Лекция 9. Классификация эллиптических кривых

На прошлой лекции мы работали с индивидуальной эллиптической кривой $E = \mathbb{C}/L$. Сейчас мы изучим, как конструкции прошлой лекции зависят от L.

Обозначим множество решеток в $\mathbb{C}$ через $\mathfrak{L}$. Если $L \in \mathfrak{L}$ и $\lambda \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$, то через λL обозначим решетку, полученную умножением на λ всех элементов решетки L.

У всякой эллиптической кривой $E = \mathbb{C}/L$ существует семейство автоморфизмов (сдвигов), индуцированных отображениями $z \mapsto z + a$, где $a \in \mathbb{C}$; поскольку любой изоморфизм эллиптических кривых можно скомпоновать со сдвигом, при изучении вопроса о том, изоморфны ли две данные эллиптические кривые, всегда можно считать, что искомый изоморфизм переводит 0 в 0, где $0 \in E$ — образ числа $0 \in \mathbb{C}$, что мы и будем делать в дальнейшем.

Предложение 9.1. *Эллиптические кривые $E = \mathbb{C}/L$ и $E' = \mathbb{C}/L'$ изоморфны тогда и только тогда, когда $L' = \lambda L$ для некоторого $\lambda \in \mathbb{C} \setminus \{0\}$.*

Доказательство. Поскольку часть «тогда» очевидна (изоморфизм $\mathbb{C}/L \to \mathbb{C}/L'$ задается умножением на λ), предположим, что $\varphi\colon E \to E'$ — изоморфизм (считаем, что $\varphi(0) = 0$). Если поднять отображение φ до отображения универсальных накрытий кривых E и E', получится голоморфное отображение $\tilde{\varphi}\colon \mathbb{C} \to \mathbb{C}$ (то есть целая функция), удовлетворяющее условию $\tilde{\varphi}(z+u) - \tilde{\varphi}(z) \in L'$ для всех $z \in \mathbb{C}$ и $u \in L$, причем, очевидно, можно считать, что $\tilde{\varphi}(0) = 0$. Поскольку L' дискретно в $\mathbb{C}$, имеем $\tilde{\varphi}(z+u) - \tilde{\varphi}(z) = \mathrm{const}$ для всякого $u \in L$, откуда $f'(z+u) = f'(z)$ для всякого $u \in L$; поскольку целая функция f' двоякопериодична, она является константой, так что $f(z) = \lambda z + \mu$, где $\lambda, \mu \in \mathbb{C}$ и $\lambda \neq 0$. Так как $\tilde{\varphi}(0) = 0$, имеем $\mu = 0$; так как $\tilde{\varphi}$ опускается до отображения $\varphi\colon E/L \to E/L'$, можно считать, что $\lambda L \subset L'$, а так как степень отображения φ равна 1, имеем $\lambda L = L'$. $\square$

Доказанное предложение можно переформулировать так: множество классов изоморфизмов эллиптических кривых естественно отождествляется с пространством орбит $\mathfrak{L}/\mathbb{C}^*$, где $\mathbb{C}^*$ действует на решетки умножением.

Пусть $L \in \mathfrak{L}$ и $k \geqslant 2$ — целое число. Тогда ряд $\sum_{u \in L\setminus\{0\}}(1/u^{2k})$ абсолютно сходится (эти ряды называются *рядами Эйзенштейна*). Сумма этого ряда обозначается через G_k (или $G_k(L)$, если нужно подчеркнуть зависимость от решетки L). Очевидно, $G_k(\lambda L) = \lambda^{-2k}G_k(L)$. Если $m \geqslant 3$ нечетно, то ряд $\sum_{u \in L\setminus\{0\}}(1/u^m)$ также абсолютно сходится, но его сумма, очевидно, равна нулю.

Выразим через ряды Эйзенштейна коэффициенты уравнения 8.4.

Предложение 9.2. *Эллиптическая кривая $E = \mathbb{C}/L$ изоморфна римановой поверхности алгебраической функции, заданной уравнением*

$$w^2 = 4z^3 - g_2 z - g_3, \tag{9.1}$$

где $g_2 = 60G_2$, $g_3 = 140G_3$.

Доказательство. Разложим каждое из слагаемых в выражении для функции $\wp$ (формула (8.1)) в ряд в окрестности нуля:

$$\frac{1}{(z-u)^2} - \frac{1}{u^2} = \sum_{m=1}^{\infty} \frac{(m+1)z^m}{u^{m+2}}.$$

Поскольку эти ряды, так же как и ряд для $\wp$, абсолютно сходятся, их можно просуммировать и перегруппировать члены; учитывая, что $\sum_{u \in L\setminus\{0\}}(1/u^m) = 0$ при нечетных m, получаем, что ряд Лорана для $\wp$ в окрестности нуля имеет вид

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{k+1}z^{2k} = \frac{1}{z^2} + 3G_2z^2 + 5G_3z^4 + \dots. \tag{9.2}$$

