

# Десять «детских рисунков» Клейна степени 11: тема с вариациями

Г. А. ДЖОНС

Саутгемптонский университет, Великобритания  
e-mail: G.A.Jones@maths.soton.ac.uk

А. К. ЗВОНКИН

Университет Бордо, Франция  
e-mail: zvonkin@labri.fr

УДК 512.542.74

**Ключевые слова:** плоское дерево, детский рисунок, карта, группа монодромии, проективные группы простой степени, группы, содержащие цикл, рисунки на эллиптических кривых, функции Белого, гипотеза Бейтмана–Хорна.

## Аннотация

В статье дана современная интерпретация идей статьи Ф. Клейна о преобразованиях степени 11, основанная на теории детских рисунков. Мы развиваем далее эти идеи, рассматривая рисунки типа  $(3, 2, p)$  и степени  $p$  или  $p + 1$ , где  $p$  — простое число. Во многих случаях мы находим их паспорта и группы монодромии. В примерах, где степень невелика, мы приводим и сами рисунки с правильной топологической, а иногда и метрической структурой. Мы используем гипотезу Бейтмана–Хорна и обширный компьютерный эксперимент для подтверждения гипотезы о том, что существует бесконечно много простых чисел вида  $p = (q^n - 1)/(q - 1)$ , где  $q$  — степень простого числа. Это, в свою очередь, означает, что имеется бесконечно много групп  $\mathrm{PSL}_n(q)$ , реализуемых в виде групп перестановок и групп монодромии степени  $p$  (открытая проблема в теории групп).

## Abstract

*G. A. Jones, A. K. Zvonkin, Klein's ten "dessins d'enfants" of degree 11: theme with variations, Fundamentalnaya i prikladnaya matematika, vol. 25 (2024), no. 2, pp. 103–175.*

We reinterpret ideas in Klein's paper on transformations of degree 11 from the modern point of view of dessins d'enfants, and extend his results by considering dessins of type  $(3, 2, p)$  and degree  $p$  or  $p + 1$ , where  $p$  is prime. In many cases, we determine the passports and monodromy groups of these dessins, and in a few small cases we give drawings which are topologically (or, in certain examples, even geometrically) correct. We use the Bateman–Horn conjecture and extensive computer searches to support the conjecture that there are infinitely many primes of the form  $p = (q^n - 1)/(q - 1)$  for some prime power  $q$ , in which case infinitely many groups  $\mathrm{PSL}_n(q)$  arise as permutation groups and monodromy groups of degree  $p$  (an open problem in group theory).

*Эта статья посвящается нашему другу и коллеге  
Георгию Борисовичу Шабату*

## 1. Введение

В 1878—1879 годах Ф. Клейн опубликовал две статьи [54, 55] с почти идентичными названиями. В первой статье изучались уравнения степени 7, во второй — степени 11. При этом существенную роль играли свойства и действия групп  $\mathrm{PSL}_2(p)$  при  $p = 7$  и  $p = 11$  соответственно. Статья [54] заслуженно знаменита — не в последнюю очередь благодаря введённой в ней так называемой Hauptfigur (нем. «главная фигура»), хрестоматийному изображению замощения гиперболического 14-угольника, который после отождествления его сторон даёт комплексную кривую степени 4 и рода 3, называемую кватрикой Клейна (см., в частности, книгу [28], целиком посвящённую этой кривой). В то время как в [54] принят в основном геометрический подход, в [55] Ф. Клейн подчёркивает алгебраические аспекты конструкции. В то же время эта статья содержит рисунок<sup>1</sup>, изображающий десять плоских деревьев и, по существу, предвосхищающий концепцию *детских рисунков* Гротендика [39] более чем на век. Цель нашей статьи — дать современную интерпретацию этого рисунка и лежащей в его основе математики, а также исследовать некоторые обобщения, которые Ф. Клейн мог бы получить, имея он доступ к таким инструментам, как теория характеров, компьютерная алгебра и классификация простых конечных групп.

В частности, мы изучаем рисунки типа  $(3, 2, p)$  степеней  $p$  и  $p + 1$  для произвольного простого  $p$ , обобщая результаты Ф. Клейна для  $p = 11$ , изложенные в [55]. Эти рисунки лучше всего изучать с помощью их групп монодромии, которые являются группами перестановок соответствующих степеней. В принципе, все такие группы хорошо известны — это одно из следствий классификации конечных простых групп. Тем не менее, из-за того что некоторые проблемы в теории чисел остаются открытыми, мы по-прежнему не знаем, конечны или бесконечны два семейства таких групп, а именно проективные и аффинные группы степеней  $p$  и  $p + 1$ . Основываясь на гипотезе Бейтмана—Хорна, а также на результатах обширного компьютерного эксперимента, мы приводим убедительные аргументы в пользу того, что первое из этих двух семейств бесконечно. Второе семейство связано с простыми числами Мерсенна, и нам нечего добавить к вопросу о том, конечно или бесконечно их множество.

В разделе 2 мы приводим описание десяти плоских деревьев — сначала в том виде, в каком Ф. Клейн изображает их в [55] в качестве представлений возможных 11-листных накрытий сферы Римана  $\Sigma = \mathbb{P}^1(\mathbb{C})$  с ветвлениями типа

<sup>1</sup>К сожалению, этот рисунок и Hauptfigur в [54] отсутствуют в онлайн версиях этих статей, поскольку в оригинальной журнальной публикации они расположены на отдельных вклейках. Оба рисунка, однако, можно найти в собрании сочинений Ф. Клейна [56, т. 3, с. 126, 143]: они вставлены в обновлённые версии обеих статей (см. также [28, с. 115, 320], где приведена Hauptfigur).

$3^3 1^2$ ,  $2^4 1^3$  и  $11^1$  над точками  $0$ ,  $1$  и  $\infty$ . Затем мы используем более современную терминологию и графические соглашения и описываем их в виде «детских рисунков», а именно в виде двудольных карт (рис. 2), а также в виде карт с висячими рёбрами (рис. 3). Ф. Клейн утверждает без доказательства, что его список полон; мы описываем метод, который он мог использовать для того, чтобы прийти к этому заключению.

Важным инвариантом рисунка является его группа монодромии (она изоморфна группе монодромии накрытия сферы, которое представляется этим рисунком): мы обсуждаем соответствующую конструкцию в разделе 3. Группа монодромии — это транзитивная группа перестановок, действующая на листах накрытия (более точно, на слое над базовой точкой) и порождённая перестановками монодромии, описывающими ветвление над критическими значениями. Ф. Клейн доказал, что только одна киральная пара построенных им деревьев, соответствующих нашим картам  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ , порождает группу монодромии  $\mathrm{PSL}_2(11)$  с действием степени 11; мы покажем, что остальные восемь деревьев порождают группу  $A_{11}$ .

Эффективной техникой перечисления рисунков с данной группой монодромии, к сожалению недоступной Ф. Клейну в период написания его статей, является основанная на теории характеров формула перечисления троек перестановок, введённая Ф. Г. Фробениусом [29] в 1896 году. Мы применяем её в разделе 4, используя таблицы характеров, получаемые с помощью пакета GAP [32] или же заимствованные из «Атласа» [21]. Эти вычисления подтверждают полученное Ф. Клейном перечисление деревьев, а также наше описание их групп монодромии. Среди прочего они позволяют исключить из рассмотрения группу Матьё  $M_{11}$  — возможного кандидата.

Каждому рисунку  $\mathcal{D}$  с группой монодромии  $G$  отвечает единственное минимальное регулярное накрытие  $\mathcal{R}$  с группой автоморфизмов  $\mathrm{Aut} \mathcal{R} \cong G$ . Существенная часть статьи Ф. Клейна [55] посвящена общему для рисунков  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$  регулярному накрытию  $\mathcal{R}_1$ . Оно представляет собой карту рода 26 на модулярной кривой  $X(11)$ . В разделе 5 мы показываем, что остальным восьми деревьям с группой  $G \cong A_{11}$  отвечают попарно неизоморфные накрытия рода 756 001.

Каждому из десяти деревьев Клейна соответствует 11-листное накрытие  $\Sigma \rightarrow \Sigma$ , реализуемое многочленом Шабата  $P$  степени 11. В разделе 6 мы находим эти многочлены для  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ : они определены над полем  $\mathbb{Q}(\sqrt{-11})$  и переходят друг в друга под действием группы Галуа. Остальные восемь деревьев составляют единую орбиту Галуа. В то время как во всех предыдущих примерах иллюстрации рисунков сохраняли лишь их топологическую структуру, в этом разделе мы вычисляем и показываем на рис. 8 геометрически правильный рисунок дерева  $\mathcal{M}_1$ : он является прообразом единичного отрезка относительно многочлена  $P$ .

В разделе 7 мы распространяем классификацию Клейна на все рисунки степени 11, имеющие тип  $(3, 2, r)$  для  $r \neq 11$ . Всего таких рисунков 16 (рис. 9); все они имеют род 0, и группой монодромии у всех у них служит симметрическая группа  $S_{11}$ .

В разделах 8—10 мы продолжаем исследование Ф. Клейна, рассматривая рисунки  $\mathcal{D}$  степени  $p$  и типа  $(3, 2, p)$  для произвольного простого  $p$ . Это исследование весьма нетривиально, поскольку по ходу дела мы сталкиваемся с важными открытыми проблемами теории групп и теории чисел. Группа монодромии  $G$  рисунка  $\mathcal{D}$  должна быть транзитивной группой перестановок степени  $p$ . Если  $p > 3$  (что мы будем всегда предполагать), группа  $G$  является фактором треугольной группы  $\Delta(3, 2, p)$  со взаимно простыми периодами и, следовательно, является совершенной (т. е. совпадает со своим коммутатором). В разделе 8 мы используем классификацию конечных простых групп, и в том числе групп перестановок простой степени, чтобы свести набор возможных групп к следующему списку: знакопеременные группы  $A_p$ ; исключительные группы  $\mathrm{PSL}_2(11)$  и группа Матьё  $M_{11}$  с действием степени 11, а также группа Матьё  $M_{23}$  с действием степени 23; наконец, группы  $\mathrm{PSL}_n(q)$  в тех случаях, когда их естественная степень  $(q^n - 1)/(q - 1)$  является простым числом  $p$ . Мы покажем, что группа  $A_p$  возникает при  $p = 5$ , а также при всех  $p \geq 11$ , причём число соответствующих рисунков растёт как минимум экспоненциально (а, может быть, даже факториально) при  $p \rightarrow \infty$ , так что их разумная классификация вряд ли возможна. Группа  $\mathrm{PSL}_2(11)$ , как мы видели, уже была изучена Ф. Клейном. Наконец, формула Фробениуса подсчёта троек элементов группы показывает, что группы Матьё не могут быть факторами треугольной группы  $\Delta(3, 2, p)$ .

Остаются группы  $\mathrm{PSL}_n(q)$  с естественным действием степени  $(q^n - 1)/(q - 1)$ , где  $q = t^e$  — степень простого числа  $t$ . В разделе 9 мы рассматриваем следующую открытую проблему: конечно или бесконечно множество пар  $(n, q)$ , при которых эта степень оказывается простым числом? Мы называем такие простые числа *проективными*. Частными случаями проективных простых чисел являются простые числа Ферма (при  $n = 2$ ) и Мерсенна (при  $q = 2$ ). Мощным инструментом для ответа на этот вопрос является гипотеза Бейтмана—Хорна, замечательная, но сравнительно малоизвестная гипотеза из теории чисел. Для  $n \geq 3$  (которое обязано быть простым) и для заданного  $e \geq 1$  (которое обязано быть степенью числа  $n$ ) эта гипотеза даёт эвристическую оценку для количества таких простых  $t \leq x$ , что  $q = t^e$  и число  $p = (q^n - 1)/(q - 1)$  является простым. Такого рода оценки очень близки к данным, полученным с помощью компьютерных расчётов, а сами эти расчёты дают множество подтверждающих примеров. Поэтому мы вправе сформулировать гипотезу, что для любого простого  $n \geq 3$  существует бесконечно много проективных простых чисел  $p$ . Этот случай более детально разобран в [50].

В разделе 10 мы возвращаемся к рисункам типа  $(3, 2, p)$  и степени  $p$ , где  $p = (q^n - 1)/(q - 1)$  — проективное простое число. Используя теорию характеров, мы доказываем существование рисунков с группой монодромии  $\mathrm{PSL}_n(q)$  для  $n = 2$  и  $n = 3$  и для любого проективного простого числа  $p$ . В теоремах 10.1 и 10.3 мы перечисляем эти рисунки и определяем их род. В теореме 10.11 приводится аналогичный, но менее сильный результат: мы доказываем существование рисунков для всех простых чисел Мерсенна  $p = 2^n - 1$ . Наконец, мы формулируем гипотезу о том, что существование рисунков степени  $p = (q^n - 1)/(q - 1)$

с группой монодромии  $\mathrm{PSL}_n(q)$  справедливо для всех проективных простых чисел  $p$ .

В разделах 11 и 12 мы рассматриваем рисунки типа  $(3, 2, p)$  и степени  $p + 1$ , где  $p$  — произвольное простое число. Параметры 3 и 2, присутствующие в типе, указывают на то, что все группы монодромии и группы автоморфизмов соответствующих рисунков являются факторами модулярной группы  $\mathrm{PSL}_2(\mathbb{Z}) \cong C_3 * C_2$ . В большинстве случаев ядро не является конгруэнц-подгруппой; однако в разделе 11 мы рассматриваем модулярные рисунки  $\mathcal{D}_0(p)$ , возникающие в процессе редукции по модулю  $p$  коэффициентов, отвечающих действию группы  $\mathrm{PSL}_2(p)$  на проективной прямой  $\mathbb{P}^1(\mathbb{F}_p)$ . Мы делаем это сначала в планарном случае, а именно для  $p = 7$  и  $p = 13$ , после чего рассматриваем более сложный случай  $p = 11$ , для которого мы описываем принадлежащее Дж. Войту вычисление эллиптической кривой  $E$ , на которой лежит этот рисунок, и его функцию Белого  $E \rightarrow \Sigma$ . Для  $p = 11$  и  $p = 13$  мы также вычисляем и приводим геометрически правильное изображение соответствующих рисунков.

Мы расширяем сферу исследования в разделе 12, где мы рассматриваем произвольные рисунки типа  $(3, 2, p)$  и степени  $p + 1$  для простых  $p > 3$ . Здесь мы используем принадлежащую П. Мюллеру [65] классификацию примитивных групп перестановок, содержащих цикл и одну неподвижную точку. Это позволяет нам ограничить список возможных групп монодромии следующими случаями:  $A_{p+1}$ ,  $\mathrm{PSL}_2(p)$ ,  $\mathrm{AGL}_n(2)$  для  $p = 2^n - 1$ ,  $M_{11}$  и  $M_{12}$  для  $p = 11$  и, наконец,  $M_{24}$  для  $p = 23$ . Мы показываем, что группа  $A_{p+1}$  возникает в этом контексте для всех  $p > 7$ . Снова этой группе соответствует слишком много рисунков, так что классификации поддаются только примеры с малыми значениями  $p$ . Группы  $\mathrm{PSL}_2(p)$  порождают только рисунки  $\mathcal{D}_0(p)$ . Группы  $M_{12}$  и  $M_{24}$  порождают каждая по киральной паре рисунков, в то время как группа  $M_{11}$ , как и ранее, не даёт ничего. Наконец, мы показываем, что аффинная группа  $\mathrm{AGL}_n(2)$  порождает по крайней мере один рисунок для любого простого числа Мерсенна  $p = 2^n - 1 > 7$ ; что касается  $p = 7$ , то для него построение не проходит, так как группа  $\mathrm{AGL}_3(2)$  не является гурвицевой.

В разделе 13 мы вкратце описываем ещё одну реализацию группы  $\mathrm{PSL}_2(11)$ : она является группой изометрий 11-ячейника — замощения неориентируемого 3-орбифолда одиннадцатью полукосаэдрами. Этот абстрактный многогранник был независимо открыт Б. Грюнбаумом [40] и Г. Коксетером [22].

Раздел 14 содержит перестановки монодромии, а также изображения некоторых рисунков, рассматриваемых в статье.

## 2. Десять плоских деревьев Клейна

В [55] Ф. Клейн приводит изображение десяти плоских деревьев, каждое из которых состоит из 11 рёбер и 12 вершин. На каждом дереве введена двудольная структура на множестве вершин: валентности пяти вершин, изображённых

белыми кружочками, — 3 либо 1, валентности оставшихся семи вершин, изображённых чёрточками, перпендикулярными рёбрам, — 2 либо 1; во всех случаях единственная клетка представляет собой 11-угольник. Эти десять деревьев распадаются на четыре киральные пары, занумерованные римскими цифрами от I до IV (каждое дерево в паре является зеркальным образом другого), и два зеркально-симметричных дерева, занумерованных цифрами V и VI. Киральная пара номер I, которая играет центральную роль в статье Ф. Клейна, показана на рис. 1 (форма деревьев ради простоты слегка изменена, но комбинаторная структура сохранена).



Рис. 1. Киральная пара номер I плоских деревьев Клейна

## 2.1. Деревья Клейна как детские рисунки

Если считать, что деревья нарисованы на комплексной плоскости  $\mathbb{C}$ , а затем компактифицировать эту плоскость и превратить её в комплексную проективную прямую  $\Sigma = \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ , то мы распознаем в этих деревьях детские рисунки в смысле Гротендика [39], а именно, двудольные графы, вложенные в компактные римановы поверхности  $X$ ; они определяют конечные накрытия  $X \rightarrow \Sigma$  сферы, неразветвлённые вне точек  $\{0, 1, \infty\}$ , или, по теореме Белого [1], проективные алгебраические кривые  $X$ , определённые над полем алгебраических чисел. (С основами теории детских рисунков можно познакомиться по [4, 34, 48].) Все наши десять рисунков имеют род 0, так что  $X = \Sigma$ . Их степень равна 11: это означает, что они задают 11-листное накрытие сферы  $\Sigma$ ; их тип равен  $(3, 2, 11)$ : это означает, что в них фигурируют ветвления порядков, делящих 3, 2 и 11, соответственно над точками 0, 1 и  $\infty$ , представленные в рисунках Клейна белыми кружками, перпендикулярными чёрточками и одной точкой в бесконечности. Современные соглашения состоят в том, чтобы использовать чёрные и белые вершины для точек над нулём и единицей, соответственно. При этом рёбра отвечают точкам над единичным отрезком  $[0, 1] \subset \Sigma$ , а точки над бесконечностью служат центрами клеток. Мы будем обозначать рисунки, отвечающие киральным парам Клейна I–IV, через  $\mathcal{M}_i$  и  $\bar{\mathcal{M}}_i$ ,  $i = 1, \dots, 4$ ; при этом дерево  $\mathcal{M}_i$  расположено на рисунке Клейна (и на нашем тоже) слева. Аналогично, мы обозначаем через  $\mathcal{M}_i$  ( $i = 5, 6$ ) деревья Клейна номер V и VI из статьи [55]<sup>1</sup>. Деревья  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ , составляющие пару номер I, показаны на рис. 2.

<sup>1</sup>Соблазн использовать вслед за Ф. Клейном римские цифры в качестве индексов был почти (но не окончательно) непреодолимым.

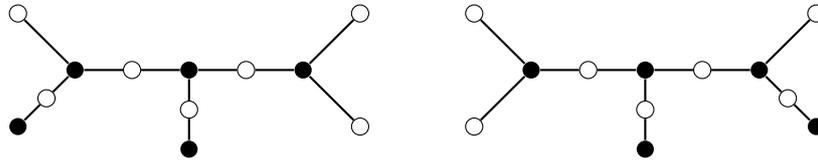


Рис. 2. Рисунки  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ , отвечающие паре Клейна номер I

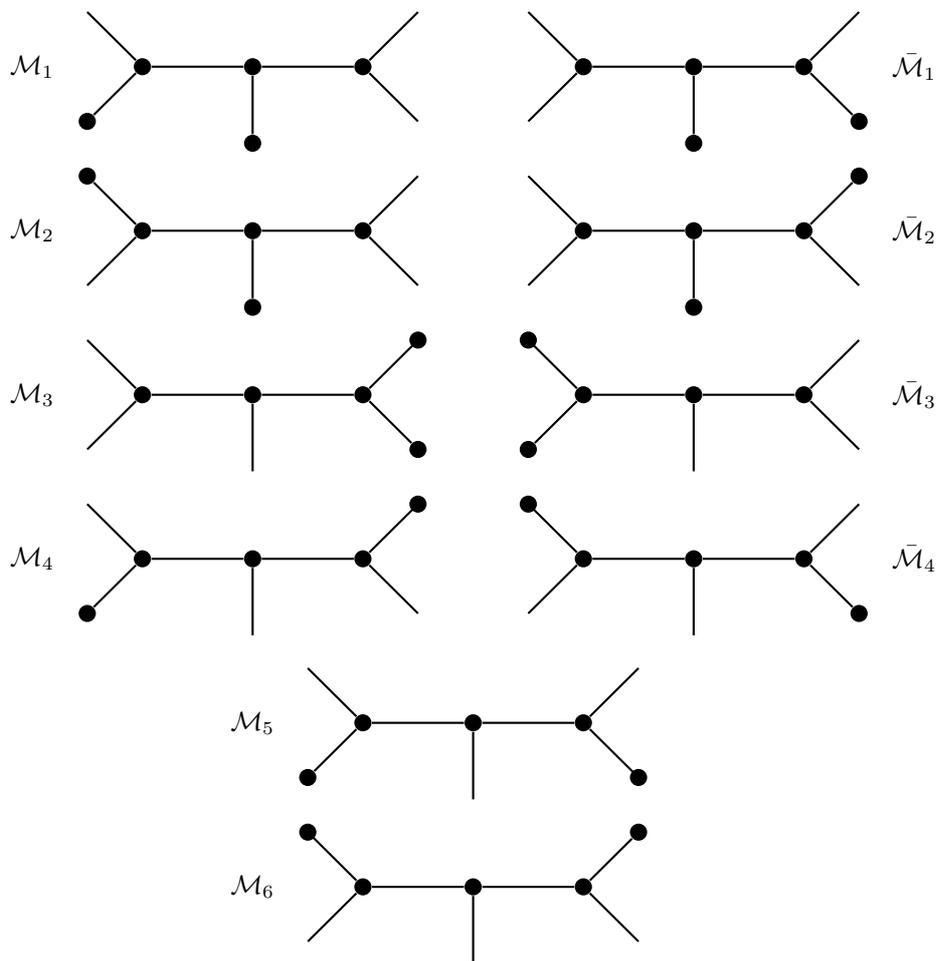


Рис. 3. Карты  $\mathcal{M}_i$  и  $\bar{\mathcal{M}}_i$ , отвечающие плоским деревьям Клейна I–VI

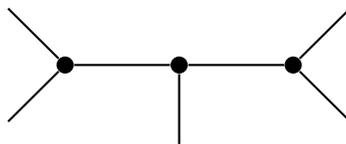
В том случае, когда порядок ветвлений над точкой 1 делит 2, как во всех наших рисунках, так что все белые вершины имеют валентности либо 1, либо 2, иногда бывает удобно удалить эти вершины, оставив карту, у которой есть только чёрные вершины; при этом могут возникнуть висячие рёбра, у которых удалён белый конец валентности 1. Эта операция, разумеется, является обратимой, так что никакой потери информации не происходит. Это соглашение использовано на рис. 3, где изображены все десять деревьев Клейна; их внешний вид практически идентичен тому, который использовал Ф. Клейн в своей исходной работе.

На самом деле эти десять рисунков составляют полный (с точностью до изоморфизма) список рисунков типа  $(3, 2, 11)$  и степени 11, каковая является наименьшей возможной степенью рисунков этого типа. Ф. Клейн использовал свои диаграммы в целях классификации 11-листных накрытий сферы  $\Sigma$  с ветвлениями типа  $3^3 1^2$  и  $2^4 1^3$  над точками 0 и 1. Он описывал их в терминах модулярной функции  $J: \mathbb{H} \rightarrow \Sigma$ , параметризующей классы изоморфных эллиптических кривых. Этот подход естественным образом приводит к модулярной группе  $\Gamma = \text{PSL}_2(\mathbb{Z})$  — подгруппе группы автоморфизмов  $\text{PSL}_2(\mathbb{R})$  римановой поверхности  $\mathbb{H}$ , оставляющей инвариантной функцию  $J$ . Эту часть работы Ф. Клейна мы в нашей статье не обсуждаем.

## 2.2. Проблема классификации

Ф. Клейн представил в [55, § 1] свои десять плоских деревьев в качестве ответа на вопрос, который он поставил в [53, § 5]. В современной терминологии вопрос звучит так: сколько имеется рисунков  $\mathcal{D}$  степени 11 с паспортом  $(3^3 1^2; 2^4 1^3; -)$ , т. е. с тремя чёрными вершинами валентности 3 и двумя валентности 1, с четырьмя белыми вершинами валентности 2 и тремя валентности 1 и при этом без всяких ограничений на валентности клеток.

На своём чертеже Ф. Клейн изобразил десять плоских деревьев, эквивалентных рассматриваемым рисункам, но не объяснил, почему этот список полон. Он написал просто: «Dass es auch nicht mehr giebt, ist ebenso evident» («Ясно также, что других не существует»). Мы приведём доказательство на языке рисунков: оно в самом деле совсем просто. Поскольку каждый рисунок  $\mathcal{D}$  имеет 10 рёбер и 11 вершин и при этом связан, он должен быть деревом. Поэтому подлежащая поверхность является сферой, и рисунок имеет единственную клетку валентности 11. Валентности белых вершин — 1 или 2, поэтому мы можем для простоты опустить их и изобразить  $\mathcal{D}$  в виде карты  $\mathcal{M}$ , у которой будет три вершины валентности 3 и две валентности 1, а также семь рёбер, три из которых висячие. Из-за связности одна из вершин валентности 3 должна лежать между двумя другими, так что карта  $\mathcal{M}$  должна строиться из «базовой» карты  $\mathcal{M}_0$ , изображённой на рис. 4, на которой нужно выбрать два из пяти висячих рёбер и поместить в их концы по вершине. Это даёт нам  $\binom{5}{2} = 10$  неизоморфных карт  $\mathcal{M}$ ; они изображены на рис. 3 в виде, соответствующем тому, который использован в работе Ф. Клейна [55].

Рис. 4. Планарная карта  $M_0$ 

Альтернативный подход к этой и аналогичным ей проблемам, основанный на теории характеров и формуле Фробениуса, будет изложен в разделе 4.

### 3. Группы монодромии

Любой рисунок  $\mathcal{D}$  степени  $n$  может быть представлен в виде упорядоченной пары  $x, y$  перестановок его  $n$  рёбер. Для этого следует использовать выбранную на подлежащей поверхности ориентацию и записать порядок вращения рёбер вокруг инцидентных им чёрных и белых вершин. Группа монодромии  $G = \langle x, y \rangle$  рисунка  $\mathcal{D}$ , действующая на  $n$  рёбрах, может быть идентифицирована с подгруппой симметрической группы  $S_n$ . В силу связности графа эта группа транзитивна. Нам будет удобно ввести третью перестановку  $z := (xy)^{-1}$ , так что  $xyz = 1$ . Легко проверить, что, в то время как циклы перестановок  $x$  и  $y$  отвечают соответственно чёрным и белым вершинам, циклы  $z$  соответствуют клеткам.

**Соглашение 3.1 (где ставить этикетки).** Мы будем ставить этикетку каждого ребра слева от этого ребра, если двигаться вдоль него от его чёрного конца к белому. В этом случае этикетки, соответствующие циклу перестановки  $z$  или, что то же самое, соответствующие клетке, будут располагаться внутри этой клетки. При этом перестановка  $z$  будет вращать их вокруг центра клетки в направлении, отвечающем ориентации поверхности. Данное соглашение проиллюстрировано на рис. 5. (Если рисунок изображён на плоскости, нам может показаться, что у внешней клетки этикетки вращаются в направлении, противоположном ориентации поверхности. Это, однако, иллюзия. На самом деле рисунок расположен не на плоскости, а на сфере, и центр внешней клетки находится «на противоположной стороне» сферы. Если смотреть из этого центра, мы увидим, что этикетки вращаются в соответствии с ориентацией.)

В случае, когда  $y^2 = 1$  и белые вершины опущены, так что  $\mathcal{D}$  оказывается картой без двудольной структуры, мы можем считать, что группа  $G$  действует на полурёбрах, или же на ориентированных рёбрах. Таким образом, ребро несёт на себе две этикетки, а висячее ребро — одну. Висячее ребро можно также представлять себе как ориентированное ребро, направленное в сторону от инцидентной ему вершины.

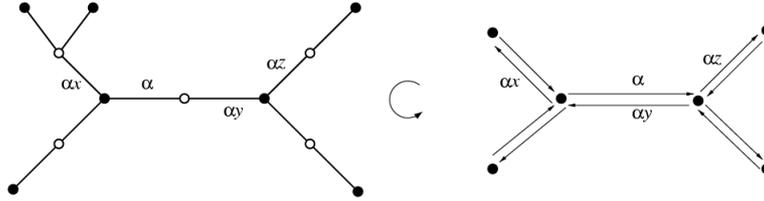


Рис. 5. Перестановки монодромии:  
 рёбра  $\alpha x$ ,  $\alpha y$  и  $\alpha z$  — образы ребра  $\alpha$  под действием перестановок  $x$ ,  $y$  и  $z = (xy)^{-1}$ .  
 Округлая стрелка в середине рисунка показывает ориентацию поверхности

**Пример 3.2.** Карта, изображённая на рис. 6, задаётся следующими перестановками:

$$\begin{aligned} x &= (1, 15, 16)(2, 3, 4)(5, 9)(6, 7, 8, 10, 11, 12), \\ y &= (1, 6)(2, 9)(3, 13, 8, 14)(4, 7)(5, 10)(11, 12), \\ z &= (1, 12, 10, 9, 4, 6, 16, 15)(2, 5, 8, 13)(3, 14, 7). \end{aligned}$$

Группа монодромии этой карты — знакопеременная группа  $A_{16}$ . Другие примеры карт с помеченными рёбрами можно увидеть на рис. 17 и 27.

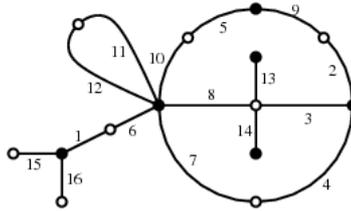


Рис. 6. Карта с помеченными рёбрами

Степень рассматриваемых нами десяти рисунков  $\mathcal{D}$  равна 11, так что их группы монодромии — это транзитивные подгруппы группы  $S_{11}$ . Во всех десяти случаях  $x^3 = y^2 = 1$ , так что группы  $G$  являются факторами модулярной группы

$$\Gamma = \text{PSL}_2(\mathbb{Z}) = \langle X, Y, Z \mid X^3 = Y^2 = XYZ = 1 \rangle \cong C_3 * C_2,$$

а образующие

$$X = \pm \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad Y = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Z = \pm \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

соответствуют преобразованиям Мёбиуса

$$t \mapsto \frac{-1}{t-1}, \quad t \mapsto \frac{-1}{t}, \quad t \mapsto t+1.$$

(Мы ставим в соответствие преобразованиям Мёбиуса  $t \mapsto \frac{at+b}{ct+d}$  пары матриц  $\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , транспонированных по отношению к тем, которые обычно фигурируют в этом контексте. Причина в том, что мы в дальнейшем должны будем рассматривать преобразования Мёбиуса как перестановки: в первую очередь это относится к преобразованиям, определённым над конечными полями. И с алгебраической, и с вычислительной точки зрения удобно перемножать перестановки слева направо, в то время как аналитические соглашения используют композицию справа налево. Таким образом, чтобы получить гомоморфизм, ставящий в соответствие матрицам преобразования Мёбиуса, мы вынуждены отказаться от обманчиво привлекательных обозначений и использовать транспонированные матрицы.)

