Глава 5

Отображения кривых

Мероморфная функция на алгебраической кривой это ее отображение в проективную прямую. Однако естественно рассматривать отображения не только в проективную прямую, но и в другие комплексные кривые. Прежде всего, естественно рассматривать взаимно-однозначные отображения комплексной кривой в себя — ее автоморфизмы. Все автоморфизмы данной кривой образуют группу. Для кривой рода 0 (проективной прямой) эта группа трехмерна. Для любой кривой рода 1 (эллиптической кривой) она одномерна, для кривых старших родов она конечна, и, для кривых рода $g > 2$, как правило, состоит лишь из тождественного отображения. Кривые с большой группой симметрий представляют особый интерес — как и всякий симметричный объект, они могут быть очень красивыми.

5.1 Автоморфизмы сферы Римана

Биголоморфное отображение кривой в себя называется *автоморфизмом* кривой. Все автоморфизмы данной кривой образуют группу. Для любой кривой рода $g > 1$ эта группа конечна. Группы автоморфизмов рациональной кривой и любой эллиптической кривой бесконечны. Следующая теорема описывает группу автоморфизмов рациональной кривой.

Теорема 5.1.1. *Пусть z — произвольная координата на сфере Римана $\mathbb{CP}^1$. Всякий автоморфизм сферы Римана записывается в виде невырожденного дробно-линейного преобразования $z \mapsto \frac{az+b}{cz+d}$, $a, b, c, d \in \mathbb{C}, ad - bc \neq 0$.*

Доказательство. Отображение сферы Римана в себя — это мероморфная функция на сфере Римана, а согласно теореме 2.7.1 любая такая функция является рациональной функцией $f(z) = P(z)/Q(z)$. Степень отображения f равна наибольшей из степеней многочленов P и Q. Действительно, пусть m равно наибольшей из степеней многочленов P и Q. Тогда для почти всех c уравнение $P(z) = cQ(z)$ является полиномиальным уравнением степени m. Поэтому для почти всех c множество $f^{-1}(c)$ состоит из m точек, а значит,

степень отображения f равна m. Автоморфизмом кривой может быть только отображение степени 1, поэтому любой автоморфизм f является дробно-линейным преобразованием. Оно должно быть невырожденным, поскольку вырожденное дробно-линейное преобразование это константа. □

Следствие 5.1.2. *Группа автоморфизмов рациональной кривой это проективная группа* $\mathrm{PSL}(2,\mathbb{C})$ *комплексных* 2×2*-матриц с определителем* 1.

Группа $\mathrm{PSL}(2,\mathbb{C})$ это факторгруппа группы $\mathrm{SL}(2,\mathbb{C})$ комплексных 2×2-матриц с определителем 1 по нормальной подгруппе, состоящей из матриц I и $-I$, где I — единичная матрица. В частности, группа автоморфизмов рациональной кривой — трехмерная комплексная группа Ли.

Доказательство. Действительно, сопоставим каждому дробно-линейному преобразованию $z \mapsto \frac{az+b}{cz+d}$ матрицу $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. То, что композиция двух дробно-линейных преобразований соответствует произведению матриц, проверяется прямым вычислением. Два невырожденных дробно-линейных преобразования задают один и тот же автоморфизм проективной прямой в том и только в том случае, если числитель и знаменатель второго преобразования получаются из числителя и знаменателя первого умножением на одну и ту же константу. Умножив числитель и знаменатель данного дробно-линейного преобразования на подходящее число, мы можем добиться, чтобы определитель соответствующей ему матрицы стал равным 1. При этом одновременное умножение числителя и знаменателя на -1 не меняет преобразования, что и вызывает необходимость факторизовать группу матриц с определителем 1 по подгруппе скалярных матриц в ней. Следствие доказано. □

5.2 Отображения эллиптических кривых

Пусть L и M — две решетки в $\mathbb{C}$, $X = \mathbb{C}/L$ и $Y = \mathbb{C}/M$ — соответствующие им эллиптические кривые. Выясним, как устроено произвольное (непостоянное) голоморфное отображение $f\colon X \to Y$. Отображение $z \mapsto z + a$ индуцирует автоморфизм кривой Y; после композиции с таким автоморфизмом можно считать, что $f(0) = 0$.

Из формулы Римана–Гурвица следует, что голоморфное отображение двух торов не имеет точек ветвления, поэтому $f\colon X \to Y$ — накрытие. Отображение $\mathbb{C} \xrightarrow{p} X \xrightarrow{f} Y$, где $p\colon \mathbb{C} \to X$ — естественная проекция, тоже является накрытием. Пространство $\mathbb{C}$ односвязно, поэтому полученное накрытие изоморфно накрытию $q\colon \mathbb{C} \to Y$ (оба эти накрытия изоморфны универсальному накрытию над Y). Таким образом, мы получаем коммута-

тивную диаграмму

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{F} & \mathbb{C} \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} \\ X & \xrightarrow{f} & Y \end{array}$$

Отображение $F\colon \mathbb{C} \to \mathbb{C}$ голоморфно, причем из равенства $f(0) = 0$ следует, что $F(0)$ — точка решетки L. Можно считать, что $F(0) = 0$, поскольку сдвиг на элемент решетки L не изменяет отображение $\mathbb{C} \xrightarrow{p} X \xrightarrow{f} Y$.

При отображении F множество $p^{-1}(0)$ отображается в $q^{-1}(0)$, поэтому $F(L) \subset M$.

Если $l \in L$, а z — произвольное комплексное число, то $F(z+l) \equiv F(z) \pmod{M}$, т.е. $F(z+l) - F(z) = w_l(z) \in M$. Множество M дискретно, а множество $\mathbb{C}$ связно, поэтому функция w_l постоянна, т.е. $w_l(z)$ зависит только от l. Следовательно, $\frac{dF(z+l)}{dz} - \frac{dF(z)}{dz} = 0$, т.е. функция $\frac{dF(z)}{dz}$ инвариантна относительно сдвигов на элементы решетки L. Таким образом, множество всех значений функции $\frac{dF(z)}{dz}$ совпадает с множеством ее значений на фундаментальном параллелограмме решетки L. Следовательно, эта функция постоянна, потому что любая ограниченная голоморфная функция постоянна. Учитывая, что $F(0) = 0$, получаем $F(z) = cz$. Константа c должна обладать тем свойством, что $cL \subset M$.

В итоге мы получаем, что любое голоморфное отображение эллиптических кривых индуцировано отображением $F(z) = cz + a$, где $cL \subset M$. Используя это свойство, можно описать группу автоморфизмов эллиптической кривой, оставляющих неподвижной точку 0.

