2*I*sqrt(2), b == -I*sqrt(2)],
[a == 1/2*I*sqrt(2), b == I*sqrt(2)]]], [I, -I, [[
a == 0, b == 0]]], [-1, 1, [[a == 1/2*sqrt(2), b
== -sqrt(2)], [a == -1/2*sqrt(2), b == sqrt(2)], [
a == -1/2*I*sqrt(2), b == -I*sqrt(2)], [a == 1/2*I
*sqrt(2), b == I*sqrt(2)]]], [-1, -1, [[a == r10,
b == r9]]], [-I, I, [[a == 0, b == 0]]]]
```

имеются только два, порядок которых равен 4, а не 2, это преобразование $\sim \text{diag}(i, i)$ и его куб. Это преобразование, если оно и правда имеется, дается формулами

$$\begin{cases} \frac{dx'}{y'} = i \frac{dx}{y} \\ \frac{x'dx'}{y'} = -i \frac{xdx}{y} \end{cases}$$

откуда

$$x' = -x, \quad y' = iy.$$

Разумеется, такое преобразование действительно является автоморфизмом кривой.

От 5 до 10 нам не попадаетея ничего нового:

```
sage: hurwitz_transformation(G,5) 26
[[1, 1, [[a == r12, b == r11]]]] 27
sage: hurwitz_transformation(G,6) 28
[[1, 1, [[a == r14, b == r13]]], [1, -1, [[a == 1/2* 29
sqrt(2), b == -sqrt(2)], [a == -1/2*sqrt(2), b ==
```

```

sqrt(2)], [a == -1/2*I*sqrt(2), b == -I*sqrt(2)],
[a == 1/2*I*sqrt(2), b == I*sqrt(2)]]], [-1, 1, [[
a == 1/2*sqrt(2), b == -sqrt(2)], [a == -1/2*sqrt
(2), b == sqrt(2)], [a == -1/2*I*sqrt(2), b == -I*
sqrt(2)], [a == 1/2*I*sqrt(2), b == I*sqrt(2)]]],
[-1, -1, [[a == r16, b == r15]]]]
sage: hurwitz_transformation(G,7) 30
[[1, 1, [[a == r18, b == r17]]]] 31
sage: hurwitz_transformation(G,8) 32
[[1, 1, [[a == r20, b == r19]]], [1, -1, [[a == 1/2* 33
sqrt(2), b == -sqrt(2)], [a == -1/2*sqrt(2), b ==
sqrt(2)], [a == -1/2*I*sqrt(2), b == -I*sqrt(2)],
[a == 1/2*I*sqrt(2), b == I*sqrt(2)]]], [I, -I, [[
a == 0, b == 0]]], [-1, 1, [[a == 1/2*sqrt(2), b
== -sqrt(2)], [a == -1/2*sqrt(2), b == sqrt(2)], [
a == -1/2*I*sqrt(2), b == -I*sqrt(2)], [a == 1/2*I
*sqrt(2), b == I*sqrt(2)]]], [-1, -1, [[a == r22,
b == r21]]], [-I, I, [[a == 0, b == 0]]]]
sage: hurwitz_transformation(G,9) 34
[[1, 1, [[a == r24, b == r23]]]] 35
sage: hurwitz_transformation(G,10) 36
[[1, 1, [[a == r26, b == r25]]], [1, -1, [[a == 1/2* 37
sqrt(2), b == -sqrt(2)], [a == -1/2*sqrt(2), b ==
sqrt(2)], [a == -1/2*I*sqrt(2), b == -I*sqrt(2)],
[a == 1/2*I*sqrt(2), b == I*sqrt(2)]]], [-1, 1, [[
a == 1/2*sqrt(2), b == -sqrt(2)], [a == -1/2*sqrt
(2), b == sqrt(2)], [a == -1/2*I*sqrt(2), b == -I*
sqrt(2)], [a == 1/2*I*sqrt(2), b == I*sqrt(2)]]],
[-1, -1, [[a == r28, b == r27]]]]

```

Итак, все автоморфизмы кривой (4) перечислены в таблице:

Преобразование	Экв. матрица	Порядок
$x' = x, y' = y$	$\text{diag}(1, 1)$	1
$x' = x, y' = -y$	$\text{diag}(-1, -1)$	2
$x' = \frac{2}{x}, y' = \frac{2\sqrt{2}y}{x^3}$	$\text{diag}(1, -1)$	2
$x' = \frac{2}{x}, y' = \frac{2\sqrt{2}y}{x^3}$	$\text{diag}(1, -1)$	2
$x' = \frac{2}{x}, y' = -\frac{2\sqrt{2}y}{x^3}$	$\text{diag}(-1, 1)$	2
$x' = -\frac{2}{x}, y' = \frac{2\sqrt{2}iy}{x^3}$	$\text{diag}(1, -1)$	2
$x' = -\frac{2}{x}, y' = -\frac{2\sqrt{2}iy}{x^3}$	$\text{diag}(-1, 1)$	2
$x' = -x, y' = iy$	$\text{diag}(i, i)$	4
$x' = -x, y' = -iy$	$\text{diag}(-i, -i)$	4

Эта группа порождается двумя элементами

$$T : x' = -x, y' = iy$$

и

$$R : x' = \frac{2}{x}, y' = \frac{2\sqrt{2}y}{x^3}$$

и поэтому ее можно описать так:

$$\langle T, R : T^4 = R^2 = (TR)^2 = (T^{-1}R)^2 = E \rangle$$