Ф. Клейн задался вопросом о том, какие из этих групп монодромии являются конгруэнц-факторами, т. е. факторами по конгруэнц-подгруппе группы  $\Gamma$ . Единственный возможный уровень такой конгруэнц-подгруппы — это 11 (поскольку это порядок элемента  $z := (xy)^{-1}$ ). В самом деле, получающаяся при этом фактор-группа  $L := \text{PSL}_2(11)$ , простая группа порядка 660, действует как транзитивная группа степени 11 на смежных классах подгруппы  $H \cong A_5$ , что мы сейчас и продемонстрируем. Это один из тех трёх случаев, известных уже Э. Галуа (см. [30, с. 411, 412]), в которых простая группа  $\text{PSL}_2(p)$ , где  $p$  простое, имеет собственную подгруппу индекса меньше, чем  $p + 1$ ; два оставшихся случая — это  $A_4 < \text{PSL}_2(5)$  и  $S_4 < \text{PSL}_2(7)$ .

В качестве образующих группы  $L$  мы можем взять образы

$$x = \pm \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad y = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad z = \pm \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

образующих  $X, Y, Z$  группы  $\Gamma$ . Они удовлетворяют соотношениям

$$x^3 = y^2 = z^{11} = xyz = 1. \quad (1)$$

Возьмём следующие элементы группы  $L$ :

$$u = \pm \begin{pmatrix} 4 & -1 \\ 2 & -3 \end{pmatrix}, \quad v = y = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad w = \pm \begin{pmatrix} 2 & -4 \\ -3 & 1 \end{pmatrix}.$$

Заметим, что  $\det(u) = \det(w) = -10 \equiv 1 \pmod{11}$ . Они удовлетворяют соотношениям

$$u^3 = v^2 = w^5 = uvw = 1,$$

так что они порождают фактор  $H \leq L$  треугольной группы  $\Delta(3, 2, 5) \cong A_5$ . Из простоты группы  $A_5$  следует, что  $H \cong A_5$ , поэтому  $|L : H| = 11$ .

Сопряжение элементом

$$\pm \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \text{PGL}_2(11) \cong \text{Aut } L$$

индуцирует внешний автоморфизм группы  $L$ , осуществляя транспозицию элементов  $u, v$  и  $w$  с элементами

$$\bar{u} = \pm \begin{pmatrix} 4 & 1 \\ -2 & -3 \end{pmatrix}, \quad \bar{v} = v = y = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \bar{w} = \pm \begin{pmatrix} 2 & 4 \\ 3 & 1 \end{pmatrix},$$

которые удовлетворяют тем же соотношениям и, следовательно, порождают подгруппу  $\bar{H} \cong A_5$ . Эта подгруппа не сопряжена в  $L$  подгруппе  $H$ . Если бы она была сопряжена, то нашёлся бы такой неединичный элемент группы  $\text{PGL}_2(11)$ , который коммутировал с  $u$ ,  $v$  и  $w$ , в то время как несложно проверить, что этим свойством обладает только единичный элемент. Отсюда следует, что группа  $L$  имеет два неэквивалентных транзитивных представления степени 11 — на классах смежности подгрупп  $H$  и  $\bar{H}$ , или, что то же самое (поскольку эти подгруппы совпадают со своими нормализаторами в  $L$ ), действием сопряжением на представляемых ими двух классах сопряжённости подгрупп.

В наши дни, используя такие программы, как GAP [32], мы можем легко определить группы монодромии десяти рассматриваемых рисунков и, в частности, показать, что два из них, а именно  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ , имеют группу монодромии  $L = \text{PSL}_2(11)$ . Можно, однако, выделить эту пару и вручную: для  $i = 1, \dots, 6$  коммутатор  $[x, y] = x^{-1}y^{-1}xy$  имеет в  $\mathcal{M}_i$  (а следовательно, и в  $\bar{\mathcal{M}}_i$ ) цикловую структуру  $5^2 1^1$ ,  $7^1 3^1 1^1$ ,  $8^1 2^1 1^1$ ,  $5^1 4^1 2^1$ ,  $7^1 2^2$  и  $4^2 3^1$  соответственно, так что только для  $i = 1$  он имеет один из возможных порядков элементов группы  $L$  (1, 2, 3, 5, 6 и 11). В обратную сторону, легко показать, что если  $L$  представлена действием на классах смежности подгрупп  $H$  или  $\bar{H}$ , то цикловые структуры образующих  $x$  и  $y$  будут  $3^3 1^2$  и  $2^4 1^3$ , так что  $L$  будет группой монодромии по крайней мере одного из десяти рисунков, и это должна быть пара  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ , два рисунка которой отвечают двум неэквивалентным представлениям степени 11.

Ф. Клейн [55, § 2] использовал похожие аргументы. Основываясь на рассмотрении слова, эквивалентного (в наших обозначениях) слову  $yz^3$ , он показал, что деревья II–VI имеют группу монодромии, отличную от  $L$ . Детали он приводит только для дерева V, соответствующего рисунку  $\mathcal{M}_5$ . В остальном его статья целиком посвящена деревьям, обозначенным I (см. наш рис. 1) с группой монодромии  $L$ , а также их минимальному регулярному накрытию: все они соответствуют конгруэнц-подгруппам модулярной группы. Деревья II–VI, отвечающие не-конгруэнц-подгруппам, а также их группы монодромии, Ф. Клейн игнорирует.

На самом деле приведённые выше цикловые структуры коммутатора  $[x, y]$  показывают, что для  $i = 2, 4, 5, 6$  группа монодромии  $G$  равна  $A_{11}$ . В самом деле, группа  $G$ , будучи транзитивной и имея простую степень, является примитивной. Теорема Жордана (см., например, [73, теорема 13.9]) утверждает, что любая конечная примитивная группа, содержащая цикл простой длины и как минимум три фиксированные точки, должна содержать знакопеременную группу. Во всех четырёх указанных случаях подходящая степень коммутатора  $[x, y]$  обладает этим свойством, так что  $G \geq A_{11}$ . Поскольку образующие  $x$  и  $y$  являются чётными перестановками, мы получаем, что  $G = A_{11}$ . Для случая  $i = 3$  требуется отдельный аргумент. Мы можем, например, использовать тот факт, что элемент  $xz^3xz^5$  имеет цикловую структуру  $5^1 3^1 1^3$ . (Теорема Жордана, которую мы здесь использовали, следует непосредственно из статей [51, 52], опубликованных в 1871 и 1873 годах. Таким образом, Ф. Клейн мог быть знаком с этой теоремой и использовать её в своих рассуждениях. Дополнительные исто-

рические комментарии, касающиеся теоремы Жордана, а также её современных обобщений, можно найти в [45].)

Тот факт, что группы монодромии этих восьми деревьев — это  $G \cong A_{11}$ , указывает на то, что, как уже было отмечено выше, они не являются конгруэнц-подгруппами группы  $\Gamma$ . В самом деле, неабелевыми композиционными факторами факторов группы  $\Gamma$  могут быть только группы, изоморфные  $\mathrm{PSL}_2(p)$  для простых  $p \geq 5$ , делящих уровень (см. [64]). Сравнивая порядки, легко показать, что простая группа  $A_{11}$  такой формы не имеет.

#### 4. Подсчёт троек элементов группы

Мы уже ранее привели очень простые аргументы, показывающие, что существует в точности десять рисунков с данными характеристиками. В то же время этот простой пример даёт нам возможность проиллюстрировать ещё одну важную перечислительную технику, основанную на теории характеров. Очень часто в более сложных случаях, когда степень или род рисунка не столь малы, этот подход является единственным доступным методом. Он основан на формуле Фробениуса [29]

$$\frac{|\mathcal{X}| \cdot |\mathcal{Y}| \cdot |\mathcal{Z}|}{|G|} \sum_x \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)} \quad (2)$$

для числа троек  $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ , таких что  $xyz = 1$ , где  $\mathcal{X}$ ,  $\mathcal{Y}$  и  $\mathcal{Z}$  — классы сопряжённости в конечной группе  $G$ , а сумма берётся по всем неприводимым комплексным характерам  $\chi$  группы  $G$ . (В конкретных приложениях часто оказывается, что многие характеры на одном или нескольких классах  $\mathcal{X}$ ,  $\mathcal{Y}$ ,  $\mathcal{Z}$  равны нулю, так что их можно исключить из суммирования.) Статья Ф. Г. Фробениуса [29] была опубликована на 17 лет позже статьи Ф. Клейна [55], так что эта мощная техника была Ф. Клейну недоступна. Мы здесь покажем, как она работает в совсем простой ситуации; при этом мы не будем опираться на ранее полученные результаты. В качестве бонуса мы определим также группы монодромии всех десяти рисунков.

Перед тем как приступить к подсчёту, мы приведём альтернативный вид формулы (2): он часто бывает более удобным, например при использовании «Атласа» [21], в котором вместо порядков классов сопряжённости даны порядки их централизаторов. Имеет место следующее соотношение:  $|\mathcal{X}| = |G|/|C(x)|$ , где  $C(x) = C_G(x)$  обозначает централизатор элемента  $x$  в  $G$ , и аналогичные равенства справедливы для  $|\mathcal{Y}|$  и  $|\mathcal{Z}|$ . Таким образом, мы можем переписать формулу (2) в следующем виде:

$$\frac{|G|^2}{|C(x)| \cdot |C(y)| \cdot |C(z)|} \sum_x \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)}. \quad (3)$$

Если рисунок  $\mathcal{D}$  имеет тип  $(3, 2, 11)$  и степень 11, его перестановки монодромии должны удовлетворять соотношениям (1). Перестановки  $x$  и  $z$  имеют

нечётный порядок и, следовательно, являются чётными, а потому чётна также и  $y$ , так что группа монодромии  $G = \langle x, y, z \rangle$  является подгруппой группы  $A := A_{11}$ . Наша цель — подсчитать тройки элементов  $x, y, z$  в группе  $A$ , удовлетворяющих соотношениям (1), а также определить соответствующие им рисунки  $\mathcal{D}$  и их группы монодромии  $G$ . В более общих ситуациях при применении формулы (2) следует исключать тройки, порождающие нетранзитивные подгруппы  $G$ , поскольку такие группы не могут быть группами монодромии связных накрытий. Однако в нашем случае тот факт, что  $z$  является 11-циклом, гарантирует транзитивность, так что эта проблема не возникает. Поскольку порядки 3, 2 и 11 перестановок  $x, y$  и  $z$  взаимно просты, группа  $G$  должна быть совершенной (т. е. иметь тривиальную абелианизацию) и, следовательно, не может быть разрешимой. Если  $G \neq A$ , то  $G$  должна содержаться в неразрешимой максимальной подгруппе  $M$  группы  $A$ , а её порядок должен делиться на 11. Список максимальных подгрупп группы  $A_{11}$  можно найти в [21]; мы увидим, что таких максимальных подгрупп  $M$  всего две и обе они изоморфны группе Матьё  $M_{11}$ , образуя два класса сопряжённости подгрупп индекса 2520, переставляемых группой  $\text{Out } A$ . Аналогично, имеющийся в [21] список максимальных подгрупп группы  $M_{11}$  сообщает нам, что если  $G \neq M$ , то  $G$  изоморфна  $L = \text{PSL}_2(11)$ . При этом каждая подгруппа  $M \cong M_{11}$  содержит один класс сопряжённости таких подгрупп, и их индекс в  $M$  равен 12. Итак, группа  $G$  либо равна  $A$ , либо изоморфна  $M_{11}$  или  $\text{PSL}_2(11)$ . Мы подсчитаем количество троек, образующих эти группы, начав с наименьшей.

**Пример 4.1.** Покажем, что группа  $L = \text{PSL}_2(11)$  имеет, с точностью до автоморфизма (или с точностью до сопряжения в  $\text{PGL}_2(11) \cong \text{Aut } L$ ), единственную порождающую тройку  $x, y, z$ , удовлетворяющую соотношениям (1). Ниже приведена таблица характеров группы  $L$ , вычисленная программой GAP [32]. Её столбцы отвечают классам сопряжённости: стоящие сверху наименования  $na, nb$  и т. д. ( $nA, nB$  и т. д. в обозначениях «Атласа» [21]) указывают на последовательные классы элементов порядка  $n$ ; строки, помеченные  $X.j$ , отвечают неприводимым характерам  $\chi_j, j = 1, 2, \dots$ . Таблица включает данные вида  $A, *A := (-1 \mp \sqrt{5})/2$  и  $B, /B := (-1 \pm i\sqrt{11})/2$ , а точка означает 0.

	1a	3a	2a	5a	5b	6a	11a	11b
X.1	1	1	1	1	1	1	1	1
X.2	5	-1	1	.	.	1	B	/B
X.3	5	-1	1	.	.	1	/B	B
X.4	10	1	-2	.	.	1	-1	-1
X.5	10	1	2	.	.	-1	-1	-1
X.6	11	-1	-1	1	1	-1	.	.
X.7	12	.	.	A	*A	.	1	1
X.8	12	.	.	*A	A	.	1	1

$$\begin{aligned}
A &= E(5)^2 + E(5)^3 \\
&= (-1 - \sqrt{5})/2 = -1 - b_5 \\
B &= E(11) + E(11)^3 + E(11)^4 + E(11)^5 + E(11)^9 \\
&= (-1 + \sqrt{-11})/2 = b_{11}
\end{aligned}$$

Возьмём в качестве классов  $\mathcal{X}$  и  $\mathcal{Y}$  классы 3a и 2a, а в качестве  $\mathcal{Z}$  один из классов 11a или 11b. Каков бы ни был этот выбор, сумма по характеристам в формуле (3) даёт

$$\begin{aligned}
\Sigma_L &= 1 + \frac{(-1) \cdot 1 \cdot B}{5} + \frac{(-1) \cdot 1 \cdot /B}{5} + \frac{1 \cdot (-2) \cdot (-1)}{10} + \frac{1 \cdot 2 \cdot (-1)}{10} = \\
&= 1 - \frac{B + /B}{5} = \frac{6}{5}.
\end{aligned}$$

Централизаторы  $C_L(x)$ ,  $C_L(y)$  и  $C_L(z)$  типичных элементов  $x$ ,  $y$  и  $z$  классов  $\mathcal{X}$ ,  $\mathcal{Y}$  и  $\mathcal{Z}$  имеют порядок 6, 12 и 11 соответственно, так что

$$\frac{|L|^2}{|C(x)| \cdot |C(y)| \cdot |C(z)|} = \frac{2^4 \cdot 3^2 \cdot 5^2 \cdot 11^2}{6 \cdot 12 \cdot 11} = 2 \cdot 5^2 \cdot 11.$$

Умножая этот результат на  $\Sigma_L$ , получаем  $2^2 \cdot 3 \cdot 5 \cdot 11$  троек  $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ , удовлетворяющих равенству  $xyz = 1$ , и это для любого выбора  $\mathcal{Z}$ , так что всего выходит  $2^3 \cdot 3 \cdot 5 \cdot 11$ . Каждая из этих троек порождает  $L$ , поскольку эта группа не имеет собственных подгрупп, порядок которых делился бы на 66 (на самом деле ни одной подгруппы индекса меньше 11). Поскольку группа  $\text{Aut } L$  действует на порождающих тройках полурегулярно, мы можем поделить предыдущий результат на порядок этой группы  $|\text{PGL}_2(11)| = 2^3 \cdot 3 \cdot 5 \cdot 11$ , откуда видно, что  $\text{Aut } L$  имеет на таких тройках единственную орбиту, что и утверждалось.

Поскольку нормальные подгруппы произвольной группы  $\Delta$  с фактором, изоморфным группе  $G$ , находятся во взаимно однозначном соответствии с орбитами группы  $\text{Aut } G$ , действующей композициями на эпиморфизмах  $\Delta \rightarrow G$ , мы получаем, что треугольная группа

$$\Delta := \Delta(3, 2, 11) = \langle X, Y, Z \mid X^3 = Y^2 = Z^{11} = XYZ = 1 \rangle$$

имеет единственную нормальную подгруппу с фактором, изоморфным группе  $L$ . Далее,  $L$  имеет два класса сопряжённости подгрупп индекса 11. Эти подгруппы изоморфны  $A_5$ , а классы переводятся друг в друга группой автоморфизмов  $\text{PGL}_2(11)$  (см. [21] или [25, § 259]). Они поднимаются до двух классов сопряжённости подгрупп индекса 11 в группе  $\Delta$ ; эти классы переходят друг в друга под действием сопряжения в расширенной треугольной группе

$$\Delta[3, 2, 11] = \langle R_0, R_1, R_2 \mid R_i^2 = (R_1 R_2)^3 = (R_2 R_0)^2 = (R_0 R_1)^{11} = 1 \rangle,$$

содержащей  $\Delta$  в качестве подгруппы индекса 2. Они соответствуют киральной паре рисунков  $\mathcal{D}$  типа  $(3, 2, 11)$  и степени 11 с группой монодромии, изоморфной группе  $L$ . Это вычисление показывает, что других таких рисунков нет, так что

они не могут быть ничем иным, кроме как рассмотренными ранее рисунками  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ .

**Пример 4.2.** Теперь давайте сосчитаем тройки, удовлетворяющие соотношению (1), в простой группе  $M = M_{11}$  порядка  $7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$ . Ниже приведена таблица характеров этой группы, вычисленная программой GAP.

	1a	11a	11b	2a	4a	8a	8b	3a	6a	5a
X.1	1	1	1	1	1	1	1	1	1	1
X.2	10	-1	-1	2	2	.	.	1	-1	.
X.3	10	-1	-1	-2	.	B	-B	1	1	.
X.4	10	-1	-1	-2	.	-B	B	1	1	.
X.5	11	.	.	3	-1	-1	-1	2	.	1
X.6	16	A	/A	.	.	.	.	-2	.	1
X.7	16	/A	A	.	.	.	.	-2	.	1
X.8	44	.	.	4	.	.	.	-1	1	-1
X.9	45	1	1	-3	1	-1	-1	.	.	.
X.10	55	.	.	-1	-1	1	1	1	-1	.

$$\begin{aligned}
 A &= E(11)^2 + E(11)^6 + E(11)^7 + E(11)^8 + E(11)^{10} \\
 &= (-1 - \sqrt{-11})/2 = -1 - b11 \\
 B &= -E(8) - E(8)^3 \\
 &= -\sqrt{-2} = -i2
 \end{aligned}$$

В качестве  $\mathcal{X}$  и  $\mathcal{Y}$  мы должны взять единственные классы сопряжённости  $3a$  и  $2a$ , состоящие из элементов порядка 3 и 2 соответственно, а в качестве  $\mathcal{Z}$  — один из двух классов  $11a$  или  $11b$ , состоящих из элементов порядка 11. Мы обнаруживаем, что сумма по характерам для группы  $M$  равна

$$\Sigma_M = 1 + \frac{1 \cdot 2 \cdot (-1)}{10} + \frac{1 \cdot (-2) \cdot (-1)}{10} + \frac{1 \cdot (-2) \cdot (-1)}{10} = \frac{6}{5}.$$

Согласно [21] централизаторы элементов  $x$ ,  $y$  и  $z$  в группе  $M$  имеют порядок 18, 48 и 11 соответственно, так что

$$\frac{|M|^2}{|C(x)| \cdot |C(y)| \cdot |C(z)|} = \frac{2^8 \cdot 3^4 \cdot 5^2 \cdot 11^2}{18 \cdot 48 \cdot 11} = 2^3 \cdot 3 \cdot 5^2 \cdot 11.$$

Умножив это выражение на  $2\Sigma_M$ , мы получим число троек в  $M$ : оно равно  $2^5 \cdot 3^2 \cdot 5 \cdot 11$ . Далее,  $M$  содержит единственный класс сопряжённости, состоящий из 12 подгрупп  $L \cong \text{PSL}_2(11)$ , а мы видели в примере 4.1, что каждая из этих подгрупп порождена тройками в количестве  $2^3 \cdot 3 \cdot 5 \cdot 11$ , так что  $2^5 \cdot 3^2 \cdot 5 \cdot 11$  троек в группе в  $M$  порождают собственные подгруппы. Следовательно, ни одна из этих троек не порождает  $M$ . (См. также [19, 74], где подтверждается тот факт, что  $M_{11}$  не является фактором группы  $\Delta$ .)

Группы  $M_{11}$  и  $M_{12}$  были введены Э. Л. Матьё [61] в 1861 году, так что они могли быть знакомы Ф. Клейну. В отличие от  $M_{12}$  (см., например, [48, § 2.1.6]),

группа  $M_{11}$  не может быть группой монодромии никакой ориентированной кубической карты, поскольку, развивая нашу аргументацию, мы могли бы показать, что эта группа не является фактором группы  $\Gamma$ .

**Пример 4.3.** Теперь подсчитаем количество троек, удовлетворяющих условию (1), в группе  $A = A_{11}$ . В этом случае имеется три класса сопряжённости элементов порядка 3 и два класса элементов порядка 2. Простое рассуждение показывает, что, для того чтобы элементы  $x, y \in A$  порядков 3 и 2 порождали транзитивную группу, их цикловые структуры должны быть  $3^3 1^2$  и  $2^4 1^3$ , так что они принадлежат классам  $\mathcal{X} = 3c$  и  $\mathcal{Y} = 2b$  группы  $A$ ; при этом  $z$  должен лежать в одном из классов 11a или 11b, состоящих из циклов длины 11.

Таблица характеров группы  $A$  слишком велика, чтобы привести её здесь. Однако те неприводимые характеры  $\chi$ , для которых  $\chi(x)\chi(y)\chi(z) \neq 0$ , — это только лишь главный характер  $\chi_1$ , а также характеры  $\chi_2$ ,  $\chi_6$  и  $\chi_{11}$  степеней 10, 120 и 210, так что мы можем привести здесь небольшой фрагмент таблицы, содержащий перечисленные выше классы и характеры.

	1a	2b	3c	11a	11b
χ.1	1	1	1	1	1
χ.2	10	2	1	-1	-1
χ.6	120	-8	3	-1	-1
χ.11	210	2	3	1	1

Сумма

$$\Sigma_A := \sum_x \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)}$$

равна

$$1 + \frac{1 \cdot 2 \cdot (-1)}{10} + \frac{3 \cdot (-8) \cdot (-1)}{120} + \frac{3 \cdot 2 \cdot 1}{210} = 1 - \frac{1}{5} + \frac{1}{5} + \frac{1}{35} = \frac{36}{35} = \frac{2^2 \cdot 3^2}{5 \cdot 7}.$$

Имеем  $|A| = 11!/2 = 2^7 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$ , и согласно [21] порядки централизаторов элементов  $x$ ,  $y$  и  $z$  в  $A$  — это  $162 = 2 \cdot 3^4$ ,  $1152 = 2^7 \cdot 3^2$  и 11, так что

$$\frac{|A|^2}{|C(x)| \cdot |C(y)| \cdot |C(z)|} = 2^6 \cdot 3^2 \cdot 5^4 \cdot 7^2 \cdot 11.$$

Умножая это число на  $2\Sigma_A$ , получаем, что количество троек в  $A$ , удовлетворяющих условию (1), равно

$$t := 2^9 \cdot 3^4 \cdot 5^3 \cdot 7 \cdot 11 = 10 \times 11!.$$

Из этого числа мы должны вычесть количество троек, порождающих собственные подгруппы группы  $A$ . Мы видели, что все такие подгруппы изоморфны группе  $\text{PSL}_2(11)$ . Каждая подгруппа  $L \cong \text{PSL}_2(11)$  в  $A$  содержится в единственной подгруппе  $M \cong M_{11}$ . Имеется два класса сопряжённости таких подгрупп, по 2520 подгрупп в каждом, и каждая такая подгруппа содержит один класс

сопряжённости, содержащий 12 подгрупп  $L$ . В итоге число таких подгрупп  $L$  в  $A$  равно  $2 \cdot 2520 \cdot 12 = 60480 = 2^6 \cdot 3^3 \cdot 5 \cdot 7$ . Как показано в примере 4.1, для каждой подгруппы  $L$  имеется  $2^3 \cdot 3 \cdot 5 \cdot 11$  порождающих её троек, удовлетворяющих условию (1). Итого количество троек в  $A$ , порождающих подгруппы  $L \cong \text{PSL}_2(11)$ , равно  $2^9 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 = t/5 = 2 \times 11!$ .

Поскольку в  $A$  имеется  $10 \times 11!$  троек и из них  $2 \times 11!$  троек порождают собственные подгруппы, мы заключаем, что существует  $8 \times 11!$  троек, порождающих всю группу  $A$ . Они составляют восемь орбит под действием группы  $\text{Aut } A = S_{11}$ . Эти орбиты соответствуют восьми нормальным подгруппам группы  $\Delta$  с фактором  $A$  и, следовательно, восьми регулярным рисункам, у которых группа (сохраняющих ориентацию) автоморфизмов равна  $A$ . Группа  $A$  имеет единственный класс сопряжённости подгрупп индекса 11, состоящий из стабилизаторов точки, изоморфных  $A_{10}$ . Они поднимаются до восьми классов сопряжённости подгрупп индекса 11 в  $\Delta$  — в дополнение к тем двум, которые мы видели в примере 4.1, и дают восемь рисунков  $\mathcal{D}$  типа  $(3, 2, 11)$  и степени 11. Все эти восемь рисунков имеют группу монодромии  $G \cong A_{11}$ .

Итак, мы получили десять рисунков требуемого типа и степени. Это подтверждает предшествующее перечисление, а также тот факт, что  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$  имеют группу монодромии  $\text{PSL}_2(11)$ , в то время как группа монодромии восьми оставшихся рисунков равна  $A_{11}$ . Конкретные порождающие тройки, соответствующие этим рисункам, даны в разделе 14.1.

**Замечание 4.4.** В каждом из приведённых выше примеров вычисления, использующие формулы Фробениуса (2) или (3), были совсем простыми, так что их можно было провести вручную. Однако в более сложных случаях, когда имеется много слагаемых или когда некоторые характеры оказываются иррациональными, может оказаться необходимым воспользоваться услугами программы GAP. Приведённый ниже пример повторяет вычисления, которые мы проделали в примере 4.1.

```
> G:=PSL(2,11);;
> T:=CharacterTable(G);;
> OrdersClassRepresentatives(T);
[ 1, 3, 2, 5, 5, 6, 11, 11 ]
> ClassStructureCharTable(T,[2,3,7]);
660
> ClassStructureCharTable(T,[2,3,8]);
660
```

Здесь индексы 2, 3, 7 и 2, 3, 8 указывают положение выбранных нами классов  $\mathcal{X}$ ,  $\mathcal{Y}$  и  $\mathcal{Z}$  в предшествующем списке. Двойная точка с запятой после команды указывает программе, что эту команду следует исполнить, но результат вычисления выводить на печать не надо. Как и в примере 4.1, мы получаем 1320 троек.

## 5. Рисунки и их регулярные накрытия

Наше перечисление троек в группе  $L$  показывает, что существует единственный регулярный рисунок  $\mathcal{R}_1$  типа  $(3, 2, 11)$  с группой автоморфизмов  $L \cong \text{PSL}_2(11)$ : это минимальное регулярное накрытие обоих рисунков  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$  с группой монодромии  $L$ . В свою очередь, эти два рисунка представляют собой факторы рисунка  $\mathcal{R}_1$  по несопряжённым подгруппам группы  $L$ , изоморфным  $A_5$ . По формуле Римана—Гурвица регулярный рисунок такого типа с группой монодромии  $G$  имеет род  $1 + (5/132)|G|$ , т. е. в данном случае 26. В силу его единственности, а также в соответствии с наблюдением Д. Сингермана [70], касающимся троек в  $\text{PSL}_2(q)$ , рисунок  $\mathcal{R}_1$  является регулярной картой, соответствующей подгруппе группы  $\Delta$ , которая нормальна в расширенной треугольной группе  $\Delta[3, 2, 11]$ . Эта карта является двойственной к регулярной карте рода 26 и типа  $\{3, 11\}$ , которая обозначена R26.2 в каталоге регулярных карт М. Д. Кондера [20]. Её полная группа автоморфизмов, содержащая также автоморфизмы, обращающие ориентацию, изоморфна группе  $\text{PGL}_2(11)$ . Правильное комбинаторно, но не геометрически изображение карты R26.2, содержащей 60 вершин валентности 11, 330 рёбер и 220 треугольных клеток, можно найти в [44, рис. 6 и табл. 1]. Там эта карта изображена в виде 198-угольника с указанием идентификации его сторон. Авторы [44] дают интерпретацию регулярных карт из статей Ф. Клейна [54] и [55] в терминах дробей Фарея.

Восемь рисунков  $\mathcal{D}$  с группой монодромии  $A_{11}$  включают три киральные пары  $\mathcal{M}_i$  и  $\bar{\mathcal{M}}_i$ ,  $i = 2, 3, 4$ , плюс два рисунка  $\mathcal{M}_5$  и  $\mathcal{M}_6$ . Минимальные регулярные накрытия этих рисунков — это восемь регулярных рисунков  $\mathcal{R}$  рода 756 001, и каждый рисунок  $\mathcal{D}$  является фактором рисунка  $\mathcal{R}$  по подгруппе, изоморфной  $A_{10}$ , его группы автоморфизмов  $A_{11}$ . Эти восемь рисунков  $\mathcal{R}$  не изоморфны друг другу, поскольку  $A_{11}$  имеет единственный класс сопряжённости таких подгрупп (это стабилизаторы точек в естественном представлении), так что любой изоморфизм рисунков  $\mathcal{R}$  индуцировал бы изоморфизм их факторов  $\mathcal{D}$ , что, разумеется, невозможно (см. рис. 3).

Осевая симметрия рисунков  $\mathcal{M}_5$  и  $\mathcal{M}_6$  легко объяснима: во всех случаях имеется перестановка в  $S_{11}$ , одновременно обращающая образующие  $x$  и  $y$  группы монодромии  $A_{11}$ , и она индуцирует изоморфизм рисунка и его зеркального образа. (Разумеется, в силу того что  $y^2 = 1$ , обращение  $y$  — это то же самое, что коммутирование с ним.) Эквивалентное утверждение состоит в том, что каждая отвечающая карте подгруппа  $M$  в  $\Delta(3, 2, 11)$  содержится с индексом 2 в подгруппе группы  $\Delta[3, 2, 11]$ , которая индуцирует указанный выше изоморфизм. То же самое относится к регулярным накрытиям рисунков  $\mathcal{M}_5$  и  $\mathcal{M}_6$ , которые соответствуют *ядру* (пересечению сопряжённых) групп  $M$  в  $\Delta(3, 2, 11)$ . Остальные шесть регулярных накрытий образуют три киральные пары, так же как и их факторы.