Теорема 5.2.1. *Группа автоморфизмов (сохраняющих точку 0) эллиптической кривой $X = \mathbb{C}/L$ — циклическая группа порядка 4, если решетка квадратная, порядка 6, если решетка состоит из правильных треугольников, порядка 2 во всех остальных случаях.*

Доказательство. Прежде всего заметим, что автоморфизму эллиптической кривой соответствует такое отображение $F(z) = cz$, что $cL = L$. Действительно, если $cL = L$, то $c^{-1}L = L$, поэтому отображение $z \mapsto c^{-1}z$ индуцирует обратное отображение. Наоборот, если отображение $z \mapsto c_1c_2z$ индуцирует тождественное отображение тора, то $c_1c_2 = 1$ (для доказательства достаточно рассмотреть малые z). Поэтому из включений $c_1L \subset L$ и $c_2L \subset L$ следует, что $L \subset c_2^{-1}L = c_1L \subset L$.

При преобразовании $z \mapsto cz$ площадь фундаментального параллелограмма решетки умножается на $|c|^2$, поэтому $|c| = 1$. Более того c — корень из единицы. Действительно, иначе концы векторов $1, c, c^2, c^3, \ldots$ образовывали бы всюду плотное множество точек окружности, а все эти векторы являются векторами решетки. У любой эллиптической кривой есть автоморфизмы, соответствующие $c = \pm 1$. Выясним, для каких эллиптических кривых есть другие автоморфизмы. Прежде всего заметим, что число c должно быть корнем квадратного уравнения с целыми коэффициентами. Действительно, если векторы ω_1 и ω_2 порождают решетку, то $c\omega_1 = p\omega_1 + q\omega_2$ и $c\omega_2 =$

$r\omega_1 + s\omega_2$, поэтому c — корень квадратного уравнения $\begin{vmatrix} p-x & q \\ r & s-x \end{vmatrix} = 0$. Многочлен $x^n - 1$ раскладывается в произведение неприводимых круговых многочленов $\Phi_d(x)$, где d пробегает все делители числа n; при этом степень многочлена $\Phi_d(x)$ равна $\varphi(d)$, где φ — функция Эйлера, т.е. $\varphi(d)$ есть число натуральных чисел меньших d и взаимно простых с ним (доказательство можно найти, например, в [?]). Квадратные неприводимые круговые многочлены это x^2+x+1 и x^2+1. В первом случае получаем решетку, состоящую из правильных треугольников, так как $x^3 = 1$, а во втором — квадратную решетку. □

Следствие 5.2.2. *Существуют неизоморфные эллиптические кривые.*

Действительно, группы автоморфизмов изоморфных кривых изоморфны, а мы привели примеры эллиптических кривых с отмеченной точкой, группы автоморфизмов которых имеют разный порядок.

На всякой эллиптической кривой C существует мероморфная функция $f : C \to \mathbb{CP}^1$ степени 2. Такая функция имеет 4 критических значения, т.е. 4 точки ветвления. Мы можем выбрать функцию таким образом, чтобы отмеченная точка на эллиптической кривой была ее критической точкой.

Автоморфизмы кривой C тесно связаны с автоморфизмами четверки критических значений функции. Самое симметричное расположение четырех точек на сфере — это помещение их в вершины правильного тетраэдра. Эллиптическая кривая, двукратно накрывающая $\mathbb{CP}^1$ с таким набором точек ветвления, отвечает решетке правильных треугольников, и группа ее автоморфизмов это $\mathbb{Z}_6$. Если (при подходящем выборе проективной координаты) точки ветвления расположены в вершинах квадрата на экваторе сферы, то накрывающая кривая отвечает квадратной решетке, и группа ее автоморфизмов изоморфна $\mathbb{Z}_4$. Все остальные кривые не имеют симметрий, отличных от перестановки листов накрытия.

Упражнение 5.2.3. Докажите, что при факторизации эллиптической кривой по группе автоморфизмов, сохраняющих точку 0, в двух исключительных случаях получается сфера Римана, а во всех остальных — снова эллиптическая кривая.

5.3 Модули эллиптических кривых

Доказанные в предыдущем параграфе свойства голоморфных отображений эллиптических кривых позволяют описать, как устроено пространство модулей эллиптических кривых. Прежде всего заметим, что любая эллиптическая кривая изоморфна эллиптической кривой, полученной при факторизации комплексных чисел по решетке L_τ, порожденной числами 1 и τ, где $\operatorname{Im}\tau > 0$. Действительно, если решетка L порождена числами ω_1 и ω_2, то отображение $z \mapsto cz$, где $c = \pm 1/\omega_1$, переводит решетку L в решетку, порожденную числами 1 и ω_2/ω_1. В качестве τ можно взять то из чисел $\pm\omega_2/\omega_1$, мнимая часть которого положительна.

Рис. 5.1: Фундаментальная область модулярной группы

Выясним теперь, когда эллиптические кривые, соответствующие параметрам τ и τ', изоморфны. Для этого должно существовать такое число c, что $cL_\tau = L_{\tau'}$, т.е. числа c и $c\tau$ порождают решетку $L_{\tau'}$. Следовательно, $c = p + q\tau'$ и $c\tau = r + s\tau'$, где p, q, r, s, — целые числа. Таким образом, $\tau = \frac{r+s\tau'}{p+q\tau'}$. Пока мы воспользовались только тем, что числа c и $c\tau$ принадлежат решетке $L_{\tau'}$. Они порождают ее тогда и только тогда, когда $qr - ps = \pm 1$. Учитывая, что $\operatorname{Im}\tau > 0$ и $\operatorname{Im}\tau' > 0$, получаем $qr - ps = 1$. Таким образом, эллиптические кривые, соответствующие параметрам τ и τ', изоморфны тогда и только тогда, когда эти параметры связаны дробно-линейным преобразованием $\tau = \frac{r+s\tau'}{p+q\tau'}$, где $\begin{pmatrix} r & s \\ p & q \end{pmatrix}$ — целочисленная матрица с определителем 1.

Группу матриц размером 2×2 с целочисленными элементами и определителем 1 обозначают $\mathrm{SL}(2, \mathbb{Z})$. Любым двум пропорциональным матрицам (и только им) соответствует одно и то же дробно-линейное преобразование. Поэтому рассматриваемая группа преобразований изоморфна факторгруппе $\mathrm{SL}(2, \mathbb{Z})/\pm I = \mathrm{PSL}(2, \mathbb{Z})$; здесь I — единичная матрица.

Упражнение 5.3.1. Проверьте, что подгруппа $\pm I$ в группе $\mathrm{SL}(2, \mathbb{Z})$ нормальна.

Группу $\mathrm{PSL}(2, \mathbb{Z})$ называют *модулярной группой*.

Теорема 5.3.2. *Треугольник D с углами $(0, \frac{\pi}{3}, \frac{\pi}{3})$, изображенный на рис. 5.1, является фундаментальной областью модулярной группы.*

Доказательство. Рассмотрим в группе $G = \mathrm{PSL}(2, \mathbb{Z})$ элементы $S(z) = -1/z$ и $T(z) = z + 1$. Они порождают некоторую подгруппу $G' \subset G$. Мы докажем сначала, что D — фундаментальная область группы G', а затем докажем, что $G' = G$, т.е. элементы S и T порождают всю группу G.