Например, на рис. 7 показана карта  $\mathcal{M}_5$ , соответствующая рисунку  $\mathcal{D}_5$ ; ориентированные рёбра помечены  $1, 2, \dots, 11$ , так что

$$x = (1, 11, 6)(2, 5, 4)(7, 10, 8), \quad y = (1, 5)(2, 3)(6, 10)(8, 9)$$

и, следовательно,

$$z = (1, 2, \dots, 11).$$

Перестановка  $t = (1, 6)(2, 8)(3, 9)(4, 7)(5, 10)$  обращает  $x$  и  $y$ , индуцируя автоморфизм рисунка  $\mathcal{M}_5$ , представляющий собой отражение относительно вертикальной оси. Аналогичная ситуация имеет место и для  $\mathcal{M}_6$  — с образующими

$$x = (1, 11, 6)(2, 5, 3)(7, 10, 9), \quad y = (1, 5)(3, 4)(6, 10)(7, 8),$$

которые обращает перестановка  $t = (1, 6)(2, 9)(3, 7)(4, 8)(5, 10)$ .

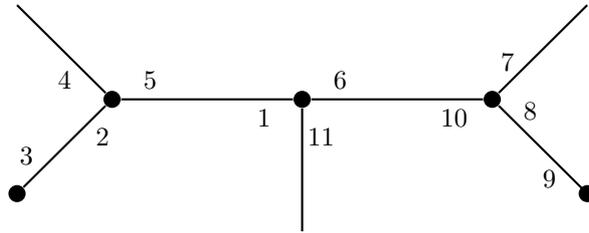


Рис. 7. Карта  $\mathcal{M}_5$ , соответствующая дереву Клейна номер V

## 6. Вычисления и орбиты Галуа

Каждый из обсуждаемых здесь рисунков  $\mathcal{D}$  задаёт функцию Белого, которая в данном случае представляет собой 11-листное накрытие  $\beta: \Sigma \rightarrow \Sigma$ . Тем самым  $\beta$  является рациональной функцией степени 11, а поскольку она имеет единственный полюс в бесконечности, она является многочленом, называемым многочленом Шабата.

Вычисления с помощью Maple дают многочлены Шабата  $P: \Sigma \rightarrow \Sigma$  для рисунков  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$  (см. рис. 2) в следующем виде:

$$P = \frac{1}{2^{12}3^{14}}p_1^3p_2^3p_3,$$

где

$$\begin{aligned} p_1(x) &= 2x + (11 - 3\sqrt{-11}), \\ p_2(x) &= 2x^2 - (11 - 3\sqrt{-11})x - (22 + 6\sqrt{-11}), \\ p_3(x) &= x^2 + 11x + (55 + 9\sqrt{-11}), \end{aligned}$$

так что

$$P - 1 = -\frac{1}{2^{11}3^{14}}q_1^2q_2^2q_3,$$

где

$$\begin{aligned} q_1(x) &= 2x + (5 + 3\sqrt{-11}), \\ q_2(x) &= 2x^3 + (15 - 3\sqrt{-11})x^2 - (12 - 12\sqrt{-11})x + (56 + 96\sqrt{-11}), \\ q_3(x) &= 2x^3 - 18x^2 + (21 + 45\sqrt{-11})x - (175 + 279)\sqrt{-11}. \end{aligned}$$

Два возможных выбора для  $\sqrt{-11}$  дают два рисунка. Они определены над полем  $\mathbb{Q}(\sqrt{-11})$  (что неудивительно, так как  $\sqrt{-11}$  присутствует в таблице характеров группы  $\mathrm{PSL}_2(11)$ ) и переставляются группой Галуа этого поля, порождённой комплексным сопряжением.

В каждом из рисунков чёрные вершины расположены в корнях многочлена  $P$ . Три вершины валентности 3 — корни многочленов  $p_1$  и  $p_2$ ; как корни многочлена  $P$  они имеют кратность 3. Две вершины валентности 1 — корни многочлена  $p_3$ . Белые вершины расположены в корнях многочлена  $P - 1$ . Четыре вершины валентности 2 соответствуют корням кратности 2 многочлена  $P - 1$ , т. е. корням многочленов  $q_1$  и  $q_2$ . Три вершины валентности 1 — корни многочлена  $q_3$ . Центр единственной клетки лежит в точке  $\infty$ : это полюс многочлена  $P$ , его кратность равна 11. На рис. 8 показано геометрически правильное изображение рисунка  $\mathcal{M}_1$  на плоскости  $\mathbb{C}$ . За редкими исключениям (см. рис. 15, 16 и 18) все деревья, рисунки и карты в этой статье изображаются в виде, правильном комбинаторно и топологически, но не геометрически.

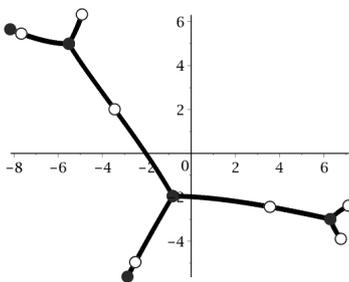


Рис. 8. Геометрически правильное изображение рисунка  $\mathcal{M}_1$

Оставшиеся восемь рисунков представляют собой единую орбиту Галуа. Вычисление с помощью системы Pari/GP выдаёт несколько многочленов, корни которых порождают поле модулей этой орбиты. Один из самых простых многочленов такой:

$$Z^8 + 2Z^6 - 3Z^5 + 10Z^4 - 14Z^3 + 14Z^2 - 8Z + 1.$$

Группа Галуа этого поля равна  $S_8$ , так что она переставляет восемь рисунков всеми возможными способами. Полученное поле не содержит ни  $\mathbb{Q}(\sqrt{-11})$ , ни  $\mathbb{Q}(\sqrt{21})$ , хотя  $\sqrt{21}$  и фигурирует в таблице характеров группы  $A_{11}$ .

## 7. Родственные рисунки степени 11

Кроме тех десяти рисунков, которые мы до сих пор рассматривали, существуют и другие рисунки степени 11 и типа  $(3, 2, r)$ , где  $r$  — наименьшее общее кратное валентностей клеток. Легко видеть, что у любого такого рисунка распределение валентностей чёрных вершин должно быть  $3^3 1^2$ , в то время как для белых вершин есть две возможности:  $2^4 1^3$  и  $2^5 1^1$ . В первом случае мы получаем знакомые нам десять рисунков Клейна, и у всех у них  $r = 11$ . Во втором же случае мы получаем плоские рисунки не с одной, а с двумя клетками; их Ф. Клейн не рассматривал.

Все карты, соответствующие этим дополнительным рисункам, можно построить исходя из базовой карты  $M_0$ , изображённой на рис. 4, добавив чёрные вершины валентности 1 к двум висячим рёбрам, как это было сделано при построении карт  $M = M_i$  и  $M_i$ , а затем соединив друг с другом два из трёх оставшихся висячих рёбер, сформировав из них одно невисячее ребро. Можно вместо этого проделать последнюю операцию с каждой из десяти карт  $M$ . Для каждой карты имеется три возможности сделать такую склейку, что даёт нам 30 карт нужного вида, однако многие из них оказываются изоморфными друг другу, так что с точностью до изоморфизма мы получаем 16 карт (проверено на GAP). Это множество складывается из четырёх карт, обладающих зеркальной симметрией (верхний ряд рис. 9) и из шести киральных пар (это шесть карт в втором ряду рис. 9 и их зеркальные образы). Имеется шесть карт, у которых валентности клеток — 10 и 1, по три карты с валентностями 9 и 2 или 7 и 4 и по две с валентностями 8 и 3 или 6 и 5. Этим рисункам соответствуют 16 дополнительных классов сопряжённости подгрупп индекса 11 в модулярной

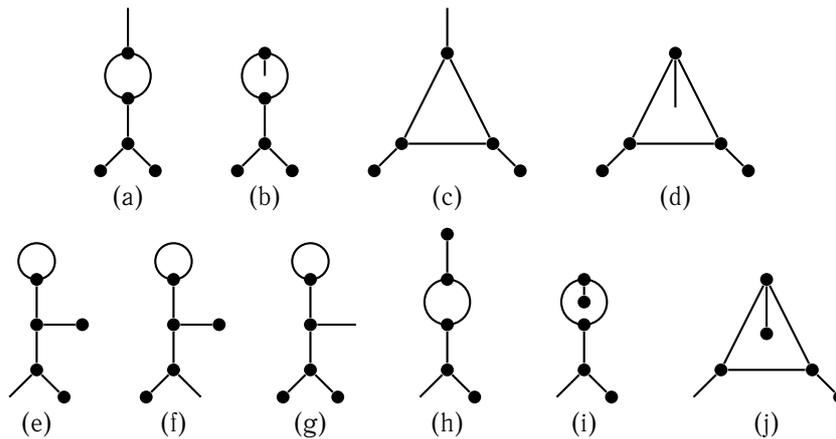


Рис. 9. Карты степени 11 и типа  $(3, 2, r)$ ,  $r \neq 11$ .  
В нижнем ряду для каждой киральной пары дан один представитель

группе  $\Gamma$ , кроме тех десяти, что отвечают плоским деревьям Клейна. (Этот факт подтверждает также теорема 1 из [35]. В этой теореме приводится рекуррентное соотношение для количества  $N_n$  подгрупп индекса  $n$  в  $\Gamma$ . В нашем случае  $N_{11} = 286$ : имеется  $10 + 16 = 26$  классов сопряжённости, каждый из которых содержит 11 подгрупп.) Во всех случаях, кроме разбиения  $10 + 1$ , одна из валентностей клеток является простым числом  $p$ , и  $z^{11-p}$  — это  $p$ -цикл плюс  $11 - p \geq 3$  неподвижных точек. Будучи транзитивной группой простой степени, группа  $G = \langle x, y \rangle$  примитивна, поэтому из теоремы Жордана и из нечётности перестановки  $y$  следует, что  $G = S_{11}$ . В случае  $10 + 1$  мы можем применить усиленную версию теоремы Жордана [45] к циклам длины 10 и 11; из неё следует, что группа  $G$  действует либо как  $S_{11}$ , либо как  $AGL_1(11)$ . Последний случай, однако, исключается, поскольку группа  $AGL_1(11)$  не имеет элементов порядка 3. В результате заключаем, что эти рисунки соответствуют не-конгруэнт-подгруппам группы  $\Gamma$ .

Регулярные накрытия всех перечисленных рисунков имеют род

$$1 + \frac{(r-6)}{12r} 11!,$$

как указано в таблице 1.

Таблица 1.

Клетки	10, 1	9, 2	8, 3	7, 4	6, 5
$r$	10	18	24	28	30
Род накрытия	1 330 561	2 217 601	2 494 801	2 613 601	2 661 121
Карты (см. рис. 9)	e, f, g	a, h	b, c	d, i	j
Число карт	6	3	2	3	2

## 8. Группы монодромии рисунков типа $(3, 2, p)$ и степени $p$

Мы можем обобщить наши рассуждения и рассмотреть рисунки  $\mathcal{D}$  типа  $(3, 2, p)$  и степени  $p$  для произвольных простых  $p$ , а не только для  $p = 11$ . Группа монодромии  $G$  такого рисунка — это транзитивная группа перестановок степени  $p$ . Она будет совершенной, если  $p > 3$ , что мы и будем в дальнейшем предполагать. Такая группа совершенна, поскольку числа 3, 2 и  $p$  взаимно просты. Транзитивные группы простой степени  $p$  все известны (по модулю очень трудной открытой проблемы из теории чисел, которую мы обсудим в следующем разделе); они описаны, например, в [17, 26, 43]. Вот список этих групп.

**Теорема 8.1.** *Транзитивные группы перестановок  $G$  простой степени принадлежат одной из следующих категорий:*

- (a) подгруппы  $G$  группы  $\text{AGL}_1(p)$ , содержащие циклическую группу  $C_p$ ;
- (b)  $G = A_p$  или  $G = S_p$  для простого  $p \geq 5$ ;
- (c)  $G = \text{PSL}_2(11)$ ,  $G = M_{11}$  или  $G = M_{23}$  при  $p = 11$ ,  $p = 11$  или  $p = 23$  соответственно;
- (d) такие группы  $G$ , что  $\text{PSL}_n(q) \leq G \leq \text{PGL}_n(q)$ , если степень их естественного представления  $(q^n - 1)/(q - 1)$  является простым числом.

Согласно результату Галуа [31] разрешимые группы простой степени  $p$  — это группы, перечисленные в пункте (a). У. Бёрнсайд показал (см. [15] или [16, § 251]), что любая неразрешимая группа  $G$  простой степени  $p$  дважды транзитивна. В этом случае простой аргумент показывает, что  $S \leq G \leq \text{Aut } S$ , причём группа  $S$  — единственная минимальная нормальная подгруппа группы  $G$  — является дважды транзитивной неабелевой простой группой. Согласно теореме классификации конечных простых групп для группы  $S$  имеются следующие возможности: группы  $S = A_p$  для простого  $p \geq 5$ , порождающие группы из пункта (b), три группы  $S = G$  из пункта (c) и группы  $S = \text{PSL}_n(q)$ , порождающие группы из пункта (d).

В пунктах (a) и (b) имеются в виду естественные действия упомянутых групп. В пункте (c) группа  $\text{PSL}_2(11)$  имеет два разных действия степени 11: она действует на классах смежности двух классов сопряжённости подгрупп, изоморфных группе  $A_5$ . Группы Матьё  $M_{11}$  и  $M_{23}$  действуют на системах Штейнера из 11 и 23 точек. В пункте (d) группы действуют на точках проективной геометрии  $\mathbb{P}^{n-1}(\mathbb{F}_q)$ , а при  $n \geq 3$  имеется ещё и двойственное действие на гиперплоскостях той же геометрии. В частности, поскольку группа внешних автоморфизмов  $\text{Out } S$  всегда разрешима, справедливо следующее утверждение.

**Следствие 8.2.** *Единственными совершенными группами простой степени являются простые группы  $A_p$ ,  $\text{PSL}_2(11)$ ,  $M_{11}$ ,  $M_{23}$  и  $\text{PSL}_n(q)$ , фигурирующие в пунктах (b), (c) и (d) теоремы 8.1.*

У всех этих простых групп имеются элементы  $x$ ,  $y$  и  $z$  порядков 3, 2 и  $p$ , так как порядки этих групп делятся на упомянутые простые числа. Остаётся вопрос, существуют ли такие тройки, удовлетворяющие условию  $xyz = 1$ , порождают ли они группу  $G$  и, если так, можно ли описать (или хотя бы перечислить) соответствующие рисунки  $\mathcal{D}$ . Мы рассмотрим эти вопросы отдельно для разных случаев в этом и двух следующих разделах. А пока что вычислим род этих рисунков и род их регулярных накрытий.

Если  $x$  и  $y$  имеют цикловые структуры  $3^a 1^\alpha$  и  $2^b 1^\beta$  соответственно, где  $\alpha = p - 3a$  и  $\beta = p - 2b$ , то рисунок  $\mathcal{D}$  имеет  $p - 2a$  чёрных вершин,  $p - b$  белых вершин,  $p$  рёбер и одну клетку. Следовательно, его эйлерова характеристика равна

$$\chi = (p - 2a) + (p - b) - p + 1 = p - 2a - b + 1 = \frac{4\alpha + 3\beta - p}{6} + 1,$$

а род равен

$$1 - \frac{\chi}{2} = \frac{2a + b + 1 - p}{2} = \frac{p - 4\alpha - 3\beta + 6}{12}.$$

(Заметим, что из этих формул следуют два эквивалентных неравенства:  $2a + b \geq p - 1$  и  $4\alpha + 3\beta \leq p + 6$ .) Если такой рисунок  $\mathcal{D}$  существует, то у него есть регулярное накрытие  $\mathcal{R}$  типа  $(3, 2, p)$  с группой автоморфизмов  $G$ . Этот накрывающий рисунок имеет  $|G|/3$  чёрных вершин валентности 3,  $|G|/2$  белых вершин валентности 2,  $|G|$  рёбер и  $|G|/p$  клеток валентности  $p$ . Поэтому его эйлерова характеристика равна

$$\chi = \left( \frac{1}{3} + \frac{1}{2} + \frac{1}{p} - 1 \right) \cdot |G| = \frac{6-p}{6p}|G|$$

и род, соответственно, равен

$$g = 1 - \frac{\chi}{2} = \frac{p-6}{12p}|G| + 1.$$

### 8.1. Случай (с): спорадические примеры

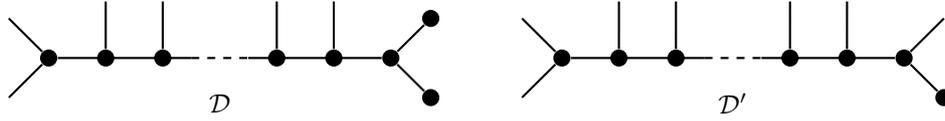
Удобно сначала разобраться со случаем (с). В примерах 4.1 и 4.2 мы видели, что для  $p = 11$  группа  $M_{11}$  в качестве группы монодромии рисунка типа  $(3, 2, p)$  и степени  $p = 11$  не возникает, в то время как группа  $\text{PSL}_2(11)$  служит группой монодромии киральной пары деревьев  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ . Формула Фробениуса позволяет исключить случай  $M_{23}$ : эта группа не содержит троек  $(x, y, z)$  типа  $(3, 2, 23)$ , таких что  $xyz = 1$ .

### 8.2. Случай (b): знакопеременные группы

Группа, рассматриваемая в случае (b), — это  $G = A_p$  для некоторого простого  $p$ . Следующий результат показывает, что почти все такие группы реализуются в качестве групп монодромии в требуемом контексте.

**Теорема 8.3.** *Для любого простого  $p \neq 2, 3, 7$  существует рисунок  $\mathcal{D}$  степени  $p$  и типа  $(3, 2, p)$  с группой монодромии  $A_p$ .*

**Доказательство.** Для начала предположим, что  $p \equiv 2 \pmod{3}$ , и обозначим  $p = 3k + 2$ . Для  $p = 5$  карта очевидна, так что предположим, что  $p \geq 11$  и, следовательно,  $k \geq 3$ . Пусть  $\mathcal{D}$  — это левая карта на рис. 10: у неё  $k$  вершин валентности 3, так что её паспорт равен  $(3^k 1^2, 2^{k+1} 1^k, p^1)$ . Мы намереемся доказать, что её группа монодромии  $G$  равна  $A_p$ . Согласно следствию 8.2 и обсуждению спорадических примеров в случае (с) достаточно доказать, что группа  $G$  не совпадает ни с  $\text{PSL}_2(11)$  с действием степени 11, ни с  $\text{PSL}_n(q)$  с естественным действием для некоторого  $n \geq 2$  и степени простого числа  $q$ . На самом деле при  $p = 11$  и  $k = 3$  рисунок  $\mathcal{D}$  изоморфен рисунку  $\bar{\mathcal{M}}_3$  (см. рис. 3), а мы видели, что его группа монодромии равна  $A_{11}$ . Тогда предположим

Рис. 10. Карты  $\mathcal{D}$  и  $\mathcal{D}'$  для  $p = 3k + 2$  и  $p = 3k + 1$ 

от противного, что  $G = \text{PSL}_n(q)$  с естественным действием, причём  $p \geq 17$ , так что  $k \geq 5$ .

Пусть  $\pi$  обозначает перестановочный характер группы  $S_p$ , подсчитывающий количество неподвижных точек её элементов. Мы видим, что для инволюции  $y$ , отвечающей рисунку  $\mathcal{D}$ , доля неподвижных точек

$$\frac{\pi(y)}{\pi(1)} = \frac{k}{p} = \frac{k}{3k+2} \geq \frac{5}{17}.$$

Сравним это с числом неподвижных точек инволюций в группе  $\text{PSL}_n(q)$ . Любая инволюция в  $\text{PSL}_2(q)$  оставляет на месте не больше двух точек. Следовательно,  $n \neq 2$ , поскольку  $\pi(y) = k \geq 5$ . При  $n \geq 3$  доля неподвижных точек  $\pi(g)/\pi(1)$  инволюций  $g \in \text{PSL}_n(q)$  ограничена сверху числом

$$b_{\text{even}} = \frac{q^{n-2} + q^{n-3} + \dots + q + 1}{q^{n-1} + q^{n-2} + \dots + q + 1} \quad \text{или} \quad b_{\text{odd}} = \frac{(q^{n-3} + \dots + q + 1) + (q + 1)}{q^{n-1} + q^{n-2} + \dots + q + 1}$$

для  $q$  чётных или нечётных. Эти оценки достигаются в том случае, когда  $g$  оставляет неподвижными соответственно точки гиперплоскости либо же два непересекающихся подпространства размерностей  $n - 3$  и  $1$ . Эти ситуации соответствуют матрицам из  $\text{SL}_n(q)$  с жордановой нормальной формой, заданной блочными матрицами

$$\begin{pmatrix} J & O \\ O & I \end{pmatrix}, \quad \text{где } J = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{и } I = I_{n-2}.$$

Легко проверить, что если  $q$  нечётно, то  $b_{\text{odd}} < 5/17$ , так что  $G \neq \text{PSL}_n(q)$ , кроме, может быть, случая  $n = q = 3$ , при котором  $b_{\text{odd}} = 5/13$ . Однако этот исключительный случай соответствует  $p = 13 \not\equiv 2 \pmod{3}$ . Следовательно,  $q$  чётно. Но тогда  $q = 2$ , поскольку  $b_{\text{even}} < 1/q$ . Это даёт  $3k + 2 = p = 2^n - 1$ , откуда следует, что  $2^n \equiv 0 \pmod{3}$ , что невозможно.

Мы можем применить сходные аргументы, когда  $p \equiv 1 \pmod{3}$ . Пусть  $p = 3k + 1$ . Мы можем считать, что  $p \geq 13$ , т. е.  $k \geq 4$ . Удалив из  $\mathcal{D}$  вершину валентности  $1$ , мы получим карту  $\mathcal{D}'$  степени  $p$  и типа  $(3, 2, p)$  с паспортом  $(3^k 1^1, 2^k 1^{k+1}, p^1)$ , показанную справа на рис. 10. Соответствующая инволюция  $y$  теперь имеет долю неподвижных точек

$$\frac{\pi(y)}{\pi(1)} = \frac{k+1}{p} = \frac{k+1}{3k+1} \geq \frac{5}{13}.$$

Как и ранее, если  $G = \mathrm{PSL}_n(q)$ , то из  $\pi(y) > 2$  следует, что  $n \geq 3$ . Мы уже видели, что если  $q$  нечётно, то  $b_{\mathrm{odd}} < 5/17$ , откуда следует, что  $b_{\mathrm{odd}} < 5/13$ . Следовательно,  $G \neq \mathrm{PSL}_n(q)$ , за исключением, может быть, случая  $n = q = 3$ . Однако в этом случае  $p = 13$ , и вычисление на GAP показывает, что группа монодромии рисунка  $\mathcal{D}'$  — это не  $\mathrm{PSL}_3(3)$ , а  $A_{13}$ . Значит,  $q$  должно быть чётным. Но тогда снова  $q = 2$ , поскольку  $b_{\mathrm{even}} < 1/q$ . Отсюда следует, что если какой-то элемент группы  $G = \mathrm{PSL}_n(2)$  имеет неподвижные точки, эти точки должны образовывать проективное подпространство. Таким образом,  $k = \pi(y)$  нечётно, откуда следует, что  $p = 3k + 1$  чётно: противоречие.  $\square$

Легко обнаружить, что рисунков, соответствующих  $p = 2$  и  $p = 3$ , не существует. При  $p = 7$  имеется киральная пара рисунков требуемой степени и типа: один из представителей этой пары — это  $\mathcal{D}'$  на рис. 10 при  $k = 2$ . Но их группа монодромии — это  $\mathrm{PSL}_2(7)$ , а не  $A_7$  (последняя, кстати, не гурвицева).

Простые модификации карт рис. 10 показывают, что в доказательстве теоремы 8.3 число возможных выборов для  $\mathcal{D}$  и  $\mathcal{D}'$  растёт экспоненциально с ростом  $p$ , и это несмотря на то, что данная конструкция даёт только планарные рисунки.

### 8.3. Случай (d): проективные группы

В оставшейся части этого раздела мы будем рассматривать случай (d), т. е. будем предполагать, что наша группа — это группа  $G = \mathrm{PSL}_n(q)$ , действующая на точках или гиперплоскостях проективного пространства  $\mathbb{P}^{n-1}(\mathbb{F}_q)$ . (Этот случай и теоретико-числовые оценки и компьютерный поиск из раздела 9 освещены более детально в [50].)

**Предупреждение:** вопреки общепринятым обозначениям, неназванное простое число, степенью которого является параметр  $q$ , *не будет* обозначаться буквой  $p$ . Напротив,  $p$  будет обозначать степень  $(q^n - 1)/(q - 1)$  группы  $G$ .

Прежде чем продолжить, затронем вкратце некоторые вопросы теории чисел. Назовём простое число  $p$  *проективным*, если оно имеет вид

$$p = \frac{q^n - 1}{q - 1} = 1 + q + q^2 + \dots + q^{n-1},$$

где  $q \geq 2$  является степенью простого числа и  $n \geq 2$ . Проективные простые числа включают как частные случаи простые числа Ферма  $p = 2^{2^k} + 1$  (здесь  $q = 2^{2^k}$  и  $n = 2$ ), простые числа Мерсенна  $p = 2^n - 1$  (здесь  $q = 2$ , а  $n$  простое), а также многие другие примеры с  $q, n \geq 3$ , как, например,  $p = 13$  с  $q = n = 3$  или  $p = 31$  с  $q = 5$  и  $n = 3$  (заметим, что  $p = 31$  является также простым числом Мерсенна). Разумеется, вопросы о том, конечно или бесконечно количество простых чисел Ферма и Мерсенна, являются открытыми. В настоящий момент известно только 5 простых чисел Ферма (при  $k = 0, \dots, 4$ ) и 52 простых числа Мерсенна. Более общий вопрос о том, конечно или бесконечно множество проективных простых чисел, тоже, судя по всему, является открытым. В [50] мы

приводим эвристические аргументы, основанные на гипотезе Бейтмана—Хорна, а также на компьютерных вычислениях, в пользу гипотезы, что для любого простого  $n \geq 3$  количество проективных простых чисел бесконечно. Эти аргументы кратко сформулированы в следующем разделе. Но сначала приведём несколько необходимых условий для того, чтобы число  $(q^n - 1)/(q - 1)$  было простым.

**Лемма 8.4.** Пусть  $q$  — степень простого числа и  $n \geq 2$ . Если число  $p = (q^n - 1)/(q - 1)$  простое, то

- (а) число  $n$  простое;
- (б)  $q \not\equiv 1 \pmod{n}$ ;
- (в)  $\text{PSL}_n(q) = \text{SL}_n(q)$ ;
- (г) если  $e$  — показатель степени простого числа в  $q$ , то  $e$  является степенью показателя  $n$ .

**Доказательство.** (а) Если число  $n$  составное, то существует очевидное разложение многочлена  $1 + q + \dots + q^{n-1}$  на множители.

(б) Если  $q \equiv 1 \pmod{n}$ , то  $p = 1 + q + \dots + q^{n-1} \equiv 0 \pmod{n}$ , причём  $p > n$ .

(в) Для произвольных  $q$  и  $n$  имеет место равенство  $\text{PSL}_n(q) = \text{SL}_n(q)/Z$ , где  $Z = \{\lambda I \in \text{GL}_n(q) \mid \lambda^n = 1\} \cong C_d$  — это центр группы  $\text{SL}_n(q)$ , и  $d = \gcd(q-1, n)$ . Если  $p$  простое, то в силу (а) и (б) мы получаем  $d = 1$ .

(г) Пусть  $k \in \mathbb{N}$ . Циклотомический многочлен  $\Phi_k(x)$  — это, по определению, многочлен с целыми коэффициентами, корнями которого являются все примитивные корни степени  $k$  из единицы. Например, если  $k$  простое, то

$$\Phi_k(x) = 1 + x + \dots + x^{k-1},$$

в то же время  $\Phi_4(x) = x^2 + 1$ ,  $\Phi_6(x) = x^2 - x + 1$ . Степень многочлена  $\Phi_k$  равняется  $\varphi(k)$ , где  $\varphi$  — это функция Эйлера. Важным свойством циклотомических многочленов является то, что для произвольного (не обязательно простого)  $n \in \mathbb{N}$  имеет место равенство

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Пусть теперь  $q = r^e$ , где  $r$  простое. Возьмём  $x = r$  и рассмотрим многочлен

$$p = 1 + q + \dots + q^{n-1} = 1 + r^e + \dots + r^{e(n-1)} = \frac{r^{en} - 1}{r^e - 1} = \prod_d \Phi_d(r);$$

произведение в правой части берётся по всем  $d$ , которые делят  $en$ , но не делят  $e$ . Учитывая тот факт, что число  $p$  простое, а  $\Phi_d(r) \neq \pm 1$ , мы заключаем, что произведение справа содержит всего один многочлен  $\Phi_d$  и параметр  $d$  тоже принимает единственное значение. Это означает, что множество делителей числа  $e$  содержит все делители числа  $en$ , кроме одного (этот отсутствующий делитель — это, разумеется, само  $en$ ), что возможно только если  $e$  является степенью  $n$ .  $\square$

## 9. Гипотеза Бейтмана—Хорна

Гипотеза Бейтмана—Хорна [10] — это количественная форма качественной гипотезы Н. А. Шинцеля [68]. Обе гипотезы отвечают на вопрос, при каких условиях на конечное семейство многочленов  $f_1(t), \dots, f_k(t) \in \mathbb{Z}[t]$  существует бесконечно много значений  $t \in \mathbb{N}$ , при которых все  $f_i(t)$  одновременно являются простыми числами. (Гипотеза Н. А. Шинцеля, в свою очередь, является обобщением гипотезы Буняковского (1857, см. [3, 14]), относящейся к случаю  $k = 1$ .) Очевидно, следующие условия являются необходимыми для того, чтобы все  $f_i(t)$  принимали простые значения бесконечно много раз:

- старший коэффициент каждого из многочленов  $f_i$  положителен,
- многочлены  $f_i$  неприводимы,
- произведение  $f := f_1 \dots f_k$  не равно тождественно нулю по модулю любого простого числа.

Последнее условие может быть проверено следующим образом. Для простого  $p > \deg(f)$  многочлен  $f$  тождественно равен нулю по модулю  $p$  только в случае, когда все его коэффициенты делятся на  $p$ . Для простых  $p \leq \deg(f)$  достаточно вычислить  $f(t)$  для всех элементов  $t \in \mathbb{Z}_p$ .

А. Шинцель (следуя В. Я. Буняковскому для  $k = 1$ ) выдвинул гипотезу, что эти три условия являются также и достаточными. Из этой гипотезы, если она окажется верной, следует множество других гипотез теории чисел. Например, взяв  $f_1(t) = t^2 + 1$ , мы получим гипотезу Эйлера—Ландау о бесконечности простых чисел вида  $t^2 + 1$ ; взяв  $f_1(t) = t$  и  $f_2(t) = t + 2$ , мы получим гипотезу о бесконечности простых чисел-близнецов; взяв  $f_1(t) = t$  и  $f_2(t) = 2t + 1$  — гипотезу о бесконечности множества простых чисел Софи Жермен.