Прежде всего проверим, что треугольники $g'D$ ($g' \in G'$) покрывают всю верхнюю полуплоскость, т.е. если $\operatorname{Im}(z) > 0$, то $g'z \in D$ для некоторого $g' \in G'$.

Лемма 5.3.3. *Если $\operatorname{Im}(z) > 0$, то при $g \in G$ величина $\operatorname{Im}(gz)$ принимает лишь конечное число значений, превосходящих $\operatorname{Im}(z)$.*

Доказательство. Ясно, что

$$\operatorname{Im}(gz) = \operatorname{Im}\left(\frac{az+b}{cz+d}\right) = \operatorname{Im}\frac{adz + bc\bar{z}}{|cz+d|^2} = \frac{\operatorname{Im}(z)}{|cz+d|^2}.$$

Поэтому $\operatorname{Im}(gz) \geqslant \operatorname{Im}(z)$ лишь в том случае, когда $|cz + d| \leqslant 1$. Последнее неравенство выполняется лишь для конечного множества пар целых чисел (c, d), причем для каждой такой пары величина $\operatorname{Im}(gz)$ определена однозначно. □

Группа G' содержится в G, поэтому для любой точки z в верхней полуплоскости можно выбрать элемент $g' \in G'$, для которого величина $\operatorname{Im}(g'z)$ максимальна. Преобразование $T(z) = z + 1$ не изменяет мнимую часть числа z, поэтому для некоторого элемента $w = T^k g' z, \quad k \in \mathbb{Z}$, выполняется неравенство $|\operatorname{Re}(w)| \leqslant 1/2$, а величина $\operatorname{Im}(w)$ по-прежнему максимальна. В частности,

$$\operatorname{Im}(w) \geq \operatorname{Im}\left(-\frac{1}{w}\right) = \frac{\operatorname{Im}(w)}{|w|^2}.$$

Поэтому $|w| \geq 1$, а значит, $w \in D$.

Лемма 5.3.4. *Если z — внутренняя точка области D и $gz \in D$ для $g \in G$, то g — тождественное преобразование.*

Доказательство. Пусть $g(z) = \dfrac{az+b}{cz+d}$. Рассмотрим сначала случай $c = 0$. В этом случае $ad = 1$, т.е. $g(z) = z \pm b$. Если $b \neq 0$, то лишь для преобразований $g(z) = z \pm 1$ образ множества D пересекается с множеством D. Но их пересечение принадлежит множеству $|\operatorname{Re}(z)| = 1/2$, которое не содержит внутренних точек множества D.

Предположим теперь, что $c \neq 0$. Тогда

$$g(z) = \frac{a}{c} - \frac{1}{c(cz+d)},$$

поэтому

$$\left|g(z) - \frac{a}{c}\right| \cdot \left|z + \frac{d}{c}\right| = \frac{1}{c^2}. \tag{5.1}$$

Числа a/c и d/c вещественны, поэтому мнимые части чисел $g(z) - a/c$ и $z + d/c$ равны мнимым частям чисел $g(z)$ и z. А так как мнимая часть любой точки области D не меньше $\sqrt{3}/2$, то модули чисел $g(z) - a/c$ и $z + d/c$ тоже не меньше $\sqrt{3}/2$. Следовательно, $|c| \leqslant 2/\sqrt{3}$, причем c — ненулевое целое число. Таким образом, $c = \pm 1$, поэтому соотношение (5.1) можно записать в виде

$$|g(z) \mp a| \cdot |z \pm d| = 1.$$

Но если $g(z) \in D$ и z — внутренняя точка области D, то для любых целых чисел a и d выполняются неравенства $|g(z) \mp a| \geq 1, \quad |z \pm d| > 1$. □

Из леммы 2, в частности, следует, что для несовпадающих элементов g_1' и g_2' группы G' множества $g_1'D$ и $g_2'D$ не имеют общих внутренних точек. Таким образом, D — фундаментальная область группы G'.

Теперь можно без труда доказать, что $G = G'$. В самом деле, пусть g — произвольный элемент группы G. Возьмем произвольную внутреннюю точку z области D. Точка gz лежит в верхней полуплоскости, поэтому существует элемент $g' \in G'$, для которого $g'(gz) \in D$. Движение $g'g \in G$ переводит внутреннюю точку z области D в некоторую точку области D. Поэтому согласно лемме 2 преобразование $g'g$ тождественно, т.е. $g = (g')^{-1} \in G'$.

Доказательство теоремы завершено. □

5.4 Кубики как эллиптические кривые

Гладкая плоская кубическая кривая (*кубика*) имеет род 1, поэтому естественно ожидать, что она изоморфна эллиптической кривой. (Впоследствии мы покажем, что любая гладкая кривая рода 1 изоморфна эллиптической кривой, поэтому эллиптические кривые — это то же самое, что гладкие кривые рода 1.) Здесь мы опишем явно изоморфизм эллиптической кривой на кубику, т.е. сопоставим каждой решетке некоторое уравнение кубики.

Предварительно выясним, к какому виду можно привести уравнение кубики. У каждой кубики есть точка перегиба (и даже 9 точек перегиба, см. раздел 2.3). Выберем координаты в плоскости таким образом, чтобы одна из точек перегиба имела однородные координаты $(0:1:0)$, причем касательная в этой точке задавалась уравнением $z=0$. Тогда если кубика задается уравнением $\sum a_{ij}x^iy^jz^{3-i-j}=0$, то многочлен $a_{30}x^3+a_{21}x^2y+a_{12}xy^2+a_{03}y^3$ имеет корень $x=0$ кратности 3. Следовательно, $a_{21}=a_{12}=a_{03}=0$ и $a_{30}\ne 0$. Касательная в точке $(0:1:0)$ задается уравнением $F_xx+F_yy+F_zz=0$, где значения производных берутся в точке $(0:1:0)$; следовательно, $F_xx=0$, $F_yy=0$ и $F_zz\ne 0$. Можно считать, что $F_zz(0,1,0)=1$. Таким образом, в аффинных координатах кривая задается уравнением $y^2-2(ax+b)y+P_3(x)=0$, где P_3 — многочлен 3-й степени. Заменой $y_1=y-ax-b$ это уравнение можно привести к виду $y^2=Q_3(x)$, где Q_3 — многочлен 3-й степени, не имеющий кратных корней (иначе кривая имела бы особую точку). Итак, после замены переменных можно считать, что кривая задана уравнением $y^2=x(x-1)(x-\lambda)$, где число λ отлично от 0 и 1. Сделав замену $x=x_1+\frac{1+\lambda}{3}$, можно также считать, что кривая задана уравнением $y^2=x^3+ax+b$, где $a=\frac{-\lambda^2+\lambda-1}{3}$ и $b=\frac{-2\lambda^3+3\lambda^2+3\lambda-2}{27}$. При этом $4a^3+27b^2=-\lambda^2(1-\lambda)^2\ne 0$.

Для любой решетки $\Lambda=\{m\omega_1+n\omega_2 \mid m,n\in\mathbb{Z}\}$, $\omega_1,\omega_2\in\mathbb{C}$, $\operatorname{Im}\omega_1/\omega_2>0$, можно рассмотреть функцию

$$\wp(z)=\frac{1}{z^2}+{\sum}'\left[\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right], \tag{5.2}$$

где штрих у знака суммы означает, что суммирование ведется по всем ненулевым элементам $\omega\in\Lambda$. Группировка членов в квадратных скобках существенна, потому что по отдельности ряды ${\sum}'(z-\omega)^{-2}$ и ${\sum}'\omega^{-2}$ расходятся.

Докажем сначала, что ряд (5.2) определяет мероморфную функцию на комплексной прямой $\mathbb{C}$. На любом компакте K, не содержащем точек решетки, этот ряд сходится равномерно и абсолютно. В самом деле,

$$\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}=\frac{2z\omega-z^2}{\omega^2\,(z-\omega)^2}=\frac{\omega}{\omega^4}\,\frac{2z-z^2\omega^{-1}}{(z\omega^{-1}-1)^2}\,.$$

Если число $|\omega|$ достаточно велико, то $\frac{2z-z^2\omega^{-1}}{(z\omega^{-1}-1)^2}\approx 2z$. Поэтому для всех $\omega\in\Lambda'$ с достаточно большим значением $|\omega|$ и для всех $z\in K$ найдется такая константа C, что

$$\left|\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right|<\frac{C}{|\omega|^3}\,.$$

Кроме того, $|z-\omega|>\epsilon$ для всех $z\in K$ и $\omega\in\Lambda'$, поэтому такая константа найдется и для всех $\omega\in\Lambda'$. Легко проверить, что ряд $\sum'|\omega|^{-3}$ сходится. В самом деле,

$$\sum{}'|\omega|^{-3}=\sum_{n=1}^{\infty}\sum_{\max(|p|,|q|)=n}|p\omega_1+q\omega_2|^{-3}\le\sum_{n=1}^{\infty}8n\,(nh)^{-3},$$

где h — меньшая из высот фундаментального параллелограмма. Таким образом, $\wp(z)$ — мероморфная функция с полюсами в узлах решетки. Она называется *функцией Вейерштрасса*.

Перейдем к доказательству периодичности функции $\wp(z)$. Рассмотрим для этого ее производную

$$\wp'(z)=-2\sum(z-\omega)^{-3}$$

(здесь суммирование ведется уже по всем узлам решетки). Очевидно, что ω_1 и ω_2 — периоды функции $\wp'(z)$. Поэтому функции $\wp(z+\omega_i)$ и $\wp(z)$ могут отличаться лишь на константу c. Подставив значение $z=-\omega_i/2$ в равенство $\wp(z+\omega_i)=\wp(z)+c$, получим $\wp(\omega_i/2)=\wp(-\omega_i/2)+c$. Но из формулы (3.1) видно, что функция $\wp(z)$ четная. Поэтому $c=0$, т. е. ω_1 и ω_2 — периоды функции $\wp(z)$.

Функция $\wp$ имеет в узлах решетки двукратные полюсы, других особых точек у нее нет. Внутри фундаментального параллелограмма расположен ровно один узел решетки. Поэтому сумма полюсов функции $\wp$, расположенных внутри фундаментального параллелограмма, сравнима с нулем по модулю Λ. Следовательно, внутри фундаментального параллелограмма расположены два нуля u и v функции $\wp$, причем $u+v\equiv 0\ (\mathrm{mod}\,\Lambda)$. Для любой константы c полюсы функции $\wp(z)-c$ совпадают с полюсами функции $\wp(z)$, поэтому внутри фундаментального параллелограмма есть ровно две точки u и v, для которых $\wp(u)=\wp(v)=c$, причем $u+v\equiv 0\ (\mathrm{mod}\,\Lambda)$. В том случае, когда $u\equiv -u\ (\mathrm{mod}\,\Lambda)$, эти две точки совпадают, т. е. соответствующее значение функция $\wp$ принимает двукратно. В точках, в которых сливаются два нуля функции $\wp(z)-c$, производная $\wp'(z)$ обращается в нуль. Фундаментальный параллелограмм можно выбрать так, чтобы внутри него лежали ровно четыре точки, для которых $u\equiv -u\ (\mathrm{mod}\,\Lambda)$, а именно точки

$$0,\quad \frac{\omega_1}{2},\quad \frac{\omega_2}{2}\quad\text{и}\quad\frac{\omega_1+\omega_2}{2}$$

Первая из этих точек — полюс функции $\wp$, а три другие — нули функции $\wp'$. Итак, значения

$$e_1=\wp\left(\frac{\omega_1}{2}\right),\quad e_2=\wp\left(\frac{\omega_1+\omega_2}{2}\right)\quad\text{и}\quad e_3=\wp\left(\frac{\omega_2}{2}\right)$$

для функции $\wp$ двукратные, причем других двукратных значений нет. Двукратные значения соответствуют нулям производной, поэтому $\wp'(z)=0$

тогда и только тогда, когда

$$z \equiv \frac{\omega_1}{2}\,, \quad \frac{\omega_2}{2}\,, \quad \frac{\omega_1+\omega_2}{2} \pmod{\Lambda}.$$

Отметим, что числа e_1, e_2 и e_3 попарно различны. Предположим, например, что $e_1 = e_3$. Тогда функция $\wp(z) - e_1$ имеет двукратные нули в точках $\omega_1/2$ и $\omega_2/2$, т. е. внутри фундаментального параллелограмма расположено не менее четырех нулей этой функции, чего не может быть.

Выведем дифференциальное уравнение для функции $\wp(z)$. Если коэффициенты при неположительных степенях z в разложениях Лорана функций $(\wp'(z))^2$ и $a\wp^3(z) + b\wp^2(z) + c\wp(z) + d$ совпадают, то эти функции равны. В самом деле, их разность — эллиптическая функция без полюсов, в нуле принимающая нулевое значение. Следовательно, их разность — константа, причем нулевая.