Гипотеза Бейтмана—Хорна идёт ещё дальше: основываясь на теореме о распределении простых чисел, она даёт эвристическую оценку для числа  $Q(x)$  таких  $t \leq x$  в  $\mathbb{N}$ , при которых все значения  $f_i(t)$  являются простыми. Эта оценка имеет следующий вид:

$$Q(x) \sim E(x) := \frac{C}{\prod_{i=1}^k \deg f_i} \int_2^x \frac{dt}{(\ln t)^k} \quad \text{при } x \rightarrow \infty, \quad (4)$$

где

$$C = C(f_1, \dots, f_k) := \prod_r \left(1 - \frac{1}{r}\right)^{-k} \left(1 - \frac{\omega_f(r)}{r}\right). \quad (5)$$

Последнее произведение берётся по всем простым числам  $r$ , а  $\omega_f(r)$  — это число таких  $t \in \mathbb{F}_r$ , при которых  $f(t) = 0$ .

Если функции  $f_1, \dots, f_k$  удовлетворяют перечисленным выше условиям, то бесконечное произведение в (5) сходится к конечному пределу  $C > 0$  (этот факт ни в коей мере не тривиален: см. теорему 5.4.3 в [9]). Поскольку интеграл в (4) при  $x \rightarrow \infty$  расходится, то из гипотезы Бейтмана—Хорна следует, что значения

$f_1(t), \dots, f_k(t)$  являются одновременно простыми для бесконечно многих  $t \in \mathbb{N}$ . К настоящему времени все три гипотезы доказаны только в одном случае:  $k = 1$ ,  $\deg f_1 = 1$ . Гипотезы Буняковского и Шинцеля в этом случае совпадают с теоремой Дирихле о простых числах в арифметической прогрессии  $at + b$ , где  $a$  и  $b$  взаимно просты; гипотеза Бейтмана—Хорна даёт более сильную формулировку этой теоремы, утверждая, что простые числа асимптотически распределены поровну среди классов  $b \pmod{a}$  (см. доказательство в [2, § 5.3.2] и оценку для ошибки в [72]).

Тем не менее гипотеза Бейтмана—Хорна даёт оценки, замечательные по своей точности и близости к экспериментальным результатам. Приведём всего один пример. Количество пар простых чисел-близнецов, не превышающих  $10^{18}$ , равно 808 675 888 577 436 (см. раздел A007508 в [67]). Оценка Бейтмана—Хорна равна 808 675 900 456 220; относительная погрешность этой оценки равна  $-0,000000147\%$  (см. также [9, рис. 10]). Константа  $C$  в этом случае равна  $1,320323630\dots$ , а её половина  $C/2 = 0,660161815\dots$  по традиции носит название «константы простых чисел-близнецов».

**Замечание 9.1.** В. Ли [58] предложил модифицированную версию гипотезы Бейтмана—Хорна: в ней произведение  $\prod_i \deg f_i$  в знаменателе отсутствует, но зато каждый множитель  $1/\ln(t)$  в подынтегральном выражении заменён на  $1/\ln(f_i(t))$ . Нижний предел интегрирования можно скорректировать таким образом, чтобы избежать логарифмической сингулярности при  $f_i(t) = 1$ . Получающийся результат асимптотически эквивалентен тому, что даёт исходная гипотеза, но в тех случаях, когда в задаче присутствуют многочлены со старшим коэффициентом, большим единицы (как это имеет место, например, в гипотезе о простых числах Софи Жермен), аппроксимация Ли даёт существенно лучший результат.

Возьмём теперь  $k = 2$ ,  $f_1(t) = t$  и  $f_2(t) = 1 + t^e + t^{2e} + \dots + t^{(n-1)e}$  с фиксированным простым  $n \geq 3$  и фиксированным показателем  $e \geq 1$ , являющимся степенью числа  $n$ . Тогда гипотеза даст нам оценку  $E(x)$  для количества  $Q(x)$  простых чисел  $t \leq x$ , таких что число  $1 + q + q^2 + \dots + q^{n-1}$ , где  $q = t^e$ , тоже является простым. Компьютерные подсчёты подтверждают очевидную догадку, что  $Q(x)$  растёт быстрее всего, когда  $n$  и  $e$  принимают наименьшие значения  $n = 3$  и  $e = 1$  (так что  $q$  является простым) и функция  $f_2$  равна  $f_2(t) = 1 + t + t^2$ . Так, например<sup>1</sup>, из 1974311 проективных простых чисел  $p \leq 10^{18}$  только 301 число имеет форму, отличающуюся от  $p = 1 + q + q^2$  для некоторого простого  $q$ .

Взяв  $n = 3$  и  $e = 1$ , так что  $f = t(1 + t + t^2)$ , мы получаем

$$\omega_f(r) = \begin{cases} 3, & \text{если } r \equiv 1 \pmod{3}, \\ 2 & \text{при } r = 3, \\ 1 & \text{в остальных случаях.} \end{cases}$$

<sup>1</sup>Вычисления провёл наш коллега Жан Бетрема [13]; при этом он использовал систему Julia, которая в данном случае оказалась более эффективной, чем Maple.

Таблица 2. Сравнение оценок  $E(x)$ , которые даёт гипотеза Бейтмана—Хорна, с истинными значениями  $Q(x)$ . Здесь  $Q(x)$  — это число таких простых  $t \leq x$ , что число  $1 + t + t^2$  тоже простое

$x$	$Q(x)$	$E(x)$	$E(x)/Q(x)$
$1 \cdot 10^{10}$	15 801 827	$1,579642126 \times 10^7$	0,9996579044
$2 \cdot 10^{10}$	29 684 763	$2,968054227 \times 10^7$	0,9998578150
$3 \cdot 10^{10}$	42 963 858	$4,296235691 \times 10^7$	0,9999650617
$4 \cdot 10^{10}$	55 877 571	$5,587447496 \times 10^7$	0,9999445924
$5 \cdot 10^{10}$	68 522 804	$6,852175590 \times 10^7$	0,9999847043
$6 \cdot 10^{10}$	80 962 422	$8,096382889 \times 10^7$	1,0000173771
$7 \cdot 10^{10}$	93 236 613	$9,323905289 \times 10^7$	1,0000261688
$8 \cdot 10^{10}$	105 372 725	$1,053741048 \times 10^8$	1,0000130940
$9 \cdot 10^{10}$	117 383 505	$1,173885689 \times 10^8$	1,0000431394
$10^{11}$	129 294 308	$1,292974079 \times 10^8$	1,0000239757

Используя Maple, находим константу  $C \approx 1,52173006$ , вычисляя произведение (5) по всем простым  $r < 10^9$ , после чего, вновь с помощью Maple, вычисляем

$$\int_2^x \frac{dt}{(\ln t)^2}.$$

Получающиеся оценки  $E(x)$  при  $x = i \cdot 10^{10}$  ( $i = 1, 2, \dots, 10$ ) сравниваются с истинными значениями  $Q(x)$  (на этот раз вычисленными с помощью Julia [13]) в табл. 2. Заметим, что в данном случае использование улучшенной оценки Ли, упоминавшейся в замечании 9.1, даёт пренебрежимо малый эффект. Например, для  $x = 10^{11}$  использование  $1/\ln(1+t+t^2)$  вместо  $1/2\ln(t)$  в подынтегральном выражении даёт оценку 129 297 407,4 вместо оценки 129 297 407,9, стоящей в табл. 2. Относительные ошибки, показанные в этой таблице, все меньше, чем 0,00034, т. е. 0,034 %.

Аналогичные сравнения для других значений  $n$  и  $e$  тоже обнадеживают, хотя они и несколько менее убедительны, поскольку количество проективных простых чисел в рассматриваемом нами промежутке гораздо меньше. Так, например, при  $n = 5$  и  $e = 1$  количество простых  $p = 1 + q + \dots + q^4 < 10^{18}$  при простых  $q$  равно 252, а получаемая оценка равна 246,718... Следует заметить, что для того, чтобы оценить количество простых  $p = 1 + q + q^2 \leq 10^{18}$ , верхний предел в интеграле (4) должен быть  $x \approx 10^{18/2}$ , а для оценки аналогичного числа для  $p = 1 + q + \dots + q^4 < 10^{18}$  интеграл берётся до  $x \approx 10^{18/4}$ , т. е. по гораздо меньшему промежутку.

Основываясь на полученных наблюдениях, мы можем сформулировать следующую гипотезу.

**Гипотеза 9.2.** Существует бесконечно много проективных простых чисел вида  $p = 1 + q + q^2$ , где  $q$  простое.

Основываясь на аналогичных наблюдениях для бóльших значений  $n$  и  $e$ , хотя и поневоле включающих меньшее количество проективных простых чисел, мы можем сформулировать следующую более общую гипотезу.

**Гипотеза 9.3.** Для любого фиксированного простого  $n \geq 3$  и для любого фиксированного показателя  $e$ , являющегося степенью числа  $n$ , существует бесконечно много проективных простых чисел вида  $p = 1 + q + \dots + q^{n-1}$ , где  $q = r^e$  и  $r$  простое.

Разумеется, существование бесконечного количества проективных простых чисел следует из гораздо более слабых утверждений, чем те, что были сделаны выше. Например, было бы достаточно доказать, что для бесконечного количества простых  $n$  (степеней простого числа  $q$ ) существует хотя бы одна степень простого числа  $q$  (соответственно хотя бы одно простое  $n$ ), для которых число  $(q^n - 1)/(q - 1)$  простое.

## 10. Группы и рисунки, степень которых — проективное простое число

Возвратимся к группам. Элементы  $z$  порядка  $p = (q^n - 1)/(q - 1)$  в группе  $G = \text{PSL}_n(q)$  — это циклы Зингера (см., например, [43, теорема II.7.3]), индуцированные подходящим ненулевым элементом поля  $\mathbb{F}_{q^n}$ , умножение на который служит линейным оператором в этом поле, рассматриваемом как  $n$ -мерное векторное пространство над полем  $\mathbb{F}_q$ . Этот оператор переставляет одномерные подпространства, действуя на их множестве как регулярная перестановка. Из результатов А. Березцкого [12] следует, что в случае, когда цикл Зингера  $z$  имеет простой порядок  $p$ , единственная максимальная подгруппа группы  $G$ , содержащая  $z$ , — это нормализатор  $N_G(\langle z \rangle) \cong C_p \rtimes C_n$ , в котором дополнение индуцируется группой Галуа  $\text{Gal } \mathbb{F}_{q^n}/\mathbb{F}_q = \langle t \mapsto t^q \rangle \cong C_n$ . Будучи разрешимой, группа  $N_G(\langle z \rangle)$  не может содержать совершенную подгруппу  $\langle x, y, z \rangle$ . Следовательно, любая тройка типа  $(3, 2, p)$ , если она существует, порождает всю группу  $G$ . Более того, существует  $(p - 1)/n$  классов сопряжённости  $\mathcal{Z}$  циклов Зингера  $z$  в  $G$ , по одному для каждой орбиты группы  $\text{Gal } \mathbb{F}_{q^n}/\mathbb{F}_q$  на элементах мультипликативного порядка  $p$  в  $\mathbb{F}_{q^n}$ . (Заметим, что, поскольку  $n$  простое, справедливо равенство  $p - 1 = q + q^2 + \dots + q^{n-1} \equiv 0 \pmod{n}$ . Оно очевидно для  $q \equiv 0 \pmod{n}$  и  $q \equiv 1 \pmod{n}$ , а для остальных  $q$ , поскольку опять-таки  $n$  простое, слагаемые представляют собой ненулевые классы вычетов по модулю  $n$ , которые попарно сокращаются.)

Для малых проективных простых чисел  $p = 5, 7, 13, 17$  группы  $\text{PSL}_2(4)$  ( $\cong \text{PSL}_2(5) \cong A_5$ ),  $\text{PSL}_3(2)$  ( $\cong \text{PSL}_2(7)$ ),  $\text{PSL}_3(3)$  и  $\text{PSL}_2(16)$  реализуются

в качестве групп монодромии. Ниже мы систематически исследуем различные возможности для реализации групп монодромии  $\mathrm{PSL}_n(q)$ , начиная с малых значений  $n$ .

### 10.1. Случай $n = 2$ : простые числа Ферма

Для простых чисел Ферма, когда  $n = 2$ , справедлива следующая теорема.

**Теорема 10.1.** *Для любого простого числа Ферма  $p = 2^{2^k} + 1 \geq 5$  существует  $2^{2^k - k - 1}$  рисунков  $\mathcal{D}$  типа  $(3, 2, p)$  и степени  $p$  с группой монодромии  $G = \mathrm{PSL}_2(2^{2^k})$  с естественным действием. Их род равен  $(p-5)/12$ , а их регулярные накрытия  $\mathcal{R}$ , которые попарно не изоморфны, имеют род  $p(p-4)(p-5)/12$ . И рисунок  $\mathcal{D}$ , и рисунок  $\mathcal{R}$  зеркально симметричны.*

**Доказательство.** Пусть  $G = \mathrm{PSL}_2(q)$ , где  $q = 2^{2^k} \geq 4$ , и пусть  $p = q + 1$  — простое число. Классы сопряжённости  $\mathcal{X}$  и  $\mathcal{Y}$  элементов  $x$  и  $y$  порядка 3 и 2 единственны, при этом имеется  $q/2$  классов  $\mathcal{Z}$  элементов  $z$  порядка  $p$ . Числа 3 и  $p$  делят  $q-1$  и  $q+1$  соответственно. Из таблицы характеров группы  $G$  (см., например, [48, § 5.5]) видно, что только для одного главного характера  $\chi = \chi_1$  имеет место неравенство  $\chi(x)\chi(y)\chi(z) \neq 0$ . Следовательно, для любого выбора класса  $\mathcal{Z}$  сумма по характерам  $\Sigma$  равна 1. Имеем  $|C(x)| = q-1$ ,  $|C(y)| = q$ ,  $|C(z)| = q+1$  и, наконец,  $|G| = q(q^2-1)$ . Отсюда получаем число троек типа  $(3, 2, p)$  в  $G$ :

$$\frac{q}{2} \cdot \frac{|G|^2}{|C(x)| \cdot |C(y)| \cdot |C(z)|} \cdot \Sigma = \frac{q}{2} \cdot |G|.$$

Как мы уже раньше объясняли, из результатов А. Березцкого [12] о циклах Зингера следует, что каждая тройка порождает целиком всю группу  $G$ . Группа  $\mathrm{Aut} G \cong G \rtimes \mathrm{Gal} \mathbb{F}_q \cong G \rtimes C_{2^k}$  действует на тройках полурегулярно, поэтому число её орбит равно

$$\frac{q}{2} \cdot \frac{1}{2^k} = 2^{2^k - k - 1}.$$

Следовательно, это также число нормальных подгрупп группы  $\Delta = \Delta(3, 2, p)$  с фактором, изоморфным группе  $G$ , и тем самым число регулярных рисунков  $\mathcal{R}$  типа  $(3, 2, p)$  с группой автоморфизмов  $G$ .

В группе  $G$  имеется единственный класс сопряжённости подгрупп индекса  $p = q + 1$ : он состоит из стабилизаторов точек в  $\mathbb{P}^1(\mathbb{F}_q)$ . Они поднимаются до  $2^{2^k - k - 1}$  классов сопряжённости подгрупп того же индекса в группе  $\Delta$ , поэтому они соответствуют такому же количеству рисунков  $\mathcal{D}$  типа  $(3, 2, p)$  и степени  $p$  с группой монодромии  $G$  и с одним из рисунков  $\mathcal{R}$  в качестве регулярного накрытия. Элементы  $x$ ,  $y$  и  $z$  имеют цикловые структуры  $3^{(q-1)/3}1^2$ ,  $2^{q/2}1^1$  и  $p^1$  соответственно на  $\mathbb{P}^1(\mathbb{F}_q)$ , так что их эйлерова характеристика равна

$$\chi = \frac{q-1}{3} + 2 + \frac{q}{2} + 1 - (q+1) + 1 = \frac{16-q}{6},$$

а род равен

$$g = 1 - \frac{\chi}{2} = \frac{q-4}{12} = \frac{p-5}{12}.$$

Наконец, по формуле Римана—Гурвица род регулярных рисунков равен

$$\frac{p-6}{12p} |G| + 1 = \frac{p(p-4)(p-5)}{12}.$$

Классы сопряжённости  $\mathcal{Z}$  состоят из пар взаимно обратных элементов  $z$ ,  $z^q = z^{-1}$ , так что карты  $\mathcal{D}$  и  $\mathcal{R}$  изоморфны своим зеркальным отражениям. (На самом деле, как подметил Д. Сингерман [70], из результатов А. М. Макбета [59] следует, что для *любой* степени простого числа  $q$  оба элемента любой порождающей пары в группе  $\mathrm{PSL}_2(q)$  переходят в свои обратные под действием любого автоморфизма. Это влечёт результат более общий, чем тот, что был доказан выше.)  $\square$

**Пример 10.2.** При  $k = 1$  и  $p = 5$  мы получаем планарный рисунок  $\mathcal{D}$ , изображённый слева на рис. 11. Его группа монодромии равна  $G = \mathrm{PSL}_2(4) \cong A_5$ , а его регулярным накрытием  $\mathcal{R}$  служит додекаэдр. Сам рисунок  $\mathcal{D}$  является фактором рисунка  $\mathcal{R}$  по стабилизатору точки в  $G$ , который изоморфен группе  $A_4$ . При  $k = 2$  и  $p = 17$  мы получаем два рисунка рода 1, они приведены в разделе 14, рис. 25. Их регулярные накрытия имеют род 221. При  $k = 3$  и  $p = 257$  имеется 16 рисунков рода 21 с регулярными накрытиями рода 1365441. При  $k = 4$  и  $p = 65537$  имеется 2048 рисунков рода 5461, а их регулярные накрытия имеют род 23454100602881. Никаких простых чисел Ферма для  $k \geq 5$  на данный момент не обнаружено. Предполагается, что их и нет. Но если таковые вдруг найдутся, они тоже покрываются теоремой 10.1.

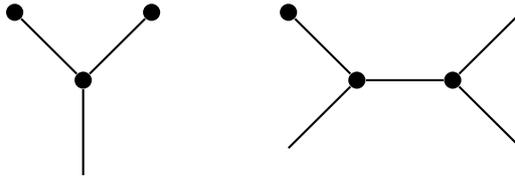


Рис. 11. Рисунки типа  $(3, 2, p)$  и степени  $p$  для  $p = 5, 7$

Покончив со случаем  $n = 2$ , предположим теперь, что  $n \geq 3$ . В этом случае группа  $\mathrm{PSL}_n(q)$  имеет два естественных представления, действуя на точках и на гиперплоскостях геометрии  $\mathbb{P}^{n-1}(\mathbb{F}_q)$ . Эти представления переходят одно в другое под действием внешнего автоморфизма, индуцированного двойственностью геометрии. Ещё одно отличие по сравнению со случаем  $n = 2$  состоит в том, что при  $n \geq 3$  классы сопряжённости  $\mathcal{Z}$  циклов Зингера не инвариантны относительно обращения. Вместо этого они образуют взаимно обратные пары; классы каждой пары переходят друг в друга под действием двойственности. Отсюда

следует, что множество рисунков  $\mathcal{D}$  состоит из киральных пар, причём каждая пара имеет общее регулярное накрытие  $\mathcal{R}$ , изоморфное своему зеркальному образу.

## 10.2. Случай $n = 3$ : проективные плоскости

Подавляющее большинство проективных простых чисел вплоть до любой заданной границы отвечает параметру  $n = 3$ , так что группа  $G = \mathrm{PSL}_3(q)$  действует на точках и на прямых проективной плоскости  $\mathbb{P}^2(\mathbb{F}_q)$ . В этом случае мы имеем возможность перечислить и описать соответствующие рисунки, основываясь на общем виде таблицы характеров группы  $G$ , который приведён в [69] (см. также [21] для  $q \leq 9$ ).

**Теорема 10.3.** *Если  $q$  — степень простого числа с показателем  $e$  и число  $p = 1 + q + q^2$  простое, то существует  $(p - 1)/3e$  рисунков типа  $(3, 2, p)$  и степени  $p$  с группой монодромии  $\mathrm{PSL}_3(q)$  с естественным действием. Если  $q$  нечётно, то их паспорт имеет вид  $(3^{q(q+1)/3} 1^1, 2^{(q^2-1)/2} 1^{q+2}, p^1)$ , а род равен  $(q - 3)(q + 1)/12$ . Если же  $q = 2^e$ , то паспорт равен  $(3^{q(q+1)/3} 1^1, 2^{q^2/2} 1^{q+1}, p^1)$ , а род равен  $q(q - 2)/12$ . Все указанные рисунки киральны.*

**Доказательство.** Положим  $G := \mathrm{PSL}_3(q)$ . По лемме 8.4 (с) эта группа совпадает с  $G = \mathrm{SL}_3(q)$ . Применим формулу Фробениуса (2), используя общий вид таблицы характеров группы  $\mathrm{SL}_3(q)$ , приведённый в [69, таблица 1b].

Пусть для начала  $q$  взаимно просто с числом 6. Тогда в  $G$  имеются уникальные классы  $\mathcal{X}$  и  $\mathcal{Y}$  элементов порядка 3 и 2 и  $(p - 1)/3 = q(q + 1)/3$  классов  $\mathcal{Z}$  элементов порядка  $p$  (циклов Зингера). В обозначениях таблицы 1a из [69] класс  $\mathcal{X}$  имеет тип  $\mathcal{C}_7$ , класс  $\mathcal{Y}$  — тип  $\mathcal{C}_4$ , а классы  $\mathcal{Z}$  все имеют тип  $\mathcal{C}_3$ . Элементы этих классов имеют централизаторы порядка  $q^2 - 1$ ,  $q(q - 1)^2(q + 1)$  и  $p$  соответственно. Единственный неглавный неприводимый характер группы  $G$ , не обращающийся в ноль на классах  $\mathcal{X}$ ,  $\mathcal{Y}$  и  $\mathcal{Z}$  — это характер Штейнберга, т. е. единственный неприводимый характер степени  $q^3$ , принимающий значения  $-1$ ,  $q$  и  $1$  на соответствующих классах. Поскольку порядок группы равен  $|G| = q^3(q - 1)^2(q + 1)(q^2 + q + 1)$ , мы получаем количество троек типа  $(3, 2, p)$  в группе  $G$ :

$$\frac{p - 1}{3} \cdot \frac{(q^3(q - 1)^2(q + 1)(q^2 + q + 1))^2}{(q^2 - 1) \cdot q(q - 1)^2(q + 1) \cdot p} \left( 1 + \frac{(-1) \cdot q \cdot 1}{q^3} \right) = \frac{p - 1}{3} |G|.$$

Согласно [12] единственная максимальная подгруппа группы  $G$ , содержащая  $z$  — это нормализатор  $N_G(\langle z \rangle)$ , имеющий порядок  $3p$ ; следовательно, любая тройка порождает  $G$ . Если  $q$  — это степень простого числа с показателем  $e$ , то  $|\mathrm{Out} G| = 2e$ : здесь множитель 2 соответствует двойственности проективной плоскости  $\mathbb{P}^2(\mathbb{F}_q)$ , на которой действует группа  $G$ , а множитель  $e$  — это порядок группы Галуа поля  $\mathbb{F}_q$ . Следовательно, группа  $\Delta(3, 2, p)$  имеет  $(p - 1)/6e$  нормальных подгрупп с фактором  $G$ . Поскольку  $G$  имеет два класса сопряжённости подгрупп индекса  $p$ , состоящих из стабилизаторов точек и прямых

соответственно на плоскости  $\mathbb{P}^2(\mathbb{F}_q)$ , мы получаем  $(p-1)/3e$  рисунков типа  $(3, 2, p)$  и степени  $p$  с группой монодромии  $G$ .

В каждом из двух действий степени  $p$  группы  $G$  число неподвижных точек элементов  $x$ ,  $y$  и  $z$  равно соответственно  $1$ ,  $q+2$  и  $0$ . Таким образом, паспорт этих рисунков равен  $(3^{q(q+1)/3} 1^1, 2^{(q^2-1)/2} 1^{q+2}, p^1)$ , а род равен  $(q-3)(q+1)/12$ .

Если  $q = 3^e$ , имеются два класса сопряжённости элементов порядка  $3$  типов  $C_2$  и  $C_3$  с централизаторами порядка  $q^3(q-1)$  и  $q^2$  соответственно. Если  $x$  взят из первого класса, только главный характер, а также компонента перестановочного характера степени  $p-1 = q(q+1)$  вносят вклад в сумму по характерам  $\Sigma$ , и эта сумма равна

$$\Sigma = 1 + \frac{q \cdot (q+1) \cdot (-1)}{q(q+1)} = 0.$$

Если  $x$  взят из второго класса, то только главный характер вносит вклад в  $\Sigma$ , так что получающееся в результате число троек в  $G$  равно

$$\frac{p-1}{3} \cdot \frac{(q^3(q-1)^2(q+1)(q^2+q+1))^2}{q^2 \cdot q(q-1)^2(q+1) \cdot p} = \frac{p-1}{3} |G|,$$

как и в предыдущем случае. Тем самым количество рисунков равно  $(p-1)/3e$ , а паспорт и род такие же, как раньше.

Если  $q = 2^e$ , то главное отличие от предыдущих случаев состоит в том, что единственный класс инволюций  $\mathcal{Y}$  имеет тип  $C_2$  и централизаторы его элементов имеют порядок  $q^3(q-1)$ . Ещё одно отличие заключается в том, что любой неглавный неприводимый характер обращается в ноль на  $x$ ,  $y$  или  $z$ , так что  $\Sigma = 1$ . Таким образом, число троек типа  $(3, 2, p)$  в  $G$  равно

$$\frac{p-1}{3} \cdot \frac{(q^3(q-1)^2(q+1)(q^2+q+1))^2}{(q^2-1) \cdot q^3(q-1) \cdot p} = \frac{p-1}{3} |G|,$$

так что число рисунков опять равно  $(p-1)/3e$ . Элемент  $y$  на этот раз имеет  $q+1$  неподвижных точек, и мы получаем паспорт  $(3^{q(q+1)/3} 1^1, 2^{q^2/2} 1^{q+1}, p^1)$  и род  $q(q-2)/12$ .

Во всех случаях киральность рисунков следует из того факта, что двойственные представления степени  $p$  группы  $G$  соответствуют взаимно обратным классам сопряжённости  $\mathcal{Z}$ , и группа  $\text{Out } G$  действует на множестве таких пар классов полурегулярно.  $\square$

**Пример 10.4.** Наименьший пример к теореме 10.3 даёт киральная пара рисунков степени  $p = 7$  с группой монодромии  $\text{PSL}_3(2) \cong \text{PSL}_2(7)$ . Один из рисунков этой пары показан на рис. 11 справа.

**Пример 10.5.** Возьмём  $p = 13$  и  $G = \text{PSL}_3(3)$ . Требуемые классы сопряжённости (в обозначениях [21]) —  $\mathcal{X} = 3B$ ,  $\mathcal{Y} = 2A$  и  $\mathcal{Z} = 13A, 13B, 13C, 13D$ . Они дают четыре рисунка  $\mathcal{D}$  типа  $(3, 2, 13)$  и степени  $13$ , которые образуют две киральные пары, причём каждая пара имеет общее регулярное накрытие. Каждый из этих рисунков (см. рис. 12 или же [8, орбита 13.1, рис. 8.22 (A)]) имеет паспорт  $(3^4 1^1, 2^4 1^5, 13^1)$  и род  $0$ , а оба их регулярных накрытия имеют

род 253. (Они являются двойственными к регулярным картам R253.1 и R253.2 типа  $\{3, 13\}_8$  и  $\{3, 13\}_{12}$  из каталога [20].)

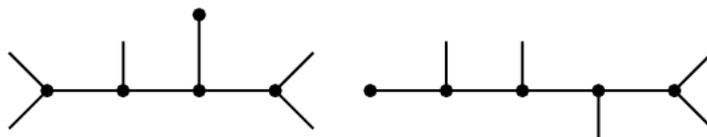


Рис. 12. Два рисунка с группой монодромии  $\mathrm{PSL}_3(3)$

**Пример 10.6.** Пусть теперь  $p = 31$  и  $G = \mathrm{PSL}_3(5)$ . В этом случае  $\mathcal{X} = 3A$ ,  $\mathcal{Y} = 2A$ , и имеется десять возможных классов  $\mathcal{Z} = 31A, 31B, \dots, 31J$ . Они дают десять рисунков  $\mathcal{D}$  типа  $(3, 2, 31)$  и степени 31, которые образуют пять киральных пар и имеют пять регулярных накрытий. Каждый рисунок  $\mathcal{D}$  имеет род 1 и паспорт  $(3^{10}1^1, 2^{12}1^7, 31^1)$ , а их регулярные накрытия имеют род 25 001. Образующие группы монодромии десяти рисунков  $\mathcal{D}$  приведены в разделе 14.4, один из них изображён на рис. 26.

**Пример 10.7.** Возьмём, наконец,  $p = 73$  и  $G = \mathrm{PSL}_3(8)$ . В этом случае  $\mathcal{X} = 3A$  и  $\mathcal{Y} = 2A$ , и имеется 24 класса  $\mathcal{Z} = 73A, \dots$  элементов порядка 73. Поскольку  $e = 3$ , мы получаем  $24/3 = 8$  рисунков  $\mathcal{D}$ . Они имеют род 4, а их паспорт равен  $(3^{24}1^1, 2^{32}1^9, 73^1)$ . Их представления в виде перестановок даны в разделе 14.7. Они образуют четыре киральные пары, и каждая пара имеет общее регулярное накрытие рода 1 260 673.

Разумеется, мы не рассматриваем такие значения параметра  $q$ , как  $q = 4, 7, 9$  или 11, поскольку соответствующие значения  $1 + q + q^2$  не являются простыми. Квадраты простых чисел вообще можно игнорировать, поскольку, как ранее было доказано, чтобы  $p$  было простым, показатель  $e$  должен быть степенью числа  $n = 3$ . Для любого такого  $e$  гипотеза Бейтмана—Хорна, будучи применённой к многочленам  $t$  и  $1 + t^e + t^{2e}$ , влечёт бесконечность множества проективных простых чисел данного вида. Однако даже если  $e = 3$ , количество примеров в пределах наших вычислительных возможностей столь мало (10 простых значений  $p = 1 + q + q^2 < 10^{18}$ , в то время как оценка Бейтмана—Хорна даёт примерно 12), что опираться на данные вычислений мы не можем.

### 10.3. Фиксированное $n > 3$

В случае простого  $n > 3$  мы не располагаем таблицами характеров групп  $\mathrm{PSL}_n(q)$  в каком-либо общем виде. Однако гипотеза Бейтмана—Хорна по-прежнему применима, и из неё следует, что если мы фиксируем простое  $n$  и возьмём  $e$  равным некоторой фиксированной степени  $n$ , то получим бесконечно много проективных простых чисел. Единственный случай, для которого наши вычислительные данные выглядят достаточно убедительно, отвечает параметрам

$n = 5$  и  $e = 1$ . При этих значениях мы получили 252 проективных простых числа  $p < 10^{18}$ , в то время как оценка Бейтмана—Хорна даёт приблизительно 246.

#### 10.4. Случай $q = 2$ : простые числа Мерсенна

Взяв  $q = 2$ , мы должны рассмотреть группы  $G = \text{PSL}_n(2) = \text{GL}_n(2)$  степени  $p = 2^n - 1$ . Количество чисел  $n$ , для которых на данный момент известно, что  $p = 2^n - 1$  является простым, равно 52. Таблиц характеров общего вида для групп  $\text{GL}_n(2)$  нет, хотя имеется общая теория характеров групп  $\text{GL}_n(q)$ , в большой степени основанная на работе Дж. А. Грина [38] (краткий и доступный обзор этой теории можно найти в [57, § 4] или в [7, Гл. IV]). Мы приведём два небольших примера, в которых можно воспользоваться таблицами характеров из [21].

**Пример 10.8.** Пусть  $p = 2^3 - 1 = 7$  и  $G = \text{PSL}_3(2) (= \text{GL}_3(2) \cong \text{PSL}_2(7))$ . Единственные классы сопряжённости элементов группы  $G$  порядка 3 и 2 — это 3A и 2A. Их цикловые структуры в обоих естественных представлениях этой группы (на точках и на прямых плоскости Фано  $\mathbb{P}^2(\mathbb{F}_2)$ ) —  $3^2 1^1$  и  $2^2 1^3$  соответственно. Имеются также два класса 7A, 7B элементов порядка  $p = 7$ . Единственный характер, который не даёт ноль в суммировании по характерам, это  $\chi_1$ , так что сумма по характерам равна  $\Sigma = 1$ . Поскольку  $|C(x)| = 3$ ,  $|C(y)| = 8 = 2^3$ ,  $|C(z)| = 7$  и  $|G| = 168 = 2^3 \cdot 3 \cdot 7$ , число троек типа  $(3, 2, 7)$  в  $G$  равно

$$2 \cdot \frac{2^6 \cdot 3^2 \cdot 7^2}{3 \cdot 2^3 \cdot 7} = 2^4 \cdot 3 \cdot 7 = 2|G| = |\text{Aut } G|.$$

(Заметим, что группа  $\text{Out } G \cong C_2$  индуцирована двойственностью плоскости Фано или, что то же самое, сопряжением группы  $\text{PSL}_2(7)$  в  $\text{PGL}_2(7)$ .) Все эти тройки порождают группу  $G$ , так что в группе  $\Delta = \Delta(3, 2, 7)$  имеется единственная нормальная подгруппа с фактором  $G$ , отвечающая регулярному рисунку  $\mathcal{R}$  типа  $(3, 2, 7)$  с группой автоморфизмов  $G$ . В группе  $G$  имеется два класса сопряжённости подгрупп индекса 7: это стабилизаторы точек и прямых плоскости Фано. Они поднимаются до двух классов сопряжённости подгрупп индекса 7 в  $\Delta$ , соответствующих двум рисункам  $\mathcal{D}$  типа  $(3, 2, 7)$  и степени 7. Регулярным накрытием обоих является  $\mathcal{R}$ . Паспорт рисунков  $\mathcal{D}$  равен  $(3^2 1^1, 2^2 1^3, 7^1)$ , так что их род равен 0, а род  $\mathcal{R}$  равен 3. Один из рисунков  $\mathcal{D}$  изображён справа на рис. 11, а второй является его зеркальным отражением  $\bar{\mathcal{D}}$ . Эти две карты отвечают выбору одного из двух классов сопряжённости  $\mathcal{Z}$  или выбору одного из двух классов сопряжённости подгрупп индекса 7. Они не изоморфны, потому что внешний автоморфизм группы  $G$  в обоих случаях заменяет один класс на другой. Рисунок  $\mathcal{R}$  — это карта из семиугольников, живущая на квартике Клейна, введённой в [54]. Она обозначается  $\{7, 3\}_8$  в [6] и является двойственной к карте R3.1 из [20]. Будучи общим регулярным накрытием

для киральной пары рисунков, а также в силу своей единственности, эта карта зеркально симметрична.

**Пример 10.9.** Возьмём снова  $p = 31$ , только на этот раз 31 будет рассматриваться как число Мерсенна  $2^5 - 1$ , и рассмотрим группу  $G = \mathrm{PSL}_5(2) = \mathrm{GL}_5(2)$ . В этой группе присутствуют два класса сопряжённости элементов порядка 3, обозначаемые 3A и 3B, с цикловыми структурами  $3^8 1^7$  и  $3^{10} 1^1$  соответственно и два класса сопряжённости элементов порядка 2, обозначаемые 2A и 2B, с цикловыми структурами  $2^8 1^{15}$  и  $2^{12} 1^7$  соответственно, а также шесть классов 31A, ..., 31F элементов порядка 31. Из обсуждавшегося ранее неравенства  $2a + b \geq p - 1$  следует, что в качестве классов  $\mathcal{X}$  и  $\mathcal{Y}$  нам годятся только 3B и 2B. Для каждого из шести выборов класса  $\mathcal{Z}$  только  $\chi_1$  и  $\chi_6$  присутствуют в сумме по характерам, и мы получаем

$$\Sigma = 1 + \frac{8 \cdot (-5) \cdot 1}{280} = 1 - \frac{1}{7} = \frac{6}{7}.$$

Имеют место следующие равенства:  $|C(x)| = 180 = 2^2 \cdot 3^2 \cdot 5$ ,  $|C(y)| = 1536 = 2^9 \cdot 3$ ,  $|C(z)| = 31$  и  $|G| = 9999360 = 2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$ , так что общее число троек в  $G$  равно

$$6 \cdot 2^9 \cdot 3 \cdot 5 \cdot 7^2 \cdot 31 \cdot \frac{6}{7} = 2^{11} \cdot 3^3 \cdot 5 \cdot 7 \cdot 31 = 6|G| = 3|\mathrm{Aut} G|.$$

Каждая тройка образующих порождает  $G$ , так что  $\Delta$  имеет три нормальных подгруппы с фактором  $G$ . В  $G$  имеется два класса сопряжённости подгрупп индекса 31, а именно стабилизаторы точек и гиперплоскостей в проективном пространстве  $\mathbb{P}^4(\mathbb{F}_2)$ . Они дают шесть рисунков  $\mathcal{D}$  степени 31, разбивающиеся на три киральные пары, и каждая пара имеет общее регулярное накрытие  $\mathcal{R}$ . Каждый рисунок  $\mathcal{D}$  имеет паспорт  $(3^{10} 1^1, 2^{12} 1^7, 31^1)$  и род 1, а регулярные накрытия  $\mathcal{R}$  имеют род 672001. Образующие групп монодромии всех шести рисунков  $\mathcal{D}$ , а также изображение одного из этих рисунков даны в разделе 14.5.

**Замечание 10.10 (гипотеза Хуурмахтиха).** Отметим, что число 31 является в качестве проективного простого числа дважды, как сумма  $1 + 5 + 5^2$  и как  $1 + 2 + 2^2 + 2^3 + 2^4$ . В 1917 году бельгийский инженер и математик-любитель Рене Хуурмахтих<sup>1</sup> [36] выдвинул гипотезу, что этот пример, а также  $1 + 2 + 2^2 + \dots + 2^{12} = 8191 = 1 + 90 + 90^2$  являются единственными случаями повторения среди чисел вида  $(q^n - 1)/(q - 1)$  для  $q, n \geq 2$ . Хотя число 8191 простое (и потому является проективным простым для пары  $(q, n) = (2, 13)$ ), 90 не является степенью простого числа, так что только первый пример даёт нам случай повторения проективного простого числа. Компьютерный поиск по всем степеням простых чисел вплоть до  $10^{18}$  никаких других примеров не обнаружил. Гипотеза остаётся открытой; дополнительную информацию можно найти в [37].

<sup>1</sup>На сайте [ru.forvo.com/search/Goormaghtigh](http://ru.forvo.com/search/Goormaghtigh) можно услышать, как произносится это имя.

Прежде чем приступить к поиску троек  $(x, y, z)$  типа  $(3, 2, p)$  в группе  $G = \mathrm{GL}_n(2)$  для произвольного простого  $n \geq 3$ , полезно сначала выяснить, какие есть возможности для элементов порядка 3, 2 и  $p$  в  $G$ . Любой элемент  $x \in G$  порядка 3 имеет каноническую рациональную форму, в которой стоят  $r$  и  $(n-r)/2$  блоков вида

$$(1) \text{ или соответственно } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

где  $r < n$  нечётно. Тем самым  $x$  оставляет инвариантным подпространство размерности  $r - 1$  в  $\mathbb{P}^{n-1}(\mathbb{F}_2)$ . Это подпространство состоит из  $\alpha = 2^r - 1$  точек. Следовательно, в  $x$  имеется  $a = (p - 2^r + 1)/3$  нетривиальных циклов. Аналогично любой элемент  $y \in G$  порядка 2 имеет жорданову нормальную форму, в которой имеется  $s$  и  $(n-s)/2$  блоков вида

$$(1) \text{ или соответственно } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

где  $s < n$  нечётно. Тем самым  $y$  оставляет инвариантным подпространство размерности  $(n+s-2)/2$ , состоящее из  $\beta = 2^{(n+s)/2} - 1$  точек. Следовательно, в  $y$  имеется  $b = (p - 2^{(n+s)/2} + 1)/2$  нетривиальных циклов. Элемент  $z$  — это  $p$ -цикл. Согласно [12], если тройка  $(x, y, z)$  типа  $(3, 2, p)$  существует, она порождает группу  $G$ . Соответствующий рисунок  $\mathcal{D}$  имеет паспорт  $(3^a 1^\alpha, 2^b 1^\beta, p^1)$  и род  $(2a + b + 1 - p)/2$ , его минимальное регулярное накрытие  $\mathcal{R}$  имеет род

$$\frac{p-6}{12p} |G| + 1 = \frac{p-6}{12p} \prod_{i=0}^{n-1} (2^n - 2^i) + 1 = (p-6) 2^{(n^2-n-4)/2} \prod_{i=3}^{n-1} (2^i - 1) + 1.$$

Заметим, что получившееся выражение не зависит ни от  $r$ , ни от  $s$ . В частности, если мы выберем наиболее «активно действующие» элементы  $x$  и  $y$ , взяв  $r = s = 1$  (как это было сделано ранее в примерах с  $n = 3, 5$ ), мы получим  $\alpha = 1$  и  $\beta = 2^{(n+1)/2} - 1$ , так что  $a = (p-1)/3$  и  $b = (p - 2^{(n+1)/2} + 1)/2$ . В итоге род рисунка  $\mathcal{D}$  равен

$$\frac{1}{3} (2^{n-2} + 1) - 2^{(n-3)/2}. \quad (6)$$

**Теорема 10.11.** *Для любого простого числа Мерсенна  $p = 2^n - 1 \geq 7$  существует как минимум  $(p-1)/2n$  киральных пар рисунков типа  $(3, 2, p)$ , степени  $p$  и рода, указанного в (6), с группой монодромии  $G = \mathrm{PSL}_n(2) = \mathrm{GL}_n(2)$ .*

**Доказательство.** Мы воспользуемся формулой Фробениуса (2) и покажем, что для любого класса сопряжённости  $\mathcal{Z}$  циклов Зигера в  $G$  существует тройка  $(x, y, z)$  типа  $(3, 2, p)$ , где  $x$  и  $y$  удовлетворяют упомянутому выше условию  $r = s = 1$  и  $z \in \mathcal{Z}$ . Ключевым моментом в вычислении является тот факт, что большинство неприводимых неглавных характеров на циклах Зигера равны нулю (см., например, [57, § 4.2]) и поэтому не вносят вклад в сумму по характерам  $\Sigma$ . Среди остальных характеров тот, что имеет степень  $p-1$ , т. е. неглавное слагаемое натурального перестановочного характера, равен нулю на  $x$ , а характер Стейнберга степени  $2^{n(n-1)/2}$  равен нулю на  $y$ , так что их тоже можно

не учитывать. Остальные характеры имеют степени, существенно превосходящие их значения на  $x$ ,  $y$  и  $z$  (см. подробности в [57, § 4.1, 4.2]), так что их общий вклад в  $\Sigma$  по абсолютной величине меньше, чем вклад главного характера, который равен единице. В итоге получаем  $\Sigma > 0$ , что влечёт существование троек нужного вида. Как и ранее, согласно [12] все эти тройки порождают всю группу  $G$ . В этой группе имеется  $(p-1)/n$  классов сопряжённости  $\mathcal{Z}$  циклов Зингера  $z \in G$ , которые разбиваются на  $(p-1)/2n$  пар взаимно обратных классов. Классы каждой пары переставляются внешним автоморфизмом группы  $G$ , так же как и два перестановочных представления степени  $p$  этой группы. Таким образом, мы получаем (как минимум)  $(p-1)/2n$  киральных пар рисунков  $\mathcal{D}$ . Все они имеют один и тот же паспорт и род, вычисленные выше.  $\square$

На основании теоремы 10.11, а также других примеров, в которых фигурируют малые проективные простые числа, мы выдвигаем следующую гипотезу, являющуюся обобщением указанной выше теоремы.

**Гипотеза 10.12.** Для любого проективного простого числа

$$p = 1 + q + \dots + q^{n-1} > 3$$

существует хотя бы один рисунок типа  $(3, 2, p)$  и степени  $p$  с группой монодромии  $\mathrm{PSL}_n(q)$ .

## 10.5. Резюме

Мы можем сформулировать итоги этого довольно длинного раздела в виде следующей теоремы.

**Теорема 10.13.** Пусть  $p$  — простое число, такое что существует рисунок типа  $(3, 2, p)$  и степени  $p$  с группой монодромии  $G$ . Тогда  $p \geq 5$  и имеет место одна из следующих возможностей:

- (a) группа  $G = A_p$  с естественным действием,  $p \neq 7$ ;
- (b)  $p = 11$  и группа  $G = \mathrm{PSL}_2(p)$ , действующая на классах смежности подгрупп, изоморфных группе  $A_5$ ;
- (c)  $p$  — проективное простое число  $(q^n - 1)/(q - 1)$  для некоторого простого  $n$  и степени простого числа  $q$  и группа  $G = \mathrm{PSL}_n(q) = \mathrm{SL}_n(q)$  с естественным действием на точках и гиперплоскостях пространства  $\mathbb{P}^{n-1}(q)$ .

В случае (a) при  $p = 5$  существует единственный рисунок: он показан слева на рис. 11. Когда  $p > 7$ , существует как минимум экспоненциально много рисунков при  $p \rightarrow \infty$ , даже если мы ограничимся планарными рисунками. В случае (b) существует единственная киральная пара рисунков: это рисунки  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ , изучавшиеся  $\Phi$ . Клейном в [55]; они показаны на рис. 2 и 3. В случае (c) мы предполагаем, что существует бесконечно много проективных простых чисел  $p$ , причём это верно, даже если мы зафиксируем любое простое  $n \geq 3$ . При  $n = 2$  (простые числа Ферма) и при  $n = 3$  (проективные плоскости) все рисунки описаны в теоремах 10.1 и 10.3. При  $q = 2$  (простые числа Мерсенна) у нас есть теорема существования, но полной классификации нет.

## 11. Модулярные рисунки и кривые

Аналогично тому как мы обобщили наши рассуждения о рисунках типа  $(3, 2, p)$  и степени  $p$  с  $p = 11$  на все простые  $p$ , мы можем проделать то же самое для рисунков того же типа, но степени  $p + 1$ . В этом разделе мы рассмотрим рисунки  $\mathcal{D}_0(p)$ , возникающие естественным образом из конгруэнц-подгрупп модулярной группы, а в следующем разделе займёмся более общими рисунками того же типа и степени.

### 11.1. Рисунок $\mathcal{D}_0(p)$ и его паспорт

Так же как и в рассмотренном ранее случае  $p = 11$ , для любого простого  $p$  естественное действие группы  $\mathrm{PSL}_2(p)$  на проективной прямой  $\mathbb{P}^1(\mathbb{F}_p)$  даёт рисунок  $\mathcal{D}_0(p)$  типа  $(3, 2, p)$  и степени  $p + 1$ . Паспорт этого рисунка можно найти, исходя из того, что нетождественное преобразование Мёбиуса (над любым полем) имеет не более двух неподвижных точек. Случаи  $p = 2$  и  $3$  тривиальны, так что предположим, что  $p \geq 5$ .

Порядок перестановки  $x$ , представляющей чёрные вершины (или просто вершины), равен 3. Следовательно,

- если  $p \equiv 1 \pmod{3}$ , то  $x$  имеет две неподвижные точки, так что её цикловая структура равна  $3^{(p-1)/3}1^2$ ;
- если  $p \equiv -1 \pmod{3}$ , то  $x$  не имеет неподвижных точек, а её цикловая структура равна  $3^{(p+1)/3}$ .

Аналогично порядок перестановки  $y$ , представляющей белые вершины (или рёбра), равен 2, причём эта перестановка чётная. Следовательно,

- если  $p \equiv 1 \pmod{4}$ , то  $y$  имеет две неподвижные точки, и её цикловая структура равна  $2^{(p-1)/2}1^2$ ;
- если  $p \equiv -1 \pmod{4}$ , то  $y$  не имеет неподвижных точек, и её цикловая структура равна  $2^{(p+1)/2}$ .

Наконец, перестановка  $z$ , представляющая клетки, имеет порядок  $p$ , так что её цикловая структура равна  $p^11^1$ .

Зная паспорт, мы можем вычислить эйлерову характеристику  $\chi$ , а с ней и род  $g$  рисунка  $\mathcal{D}_0(p)$ . Возможны четыре случая:

- если  $p \equiv 1 \pmod{12}$ , то паспорт равен  $(3^{(p-1)/3}1^2, 2^{(p-1)/2}1^2, p^11^1)$ , откуда следует, что  $g = (p - 13)/12$ ;
- если  $p \equiv 5 \pmod{12}$ , то паспорт равен  $(3^{(p+1)/3}, 2^{(p-1)/2}1^2, p^11^1)$ , откуда следует, что  $g = (p - 5)/12$ ;
- если  $p \equiv 7 \pmod{12}$ , то паспорт равен  $(3^{(p-1)/3}1^2, 2^{(p+1)/2}, p^11^1)$ , откуда следует, что  $g = (p - 7)/12$ ;
- если  $p \equiv 11 \pmod{12}$ , то паспорт равен  $(3^{(p+1)/3}, 2^{(p+1)/2}, p^11^1)$ , откуда следует, что  $g = (p + 1)/12$ .

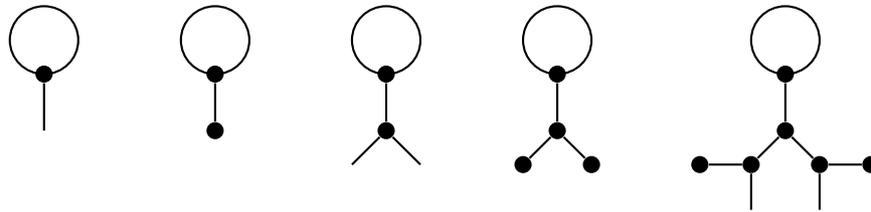
Всё это можно записать следующим образом: для простых чисел  $p \equiv c = -1, 5, 7, 13 \pmod{12}$  род рисунка  $\mathcal{D}_0(p)$  равен  $(p - c)/12$ ; он также равен 0 для  $p = 2, 3$ . Таблица 3 даёт род  $g$  для нескольких начальных значений  $p$ .

Таблица 3. Род рисунка  $\mathcal{D}_0(p)$ 

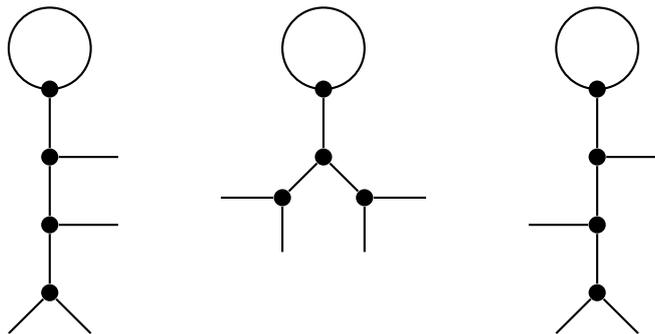
$p$	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
$g$	0	0	0	0	1	0	1	1	2	2	2	2	3	3	4	4

### 11.2. Рисунок $\mathcal{D}_0(13)$

Рисунок  $\mathcal{D}_0(p)$  планарен только при значениях  $p = 2, 3, 5, 7, 13$ . Эти пять рисунков показаны на рис. 13. Легко видеть, что четыре первых рисунка од-

Рис. 13. Рисунки  $\mathcal{D}_0(p)$  при  $p = 2, 3, 5, 7, 13$ ; белые вершины опущены

нозначно определяются своим паспортом. То же самое относится к рисунку  $\mathcal{D}_0(11)$  на торе, показанному на рис. 17. Однако для  $p = 13$  дело обстоит иначе: имеются 30 рисунков с паспортом  $(3^4 1^2, 2^6 1^2, 13^1 1^1)$ ; два из них, в том числе и  $\mathcal{D}_0(13)$ , зеркально симметричны, а остальные разбиваются на 14 киральных пар. Простое рассуждение показывает, что все они могут быть построены из трёх «остовов», показанных на рис. 14, и зеркальных образов первого и третьего-

Рис. 14. Три остова, из которых строятся рисунки с паспортом, как у  $\mathcal{D}_0(13)$ ; белые вершины снова опущены

го из них, если добавлять по чёрной вершине к двум из четырёх висячих рёбер. Это даёт  $5 \times \binom{4}{2} = 30$  рисунков.

В то время как группа монодромии рисунка  $\mathcal{D}_0(13)$  — это  $\mathrm{PSL}_2(13)$ , все остальные 29 рисунков имеют группу монодромии  $A_{14}$ . Это следует из того факта, что такая группа должна быть дважды транзитивной подгруппой группы  $A_{14}$ , а единственной другой возможностью, кроме самой  $A_{14}$ , является группа  $\mathrm{PSL}_2(13)$ . При этом согласно формуле Фробениуса этой группе соответствует ровно один рисунок, а именно  $\mathcal{D}_0(13)$ .

Тот факт, что рисунок  $\mathcal{D}_0(13)$  является планарным, даёт нам надежду, что вычисление функции Белого окажется посильной задачей. И в самом деле, функция Белого  $f: \Sigma \rightarrow \Sigma$  выглядит следующим образом:

$$f = -\frac{1}{1728} \cdot \frac{(t^4 - 7t^3 + 20t^2 - 19t + 1)^3(t^2 - 5t + 13)}{t},$$

$$f - 1 = -\frac{1}{1728} \cdot \frac{(t^6 - 10t^5 + 46t^4 - 108t^3 + 122t^2 - 38t - 1)^2(t^2 - 6t + 13)}{t}.$$

В этом случае, разумеется, функция  $f$  не является многочленом, поскольку у неё, кроме полюса в бесконечности (центра внешней клетки), есть ещё один полюс в нуле (центр клетки, окружённой петлёй).

На рис. 15 показана геометрически правильная версия рисунка  $\mathcal{D}_0(13)$ ; все чёрные и белые вершины присутствуют на рисунке. На этой картинке петля оказывается столь малой, что её полностью заслоняют инцидентные с ней чёрная и белая вершины. (Мы встретимся с таким же явлением при попытке изобразить рисунок  $\mathcal{D}_0(11)$ , см. рис. 18.) На рис. 16 петля показана в увеличенном масштабе вместе с прилегающими к ней отрезками вещественной и мнимой осей.

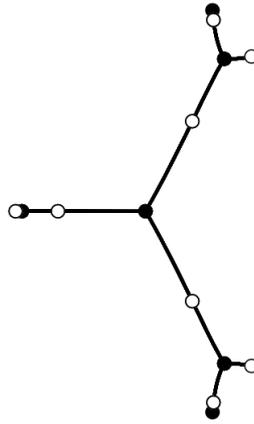


Рис. 15. Геометрически правильное изображение рисунка  $\mathcal{D}_0(13)$

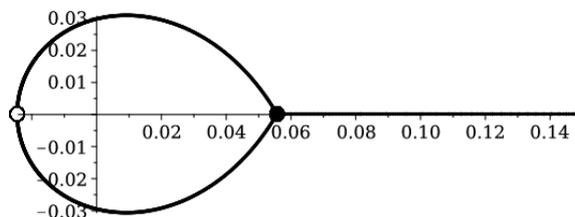


Рис. 16. Петля рисунка  $\mathcal{D}_0(13)$ . Её ширина по горизонтали составляет примерно 0,08, длина примыкающего к ней горизонтального отрезка (выходящего за пределы рисунка) равна примерно 0,46

### 11.3. Рисунок $\mathcal{D}_0(11)$

Рисунки  $\mathcal{D}_0(p)$  при  $p \leq 13$  планарны все, кроме одного: при  $p = 11$  рисунок  $\mathcal{D}_0(11)$  имеет род 1. Таким образом, перед нами встаёт дополнительная трудность: требуется найти соответствующую эллиптическую кривую. Два изображения этого рисунка показаны на рис. 17 в виде карт на торе; как обычно, противоположные рёбра квадрата, так же как и шестиугольника, следует отождествить. Минимальным регулярным накрытием рисунка  $\mathcal{D}_0(11)$  служит тот же рисунок  $\mathcal{R}_1$ , который накрывал рисунки  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$ , только в данном случае фактор накрытия  $\mathcal{R}_1$  следует брать по подгруппе группы  $L = \text{PSL}_2(11)$ , служащей стабилизатором точки на проективной прямой  $\mathbb{P}^1(\mathbb{F}_{11})$ . Эта подгруппа изоморф-

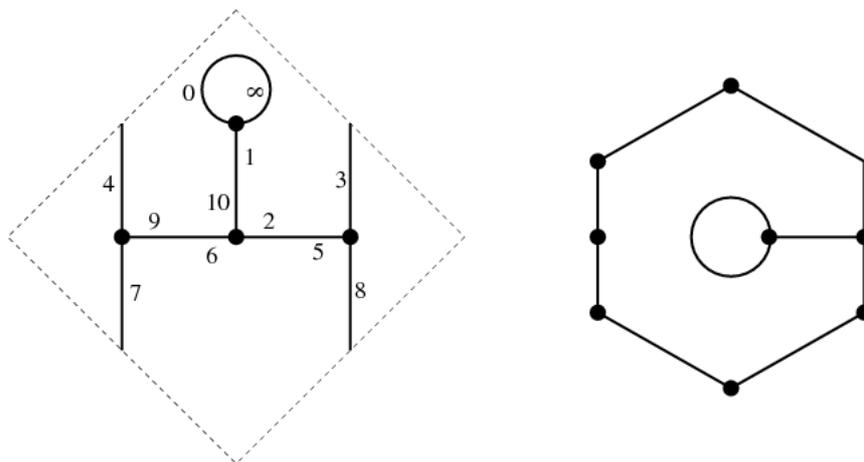


Рис. 17. Два изображения торической карты  $\mathcal{D}_0(11)$ . Этикетками полурёбер служат элементы множества  $\mathbb{P}^1(\mathbb{F}_{11}) = \mathbb{F}_{11} \cup \{\infty\}$ . Можно заметить, что если этикетка полуребра равна  $t$ , то этикетка противоположного конца того же ребра равна  $-1/t$ , а обход границы внешней клетки даёт цикл  $(0, 1, \dots, 10)$

на не группе  $A_5$ , а группе  $C_{11} \rtimes C_5$ . Надо сказать, что рисунок  $\mathcal{D}_0(11)$  не только происходит из более естественного представления группы  $L$ , но он ещё и более однородный: перестановки  $x$  и  $y$  не имеют неподвижных точек, так что все чёрные вершины имеют валентность 3, и у него нет висячих рёбер. Более того, образующие  $y: t \mapsto -1/t$  и  $z: t \mapsto t+1$  группы  $L$  можно легко разглядеть на рисунке, следуя по рёбрам и клеткам и используя в качестве этикеток полурёбер элементы множества  $\mathbb{P}^1(\mathbb{F}_{11})$ . Поскольку  $xyz = 1$ , перестановка  $x$  может легко быть вычислена: это  $x: t \mapsto -1/(t-1)$ .

Ещё одно замечательное свойство этого рисунка состоит в том, что он однозначно определяется своим паспортом  $(3^4, 2^6, 11^{11})$ . Таким образом, в данном случае не приходится рассматривать десять разных деревьев и сортировать соответствующие группы. Даже удивительно, что Ф. Клейн упустил этот пример. Возможно, причина в том, что представление карт с помощью перестановок ещё не было изобретено. Первые публикации, в которых была введена соответствующая конструкция, принадлежат В. Дику [27] (1888) и Л. Хеффтеру [42] (1891), так что появились они на десять лет позже, чем работа Ф. Клейна. На самом деле пионером в этой области был У. Р. Гамильтон [41] (1856), но он изложил свою конструкцию в частном письме. Однако даже и в близкое к нам время, когда перестановочная модель уже была общим достоянием, учёные изучали в основном группы автоморфизмов карт, в то время как группы монодромии никакого внимания не привлекали. Только с появлением теории детских рисунков группы монодромии вышли на передний план, поскольку они являются инвариантами Галуа.

С точки зрения теории детских рисунков единственность рисунка  $\mathcal{D}_0(11)$  означает, что он определён над полем  $\mathbb{Q}$ . Здесь, однако, перед нами возникает трудность иного рода. В планарном случае мы ищем *функцию Белого*, которая является рациональной функцией  $f: \Sigma \rightarrow \Sigma$ , но для рисунков рода  $g \geq 1$  нам нужна *пара Белого*  $(X, f)$ , где  $X$  — это риманова поверхность (или алгебраическая кривая) рода  $g$ , а  $f$  — мероморфная функция  $f: X \rightarrow \Sigma$ , не имеющая критических значений вне множества  $\{0, 1, \infty\}$ . Существует несчётное множество кривых любого заданного рода  $g \geq 1$ , и рисунок однозначно определяет одну из них. Поиск такой кривой (и функции Белого на ней) представляет собой задачу невероятной трудности. Данный ниже сравнительно простой ответ заслоняет многочисленные препятствия, которые приходится преодолевать, чтобы его найти. Соответствующее вычисление было по нашей просьбе проделано Джоном Войтом [71], которому мы в высшей степени признательны.

В нашем случае  $g = 1$ , так что нужная нам кривая является эллиптической кривой  $E$ . Одно из возможных её представлений выглядит так:

$$y^2 + y = x^3 - x^2 - 10x - 20. \quad (7)$$

Функция Белого  $f = f(x, y)$  строится следующим образом:

$$\begin{aligned} a &= -x^5 - 23x^4 + 697x^3 - 1031x^2 - 2170x - 353, \\ b &= -11x^6 + 148x^5 + 643x^4 - 2704x^3 - 6780x^2 + 1781x + 3308, \end{aligned}$$

$$f = \frac{ay + b}{1728(x - 16)}. \quad (8)$$

(Кривую  $E$  можно представить также в форме Вейерштрасса: положив  $y = z - 1/2$ ,  $x = t + 1/3$ , мы получим

$$z^2 = t^3 - \frac{31}{3}t - \frac{2501}{108}.$$

$J$ -инвариант кривой  $E$  равен  $J(E) = -2^{12}31^3/11^5$ .)

Даже проверка полученного результата не является простой задачей. Мы приведём краткий набросок основных шагов такой проверки.