Поскольку

$$\left(\frac{1}{1-x}\right)^2 = \frac{d}{dx}\left(\frac{1}{1-x}\right) = 1 + 2x + 3x^2 + \dots\,,$$

имеем

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + {\sum}'\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \\ &= \frac{1}{z^2} + {\sum}'\left(\frac{1}{\omega^2}\left(1 + 2\,\frac{z}{\omega} + 3\left(\frac{z}{\omega}\right)^2 + \dots\right) - \frac{1}{\omega^2}\right) = \\ &= \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \dots\,,\end{aligned}$$

где $G_k = {\sum}'\omega^{-k}$ (для нечетных k эта сумма равна нулю в силу симметрии). Поэтому

$$\begin{aligned}\wp(z) &= z^{-2} + \dots\,,\\ \wp^2(z) &= z^{-4} + 6G_4 + \dots\,,\\ \wp^3(z) &= z^{-6} + 9G_4 z^{-2} + 15G_6 + \dots\,,\\ (\wp'(z))^2 &= 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \dots\end{aligned}$$

(записаны лишь интересующие нас члены разложения Лорана). Таким образом,

$$\begin{aligned}&a\wp^3(z) + b\wp^2(z) + c\wp(z) + d = \\ &\qquad = az^{-6} + bz^{-4} + (9aG_4 + c)\,z^{-2} + (15aG_6 + 6bG_4 + d) + \dots \qquad (5.3)\end{aligned}$$

Следовательно, $a\wp^3 + b\wp^2 + c\wp + d = (\wp')^2$, если

$$\begin{cases} a = 4, \\ b = 0, \\ 9aG_4 + c = -24G_4, \\ 15aG_6 + 6bG_4 + d = -80G_6. \end{cases}$$

Полученная система уравнений, очевидно, имеет решение

$$\begin{cases} a = 4, \\ b = 0, \\ c = -60G_4, \\ d = -140G_6. \end{cases}$$

Для упрощения обозначений, обычно полагают

$$g_2 = 60G_4 = 60 \sum{}' \omega^{-4},$$
$$g_3 = 140G_6 = 140 \sum{}' \omega^{-6}.$$

Тогда

$$(\wp'(z))^2 = 4\wp^3(z) - g_2\wp(z) - g_3.$$

Кубическую кривую

$$y^2 = 4x^3 - g_2x - g_3$$

можно параметризовать с помощью функции $\wp$, положив

$$x = \wp(z), \qquad y = \wp'(z).$$

Переходя к однородным координатам в $\mathbb{CP}^2$, отображение $f\colon \mathbb{C}/\Lambda \longrightarrow \mathbb{CP}^2$ определим следующим образом

$$\begin{aligned} &z \mapsto (\wp(z) : \wp'(z) : 1) && \text{при} \quad z \neq 0, \\ &z \mapsto (0 : 1 : 0) && \text{при} \quad z = 0. \end{aligned}$$

Очевидно, что это отображение аналитично во всех точках, отличных от узлов решетки. Записав его в виде

$$z \mapsto \left(\frac{\wp(z)}{\wp'(z)} : 1 : \frac{1}{\wp'(z)} \right),$$

можно убедиться, что оно аналитично и в окрестности узла решетки. Отображение f взаимно однозначно отображает тор $\mathbb{C}/\Lambda$ на кубическую кривую

$$y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

в $\mathbb{CP}^2$. В самом деле, на бесконечно удаленной прямой $z = 0$ лежит лишь точка $(0 : 1 : 0)$ этой кривой. В нее отображаются узлы решетки — им на торе соответствует одна точка. Для остальных точек можно рассмотреть аффинную кривую

$$y^2 = 4x^3 - g_2x - g_3$$

и отображение $z \mapsto (\wp(z), \wp'(z))$. Уравнение $\wp(z) = c$ может иметь одно или два решения. Два решения оно имеет в том случае, когда $\wp'(z) \neq 0$. Решения при этом имеют вид $\pm z$. Образы этих двух точек при отображении $z \mapsto (\wp(z), \wp'(z))$ не совпадают, так как ненулевые числа $\wp'(z)$ и $\wp'(-z) = -\wp'(z)$ отличаются знаком.

5.5 Снова j-инвариант

Напомним, что на с. 37 для кубики C, заданной уравнением $y^2 = x(x-1)(x-\lambda)$, мы геометрически определили j-инвариант

$$j(C) = j(\lambda) = 2^8 \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}.$$

Используя соответствие между кубиками и эллиптическими кривыми, мы можем сопоставить каждой эллиптической кривой (и, соответственно, каждой решетке) j-инвариант.

Покажем, что j-инвариант выражается через функции g_2 и g_3, введенные в предыдущем параграфе. Для этого сделаем сначала замену $x = x' + (\lambda+1)/3$, которая переводит кривую $y^2 = x(x-1)(x-\lambda)$ в кривую $y^2 = x'^3 + ax' + b$, где $a = (-\lambda^2+\lambda-1)/3$ и $b = (-2\lambda^3+3\lambda^2+3\lambda-2)/27$, после чего сделаем замену $x' = \sqrt[3]{4}x''$, получив в результате кривую $y^2 = 4x''^3 - g_2x'' - g_3$, где $g_2 = -\sqrt[3]{4}a$ и $g_3 = -b$. Таким образом,

$$j(C) = j(\lambda) = 2^8 \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda^2)} = \frac{1728 \cdot 4a^3}{4a^3+27b^2} = \frac{1728 g_2^3}{g_2^3 - 27g_3^2},$$

и мы выразили j-инвариант через g_2 и g_3.

Функции g_2 и g_3 являются так называемыми модулярными функциями, причем все остальные модулярные функции алгебраически выражаются через них. Прежде чем давать общее определение модулярной функции, напомним, что g_2 и g_3 это такие функции решетки Λ: $g_2 = 60G_4$ и $g_3 = 140G_6$, где $G_{2k}(\Lambda) = \sum'_{\omega\in\Lambda} \omega^{-2k}$. Будем говорить, что F — функция веса $2k$ (определенная на решетках), если $F(\mu\Lambda) = \mu^{-2k}F(\Lambda)$ для любой решетки Λ и любого комплексного числа $\mu \neq 0$. В частности, G_{2k} — это функция веса $2k$.

Пусть $\omega_1, \omega_2 \in \mathbb{C}$ — положительно ориентированный базис решетки Λ. Функцию $F(\Lambda)$ можно рассматривать и как функцию пары $F(\omega_1, \omega_2)$. Тогда условие того, что вес функции F равен $2k$, приобретает вид $F(\mu\omega_1, \mu\omega_2) = \mu^{-2k}F(\omega_1, \omega_2)$. Для такой функции

$$\omega_2^{2k} F(\omega_1, \omega_2) = F(\frac{\omega_1}{\omega_2}, \frac{\omega_2}{\omega_2}) = f(\frac{\omega_1}{\omega_2}, 1) = f(\frac{\omega_1}{\omega_2})$$

для некоторой функции f на верхней полуплоскости H.