ШАГ 0. Поскольку карта  $\mathcal{D}_0(11)$  состоит из 12 полурёбер, мы ожидаем, что функция Белого должна быть степени 12. Однако, когда мы смотрим на выражение (8), это его свойство совершенно не бросается в глаза, и это ещё мягко сказано. Создаётся впечатление, что эта функция имеет степень 6. Ключ к разгадке состоит в том, что  $f$  следует рассматривать как функцию, определённую на кривой  $E$ . Обозначим

$$h(x, y) = y^2 + y - x^3 + x^2 + 10x + 20$$

(см. уравнение (7)). Выразив  $y$  из уравнения  $f(x, y) = z$  и подставив результат в  $h$ , мы в самом деле получим функцию степени 12 от  $x$ , поскольку функция  $h$  содержит  $y^2$ .

ШАГ 1. Чтобы найти критические точки на кривой, мы должны добиться того, чтобы градиенты функций  $f$  и  $h$  были коллинеарны, поэтому мы полагаем равным нулю определитель

$$\begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} \\ \frac{\partial h}{\partial x} & \frac{\partial h}{\partial y} \end{vmatrix} = 0.$$

Это даёт нам одно уравнение от двух переменных  $x$  и  $y$ . Второе уравнение мы уже знаем: это  $h(x, y) = 0$ , ведь мы ищем не какие угодно точки коллинеарности, а те, которые лежат на кривой  $E$ .

ШАГ 2. Хорошая идея — найти базис Грёбнера полученной системы, причём сделать это рекомендуется *два раза*. Используя *чисто лексикографический* порядок  $\text{plex}(y, x)$  на мономах, мы получаем в качестве первого элемента базиса многочлен от  $x$ , а используя аналогичный порядок  $\text{plex}(x, y)$ , получаем многочлен от  $y$ . Вот эти многочлены:

$$\begin{aligned} P &= (x^4 - 20x^3 + 62x^2 + 116x + 97)^2(x - 16)^2 \times \\ &\quad \times (x^6 - 30x^5 + 243x^4 - 256x^3 - 1053x^2 + 654x + 7793), \\ Q &= (y^4 + 68y^3 + 590y^2 + 556y + 7489)^2(y - 60)^2 \times \\ &\quad \times (y^6 + 102y^5 + 2619y^4 + 11272y^3 + 131211y^2 + 91074y + 253312). \end{aligned}$$

ШАГ 3. Корни этих двух многочленов являются координатами  $x$  и  $y$  критических точек функции  $f$  на кривой  $E$ . Два множителя степени 4, поскольку

они возведены в квадрат, указывают на то, что здесь имеются четыре критические точки кратности 3. Мы можем догадаться, что это чёрные вершины нашей карты. Но верно ли, что значения функции  $f$  в этих точках равны нулю? И — главное — как «соединить» друг с другом координаты  $x$  и  $y$ , т. е. указать, какое  $y$  соответствует какому  $x$ ?

Ответить на эти вопросы нетрудно. Решая систему  $f = 0$ ,  $h = 0$ , мы находим, что значения переменной  $x$  в самом деле являются корнями многочлена

$$p_1 = x^4 - 20x^3 + 62x^2 + 116x + 97$$

и при этом

$$y = -\frac{1}{23}(x^3 - 16x^2 + 90x + 62).$$

Легко также проверить, что эти значения  $y$  в самом деле являются корнями многочлена

$$q_1 = y^4 + 68y^3 + 590y^2 + 556y + 7489.$$

Нужно лишь подставить это выражение переменной  $y$  в многочлен  $q_1$  и вычислить остаток по модулю  $p_1$ . В результате получится ноль.

В многочленах  $P$  и  $Q$ , кроме найденных нами четырёх решений, есть ещё одно, тоже фигурирующее в квадрате: это точка  $(x, y) = (16, 60)$ . Что она означает? На кривой  $E$  имеются две точки, лежащие над  $x = 16$ , а именно  $(16, 60)$  и  $(16, -61)$ . Подставляя  $y = 60$  в знаменатель функции  $f$ , мы получаем

$$-(x - 16)(11x^5 + 88x^4 + 2145x^3 - 4796x^2 - 8096x - 1117).$$

Таким образом,  $x - 16$  в числителе и в знаменателе функции  $f$  сокращаются, и наша точка оказывается устранимой особенностью. Следовательно, функция  $f$  в точке  $(16, -61)$ , лежащей на кривой, имеет простой полюс.

Теперь займёмся множителями степени 6 многочленов  $P$  и  $Q$ . Они соответствуют простым критическим точкам, т. е. белым вершинам. В самом деле, решая систему  $f = 1$ ,  $h = 0$ , мы, кроме лишнего решения  $(16, 60)$ , получаем корни многочлена

$$p_2 = x^6 - 30x^5 + 243x^4 - 256x^3 - 1053x^2 + 654x + 7793,$$

в то время как

$$y = -\frac{1}{101617}(104x^5 - 2811x^4 + 15943x^3 + 64714x^2 - 44258x - 217861).$$

И снова легко проверить, что эти значения переменной  $y$  являются корнями многочлена

$$q_2 = y^6 + 102y^5 + 2619y^4 + 11272y^3 + 131211y^2 + 91074y + 253312.$$

ШАГ 4. Поскольку функция  $f$  имеет единственный простой полюс на конечной части кривой, можно заключить, что она также имеет полюс кратности 11 «над бесконечностью».

В принципе мы могли бы на этом и остановиться. Но хочется сделать последнее утверждение более явным.

Прежде всего введём проективные координаты  $(X : Y : Z)$ , где  $x = X/Z$ ,  $y = Y/Z$ , и проецируем уравнение (7) кривой:

$$Y^2Z + YZ^2 = X^3 - X^2Z - 10XZ^2 - 20Z^3. \quad (9)$$

Конечная часть кривой соответствует значению  $Z = 1$ . Точка «в бесконечности» соответствует  $Z = 0$ , что даёт также  $X = 0$ . Следовательно, мы должны взять  $Y = 1$ . Вблизи этой точки мы можем ввести новые аффинные координаты  $u = X/Y = x/y$ ,  $v = Z/Y = 1/y$ . Подставляя  $x = u/v$ ,  $y = 1/v$  в начальное уравнение, мы получаем уравнение нашей кривой вблизи бесконечности:

$$v + v^2 = u^3 - u^2v - 10uv^2 - 20v^3. \quad (10)$$

Заметим, что наличие слагаемого  $v$  в левой части этого равенства гарантирует нам, что градиент не равен нулю и, значит, кривая в окрестности точки  $(u, v) = (0, 0)$  является гладкой, а переменная  $u$  может быть выбрана в качестве локальной координаты.

Представим теперь  $v$  в виде ряда

$$v = c_0 + c_1u + c_2u^2 + c_3u^3 + c_4u^4 + \dots$$

и подставим этот ряд в разность

$$(v + v^2) - (u^3 - u^2v - 10uv^2 - 20v^3).$$

Мы хотим получить в результате  $o(u^3)$ . Приравнявая нулю коэффициенты перед степенями вплоть до 3-й, мы получаем  $c_0 = c_1 = c_2 = 0$ ,  $c_3 = 1$ . Остаётся проделать две следующие операции:

- 1) подставить  $x = u/v$ ,  $y = 1/v$  в выражение (8) для функции Белого;
- 2) подставить в получившееся выражение  $v = u^3$ .

Тогда функция Белого с точностью до членов меньшего порядка оказывается равной

$$f \sim -\frac{1}{1728} \frac{1 + 11u + 23u^2 - 148u^3 - \dots - 3308u^{13}}{u^{11}(1 - 16u^2)} \sim \frac{\text{Const}}{u^{11}} \text{ при } u \rightarrow 0.$$

Теперь полюс кратности 11 в точке  $u = 0$  виден непосредственно.

Рисунок 18 даёт геометрически «почти правильное» изображение рисунка  $\mathcal{D}_0(11)$ , поднятого с тора  $E$  на комплексную плоскость. В результате получается дважды периодическая карта. Показаны не только чёрные вершины валентности 3, но и белые вершины валентности 2, а также фундаментальный параллелограмм соответствующей решётки. Повторяющиеся копии рисунка  $\mathcal{D}_0(11)$  расположены так, как на рис. 17 справа. Мы пишем, что это изображение *почти* правильное, потому, что петля (клетка валентности 1), которая хорошо видна на рис. 17, как будто отсутствует на рис. 18: она столь мала, что разглядеть её невозможно. Заодно мы убрали и инцидентные с ней чёрную и

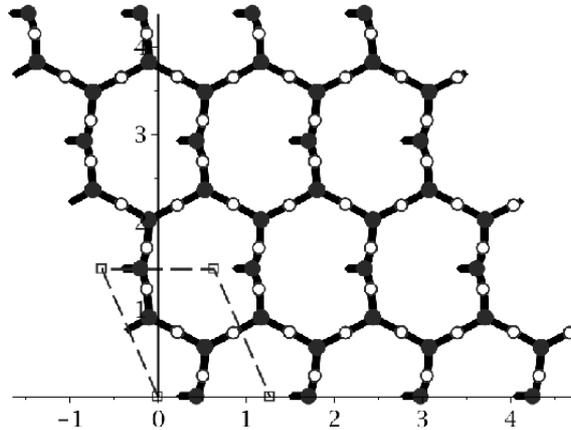


Рис. 18. Геометрически «почти правильное» изображение поднятия рисунка  $\mathcal{D}_0(11)$  на комплексную плоскость

белую вершины — они бы всё равно заслонили друг друга. Нам уже встречалась сходная проблема в связи с рисунком  $\mathcal{D}_0(13)$  (см. рис. 15 и 16). Мы вынуждены признать, что в данном случае природа, технологии и человеческое зрение оказываются несовместимыми.

Изображение, показанное на рис. 18, строится следующим образом. Сначала мы делаем замену переменных

$$y = \frac{z-1}{2}, \quad x = t + \frac{1}{3},$$

чтобы представить эллиптическую кривую  $E$  в нормальной форме Вейерштрасса

$$z^2 = 4t^3 - \frac{124}{3}t - \frac{2501}{27}.$$

Алгоритм 7.4.7 из книги А. Коэна [18], использующий арифметико-геометрическое среднее, даёт нам базис

$$\omega_1 = 1,269209304, \quad \omega_2 = -0,6346046520 + 1,458816617i$$

решётки, показанной на рис. 18. Соответствующий модуль на левой вертикальной границе стандартной фундаментальной области группы  $\Gamma$  равен

$$\tau = \frac{\omega_2}{\omega_1} = -0,5000000000 + 1,149390106i,$$

что вполне согласуется с тем, что  $J(\tau) < 0$ . Чтобы получить вложенный граф, мы сначала поднимаем отрезок  $[0, 1] \subset \Sigma$  вместе с чёрной и белой вершинами соответственно в точках 0 и 1 на кривую  $E$ , используя для этого функцию Белого  $f$ . После этого мы используем стандартную параметризацию кривой  $E$  с помощью функций Вейерштрасса  $t = \wp(w)$  и  $z = \wp'(w)$  для  $w \in \mathbb{C}$ , чтобы поднять получившийся рисунок на плоскость.

### 11.4. Рисунки $\mathcal{D}(p)$

Минимальное регулярное накрытие рисунка  $\mathcal{D}_0(p)$  — это регулярный рисунок  $\mathcal{D}(p)$  типа  $(3, 2, p)$  с группой автоморфизмов  $\mathrm{PSL}_2(p)$ . При  $p > 2$  его степень равна  $p(p^2 - 1)/2$ , а род равен  $(p + 2)(p - 3)(p - 5)/24$ . При  $p = 2$  его степень равна шести, а род равен 0. Кривые, на которых расположены рисунки  $\mathcal{D}(p)$  и  $\mathcal{D}_0(p)$ , — это модулярные кривые  $X(p) = \mathbb{H}/\Gamma(p)$  и  $X_0(p) = \mathbb{H}/\Gamma_0(p)$  (отсюда взялись и обозначения для этих двух рисунков). Здесь  $\Gamma(p)$  — это главная конгруэнц-подгруппа уровня  $p$  в группе  $\Gamma$ , т. е. ядро редукции  $\Gamma \rightarrow \mathrm{PSL}_2(p)$  группы  $\Gamma$  по модулю  $p$  (см., например, [46, § 6.9, 6.10]), а  $\Gamma_0(p)$  — это прообраз в группе  $\Gamma$  подгруппы в  $\mathrm{PSL}_2(p)$ , оставляющей неподвижной точку  $\infty$ .

**Теорема 11.1.** *Для любого простого  $p$  рисунок  $\mathcal{D}(p)$  является единственным регулярным рисунком типа  $(3, 2, p)$  с группой автоморфизмов  $G = \mathrm{PSL}_2(p)$ , а рисунок  $\mathcal{D}_0(p)$  является единственным рисунком степени  $p + 1$  и типа  $(3, 2, p)$  с группой монодромии  $G$ .*

**Доказательство.** Чтобы доказать единственность рисунка  $\mathcal{D}(p)$ , достаточно показать, что группа  $G$  с точностью до автоморфизмов имеет единственную порождающую тройку  $(x, y, z)$  типа  $(3, 2, p)$ . Элементы  $z \in G$  порядка  $p$  все эквивалентны под действием автоморфизмов. Элементы порядка 3 и 2 — это элементы, имеющие след, равный  $\pm 1$  или 0 соответственно. Следовательно, мы можем предположить, что

$$y = \pm \begin{pmatrix} a & b \\ c & -a \end{pmatrix}, \quad z = \pm \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

так что

$$yz = \pm \begin{pmatrix} a + b & b \\ c - a & -a \end{pmatrix}.$$

Мы требуем, чтобы элемент  $yz = x^{-1}$  имел порядок 3, поэтому мы должны иметь  $b = \pm 1$ , и без потери общности мы можем взять  $b = 1$ . Поскольку  $\det y = 1$ , должно быть  $c = -a^2 - 1$ , и мы получаем однопараметрическое семейство решений

$$y = y_a = \pm \begin{pmatrix} a & 1 \\ -a^2 - 1 & -a \end{pmatrix} \quad (a \in \mathbb{F}_p).$$

Действие на тройку  $(x, y, z)$  сопряжением на элемент  $z^i$  оставляет  $z$  неизменным и заменяет  $y = y_a$  на  $y_{a+i}$ . Значит, такие тройки эквивалентны относительно действия автоморфизмов, что и требовалось.

Можно было также воспользоваться формулой Фробениуса (2), как это было сделано в примере 4.1 для  $p = 11$  (таблицу характеров группы  $G$  можно найти в [48, § 5.5]). Это легко проделать для  $p \equiv \pm 5 \pmod{12}$ , поскольку в этом случае есть только один неглавный неприводимый характер (а именно степени  $p$ ), который появляется в сумме по характерам. Однако в том случае, когда  $p \equiv \pm 1 \pmod{12}$ , появляются и другие характеры, и к тому же приходится проделывать некую работу с алгебраическими числами.

Группа  $G$  имеет единственный класс сопряжённости подгрупп индекса  $p + 1$ , а именно стабилизаторы точек на проективной прямой  $\mathbb{P}^1(\mathbb{F}_p)$ . Отсюда следует, что  $\mathcal{D}_0(p)$  — это единственный рисунок степени  $p + 1$  и типа  $(3, 2, p)$  с группой монодромии  $G$ .  $\square$

## 12. Рисунки типа $(3, 2, p)$ и степени $p + 1$

Изучив в предыдущем разделе рисунки  $\mathcal{D}_0(p)$ , займёмся теперь произвольными рисунками типа  $(3, 2, p)$  и степени  $p + 1$ . Группа монодромии такого рисунка  $\mathcal{D}$  — это группа степени  $p + 1$ , содержащая  $p$ -цикл  $z$ . Отсюда следует, что она дважды транзитивна и, следовательно, примитивна. Как и раньше, если  $p > 3$ , что мы будем отныне предполагать, группа  $G$  совершенна. Конечные примитивные группы, содержащие цикл и одну неподвижную точку, были классифицированы П. Мюллером [65, теорема 6.2]. Как следствие мы имеем следующую теорему.

**Теорема 12.1.** *Совершенные группы перестановок степени  $p + 1$  (где  $p$  простое), содержащие  $p$ -цикл, принадлежат одному из следующих классов:*

- (а)  $A_{p+1}$  для простых  $p \geq 5$ ,
- (б)  $\text{PSL}_2(p)$  для простых  $p \geq 5$ ,
- (в) аффинные группы  $\text{AGL}_n(2)$  для простых чисел Мерсенна  $p = 2^n - 1 \geq 7$ ,
- (г) группы Матьё  $M_{11}$  и  $M_{12}$  для  $p = 11$  и  $M_{24}$  для  $p = 23$ ,

причём все эти группы, кроме  $M_{11}$  (см. ниже), фигурируют в их естественных представлениях.

Мы будем рассматривать эти группы по очереди вместе с их аналогами для  $p < 5$ , чтобы выяснить, какие из этих групп могут служить группами монодромии рисунков типа  $(3, 2, p)$ . Результаты будут собраны вместе в теореме 12.5. Удобно начать с простейших случаев (б) и (г), а знакопеременные группы рассмотреть в последнюю очередь.

Группы  $\text{PSL}_2(p)$  в теореме 12.1(б) присутствуют в этом контексте в качестве групп монодромии для всех простых  $p$ . Каждая из них связана с единственным рисунком, а именно с модулярным рисунком  $\mathcal{D}_0(p)$  (см. теорему 11.1).

В пункте (д) группа  $M_{11}$  допускает перестановочное представление степени 12 на классах смежности подгруппы  $\text{PSL}_2(11)$ , но, как мы уже видели в примере 4.2, она не является фактором группы  $\Delta(3, 2, 11)$ , поскольку все тройки интересующего нас типа в  $M_{11}$  порождают не всю эту группу, а её подгруппу  $\text{PSL}_2(11)$ . Следовательно,  $M_{11}$  в данном контексте группой монодромии не является.

Группа  $G = M_{12}$  в пункте (д) имеет два представления степени 12 на классах смежности двух классов сопряжённости подгрупп, изоморфных группе  $M_{11}$ ; эти классы переставляются внешними автоморфизмами из группы  $\text{Out } G$ . Группа  $G = M_{12}$  служит группой монодромии двух киральных пар планарных рисунков типа  $(3, 2, 11)$  и степени 12. По одному рисунку из каждой пары можно увидеть

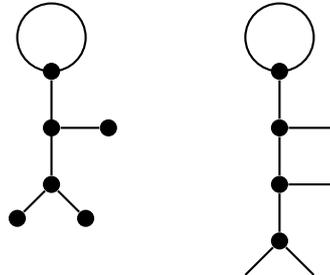


Рис. 19. Два рисунка с группой монодромии  $M_{12}$ . Поле модулей у обоих равно  $\mathbb{Q}(\sqrt{-11})$

на рис. 19. Левый рисунок имеет паспорт  $(3^3 1^3, 2^6, 11^1 1^1)$ , при этом  $\mathcal{X} = 3A$  и  $\mathcal{Y} = 2A$ . Правый рисунок имеет паспорт  $(3^4, 2^4 1^4, 11^1 1^1)$ , при этом  $\mathcal{X} = 3B$  и  $\mathcal{Y} = 2B$ . Их регулярными накрытиями служат два рисунка типа  $(3, 2, 11)$  и рода 3601. Других рисунков данного типа с группой монодромии  $G = M_{12}$  не существует. Если мы возьмём, например,  $\mathcal{X} = 3B$  и  $\mathcal{Y} = 2A$  или  $\mathcal{X} = 3A$  и  $\mathcal{Y} = 2B$ , то получим ещё две орбиты действия группы  $\text{Aut } G$  на тройках, но они порождают транзитивные или нетранзитивные подгруппы, изоморфные группе  $\text{PSL}_2(11)$ . Рисунок, отвечающий транзитивным подгруппам, мы уже видели: его изображение было дано на рис. 17 и 18. Что же касается нетранзитивных подгрупп с орбитами размера 11 и 1, то они являются группами монодромии рисунков  $\mathcal{M}_1$  и  $\bar{\mathcal{M}}_1$  степени 11 (см. рис. 1–3).

При  $p = 23$  группа  $M_{24}$  в пункте (d), найденная Э. Л. Матьё [62] в 1873 году, служит группой монодромии двух киральных пар плоских рисунков с паспортами  $(3^6 1^6, 2^{12}, 23^1 1^1)$  и  $(3^8, 2^8 1^8, 23^1 1^1)$  соответственно (см. орбиты 24.2 и 24.1 в [8, с. 129, 130]). Для первой пары имеем  $\mathcal{X} = 3A$ ,  $\mathcal{Y} = 2B$  и  $\mathcal{Z} = 23A$  или  $\mathcal{Z} = 23B$ . Для второй пары  $\mathcal{X} = 3B$ ,  $\mathcal{Y} = 2A$  и  $\mathcal{Z} = 23A$  или  $23B$ . Один рисунок из каждой пары показан на рис. 20. В отличие от случая  $M_{12}$ , группа  $M_{24}$  имеет единственное перестановочное представление степени  $p + 1$ , а именно естественное представление на классах смежности подгрупп  $M_{23}$ . У неё нет внешних автоморфизмов, так что никто не переставляет два взаимно обратных класса сопряжённости элементов порядка  $p$ .

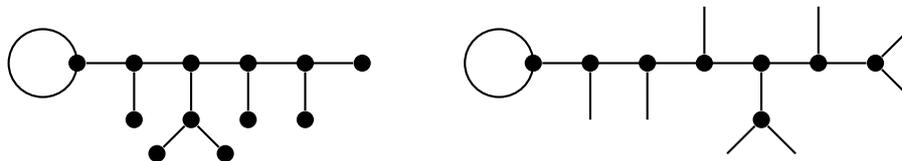


Рис. 20. Два рисунка с группой монодромии  $M_{24}$ . Поле модулей у обоих равно  $\mathbb{Q}(\sqrt{-23})$

Рассмотрим теперь случай (с) теоремы 12.1, в котором речь идёт об аффинных группах  $\text{AGL}_n(2)$ , где число  $n$  простое, а  $p$  — простое число Мерсенна  $2^n - 1$ . Случай  $p = 3$  здесь не возникает, поскольку  $\text{AGL}_2(2) \cong S_4$ , а эта группа не является фактором группы  $\Delta(3, 2, 2) \cong S_3$ . При  $p = 7$  единственный рисунок типа  $(3, 2, 7)$  и степени 8 — это рисунок  $\mathcal{D}_0(7)$  с группой монодромии  $\text{PSL}_2(7)$ , так что группа  $\text{AGL}_3(2)$  не появляется. (Заметим, что группа Гурвица рода 17 является *нерасщепляемым* расширением группы  $V_8$  при помощи группы  $\text{GL}_3(2)$ , неизоморфной группе  $\text{AGL}_3(2)$ , так что она не имеет транзитивного перестановочного представления степени 8, детали можно найти в [49].) С другой стороны, при  $p = 31$  орбита 32.1 из [8, с. 134, 135] состоит из шести планарных рисунков типа  $(3, 2, 31)$  и степени 32 с группой монодромии  $\text{ASL}_5(2) = \text{AGL}_5(2)$ . Три рисунка, по одному из трёх киральных пар, показаны в разделе 14.6, рис. 28.

**Теорема 12.2.** *Для любого простого числа Мерсенна  $p = 2^n - 1 > 7$  существуют рисунки типа  $(3, 2, p)$  и степени  $p + 1$  с группой монодромии  $\text{AGL}_n(2)$ . Их паспорт равен  $(3^{(p-1)/3}1^2, 2^{(p+1)/2}, p^11^1)$ , а род равен  $(p + 5)/12$ .*

**Доказательство.** Мы воспользуемся тем фактом, что группа  $G := \text{AGL}_n(2)$  представляет собой полупрямое произведение её подгруппы сдвигов  $T \cong (C_2)^n$  на группу  $G_0 := \text{GL}_n(2)$ , которая является стабилизатором точки 0. Пусть  $(x, y, z)$  — тройка типа  $(3, 2, p)$ , порождающая группу  $\text{GL}_n(2)$ . Допустим, что она выбрана способом, описанным в теореме 10.11, с параметрами  $r = s = 1$ , так что  $\alpha = 1$  и  $\beta = (n + 1)/2$ . Пусть теперь  $u = xa$ ,  $v = yb$  и  $w = zc$ , где  $a, b, c \in T$ . Мы попытаемся выбрать  $a$ ,  $b$  и  $c$  таким образом, чтобы тройка  $(u, v, w)$  была порождающей тройкой типа  $(3, 2, p)$  группы  $G$ .

Поскольку  $x^3 = 1$ , мы имеем

$$u^3 = (xa)^3 = x^3 a^{x^2} a^x a = a^{x^2+x+1},$$

так что  $u^3 = 1$  в том и только в том случае, когда  $a \in T_x := \ker(x^2 + x + 1)$ . (Здесь мы рассматриваем  $x^2 + x + 1$  как линейное преобразование векторного пространства  $T$  над полем  $\mathbb{F}_2$ .) Аналогично  $v^2 = 1$  тогда и только тогда, когда  $b \in T_y := \ker(y + 1)$ , и  $w^p = 1$  тогда и только тогда, когда  $c \in T_z := \ker(z^{p-1} + z^{p-2} + \dots + z + 1)$ . Кроме того,

$$uvw = xa \cdot yb \cdot zc = xya^y z b^z c = xyza^{yz} b^z c = a^{yz} b^z c,$$

так что  $uvw = 1$  тогда и только тогда, когда  $a^{yz} b^z c = 1$ .

Поскольку  $z$  является циклом Зингера в группе  $G_0$ , справедливо равенство  $T_z = T$ , так что условие на  $c$  никаким ограничением не является. В то же время из жордановых форм для  $x$  и  $y$ , использовавшихся в доказательстве теоремы 10.11, видно, что размерности подпространств  $T_x$  и  $T_y$  равны  $n - 1$  и  $(n + 1)/2$  соответственно. В этих подпространствах можно выбрать  $a$  и  $b$  произвольно, а затем положить  $c = a^{yz} b^z$ . Тогда мы получим  $a^{yz} b^z c = 1$ , и следовательно, тройка  $(u, v, w)$  имеет тип  $(3, 2, p)$ .

Цикловые структуры перестановок  $u$ ,  $v$  и  $w$  могут быть найдены следующим образом. Группу  $\text{AGL}_n(2)$  можно рассматривать как действующую естествен-

ным образом на  $T$ : элементы группы  $T$  действуют сдвигами, а элементы группы  $\mathrm{GL}_n(2)$  — линейными преобразованиями. Элемент  $u = xa$  действует на  $T$  как отображение  $t \mapsto t^x a$ , так что он оставляет на месте элемент  $t \in T$  тогда и только тогда, когда  $a = t(1-x)$  (здесь мы для векторного пространства  $T$  используем аддитивные обозначения). Жорданова форма элемента  $x$  показывает, что  $T(1-x) = T_x$ , так что для любого выбора  $a \in T_x$  элемент  $u$  имеет ровно две неподвижные точки  $t \in T$ , поскольку  $|\ker(1-x)| = 2$ . Так как  $u$  имеет порядок 3, мы заключаем, что у него есть  $(p-1)/3$  циклов длины 3. В случае  $v$  жорданова форма элемента  $y$  указывает на то, что  $T(1-y)$  является подпространством коразмерности 1 в  $T_y$ . Поэтому, выбрав  $b \in T_y \setminus T(1-y)$ , мы можем добиться того, чтобы элемент  $v$  не имел неподвижных точек. Следовательно, он будет состоять из  $(p+1)/2$  транспозиций. Наконец,  $w$ , будучи элементом порядка  $p$ , имеет цикловую структуру  $p^1 1^1$ .

Пусть теперь  $H := \langle u, v, w \rangle \leq G$ . Мы докажем, что если  $p > 7$ , то  $H = G$ . Факторизация по подгруппе  $T$  отображает группу  $H$  на  $\langle x, y, z \rangle = G_0$ , так что  $HT = G$ . Если группа  $H$  содержит неединичный сдвиг  $t \in T$ , то, поскольку  $H$  содержит  $w$ , она содержит также и все неединичные сдвиги, и следовательно,  $H = G$ , что и требовалось.

Раз так, предположим от противного, что  $H \cap T = 1$ , так что  $H$  — это дополнение группы  $T$  в  $G$ . Поскольку первая группа когомологий  $H^1(\mathrm{GL}_n(2), T)$  группы  $\mathrm{GL}_n(2)$  на её естественном модуле  $T$  тривиальна для всех  $n > 3$  (см. [11]), существует единственный класс сопряжённости таких дополнений, так что  $H$  — это стабилизатор точки в естественном действии группы  $G$ . А это противоречит тому факту, что  $v$ , согласно нашему выбору сдвига  $b$ , не имеет неподвижных точек.

Итак, тройка  $(u, v, w)$  является порождающей для группы  $G$ , так что она соответствует рисунку типа  $(3, 2, p)$  и степени  $p+1$  с группой монодромии  $G$ . Род этого рисунка легко выводится из его паспорта, который был определён выше.  $\square$

Приведённое выше доказательство не проходит для  $p = 7$ , поскольку в этом случае  $|H^1(\mathrm{GL}_3(2), T)| = 2$  (см. [11]). Это означает, что в группе  $\mathrm{AGL}_3(2)$  имеется два класса сопряжённости дополнений к подгруппе  $T$ . Один из них состоит из стабилизаторов точек, другой — из подгрупп, действующих транзитивно на  $T$  как  $\mathrm{PSL}_2(7)$ . В таком случае каждая тройка типа  $(3, 2, 7)$  порождает одно из дополнений. (Кстати сказать, тот факт, что все дополнения изоморфны фактору  $G/T$ , даёт простое доказательство того, что  $\mathrm{GL}_3(2) \cong \mathrm{PSL}_2(7)$ .)

**Пример 12.3.** Взяв  $n = 5$ , мы получим рисунок типа  $(3, 2, 31)$ , степени 32 и рода 3 с паспортом  $(3^{10}1^2, 2^{16}, 31^11^1)$ . Его не следует путать с орбитой Галуа 32.1 из [8], состоящей из шести планарных рисунков того же типа и с той же группой монодромии, но с паспортом  $(3^{10}1^2, 2^{12}1^8, 31^11^1)$ , которые соответствуют выбору  $b \in T(1-y)$ , так что  $v$  оставляет неподвижными  $|\ker(1-y)| = 8$  точек (см. пример в разделе 14.6).

Займёмся, наконец, знакопеременными группами монодромии  $A_{p+1}$ , относящимися к пункту (а) теоремы 12.1

**Теорема 12.4.** Знакопеременная группа  $A_{p+1}$ , где  $p$  простое, является группой монодромии рисунков типа  $(3, 2, p)$  и степени  $p + 1$  при  $p = 3$  и при всех  $p \geq 11$ .

**Доказательство.** При  $p = 2, 5, 7$  треугольная группа  $\Delta(3, 2, p)$  не отображается на группу  $A_{p+1}$ . Это очевидно при  $p = 2$  и  $p = 5$ , а относительно  $p = 7$  хорошо известно, что группа  $A_8$  не является гурвицевой: все тройки типа  $(3, 2, 7)$  в этой группе порождают её собственные подгруппы, изоморфные группе  $PSL_2(7)$ . С другой стороны,  $A_4$  служит группой монодромии рисунка типа  $(3, 2, 3)$  и степени 4, изображённого слева на рис. 21. Этот рисунок является фактором тетраэдра  $\{3, 3\}$  по группе  $C_3$ . (Заметим, что группа  $A_4$  также изоморфна группе  $PSL_2(3)$ , относящейся к пункту (b) теоремы 12.1.)

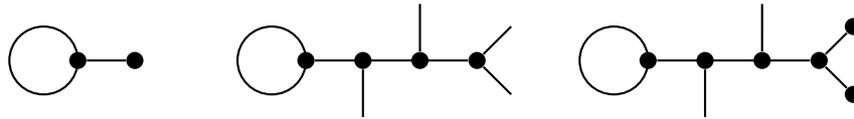


Рис. 21. Рисунки с группами монодромии  $A_4$ ,  $A_{12}$  и  $A_{14}$

Для  $p = 11$  и  $p = 13$  согласно теореме 12.1 достаточно заметить, что рисунки степени 12 и 14 на рис. 21 не изоморфны тем единственным рисункам  $\mathcal{D}_0(p)$  с группой монодромии  $PSL_2(p)$ , показанным на рис. 17 и 13.

Пусть, наконец,  $p \geq 17$ . Если  $p \equiv 2 \pmod{3}$ , например  $p = 3k + 2$  для некоторого  $k \geq 5$ , рассмотрим рисунок  $\mathcal{D}$ , изображённый на рис. 22. У него  $k$  вершин валентности 3, так что его степень равна  $p + 1$ , а паспорт равен  $(3^k 1^3, 2^{k+3} 1^{k-3}, p^{11})$ . Группа монодромии рисунка  $\mathcal{D}$  не может быть группой  $PSL_2(p)$ , поскольку неединичный элемент этой группы имеет не более двух неподвижных точек, в то время как у перестановки  $x$  их три. Аналогично она не может быть группой  $AGL_n(2)$  ни для какого  $n$ , поскольку множество неподвижных точек любого элемента этой группы либо пусто, либо является аффинным подпространством и состоит из  $2^d$  точек для некоторого  $d$ . Наконец, группа монодромии не может быть группой Матьё поскольку рисунок  $\mathcal{D}$

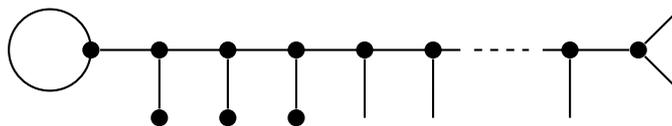


Рис. 22. Рисунок с группой монодромии  $A_{p+1}$

не изоморфен рисункам, изображённым на рис. 19 и 20 или их зеркальным отражениям. Таким образом, группе монодромии не остаётся ничего иного, кроме как быть группой  $A_{p+1}$ .

Если  $p \equiv 1 \pmod{3}$ , например  $p = 3k + 4$  для некоторого  $k \geq 5$ , мы можем использовать сходные рассуждения применительно к рисунку  $\mathcal{D}'$ , который получается из рисунка  $\mathcal{D}$  добавлением двух вершин валентности 1 к самым правым висячим рёбрам. Паспорт полученного рисунка оказывается равным  $(3^k 1^5, 2^{k+5} 1^{k-5}, p^1 1^1)$ .  $\square$

Направляя вверх произвольное подмножество висячих вершин рисунков  $\mathcal{D}$  или  $\mathcal{D}'$ , мы получим множество рисунков, растущее экспоненциально при  $p \rightarrow \infty$ , и все они будут иметь тип  $(3, 2, p)$ , степень  $p + 1$  и группу монодромии  $A_{p+1}$ . Разумеется, рисунки с той же группой монодромии можно строить и многими другими способами, так что правильная формулировка будет такая: число рисунков с группой монодромии  $A_{p+1}$  при  $p \rightarrow \infty$  растёт не менее чем экспоненциально.

Теперь мы можем сформулировать итоговый результат двух последних разделов.

**Теорема 12.5.** Пусть  $p$  — простое число, такое что существует рисунок типа  $(3, 2, p)$  и степени  $p+1$  с группой монодромии  $G$ . Тогда верно одно из следующих утверждений:

- (a)  $G = A_{p+1}$ , где  $p = 3$  или  $p \geq 11$ ,
- (b)  $G = \text{PSL}_2(p)$ ,
- (c)  $G = \text{AGL}_n(2)$  для некоторого простого числа Мерсенна  $p = 2^n - 1 \geq 31$ ,
- (d)  $G = M_{12}$  при  $p = 11$  или  $G = M_{24}$  при  $p = 23$ ,

причём каждая группа рассматривается в её естественном представлении. В случае (a) имеется как минимум экспоненциальное количество рисунков при  $p \rightarrow \infty$ , даже если ограничиться планарными рисунками. В случае (b) для каждого простого  $p$  существует единственный рисунок  $\mathcal{D}_0(p)$ . В случае (c) для каждого простого числа Мерсенна  $p \geq 31$  существует хотя бы один рисунок. В случае (d) для каждой из двух групп имеются две киральные пары рисунков.

### 13. Неизбранная дорога

Название этого раздела является аллюзией на стихотворение Роберта Фроста «The road not taken»<sup>1</sup>.

Отправной точкой работы Ф. Клейна [55] и, следовательно, наших исследований в этой статье, послужило вложение икосаздральной группы  $A_5$  в группу  $\text{PSL}_2(11)$ . Это третий и наиболее сложный случай из трёх, известных уже Э. Га-луа, когда группа  $\text{PSL}_2(p)$  имеет подгруппу индекса  $p$ . Два предыдущих случая,

<sup>1</sup>[www.poetryfoundation.org/poems/44272/the-road-not-taken](http://www.poetryfoundation.org/poems/44272/the-road-not-taken). Русский перевод: [askbooka.ru/stihi/robert-frost/neizbrannaya-doroga.html](http://askbooka.ru/stihi/robert-frost/neizbrannaya-doroga.html).

для  $p = 5$  и  $p = 7$ , послужили каждый предметом заслуженно знаменитых книг (соответственно [5] и [28]). Легко представить себе (но не так легко написать) аналогичную книгу для  $p = 11$ . В этом предпоследнем разделе мы дадим краткий набросок того направления исследований, которое могло бы послужить основой для главы в такой книге. Путь, которым мы здесь следуем, не имеет почти ничего общего с выбранным для данной статьи. Тем не менее здесь присутствует один интригующий момент, когда на краткий миг появляется мимолётный образ той дороги, которую выбрал Ф. Клейн в своей работе [54], посвящённой случаю  $p = 7$ .

В математике существует немало объектов и явлений, связанных с вложением (или, более точно, с вложениями) группы  $A_5$  в группу  $L = \text{PSL}_2(11)$ . Хорошим примером может служить неориентируемый правильный абстрактный многогранник  $\{3, 5, 3\}_5$ , *гендекахорон*, или *11-ячейник*, открытый независимо Б. Грюнбаумом [40] и Г. Коксетером [22] (по поводу этого примера см. также [23, 24], а общая теория абстрактных многогранников изложена в [63]).

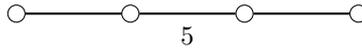


Рис. 23. Диаграмма Коксетера  $\{3, 5, 3\}$

Обозначим через  $\Gamma$  группу Коксетера с символом Шлефли  $\{3, 5, 3\}$ : она представляется диаграммой Коксетера, изображённой на рис. 23. У этой группы четыре образующих  $R_i$  ( $i = 0, \dots, 3$ ), а определяющие соотношения следующие:

$$R_i^2 = (R_0 R_1)^3 = (R_1 R_2)^5 = (R_2 R_3)^3 = 1, \quad (R_i R_j)^2 = 1 \quad \text{при } |i - j| \geq 2.$$

Эта группа действует как группа изометрий гиперболического 3-пространства  $\mathbb{H}^3$ , порождённая отражениями относительно граней тетраэдра  $T \subset \mathbb{H}^3$  со специально подобранными двугранными углами. Как показано в [47], в группе  $\Gamma$  существует единственная нормальная подгруппа  $N$ , такая что  $\Gamma/N \cong L$ . Эта подгруппа является нормальным замыканием элементов  $(R_0 R_1 R_2)^5$  и  $(R_1 R_2 R_3)^5$ , поэтому, полагая эти элементы равными единице, мы получим представление для группы  $L$ .

Фактор  $\mathbb{H}^3/N$  является компактным неориентируемым гиперболическим 3-орбифолдом  $\mathcal{N}$  с замощением  $\mathcal{T}$ , состоящим из  $|L| = 660$  тетраэдров: оно индуцировано замощением пространства  $\mathbb{H}^3$  образами тетраэдра  $T$  под действием группы  $\Gamma$ . Эти тетраэдры можно разбить на 11 подмножеств, по 60 тетраэдров в каждом, порождающих замощение  $\mathcal{I}$  орбифолда  $\mathcal{N}$  одиннадцатью полукосаэдрами  $\{3, 5\}_5$  (эти фигуры являются антиподальными факторами икосаэдра  $\{3, 5\}$  при отождествлении рёбер, находящихся на расстоянии в пять шагов друг от друга на путях Петри); при этом замощение  $\mathcal{T}$  является барицентрическим разбиением замощения  $\mathcal{I}$ . Аналогично  $\mathcal{I}$  имеет 11 вершин, и вершинной фигурой каждой из них является неориентированный регулярный полудодекаэдр  $\{5, 3\}_5$ , образованный таким же образом из додекаэдра  $\{5, 3\}$ ; индексы указывают на идентификации, но также и на дополнительные соотношения между

образующими в  $L$ . Группой автоморфизмов орбифолда  $\mathcal{I}$  служит группа  $L$ , а стабилизаторы клеток и вершин образуют два класса сопряжённости подгрупп  $H \cong A_5$  в  $L$ , представленные образами двух подгрупп

$$\langle R_0, R_1, R_2 \rangle \cong \langle R_1, R_2, R_3 \rangle \cong \Delta[3, 2, 5] \cong A_5 \times C_2$$

группы  $\Gamma$ . Заметим, что группа  $N$  не является группой без кручения (она содержит центральную инволюцию каждой из указанных подгрупп), и следовательно, орбифолд  $\mathcal{N}$  не является многообразием.

Нормализатор  $\Omega$  группы  $\Gamma$  в группе изометрий пространства  $\mathbb{H}^3$  представляет собой полупрямое произведение группы  $\Gamma$  на группу  $C_2$ , индуцированную в  $\Gamma$  автоморфизмом графа  $R_i \mapsto R_{3-i}$ . Этот автоморфизм оставляет группу  $N$  инвариантной, причём  $\Omega/N \cong \text{PGL}_2(11)$ ; на  $\mathcal{I}$  он действует как автодвойственность, отображая друг в друга вершины и трёхмерные клетки, а также рёбра и двумерные клетки.

Группа  $\Omega$  играет в теории компактных 3-многообразий роль, аналогичную той, что в теории римановых и клейновых поверхностей играют треугольные группы  $\Delta(3, 2, 7)$  и  $\Delta[3, 2, 7]$ . В частности, как показано в [33, 60],  $\Omega$  имеет наименьший кообъём среди всех кокомпактных разрывных групп изометрий пространства  $\mathbb{H}^3$ . Отсюда следует, что нормальные подгруппы  $K$  без кручения конечного индекса в  $\Omega$  униформизируют компактные гиперболические многообразия, на которых достигается максимум числа автоморфизмов (а именно,  $|\Omega/K|$ ) на единицу объёма. Тем самым эти многообразия и группы автоморфизмов служат трёхмерными аналогами кривых и групп Гурвица в размерности 2. Как показано в [47], среди всех таких подгрупп  $K$  наименьший индекс имеет группа  $K = N \cap \Omega^+$ , где  $\Omega^+$  — это сохраняющая ориентацию подгруппа индекса 2 в  $\Omega$ . Соответствующее ориентируемое многообразие  $\mathcal{K} = \mathbb{H}^3/K$ , двухкрат-

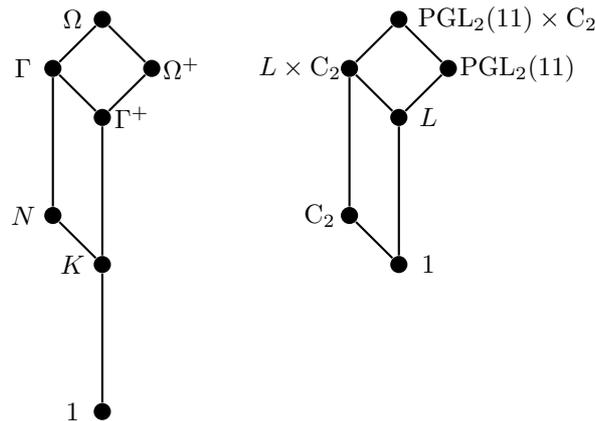


Рис. 24. Подгруппы группы  $\Omega$  и их факторы по подгруппе  $K$

ное накрытие орбифолда  $\mathcal{N}$ , имеет группу изометрий  $\Omega/K \cong \mathrm{PGL}_2(11) \times C_2$  с сохраняющей ориентацию подгруппой  $\Omega^+/K \cong \mathrm{PGL}_2(11)$ . Подгруппа  $\Gamma/K \cong L \times C_2$  сохраняет замощение многообразия  $\mathcal{K}$  одиннадцатью икосаэдрами, а два класса сопряжённости икосаэдральных подгрупп  $A_5 \times C_2$ , оставляющих инвариантными клетки и вершины, переходят друг в друга в  $\Omega/K$  по двойственности. В силу минимальности своих объёмов многообразия  $\mathcal{K}$  и  $\mathcal{N}$  являются трёхмерными аналогами квартики Клейна [54] — наименьшей римановой поверхности, на которой достигается оценка Гурвица числа автоморфизмов на единицу площади (см. [28], где объясняются связи с группой  $\mathrm{PSL}_2(7)$  и со статьёй Ф. Клейна [54]). На рис. 24 показаны упомянутые выше подгруппы группы  $\Omega$  и их факторы по подгруппе  $K$ , т. е. конечные группы изометрий, которые они индуцируют на  $\mathcal{K}$ .

## 14. Несколько дополнительных примеров

В этом разделе мы приводим стандартные образующие для групп монодромии некоторых небольших, но интересных рисунков, рассмотренных ранее, иногда сопровождая их комментариями, а также, в случае малого рода, и изображениями. Вычисления проделаны с помощью системы GAP.

### 14.1. Рисунки Клейна, степень 11

Образующие  $x_i$ ,  $y_i$  и  $z_i$  групп монодромии рисунков Клейна  $M_i$  ( $i = 1, \dots, 6$ ) (см. раздел 2 и рис. 3) как подгрупп группы  $S_{11}$  выглядят следующим образом. Во всех случаях

$$z_i = (1, 2, \dots, 11),$$

а остальные образующие  $x_i$  и  $y_i$  для  $i = 1, \dots, 6$  (единственные с точностью до сопряжения перестановкой  $z_i$ ) выписаны ниже.

$$\begin{aligned} x_1 &= (1, 4, 3)(5, 11, 9)(6, 8, 7), & y_1 &= (1, 2)(4, 11)(5, 8)(9, 10); \\ x_2 &= (1, 4, 2)(5, 11, 9)(6, 8, 7), & y_2 &= (2, 3)(4, 11)(5, 8)(9, 10); \\ x_3 &= (1, 3, 2)(4, 11, 10)(5, 9, 7), & y_3 &= (3, 11)(4, 9)(5, 6)(7, 8); \\ x_4 &= (1, 4, 3)(5, 11, 10)(6, 9, 8), & y_4 &= (1, 2)(4, 11)(5, 9)(6, 7); \\ x_5 &= (1, 11, 6)(2, 5, 4)(7, 10, 8), & y_5 &= (1, 5)(2, 3)(6, 10)(8, 9); \\ x_6 &= (1, 11, 6)(2, 5, 3)(7, 10, 9), & y_6 &= (1, 5)(3, 4)(6, 10)(7, 8). \end{aligned}$$

**Замечание 14.1.** Здесь и далее если два рисунка  $\mathcal{D}$  и  $\bar{\mathcal{D}}$  степени  $n$  образуют киральную пару и  $\mathcal{D} = (x, y, z)$ , то рисунок  $\bar{\mathcal{D}}$  можно получить как  $(x', y', z') = (x^{-1}, y^{-1}, yx)$ . Заметим, что перестановка  $z' = yx$  не обязана иметь какую бы то ни было каноническую форму. Её тем не менее можно сделать «стандартной» путём совместного сопряжения элементов  $x'$ ,  $y'$ ,  $z'$  в  $S_n$ .

В дальнейшем во избежание ошибок мы просто воспроизводим результаты вычислений на GAP.

### 14.2. Группа $\mathrm{PSL}_3(3)$ , степень 13

Всего существует 14 плоских деревьев с паспортом  $(3^4 1^1, 2^4 1^5, 13^1)$ . Четыре из них порождают группу монодромии  $\mathrm{PSL}_3(3)$ . Мы фиксируем перестановку  $z = (1, 2, \dots, 13)$ , а также помечаем единственную неподвижную точку перестановки  $x$  этикеткой 1. Деревья разбиваются на две киральные пары  $(\mathcal{M}_1, \mathcal{M}_3)$  и  $(\mathcal{M}_2, \mathcal{M}_4)$ . Деревья  $\mathcal{M}_1$  и  $\mathcal{M}_2$  показаны на рис. 12 (см. пример 10.5).

$$\mathcal{M}_1 = [ (2, 13, 6) (3, 5, 4) (7, 12, 11) (8, 10, 9), (1, 13) (2, 5) (6, 12) (7, 10), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13) ],$$

$$\mathcal{M}_2 = [ (2, 13, 3) (4, 12, 5) (6, 11, 10) (7, 9, 8), (1, 13) (3, 12) (5, 11) (6, 9), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13) ],$$

$$\mathcal{M}_3 = [ (2, 13, 9) (3, 8, 4) (5, 7, 6) (10, 12, 11), (1, 13) (2, 8) (4, 7) (9, 12), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13) ],$$

$$\mathcal{M}_4 = [ (2, 13, 12) (3, 11, 10) (4, 9, 5) (6, 8, 7), (1, 13) (2, 11) (3, 9) (5, 8), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13) ].$$

Поле модулей этих четырёх деревьев — это поле разложения многочлена  $a^4 + a^3 + 2a^2 - 4a + 3$ . Группой Галуа этого многочлена является циклическая группа  $C_4$ .

### 14.3. Группа $\mathrm{PSL}_2(16)$ , степень 17

В этой группе имеется восемь классов сопряжённости элементов порядка 17, но есть также и четыре автоморфизма поля  $\mathbb{F}_{16}$ . Поэтому, как предсказывает теорема 10.1, мы получаем две неизоморфные карты (см. пример 10.2). Паспорт этих карт равен  $(3^5 1^2, 2^8 1^1, 17^1)$ , так что сами карты имеют род 1. Можно также заметить, что они не киральны: обе являются зеркально симметричными. Они показаны на рис. 25.

Общее количество карт с данным паспортом равно 70.

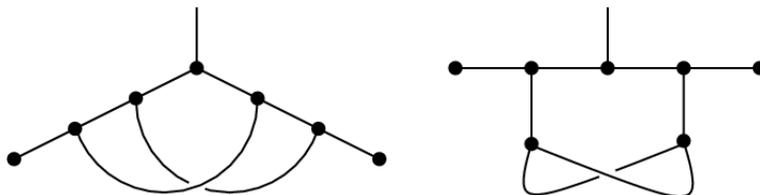


Рис. 25. Две карты, представляющие группу  $\mathrm{PSL}_2(16)$

Как обычно, мы фиксируем перестановку  $z = (1, 2, \dots, 17)$ , а этикеткой 1 помечаем единственную неподвижную точку перестановки  $y$ . Вот что получается.

$$\begin{aligned}
 M_1 = [ & (1, 10, 2) (3, 9, 13) (4, 12, 6) (7, 11, 17) (8, 16, 14), \\
 & (2, 9) (3, 12) (4, 5) (6, 11) (7, 16) (8, 13) (10, 17) (14, 15), \\
 & (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17) ] , \\
 M_2 = [ & (1, 10, 2) (3, 9, 5) (6, 8, 13) (7, 12, 14) (11, 17, 15), \\
 & (2, 9) (3, 4) (5, 8) (6, 12) (7, 13) (10, 17) (11, 14) (15, 16), \\
 & (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17) ] .
 \end{aligned}$$

**Замечание 14.2.** Следующее простое число Ферма после 17 — это 257. Бросим беглый взгляд на группу  $\mathrm{PSL}_2(256)$ . В ней имеется 128 классов сопряжённости циклов порядка 257, а поле  $\mathbb{F}_{256}$  допускает восемь автоморфизмов. Следовательно, имеются 16 неизоморфных карт, порождающих эту группу. Их паспорт  $(3^{85}1^2, 2^{128}1^1, 257^1)$ , а род соответственно равен 21 в полном согласии с теоремой 10.1. Из этой теоремы также следует, что все эти карты зеркально симметричны.

#### 14.4. Группа $\mathrm{PSL}_3(5)$ , степень 31

Ниже приведены десять рисунков типа  $(3, 2, 31)$  с паспортом  $(3^{10}1^1, 2^{12}1^7, 31^1)$ . Их род равен  $g = 1$ , и они представляют группу  $\mathrm{PSL}_3(5)$  (см. пример 10.6). Карта  $M_1$  показана на рис. 26.

- Перестановка  $z$  всегда одна и та же:  $z = (1, 2, 3, \dots, 31)$ .
- Неподвижная точка перестановки  $x$  помечена этикеткой 1. Это и предыдущее соглашения позволяют расставить все этикетки однозначным образом.
- Киральные пары — это  $(M_i, M_{i+5})$ ,  $i = 1, \dots, 5$ .

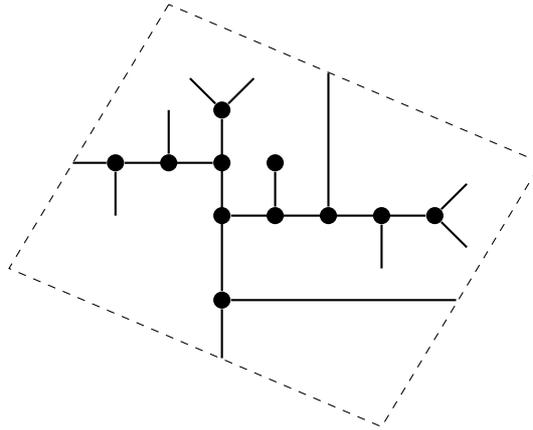


Рис. 26. Противоположные стороны внешнего параллелограмма отождествляются, что даёт нам тор. Получающийся рисунок на торе имеет степень 31, тип  $(3, 2, 31)$  и группу монодромии  $\mathrm{PSL}_3(5)$ . Рисунок соответствует тройке  $M_1 = (x_1, y_1, z)$  из приведённого выше списка

- M1 = [ (2, 31, 19) (3, 18, 11) (4, 10, 21) (5, 20, 30) (6, 29, 25) (7, 24, 23) (8, 22, 9)  
 (12, 17, 16) (13, 15, 14) (26, 28, 27),  
 (1, 31) (2, 18) (3, 10) (4, 20) (5, 29) (6, 24) (7, 22) (9, 21) (11, 17) (12, 15)  
 (19, 30) (25, 28),  
 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
 25, 26, 27, 28, 29, 30, 31) ],
- M2 = [ (2, 31, 3) (4, 30, 16) (5, 15, 6) (7, 14, 8) (9, 13, 21) (10, 20, 23) (11, 22, 12)  
 (17, 29, 18) (19, 28, 24) (25, 27, 26),  
 (1, 31) (3, 30) (4, 15) (6, 14) (8, 13) (9, 20) (10, 22) (12, 21) (16, 29) (18, 28)  
 (19, 23) (24, 27),  
 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
 25, 26, 27, 28, 29, 30, 31) ],
- M3 = [ (2, 31, 3) (4, 30, 29) (5, 28, 19) (6, 18, 13) (7, 12, 8) (9, 11, 10) (14, 17, 21)  
 (15, 20, 27) (16, 26, 22) (23, 25, 24),  
 (1, 31) (3, 30) (4, 28) (5, 18) (6, 12) (8, 11) (13, 17) (14, 20) (15, 26) (16, 21)  
 (19, 27) (22, 25),  
 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
 25, 26, 27, 28, 29, 30, 31) ],
- M4 = [ (2, 31, 24) (3, 23, 16) (4, 15, 14) (5, 13, 12) (6, 11, 7) (8, 10, 9) (17, 22, 21)  
 (18, 20, 27) (19, 26, 28) (25, 30, 29),  
 (1, 31) (2, 23) (3, 15) (4, 13) (5, 11) (7, 10) (16, 22) (17, 20) (18, 26) (19, 27)  
 (24, 30) (25, 28),  
 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
 25, 26, 27, 28, 29, 30, 31) ],
- M5 = [ (2, 31, 3) (4, 30, 8) (5, 7, 6) (9, 29, 15) (10, 14, 19) (11, 18, 24) (12, 23, 22)  
 (13, 21, 20) (16, 28, 27) (17, 26, 25),  
 (1, 31) (3, 30) (4, 7) (8, 29) (9, 14) (10, 18) (11, 23) (12, 21) (13, 19) (15, 28)  
 (16, 26) (17, 24),  
 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
 25, 26, 27, 28, 29, 30, 31) ],
- M6 = [ (2, 31, 14) (3, 13, 28) (4, 27, 8) (5, 7, 6) (9, 26, 10) (11, 25, 24) (12, 23, 29)  
 (15, 30, 22) (16, 21, 17) (18, 20, 19),  
 (1, 31) (2, 13) (3, 27) (4, 7) (8, 26) (10, 25) (11, 23) (12, 28) (14, 30) (15, 21)  
 (17, 20) (22, 29),  
 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
 25, 26, 27, 28, 29, 30, 31) ],
- M7 = [ (2, 31, 30) (3, 29, 17) (4, 16, 15) (5, 14, 9) (6, 8, 7) (10, 13, 23) (11, 22, 21)  
 (12, 20, 24) (18, 28, 27) (19, 26, 25),  
 (1, 31) (2, 29) (3, 16) (4, 14) (5, 8) (9, 13) (10, 22) (11, 20) (12, 23) (17, 28)  
 (18, 26) (19, 24),  
 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
 25, 26, 27, 28, 29, 30, 31) ],
- M8 = [ (2, 31, 30) (3, 29, 4) (5, 28, 14) (6, 13, 18) (7, 17, 11) (8, 10, 9) (12, 16, 19)  
 (15, 27, 20) (21, 26, 25) (22, 24, 23),  
 (1, 31) (2, 29) (4, 28) (5, 13) (6, 17) (7, 10) (11, 16) (12, 18) (14, 27) (15, 19)  
 (20, 26) (21, 24),  
 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,  
 25, 26, 27, 28, 29, 30, 31) ],

$$\begin{aligned}
M_9 = [ & (2, 31, 9) (3, 8, 4) (5, 7, 14) (6, 13, 15) (10, 30, 17) (11, 16, 12) (18, 29, 19) \\
& (20, 28, 21) (22, 27, 26) (23, 25, 24), \\
& (1, 31) (2, 8) (4, 7) (5, 13) (6, 14) (9, 30) (10, 16) (12, 15) (17, 29) (19, 28) \\
& (21, 27) (22, 25), \\
& (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\
& 25, 26, 27, 28, 29, 30, 31) ],
\end{aligned}$$

$$\begin{aligned}
M_{10} = [ & (2, 31, 30) (3, 29, 25) (4, 24, 18) (5, 17, 6) (7, 16, 8) (9, 15, 22) (10, 21, 11) \\
& (12, 20, 13) (14, 19, 23) (26, 28, 27), \\
& (1, 31) (2, 29) (3, 24) (4, 17) (6, 16) (8, 15) (9, 21) (11, 20) (13, 19) (14, 22) \\
& (18, 23) (25, 28), \\
& (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\
& 25, 26, 27, 28, 29, 30, 31) ].
\end{aligned}$$

### 14.5. Группа $\mathrm{PSL}_5(2)$ , степень 31

Ниже мы приводим шесть карт с тем же паспортом, что и в предыдущем примере, т. е.  $(3^{10}1^1, 2^{12}1^7, 31^1)$ , и, следовательно, рода 1, но на этот раз они представляют группу  $\mathrm{PSL}_5(2)$  (см. пример 10.9). Карта  $\mathcal{M}_1$  показана на рис. 27.

- Перестановка  $z$  всегда одна и та же:  $z = (1, 2, 3, \dots, 31)$ .
- Неподвижная точка перестановки  $x$  всегда помечена этикеткой 1.
- Киральные пары — это  $(\mathcal{M}_1, \mathcal{M}_4)$ ,  $(\mathcal{M}_2, \mathcal{M}_5)$  и  $(\mathcal{M}_3, \mathcal{M}_6)$ .

$$\begin{aligned}
M_1 = [ & (2, 31, 23) (3, 22, 4) (5, 21, 6) (7, 20, 19) (8, 18, 12) (9, 11, 10) (13, 17, 27) \\
& (14, 26, 25) (15, 24, 30) (16, 29, 28), \\
& (1, 31) (2, 22) (4, 21) (6, 20) (7, 18) (8, 11) (12, 17) (13, 26) (14, 24) (15, 29) \\
& (16, 27) (23, 30), \\
& (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\
& 25, 26, 27, 28, 29, 30, 31) ],
\end{aligned}$$

$$\begin{aligned}
M_2 = [ & (2, 31, 11) (3, 10, 25) (4, 24, 20) (5, 19, 18) (6, 17, 16) (7, 15, 27) (8, 26, 9) \\
& (12, 30, 13) (14, 29, 28) (21, 23, 22), \\
& (1, 31) (2, 10) (3, 24) (4, 19) (5, 17) (6, 15) (7, 26) (9, 25) (11, 30) (13, 29) \\
& (14, 27) (20, 23), \\
& (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\
& 25, 26, 27, 28, 29, 30, 31) ],
\end{aligned}$$

$$\begin{aligned}
M_3 = [ & (2, 31, 24) (3, 23, 22) (4, 21, 8) (5, 7, 6) (9, 20, 10) (11, 19, 28) (12, 27, 13) \\
& (14, 26, 15) (16, 25, 30) (17, 29, 18), \\
& (1, 31) (2, 23) (3, 21) (4, 7) (8, 20) (10, 19) (11, 27) (13, 26) (15, 25) (16, 29) \\
& (18, 28) (24, 30), \\
& (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\
& 25, 26, 27, 28, 29, 30, 31) ],
\end{aligned}$$

$$\begin{aligned}
M_4 = [ & (2, 31, 10) (3, 9, 18) (4, 17, 5) (6, 16, 20) (7, 19, 8) (11, 30, 29) (12, 28, 27) \\
& (13, 26, 14) (15, 25, 21) (22, 24, 23), \\
& (1, 31) (2, 9) (3, 17) (5, 16) (6, 19) (8, 18) (10, 30) (11, 28) (12, 26) (14, 25) \\
& (15, 20) (21, 24), \\
& (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\
& 25, 26, 27, 28, 29, 30, 31) ],
\end{aligned}$$

$$\begin{aligned}
 M_5 = [ & (2, 31, 22) (3, 21, 20) (4, 19, 5) (6, 18, 26) (7, 25, 24) (8, 23, 30) (9, 29, 13) \\
 & (10, 12, 11) (14, 28, 15) (16, 27, 17), \\
 & (1, 31) (2, 21) (3, 19) (5, 18) (6, 25) (7, 23) (8, 29) (9, 12) (13, 28) (15, 27) \\
 & (17, 26) (22, 30), \\
 & (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\
 & 25, 26, 27, 28, 29, 30, 31) ], \\
 M_6 = [ & (2, 31, 9) (3, 8, 17) (4, 16, 15) (5, 14, 22) (6, 21, 20) (7, 19, 18) (10, 30, 11) \\
 & (12, 29, 25) (13, 24, 23) (26, 28, 27), \\
 & (1, 31) (2, 8) (3, 16) (4, 14) (5, 21) (6, 19) (7, 17) (9, 30) (11, 29) (12, 24) \\
 & (13, 22) (25, 28), \\
 & (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\
 & 25, 26, 27, 28, 29, 30, 31) ].
 \end{aligned}$$

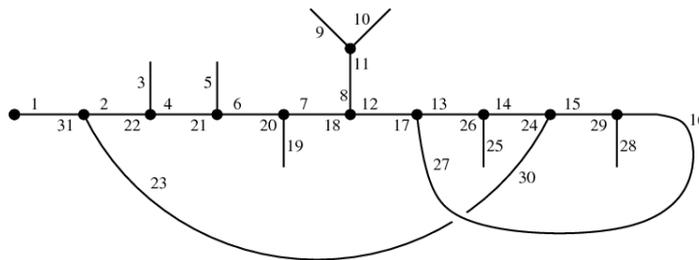


Рис. 27. Карта  $M_1$  из приведённого выше списка, представляющая группу  $PSL_5(2)$ .  
Карта  $M_4$  является её зеркальным образом

**Замечание 14.3.** Мы видим, что существуют разные способы рисовать карты на поверхностях рода  $g > 0$ : достаточно сравнить рисунки 17, 25–27. Каждый может выбрать представление, удобное для него и отвечающее его вкусу.