Функция f зависит только от решетки и не зависит от выбора базиса этой решетки, поэтому для любой матрицы

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

должно выполняться равенство

$$\omega_2^{2k} f\left(\frac{\omega_1}{\omega - 2}\right) = (c\omega_1 + d\omega_2)^{2k} f\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right),$$

т.е. $f(z) = (cz+d)^{2k} f(\frac{az+b}{cz+d})$, где $z = \omega_1/\omega_2$. Мероморфную функцию f на верхней полуплоскости будем называть *слабомодулярной*. Слабомодулярная функция *модулярна*, если она дополнительно удовлетворяет следующему условию мероморфности на бесконечности. Функцию f от переменной $z \in H$ можно рассматривать как функцию $\tilde{f}$ от переменной $q = e^{2\pi i z}$. Функция $\tilde{f}$ определена всюду, кроме кроме нуля. Если ее можно доопределить в нуле так, что получится мероморфная в нуле функция, то будем говорить, что исходная функция f мероморфна на бесконечности.

Пусть $v_p(f)$ — порядок функции f в точке p (если в точке p полюс, то порядок отрицательный, если нуль, то порядок положительный, а если в отлична от нуля в точке p, то порядок равен нулю). Определим также порядок функции f в бесконечности следующим образом. Пусть $\tilde{f}(q) = \sum_{n=-N}^{\infty} c_n q^n$, причем $c_{-N} \neq 0$. Тогда мы полагаем $v_\infty(f) = -N$.

Теорема 5.5.1. *Для любой модулярной функции f веса $2k$ имеет место равенство*

$$v_\infty(f) + \frac{1}{3} v_\rho(f) + \frac{1}{2} v_i(f) + \sum_p v_p(f) = \frac{k}{6},$$

где $\rho = \frac{1+i\sqrt{3}}{2}$, а суммирование ведется по всем точкам p фундаментальной области, причем эквивалентные точки на границе отождествляются.

Доказательство. Рассмотрим замкнутый контур C, изображенный на рис. **??**. Если в точках ρ или i есть нули или полюса функции f, то мы обходим их по дугам окружностей; если на вертикальной границе контура есть нуль или полюс, то мы вырезаем полукруг и добавляем соответствующий полукруг на параллельной границе (для нулей и полюсов на дуге единичной окружности поступаем аналогично).

Вычислим интеграл $\frac{1}{2\pi i} \int_C \frac{df(z)}{f(z)}$ по контуру C двумя способами. С одной стороны,

$$\frac{1}{2\pi i} \int_C \frac{df(z)}{f(z)} = \sum \operatorname{Res} \frac{f'(z)}{f(z)} = \sum_{p \neq i, \rho} v_p(f).$$

С другой стороны, этот интеграл можно вычислить непосредственно, чем мы сейчас и займемся.

При замене z на $e^{2\pi i z}$ верхний отрезок переходит в окружность с центром в начале координат, которая обходится по часовой стрелке, поэтому интеграл по верхнему отрезку равен $-v_\infty(f)$. Интегралы по вертикальным сторонам взаимно уничтожаются, поскольку $f(z+1) = f(z)$.

Пусть $f(z-i) = c(z-i)^m + \ldots$, где $m = v_i(f)$. Тогда

$$\frac{f'(z-i)}{f(z-i)} = \frac{m}{z-i} + \ldots,$$

поэтому интеграл по малой окружности с центром i, которая обходится по часовой стрелке, от функции f'/f равен $-v_i(f)$. Следовательно, интеграл по половине этой окружности равен $-\frac{1}{2} v_i(f)$.

Аналогично, интегралы по дугам окружностей с центрами в точках $(\pm 1 + i\sqrt{3})/2$ в сумме дают $-\frac{1}{3}v_\rho(f)$, поскольку при уменьшении радиуса каждая из этих дуг стремится к $1/6$ дуги окружности.

Наконец, самая трудная часть вычислений — вычисление интеграла по дуге единичной окружности. Мы воспользуемся тем, что преобразование $z \mapsto 1/z$ переводит одну половину дуги в другую, изменяя при этом ориентацию. Ясно, что

$$df\left(-\frac{1}{z}\right) = d(z^{2k}f(z)) = z^{2k}df(z) + 2kz^{2k-1}f(z)dz.$$

Поэтому

$$\frac{df(-\frac{1}{z})}{f-\frac{1}{z})} = \frac{z^{2k}df(z)}{z^{2k}f(z)} + 2kz^{2k1}\frac{f(z)dz}{z^{2k}f(z)} = \frac{df(z)}{f(z)} + 2k\frac{dz}{z}.$$

Таким образом, интегралы от df/f взаимно уничтожаются и остается интеграл $\frac{1}{2\pi i}\int 2k\frac{dz}{z}$ по $1/12$ части окружности, обходимой против часовой стрелки. В итоге получаем

$$\sum v_p(f) = -v_\infty(f) - \frac{1}{3}v_\rho(f) - \frac{1}{2}v_i(f) + \frac{k}{6},$$

что и требовалось. □

Функции

$$g_2(z) = 60\sum{}' \frac{1}{(nz+m)^4}; \qquad g_4(z) = \sum{}' \frac{1}{(nz+m)^6}$$

являются модулярными функциями веса 4 и 6 соответственно. Эти функции голоморфны не только на всей верхней полуплоскости, но и в бесконечности. Действительно, слагаемые с $n \neq 0$ при $z \to \infty$ обращаются в нуль, поэтому

$$g_2(\infty) = 60\sum{}' \frac{1}{m^4} = 120\sum_{m=1}^{\infty}\frac{1}{m^4} = \frac{4}{3}\pi^4$$

и

$$g_4(\infty) = 280\sum_{m=1}^{\infty}\frac{1}{m^6} = \frac{8}{27}\pi^6.$$

Теорема 5.5.1 позволяет найти нули функций g_2 и g_3. Для функции g_2 получаем разложение $\frac{2}{6} = n + \frac{n_1}{2} + \frac{n_2}{3}$, где n, n_1 и n_2 — целые неотрицательные числа. Отсюда $n = n_1 = 0$, $n_2 = 1$, т.е. функция g_2 имеет простой нуль в точке ρ и не имеет других нулей. Для функции g_3 получаем разложение $\frac{3}{6} = n + \frac{n_1}{2} + \frac{n_2}{3}$. Поэтому $n = n_2 = 0$, а $n_1 = 1$, т.е. функция g_3 имеет простой нуль в точке i и не имеет других нулей.

Теорема 5.5.2. *Пространство модулей эллиптических кривых изоморфно сфере Римана, причем этот изоморфизм задается j-инвариантом.*

Доказательство. Функция $j = \frac{1728g_2^3}{g_2^3 - 27g_3^2}$ является модулярной функцией веса 0, поскольку и числитель, и знаменатель, являются модулярными функциями веса 12. Знаменатель $\Delta = g_2^3 - 27g_3^2$ обращается в нуль на бесконечности, поскольку $g_2(\infty) = \frac{4}{3}\pi^4$ и $g_3(\infty) = \frac{8}{27}\pi^6$. Ясно, что Δ не обращается в нуль в точках i и ρ. Функция Δ голоморфна на верхней полуплоскости и $v_\infty(\Delta) \geq 1$, поэтому из теоремы 5.5.1 следует, что $v_\infty(\Delta) = 1$ и $v_p(\Delta) = 0$ при $p \neq \infty$, т.е. функция Δ не обращается в нуль на всей верхней полуплоскости. Учитывая, что $g_2(\infty) \neq 0$, получаем, что j имеет простой полюс на бесконечности.

Докажем теперь, что для каждого λ уравнение $j(z) = \lambda$ имеет единственное решение. Это уравнение эквивалентно уравнению $1728g_3^2 - \lambda\Delta = 0$. Применим теорему 5.5.1 к голоморфной модулярной функции $1728g_3^2 - \lambda\Delta$ веса 12. В результате получим соотношение вида $1 = n + \frac{n_1}{2} + \frac{n_2}{3}$. Таким образом, (n, n_1, n_2) это одна из троек $(1,0,0)$, $(0,2,0)$, $(0,0,3)$. В каждом из этих случаев рассматриваемая функция имеет ровно один нуль. □

Для кривой C, заданной уравнением $y^2 = x^3 + ax + b$, где $a = \frac{-\lambda^2+\lambda-1}{3}$ и $b = \frac{-2\lambda^3+3\lambda^2+3\lambda-2}{27}$, получаем

$$j(C) = j(\lambda) = 2^8 \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2} = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

При $a = 0$, т.е. $\lambda^2 - \lambda + 1 = 0$, получаем $j(C) = 0$. Когда $\lambda = -1$, получаем $b = 0$ и $j(C) = 1728$.

Несложные вычисления показывают, как написать уравнение плоской кубики с данным j-инвариантом: если число j отлично от 0 и 1728, то для кривой

$$y^2 = x^3 - \frac{27}{4}\frac{j}{j-1728}x - \frac{27}{4}\frac{j}{j-1728}$$

значение j-инварианта равно j.

5.6 Автоморфизмы кривых. Теорема Гурвица

Пусть C — алгебраическая кривая, G — конечная подгруппа в группе $\mathrm{Aut}(C)$. При факторизации кривой C по действию группы G получаем двумерную поверхность $C' = C/G$.

Естественная проекция $p\colon C \to C'$ является разветвленным накрытием. Для почти всех точек $x \in C$ орбита $\{gx \mid g \in G\}$ состоит из $|G|$ точек; для таких точек индекс ветвления равен 1. Для конечного числа точек $x \in C$ группа $G_x = \{g \mid gx = x\}$ (*стационарная подгруппа точки* x) нетривиальна. Орбита каждой такой точки x состоит из $|G|/|G_x|$ точек; индекс ветвления каждой из точек этой орбиты равен $|G_x|$. Поэтому, применяя формулу Римана–Гурвица, получаем

$$\chi(C) = |G|\chi(C') - \sum \frac{|G|}{|G_x|}(|G_x| - 1) = |G|\left(\chi(C') - \sum\left(1 - \frac{1}{|G_x|}\right)\right);$$

здесь суммирование ведется по всем точкам кривой C' (и вклад каждой точки, за исключением точек ветвления накрытия, равен 0). Через G_x обозначен стабилизатор прообраза такой точки. С помощью этой формулы мы докажем теоремы 5.6.1 и 5.6.7.

Теорема 5.6.1 (Гурвиц)**.** *Порядок конечной подгруппы G группы автоморфизмов кривой рода $g \geq 2$ не превосходит $84(g-1)$.*

Доказательство. Пусть g' — род топологической поверхности $C' = C/G$. Можно считать, что $|G| > 1$, поэтому $g' < g$. Рассмотрим отдельно три случая.

1. $g' \geq 2$. Тогда $2g - 2 \geq 2|G|$, т.е. $|G| \leq g - 1$. Тем самым, если факторповерхность кривой данного рода g по действию конечной группы автоморфизмов имеет род $g' \geq 2$, то в этой группе автоморфизмов не больше $g - 1$ элементов.

2. $g' = 1$. Тогда $2g - 2 = |G| \sum \left(1 - \frac{1}{|G_x|}\right)$. Если точек ветвления нет, то $2g - 2 = 0$, т.е. $g = 1$, а согласно предположению $g > 1$. Если же ветвление есть, то справа мы имеем сумму слагаемых $1 - \frac{1}{|G_x|}$, каждое которых не меньше $1/2$, поскольку $|G_x| \geq 2$. Следовательно, $2g - 2 \geq \frac{|G|}{2}$, т.е. $|G| \leq 4(g-1)$ Другими словами, если факторповерхность кривой рода $g \geq 2$ по действию группы автоморфизмов является тором, то в группе автоморфизмов не больше $4(g-1)$ элементов.

3. $g' = 0$. Тогда $2g - 2 = |G| \left(\sum \left(1 - \frac{1}{|G_x|}\right) - 2\right)$. Числа $2g - 2$ и $|G|$ положительны, а каждое из слагаемых $1 - \frac{1}{|G_x|}$ строго меньше 1, поэтому таких слагаемых должно быть не меньше 3.

Если число слагаемых больше 4, то сумма $\sum \left(1 - \frac{1}{|G_x|}\right)$ не меньше $\frac{5}{2}$, поскольку каждое из слагаемых не меньше $1/2$. Следовательно, $2(g-1) \geq \frac{|G|}{2}$, т.е. $|G| \leq 4(g-1)$.

Если число слагаемых равно 4, то хотя бы одно из чисел $|G_x|$ должно быть больше 2, поскольку иначе $\sum \left(1 - \frac{1}{|G_x|}\right) = 2$. Следовательно,

$$2(g-1) \geq |G| \left(\frac{3}{2} + \frac{2}{3} - 2\right) = \frac{1}{12}|G|,$$

т.е $|G| \leq 24(g-1)$. Тем самым, если факторповерхность кривой рода $g \geq 2$ по действию группы автоморфизмов является сферой, причем число точек ветвления накрытия факторизации равно 4, то в группе автоморфизмов не больше $24(g-1)$ элементов.

Остается рассмотреть случай, когда число слагаемых равно 3. Пусть три числа $|G_x|$ равны $a \leq b \leq c$. Сумма $\left(1 - \frac{1}{a}\right) + \left(1 - \frac{1}{b}\right) + \left(1 - \frac{1}{c}\right)$ должна быть больше 2, поэтому $c > 3$; более того, $b \geq 3$.

Если $c \geq 7$, то $|G| \leq 84(g-1)$.

Если $c = 6$ и $a = 2$, то $b \geq 4$, поэтому $|G| \leq 24(g-1)$.

Если $c = 6$ и $a \geq 3$, то $|G| \leq 12(g-1)$.

Если $c = 5$ и $a = 2$, то $b \geq 4$, поэтому $|G| \leq 40(g-1)$.

Если $c = 5$ и $a \geq 3$, то $|G| \leq 15(g-1)$.

Если $c = 4$ и $a \geq 3$, то $|G| \leq 24(g-1)$.