Кроме того, на рис. 27 мы решили привести ещё один пример, в котором все этикетки присутствуют в явном виде. Мы рекомендуем читателю сравнить их с приведённой выше тройкой  $M_1$  и, в частности, «пройти» вдоль цикла  $(1, 2, \dots, 31)$ .

## 14.6. Группа $AGL_5(2)$ , степень 32

Ниже мы приводим шесть рисунков, представляющих группу  $AGL_5(2)$  (см. пример 12.3). Их паспорт равен  $(3^{10}1^2, 2^{12}1^8, 31^11^1)$ , так что они дают альтернативный вариант по сравнению с рисунками степени 32 и паспортом  $(3^{10}1^2, 2^{16}, 31^11^1)$ , конструкция которых была использована в доказательстве теоремы 12.2.

- Перестановка  $z$  всегда одна и та же:  $z = (1, 2, 3, \dots, 31)$ .
- Этикетка 1 присвоена внешнему полурёбру единственной петли; клетка степени 1 помечена 32.
- Киральные пары — это  $(M_1, M_4)$ ,  $(M_2, M_5)$  и  $(M_3, M_6)$ .

Первые три карты показаны на рис. 28.

$$M_1 = [ (1, 2, 32) (3, 31, 4) (5, 30, 12) (6, 11, 7) (8, 10, 9) (13, 29, 17) (14, 16, 15) \\ (18, 28, 20) (21, 27, 22) (23, 26, 24) , \\ (1, 32) (2, 31) (4, 30) (5, 11) (7, 10) (12, 29) (13, 16) (17, 28) (18, 19) (20, 27) \\ (22, 26) (24, 25) , \\ (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\ 25, 26, 27, 28, 29, 30, 31) ] ,$$

$$M_2 = [ (1, 2, 32) (3, 31, 27) (4, 26, 6) (7, 25, 24) (8, 23, 18) (9, 17, 10) (11, 16, 12) \\ (13, 15, 14) (19, 22, 21) (28, 30, 29) , \\ (1, 32) (2, 31) (3, 26) (4, 5) (6, 25) (7, 23) (8, 17) (10, 16) (12, 15) (18, 22) \\ (19, 20) (27, 30) , \\ (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\ 25, 26, 27, 28, 29, 30, 31) ] ,$$

$$M_3 = [ (1, 2, 32) (3, 31, 4) (5, 30, 6) (7, 29, 8) (9, 28, 24) (10, 23, 15) (11, 14, 12) \\ (16, 22, 20) (17, 19, 18) (25, 27, 26) , \\ (1, 32) (2, 31) (4, 30) (6, 29) (8, 28) (9, 23) (10, 14) (12, 13) (15, 22) (16, 19) \\ (20, 21) (24, 27) , \\ (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\ 25, 26, 27, 28, 29, 30, 31) ] ,$$

$$M_4 = [ (1, 32, 31) (2, 30, 29) (3, 28, 21) (4, 20, 16) (5, 15, 13) (6, 12, 11) (7, 10, 9) \\ (17, 19, 18) (22, 27, 26) (23, 25, 24) , \\ (1, 30) (2, 28) (3, 20) (4, 15) (5, 12) (6, 10) (7, 8) (13, 14) (16, 19) (21, 27) \\ (22, 25) (31, 32) , \\ (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \\ 25, 26, 27, 28, 29, 30, 31) ] ,$$

$$M_5 = [ (1, 32, 31) (2, 30, 6) (3, 5, 4) (7, 29, 27) (8, 26, 9) (10, 25, 15) (11, 14, 12) \\ (16, 24, 23) (17, 22, 21) (18, 20, 19) , \\ (1, 30) (2, 5) (6, 29) (7, 26) (9, 25) (10, 14) (12, 13) (15, 24) (16, 22) (17, 20) \\ (27, 28) (31, 32) ,$$

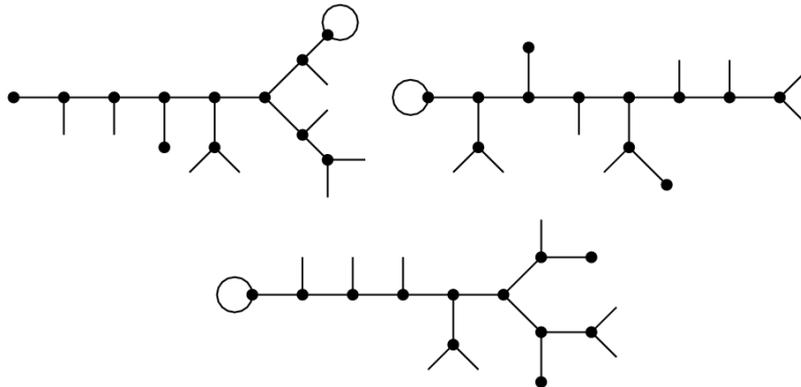


Рис. 28. Карты  $M_1, M_2, M_3$  с паспортом  $(3^{10}1^2, 2^{12}1^8, 31^11^1)$ , представляющие группу  $AGL_5(2)$ . Три оставшиеся карты являются их зеркальными образами

(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31) ],

$M_6 = [ (1, 32, 31) (2, 30, 29) (3, 28, 27) (4, 26, 25) (5, 24, 9) (6, 8, 7) (10, 23, 18) (11, 17, 13) (14, 16, 15) (19, 22, 21), (1, 30) (2, 28) (3, 26) (4, 24) (5, 8) (9, 23) (10, 17) (11, 12) (13, 16) (18, 22) (19, 20) (31, 32), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31) ]$ .

### 14.7. Группа $PSL_3(8)$ , степень 73

Ниже приведены восемь рисунков рода 4 с паспортом  $(3^{24}1^1, 2^{32}1^9, 73^1)$ , представляющие группу  $PSL_3(8)$  степени 73 (см. пример 10.7).

- Перестановка  $z$  всегда одна и та же:  $z = (1, 2, 3, \dots, 73)$ .
- Неподвижная точка перестановки  $x$  всегда помечена этикеткой 1.
- Киральные пары — это  $(M_1, M_5)$ ,  $(M_2, M_6)$ ,  $(M_3, M_7)$  и  $(M_4, M_8)$ .

$M_1 = [ (2, 73, 18) (3, 17, 36) (4, 35, 47) (5, 46, 42) (6, 41, 58) (7, 57, 50) (8, 49, 32) (9, 31, 10) (11, 30, 71) (12, 70, 69) (13, 68, 21) (14, 20, 28) (15, 27, 39) (16, 38, 37) (19, 72, 29) (22, 67, 66) (23, 65, 64) (24, 63, 55) (25, 54, 60) (26, 59, 40) (33, 48, 34) (43, 45, 44) (51, 56, 62) (52, 61, 53), (1, 73) (2, 17) (3, 35) (4, 46) (5, 41) (6, 57) (7, 49) (8, 31) (10, 30) (11, 70) (12, 68) (13, 20) (14, 27) (15, 38) (16, 36) (18, 72) (19, 28) (21, 67) (22, 65) (23, 63) (24, 54) (25, 59) (26, 39) (29, 71) (32, 48) (34, 47) (40, 58) (42, 45) (50, 56) (51, 61) (53, 60) (55, 62), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73) ]$ ,

$M_2 = [ (2, 73, 72) (3, 71, 28) (4, 27, 48) (5, 47, 41) (6, 40, 7) (8, 39, 22) (9, 21, 13) (10, 12, 11) (14, 20, 51) (15, 50, 24) (16, 23, 38) (17, 37, 59) (18, 58, 31) (19, 30, 52) (25, 49, 26) (29, 70, 53) (32, 57, 62) (33, 61, 34) (35, 60, 36) (42, 46, 68) (43, 67, 66) (44, 65, 55) (45, 54, 69) (56, 64, 63), (1, 73) (2, 71) (3, 27) (4, 47) (5, 40) (7, 39) (8, 21) (9, 12) (13, 20) (14, 50) (15, 23) (16, 37) (17, 58) (18, 30) (19, 51) (22, 38) (24, 49) (26, 48) (28, 70) (29, 52) (31, 57) (32, 61) (34, 60) (36, 59) (41, 46) (42, 67) (43, 65) (44, 54) (45, 68) (53, 69) (55, 64) (56, 62), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73) ]$ ,

$M_3 = [ (2, 73, 9) (3, 8, 51) (4, 50, 66) (5, 65, 53) (6, 52, 7) (10, 72, 71) (11, 70, 47) (12, 46, 13) (14, 45, 37) (15, 36, 57) (16, 56, 17) (18, 55, 28) (19, 27, 20) (21, 26, 22) (23, 25, 32) (24, 31, 33) (29, 54, 64) (30, 63, 34) (35, 62, 58) (38, 44, 43) (39, 42, 68) (40, 67, 49) (41, 48, 69) (59, 61, 60), (1, 73) (2, 8) (3, 50) (4, 65) (5, 52) (7, 51) (9, 72) (10, 70) (11, 46) (13, 45) (14, 36) (15, 56) (17, 55) (18, 27) (20, 26) (22, 25) (23, 31) (24, 32) (28, 54) (29, 63) (30, 33) (34, 62) (35, 57) (37, 44) (38, 42) (39, 67) (40, 48) (41, 68) (47, 69) (49, 66) (53, 64) (58, 61),$

(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73) ],

M4 = [ (2, 73, 54) (3, 53, 10) (4, 9, 33) (5, 32, 6) (7, 31, 30) (8, 29, 34) (11, 52, 44) (12, 43, 65) (13, 64, 14) (15, 63, 62) (16, 61, 23) (17, 22, 18) (19, 21, 20) (24, 60, 38) (25, 37, 50) (26, 49, 70) (27, 69, 47) (28, 46, 35) (36, 45, 51) (39, 59, 40) (41, 58, 57) (42, 56, 66) (48, 68, 71) (55, 72, 67), (1, 73) (2, 53) (3, 9) (4, 32) (6, 31) (7, 29) (8, 33) (10, 52) (11, 43) (12, 64) (14, 63) (15, 61) (16, 22) (18, 21) (23, 60) (24, 37) (25, 49) (26, 69) (27, 46) (28, 34) (35, 45) (36, 50) (38, 59) (40, 58) (41, 56) (42, 65) (44, 51) (47, 68) (48, 70) (54, 72) (55, 66) (67, 71), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73) ],

M5 = [ (2, 73, 57) (3, 56, 46) (4, 45, 64) (5, 63, 6) (7, 62, 54) (8, 53, 9) (10, 52, 11) (12, 51, 20) (13, 19, 24) (14, 23, 22) (15, 21, 50) (16, 49, 35) (17, 34, 69) (18, 68, 25) (26, 67, 43) (27, 42, 41) (28, 40, 71) (29, 70, 33) (30, 32, 31) (36, 48, 60) (37, 59, 38) (39, 58, 72) (44, 66, 65) (47, 55, 61), (1, 73) (2, 56) (3, 45) (4, 63) (6, 62) (7, 53) (9, 52) (11, 51) (12, 19) (13, 23) (14, 21) (15, 49) (16, 34) (17, 68) (18, 24) (20, 50) (25, 67) (26, 42) (27, 40) (28, 70) (29, 32) (33, 69) (35, 48) (36, 59) (38, 58) (39, 71) (43, 66) (44, 64) (46, 55) (47, 60) (54, 61) (57, 72), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73) ],

M6 = [ (2, 73, 3) (4, 72, 47) (5, 46, 22) (6, 21, 30) (7, 29, 33) (8, 32, 9) (10, 31, 20) (11, 19, 12) (13, 18, 43) (14, 42, 41) (15, 40, 39) (16, 38, 58) (17, 57, 44) (23, 45, 56) (24, 55, 61) (25, 60, 51) (26, 50, 49) (27, 48, 71) (28, 70, 34) (35, 69, 68) (36, 67, 53) (37, 52, 59) (54, 66, 62) (63, 65, 64), (1, 73) (3, 72) (4, 46) (5, 21) (6, 29) (7, 32) (9, 31) (10, 19) (12, 18) (13, 42) (14, 40) (15, 38) (16, 57) (17, 43) (20, 30) (22, 45) (23, 55) (24, 60) (25, 50) (26, 48) (27, 70) (28, 33) (34, 69) (35, 67) (36, 52) (37, 58) (44, 56) (47, 71) (51, 59) (53, 66) (54, 61) (62, 65), (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73) ],

M7 = [ (2, 73, 66) (3, 65, 4) (5, 64, 28) (6, 27, 34) (7, 33, 36) (8, 35, 26) (9, 25, 71) (10, 70, 22) (11, 21, 46) (12, 45, 41) (13, 40, 17) (14, 16, 15) (18, 39, 60) (19, 59, 58) (20, 57, 47) (23, 69, 68) (24, 67, 72) (29, 63, 62) (30, 61, 38) (31, 37, 32) (42, 44, 51) (43, 50, 52) (48, 56, 55) (49, 54, 53), (1, 73) (2, 65) (4, 64) (5, 27) (6, 33) (7, 35) (8, 25) (9, 70) (10, 21) (11, 45) (12, 40) (13, 16) (17, 39) (18, 59) (19, 57) (20, 46) (22, 69) (23, 67) (24, 71) (26, 34) (28, 63) (29, 61) (30, 37) (32, 36) (38, 60) (41, 44) (42, 50) (43, 51) (47, 56) (48, 54) (49, 52) (66, 72),

(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73) ],

$m_8 = [ (2, 73, 21) (3, 20, 8) (4, 7, 27) (5, 26, 49) (6, 48, 28) (9, 19, 33) (10, 32, 63) (11, 62, 61) (12, 60, 13) (14, 59, 52) (15, 51, 37) (16, 36, 35) (17, 34, 18) (22, 72, 65) (23, 64, 31) (24, 30, 39) (25, 38, 50) (29, 47, 40) (41, 46, 67) (42, 66, 71) (43, 70, 69) (44, 68, 45) (53, 58, 57) (54, 56, 55) , (1, 73) (2, 20) (3, 7) (4, 26) (5, 48) (6, 27) (8, 19) (9, 32) (10, 62) (11, 60) (13, 59) (14, 51) (15, 36) (16, 34) (18, 33) (21, 72) (22, 64) (23, 30) (24, 38) (25, 49) (28, 47) (29, 39) (31, 63) (37, 50) (40, 46) (41, 66) (42, 70) (43, 68) (45, 67) (52, 58) (53, 56) (65, 71) , (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73) ] ,$

Следующим кандидатом для нашей серии примеров могла бы послужить группа  $PSL_7(2)$  степени 127. Мы, однако, не видим никакого специального интереса в том, чтобы записывать в явном виде порождающие перестановки столь большой степени, поэтому останавливаемся здесь.

Мы благодарны Жану Бетрема, Юрию Билу, Джону Войту и Дмитрию Звонкину за ценную помощь и советы. Мы благодарны также участникам московского семинара «Графы на поверхностях и кривые над числовыми полями» за интерес, проявленный к нашей работе. Бессменным руководителем этого семинара в течение более 30 лет является Георгий Борисович Шабат, которому посвящается этот сборник.

Александр Звонкин получает поддержку от гранта ANR project «Combiné» (ANR-19-CE48-0011).

## Литература

- [1] Белый Г. В. О расширениях Галуа максимального кругового поля // Изв. АН СССР. Сер. матем. — 1979. — Т. 43, № 2. — С. 267—276.
- [2] Борович З. И., Шафаревич И. Р. Теория чисел. — М.: Наука, 1972.
- [3] Гипотеза Буняковского. — [fr.wikipedia.org/wiki/Conjecture\\_de\\_Bouniakovski](https://fr.wikipedia.org/wiki/Conjecture_de_Bouniakovski).
- [4] Звонкин А. К., Ландо С. К. Графы на поверхностях и их приложения. — М.: МЦНМО, 2010.
- [5] Клейн Ф. Лекции об икосаэдре и о решении уравнений пятой степени. — М.: Наука, 1989.
- [6] Коксетер Г. С. М., Мозер У. О. Дж. Порождающие элементы и определяющие соотношения дискретных групп. — М.: Наука, 1980.
- [7] Макдональд И. Симметрические функции и многочлены Холла. — М.: Мир, 1984.

- [8] Adrianov N. M., Pakovich F., Zvonkin A. K. Davenport–Zannier Polynomials and Dessins d’Enfants. — Providence: AMS, 2020. — (Math. Surveys Monographs; Vol. 249).
- [9] Aletheia-Zomlefer S. L., Fukshansky L., Garcia S. R. The Bateman–Horn conjecture: heuristics, history, and applications // Expo. Math. — 2020. — Vol. 38. — P. 430–479. — [arXiv:1807.08899v4](https://arxiv.org/abs/1807.08899v4) [math.NT].
- [10] Bateman P. T., Horn R. A. A heuristic asymptotic formula concerning the distribution of prime numbers // Math. Comput. — 1962. — Vol. 16, no. 79. — P. 363–367.
- [11] Bell G. W. On the cohomology of the finite special linear groups. I, II // J. Algebra. — 1978. — Vol. 54. — P. 216–238; 239–259.
- [12] Berecky Á. Maximal overgroups of Singer elements in classical groups // J. Algebra. — 2000. — Vol. 234, no. 1. — P. 187–206.
- [13] Bétréma J. Private communication. — 2020.
- [14] Bouniakowsky V. Sur les diviseurs numériques invariables des fonctions rationnelles entières<sup>1</sup> // Mém. Acad. Sci. St. Pétersbourg, 6<sup>e</sup> sér. — 1857. — Vol. VI. — P. 305–329. — <https://books.google.fr/books?hl=fr&id=wXIhAQAAIAAJ&pg=PA305>.
- [15] Burnside W. On simply transitive groups of prime degree // Quart. J. Math. — 1906. — Vol. 37. — P. 215–221.
- [16] Burnside W. Theory of Groups of Finite Order. — New York: Dover, 1955.
- [17] Cameron P. J. Permutation Groups. — Cambridge: Cambridge Univ. Press, 1999. — (London Math. Soc. Student Texts; Vol. 45).
- [18] Cohen H. A Course in Computational Algebraic Number Theory. — Berlin: Springer, 1993.
- [19] Conder M. D. E. The symmetric genus of the Mathieu groups // Bull. London Math. Soc. — 1991. — Vol. 23. — P. 445–453.
- [20] Conder M. D. E. Regular maps and hypermaps of Euler characteristic  $-1$  to  $-200$  // J. Combin. Theory Ser. B. — 2009. — Vol. 99. — P. 455–459. — <http://www.math.auckland.ac.nz/~conder/hypermaps.html>.
- [21] Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A. ATLAS of Finite Groups. — Oxford: Clarendon Press, 1985.
- [22] Coxeter H. S. M. A symmetrical arrangement of eleven hemi-icosahedra // Annals of Discrete Mathematics (20): Convexity and Graph Theory. Proc. of the Conf. on Convexity and Graph Theory (Jerusalem, 1981) / M. Rosenfeld, J. Zaks, eds. — Amsterdam: North-Holland, 1984. — (North-Holland Math. Stud.; Vol. 87). — P. 103–114.
- [23] Coxeter H. S. M., Edge W. L. The simple groups  $\mathrm{PSL}(2, 7)$  and  $\mathrm{PSL}(2, 11)$  // C. R. Math. Rep. Acad. Sci. Canada. — 1983. — Vol. 5. — P. 201–206.
- [24] Coxeter H. S. M., Weiss A. I. Twisted honeycombs  $\{3, 5, 3\}_t$  and their groups // Geom. Dedicata. — 1984. — Vol. 17. — P. 169–179.

<sup>1</sup>Во многих публикациях даётся следующее неверное название статьи В. Я. Буняковского: «Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs». Франкоязычная «Википедия» [3] указывает, что статья с таким названием в самом деле существует, но она опубликована не в 1857, а в 1840 году, и в ней рассматриваемая здесь гипотеза не обсуждается. Читатель может также обратиться к оригинальной статье В. Я. Буняковского, которая воспроизведена в архиве Google — см. ссылку в [14].

- [25] Dickson L. E. *Linear Groups*. — New York: Dover, 1958.
- [26] Dixon J. D., Mortimer B. *Permutation Groups*. — New York: Springer, 1996. — (Grad. Texts Math.; Vol. 163).
- [27] Dyck W. Über das Problem der Nachbargebiete // *Math. Ann.* — 1888. — Vol. 32. — P. 457–512.
- [28] *The Eightfold Way. The Beauty of Klein's Quartic Curve* / S. Levy, ed. — Cambridge: Cambridge Univ. Press, 1999.
- [29] Frobenius F. G. Über Gruppencharaktere // *Sitzber. Königl. Preuss. Akad. Wiss. Berlin*. — 1896. — P. 985–1021.
- [30] Galois É. Lettre de Galois à M. August Chevalier // *J. Math. Pures Appl.* — 1846. — Vol. XI. — P. 417–433. — <http://visualiseur.bnf.fr/CadresFenetre?O=NUMM-16390>.
- [31] Galois É. Mémoire sur les conditions de résolubilité des équations par radicaux // *J. Math. Pures Appl.* — 1846. — Vol. XI. — P. 417–433. — [http://www.bibnum.education.fr/sites/default/files/galois\\_memoire\\_sur\\_la\\_resolubilite.pdf](http://www.bibnum.education.fr/sites/default/files/galois_memoire_sur_la_resolubilite.pdf). — См. также *Écrits et Mémoires Mathématiques d'Évariste Galois* / Bourgne R., Azra J. P., eds. — Paris: Gauthier-Villars, 1962; Neumann P. M. *The Mathematical Writings of Évariste Galois*. — Zürich: European Math. Soc., 2011. — Chap. IV.
- [32] The GAP Group, GAP — Groups, Algorithms, and Programming. — <http://www.gap-system.org>.
- [33] Gehring F. W., Martin G. J. Minimal co-volume hyperbolic lattices. I. The spherical points of a Kleinian group // *Ann. Math.* — 2009. — Vol. 170, no. 2. — P. 123–161.
- [34] Gironde E., González-Diez G. *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*. — Cambridge: Cambridge Univ. Press, 2012. — (London Math. Soc. Student Texts; Vol. 79).
- [35] Godsil C., Imrich W., Razen R. On the number of subgroups of given index in the modular group // *Monatsh. Math.* — 1979. — Vol. 867. — P. 273–280.
- [36] Goormaghtigh R. *L'Intermédiaire des Mathématiciens*. — 1917. — Vol. 24, no. 88.
- [37] Goormaghtigh conjecture. — [en.wikipedia.org/wiki/Goormaghtigh\\_conjecture](http://en.wikipedia.org/wiki/Goormaghtigh_conjecture).
- [38] Green J. A. The characters of the finite general linear groups // *Trans. Amer. Math. Soc.* — 1955. — Vol. 80. — P. 402–447.
- [39] Grothendieck A. Esquisse d'un Programme // *Geometric Galois Actions 1. Around Grothendieck's Esquisse d'un Programme* / P. Lochak, L. Schneps, eds. — Cambridge: Cambridge Univ. Press, 1997. — (London Math. Soc. Lect. Note Ser.; Vol. 242). — P. 5–48.
- [40] Grünbaum B. Regularity of graphs, complexes and designs // *Problèmes Combinatoires et Théorie des Graphes, Coll. Int. CNRS, Vol. 260* — 1977. — P. 191–197.
- [41] Hamilton W. R. Letter to John T. Graves “On the Icosian” (17th October 1856) // *Hamilton W. R. Mathematical Papers. Vol. III: Algebra* / H. Halberstam, R. E. Ingram, eds. — Cambridge: Cambridge Univ. Press, 1967. — P. 612–625.
- [42] Heffter L. Über das Problem der Nachbargebiete // *Math. Ann.* — 1891. — Vol. 38. — P. 477–508.
- [43] Huppert B. *Endliche Gruppen. I*. — Berlin: Springer, 1979.

- [44] Ivrişimtziş I., Singerman D., Strudwick J. From Farey fractions to the Klein quartic and beyond // *Ars Math. Contemp.* — 2021. — Vol. 20, no. 1. — P. 37–50.
- [45] Jones G. A. Primitive permutation groups containing a cycle // *Bull. Aust. Math. Soc.* — 2014. — Vol. 89. — P. 159–165.
- [46] Jones G. A., Singerman D. *Complex Functions: an Algebraic and Geometric Viewpoint.* — Cambridge: Cambridge Univ. Press, 1987.
- [47] Jones G. A., Long C. D., Mednykh A. D. Hyperbolic manifolds and tessellations of type  $\{3, 5, 3\}$  associated with  $L_2(q)$ . — [arXiv:1106.0867\[math.GR\]](https://arxiv.org/abs/1106.0867).
- [48] Jones G. A., Wolfart J. *Dessins d’Enfants on Riemann Surfaces.* — Cham: Springer, 2016.
- [49] Jones G. A., Zvonkin A. K. Hurwitz groups as monodromy groups of dessins: several examples // *Teichmüller Theory and Grothendieck–Teichmüller Theory / Lizhen Ji, Athanase Papadopoulos, Weixu Su, eds.* — Beijing: Higher Education Press, 2022. — P. 275–302. — <https://arxiv.org/pdf/2012.07107.pdf>.
- [50] Jones G. A., Zvonkin A. K. Primes in geometric series and finite permutation groups. — <https://arxiv.org/pdf/2010.08023.pdf>.
- [51] Jordan C. Théorèmes sur les groupes primitifs // *J. Math. Pures Appl.* — 1871. — Vol. 16, no. 2. — P. 383–408.
- [52] Jordan C. Sur la limite de transitivité des groupes non alternés // *Bull. Soc. Math. France.* — 1873. — Vol. 1. — P. 40–71.
- [53] Klein F. Über die Erniedrigung der Modulgleichungen // *Math. Ann.* — 1878. — Vol. 14, no. 3. — P. 417–427.
- [54] Klein F. Über die Transformationen siebenter Ordnung der elliptischen Funktionen // *Math. Ann.* — 1878. — Vol. 14, no. 3. — P. 428–471.
- [55] Klein F. Über die Transformationen elfter Ordnung der elliptischen Funktionen // *Math. Ann.* — 1879. — Vol. 15, no. 3-4. — P. 533–555.
- [56] Klein F. *Gesammelte Mathematische Abhandlungen.* — Berlin: Springer, 1923–1973.
- [57] Lewis J. B., Reiner V., Stanton D. Reflection factorizations of Singer cycles // *J. Algebr. Combin.* — 2014. — Vol. 40. — P. 663–691.
- [58] Li W. A note on the Bateman–Horn conjecture // *J. Number Theory.* — 2020. — Vol. 208. — P. 390–399. — <https://arxiv.org/pdf/1906.03370.pdf>.
- [59] Macbeath A. M. Generators of the linear fractional groups // *Number Theory (Houston 1967) / W. J. Leveque, E. G. Straus, eds.* — (Proc. Sympos. Pure Math.; Vol. 12). — Providence: Amer. Math. Soc., 1969. — P. 14–32.
- [60] Marshall T. H., Martin G. J. Minimal co-volume hyperbolic lattices. II. Simple torsion in a Kleinian group // *Ann. Math.* — 2012. — Vol. 176, no. 2. — P. 261–301.
- [61] Mathieu É. Mémoire sur l’étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables // *J. Math. Pures Appl.* — 1861. — Vol. 6. — P. 241–323.
- [62] Mathieu É. Sur la fonction cinq fois transitive de 24 quantités // *J. Math. Pures Appl.* — 1873. — Vol. 18 — P. 25–46.
- [63] McMullen P., Schulte E. *Abstract Regular Polytopes.* — Cambridge: Cambridge Univ. Press, 2002. — (Encyclopedia of Mathematics and Its Applications; Vol. 92).
- [64] McQuillan D. L. Classification of normal congruence subgroups of the modular group // *Amer. J. Math.* — 1965. — Vol. 87. — P. 285–296.

- [65] Müller P. Reducibility behavior of polynomials with varying coefficients // Israel J. Math. — 1996. — Vol. 94. — P. 59–91.
- [66] Niven I., Zuckerman H.S., Montgomery H. L. An Introduction to the Theory of Numbers. — New York: Wiley, 1991.
- [67] Online Encyclopedia of Integer Sequences. — <https://oeis.org/>.
- [68] Schinzel A., Sierpiński W. Sur certaines hypothèses concernant les nombres premiers // Acta Arith. — 1958. — Vol. 4. — P. 185–298. (Erratum. — 1958. — Vol. 5. — P. 259.)
- [69] Simpson W. A., Frame J. S. The character tables for  $SL(3, q)$ ,  $SU(3, q^2)$ ,  $PSL(3, q)$ ,  $PSU(3, q^2)$  // Canadian J. Math. — 1973. — Vol. 25. — P. 486–494.
- [70] Singerman D. Symmetries of Riemann surfaces with large automorphism group // Math. Ann. — 1974. — Vol. 210. — P. 17–32.
- [71] Voight J. Private communication. — 2020.
- [72] Wallisz A. Zur additiven Zahlentheorie. II // Math. Z. — 1936. — Vol. 40. — P. 592–607.
- [73] Wielandt H. Finite Permutation Groups. — New York: Academic Press, 1964.
- [74] Woldar A. J. Representing  $M_{11}$ ,  $M_{12}$ ,  $M_{22}$  and  $M_{23}$  on surfaces of least genus // Commun. Algebra. — 1990. — Vol. 18. — P. 15–86. (Corrigendum. — P. 605.)