Значение $|G| = 84(g-1)$ достигается только при $a = \frac{1}{2}, b = frac13, c = \frac{1}{7}$. Таким образом, кривая рода $g \geq 2$ может иметь группу автоморфизмов из $84(g-1)$ элементов только в том случае, если на ней существует мероморфная функция с ровно тремя критическими значениями, причем все прообразы каждого из этих критических значений являются критическими точками — кратности $2, 3$ и 7 соответственно

Все случаи разобраны, и тем самым доказательство завершено. □

Замечание 5.6.2. В действительности группа автоморфизмов кривой рода $g \geq 2$ конечна, поэтому ее порядок не превосходит $84(g-1)$. Но конечность группы автоморфизмов мы докажем позже.

Пусть p — нечетное простое число. Рассмотрим гомоморфизм группы $\mathrm{PSL}(2, \mathbb{Z})$ в группу $\mathrm{PSL}(2, \mathbb{Z}_p)$, сопоставляющий каждому элементу матрицы его вычет по модулю p. Очевидно, что этот гомоморфизм является эпиморфизмом. Его ядро называется p-модулярной группой и обозначается $\Gamma(p)$. Оно состоит из всех целочисленных 2×2-матриц с определителем 1, все внедиагональные элементы которых делятся на p (рассматриваемых с точностью до умножения на -1).

Упражнение 5.6.3. Докажите, что число элементов в группе $\mathrm{PGL}(2, \mathbb{Z}_p)$ равно $p(p-1)(p+1)$, а в группе $\mathrm{PSL}(2, \mathbb{Z}_p)$ их вдвое меньше. В частности, количество элементов в группе $PSL(2, \mathbb{Z}_7)$ равно

$$\frac{1}{2} 7 \cdot 6 \cdot 8 = 168.$$

Упражнение 5.6.4. *Кривая Клейна* задается на плоскости уравнением $xy^3 + yz^3 + zx^3 = 0$.

а) Докажите, что эта кривая гладкая и что ее род равен 3.

б) Покажите, что кривая Клейна является результатом факторизации верхней полуплоскости по модулярной 7-группе $\Gamma(7) = PSL(2, 7)$, являющейся факторгруппой группы невырожденных 2×2-матриц над полем F_7 с определителем 1, профакторизованной по двухэлементной подгруппе, состоящей из единичной матрицы I и матрицы $-I$.

в) Укажите 168 автоморфизмов кривой Клейна. В частности, проверьте, что она допускает автоморфизм порядка 7

$$(x : y : z) \mapsto (\zeta^5 x : \zeta^4 y : z),$$

где ζ — примитивный корень степени 7 из 1, $\zeta^7 = 1$.

Кривая Клейна — первая кривая в ряду *кривых Гурвица*, т.е. таких кривых рода $g \geq 2$, группа автоморфизмов которых имеет порядок $84(g-1)$. Такие кривые существуют не для всякого рода g, и следующая такая кривая встречается лишь для $g = 7$ (она называется поверхностью Макбета). Однако существуют сколь угодно большие g, для которых имеются кривые Гурвица рода g. Вопрос о том, чему равен максимальный порядок группы автоморфизмов кривой данного рода g исследован не до конца.

Упражнение 5.6.5. Докажите, что не существует кривой Гурвица рода $g = 2$ и рода $g = 4$.

Упражнение 5.6.6. Вычислите группу автоморфизмов кривой Ферма $x^n + y^n + z^n = 0$.

Пусть для действия конечной группы G, состоящей из автоморфизмов кривой C, есть k орбит с нетривиальными группами G_x, порядки которых равны $r_1, \ldots, r_k$. Будем говорить, что это действие имеет тип $\{r_1, \ldots, r_k\}$.

Теорема 5.6.7. *Действие нетривиальной конечной подгруппы автоморфизмов G на сфере Римана имеет один из следующих типов: $\{r, r\}$, $\{2, 2, r\}$ (здесь $r \geq 2$ — любое число), $\{2, 3, 3\}$, $\{2, 3, 4\}$, $\{2, 3, 5\}$.*

Доказательство. Сфера Римана $C = \mathbb{CP}^1$ имеет нулевой род, поэтому топологически факторкривая C/G это сфера, и ее эйлерова характеристика равна 2. Следовательно, $2 = |G|(2 - R)$, где $R = \sum \left(1 - \frac{1}{|G_x|}\right)$. Поэтому для нетривиальной группы G получаем $0 < R < 2$; в частности, есть точки ветвления, потому что $R \neq 0$. Пусть количество орбит с нетривиальными группами G_x равно k. Если $k = 1$, то $0 < R < 1$, поэтому $2 > 2 - R > 1$ и число $|G| = \frac{2}{2-R}$ не может быть целым. Следовательно, $k \geq 2$. С другой стороны, каждое из слагаемых, входящих в R, больше $1/2$, поэтому количество слагаемых не превосходит 3, т.е. $k \leq 3$.

При $k = 2$ мы получаем две точки x_1 и x_2 с индексами ветвления r_1 и r_2. Пусть y_1 и y_2 — образы этих точек в C/G. На сфере с выколотыми точками y_1 и y_2 окружность, обходящая вокруг точки y_1, гомотопна окружности, обходящей вокруг точки y_2. Поэтому $r_1 = r_2 = r$.

Пусть теперь $k = 3$ и $R = \left(1 - \frac{1}{a}\right) + \left(1 - \frac{1}{b}\right) + \left(1 - \frac{1}{c}\right)$. Тогда $|G| = \frac{2}{2-R}$, где $2 - R = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$. Пусть для определенности $a \leq b \leq c$. Если $a \geq 3$, то $2 - R \leq 0$. Следовательно, $a = 2$ и $2 - R = \frac{1}{b} + \frac{1}{c} - \frac{1}{2}$. Поэтому $b = 2$ или 3. При $b = 2$ получаем $|G| = 2c$, а при $b = 3$ получаем $|G| = \frac{2}{\frac{1}{c} - \frac{1}{6}}$. Следовательно, $c = 3, 4$ или 5. □

Замечание 5.6.8. Действия всех указанных типов можно реализовать. Действие типа $\{r, r\}$ реализуется поворотами вокруг некоторой оси на углы, кратные $2\pi/r$. Действие типа $\{2, 2, r\}$ реализуется группой, порожденной поворотом на угол π вокруг некоторой оси и поворотами вокруг оси, перпендикулярной первой оси, на углы, кратные π/r (эту группу можно представлять себе как группу собственных движений сферы, оставляющих на месте правильный $2r$-угольник, вписанный в экваториальную окружность). Действия типа $\{2, 3, 3\}$, $\{2, 3, 4\}$ и $\{2, 3, 5\}$ реализуются собственными движениями сферы, оставляющими на месте правильный тетраэдр, куб (или октаэдр) и додекаэдр (или икосаэдр).

Упражнение 5.6.9. Вычислите порядки подгрупп автоморфизмов G указанных в теореме 5.6.7 типов.