Отсюда получаем:

$$\begin{aligned}
\wp'(z) &= -\frac{2}{z^3} + 6G_2 z + 20G_3 z^3 + \dots, \\
(\wp'(z))^2 &= \frac{4}{z^6} - \frac{24G_2}{z^2} - 80G_3 + \dots, \\
\wp(z) - e_i &= \frac{1}{z^2} - e_i + 3G_2z^2 + 5G_3z^4 + \dots,
\end{aligned} \tag{9.3}$$

$$
\begin{aligned}
4\prod_i(\wp(z)-e_i)=\frac{4}{z^6}-\frac{4(e_1+e_2+e_3)}{z^4}+&\\
+\frac{4(e_1e_2+e_1e_3+e_2e_3)+36G_2}{z^2}+&\\
+(-4e_1e_2e_3-24G_2(e_1+e_2+e_3)+60G_3)+\dots . &\quad (9.4)
\end{aligned}
$$

Сравнивая коэффициенты при одинаковых степенях z в (9.3) и (9.4), получаем последовательно:

$$e_1+e_2+e_3=0, \quad 4(e_1e_2+e_1e_3+e_2e_3)=-60G_2, \quad 4e_1e_2e_3=140G_3.$$

Теперь все следует из предложения 8.4. □

Замечание 9.3. Сравнивая коэффициенты при более высоких степенях z, мы получим соотношения между рядами Эйзенштейна; можно показать, что любой G_k представляется в виде многочлена от G_2 и G_3.

Уравнение (9.1) называется *уравнением эллиптической кривой в нормальной форме Вейерштрасса.*

И функция $\wp$, и коэффициенты в уравнении (9.1) зависят только от решетки L; далее, однако, нам предстоит иметь дело с числами e_1, e_2 и e_3 по отдельности, которые зависят не только от самой решетки, но и от выбора базиса в ней. Чтобы учесть эту зависимость, нам придется ввести небольшой дополнительный формализм. Именно, заметим, что группа точек второго порядка на кривой $\mathbb{C}/L$ изоморфна $\left(\frac{1}{2}L\right)/L$; дадим в связи с этим следующее (необщепринятое)

Определение 9.4. *Оснащенной решеткой* называется пара из решетки $L\subset\mathbb{C}$ и нумерации на множестве ненулевых элементов в $\left(\frac{1}{2}L\right)/L$. *Оснащенной эллиптической кривой* называется пара из эллиптической кривой и нумерации на множестве ее ненулевых точек второго порядка. *Изоморфизмом оснащенных эллиптических кривых* называется изоморфизм, переводящий 0 в 0 и сохраняющий нумерацию точек второго порядка.

Множество оснащенных решеток будем обозначать $\widetilde{\mathfrak{L}}$. Ввиду предложения 9.1 множество классов изоморфизма оснащенных эллиптических кривых естественно отождествляется с пространством орбит $\widetilde{\mathfrak{L}}/\mathbb{C}^*$. Ясно, что e_1, e_2 и e_3 являются функциями из $\widetilde{\mathfrak{L}}$ в $\mathbb{C}$ и что при $\widetilde{L}\in\widetilde{\mathfrak{L}}$ и $\lambda\in\mathbb{C}^*$ имеем $e_j(\lambda\widetilde{L})=\lambda^{-2}e_j(\widetilde{L})$.

Определение 9.5. Функция $k^2\colon\widetilde{\mathfrak{L}}\to\mathbb{C}\setminus\{0,1\}$ определяется по формуле $k^2(\widetilde{L})=(e_2-e_3)/(e_1-e_3)$.

(Вспомните, что числа e_1, e_2 и e_3 всегда различны!)

Из сделанного выше замечания следует, что $k^2(\lambda\widetilde{L})=k^2(\widetilde{L})$ при $\lambda\in\mathbb{C}^*$ и $\widetilde{L}\in\widetilde{\mathfrak{L}}$. Стало быть, k^2 зависит только от оснащенной эллиптической кривой. На самом деле значение k^2 оснащенную эллиптическую кривую полностью определяет:

Предложение 9.6. *Эллиптические кривые $E=C/L$ и $E'=\mathbb{C}/L'$ изоморфны тогда и только тогда, когда на них можно занумеровать точки второго порядка таким образом, что соответствующие значения k^2 будут совпадать.*

Доказательство. Часть «только тогда» очевидна ввиду сказанного выше. Пусть, стало быть, E и E' — оснащенные эллиптические кривые с совпадающим k^2. Тогда, принимая во внимание предложение 8.5, получаем, что E и E' изоморфны римановым поверхностям алгебраических функций с уравнениями $w^2=4(z-p_1)(z-p_2)(z-p_3)$ и $w^2=4(z-p_1')(z-p_2')(z-p_3')$ соответственно, причем существуют такие числа $a\in\mathbb{C}^*$, $b\in\mathbb{C}$, что $p_i'=ap_i+b$. Отображение $z\mapsto az+b$, $w\mapsto\sqrt{a^3}\cdot w$ переводит первое уравнение во второе и индуцирует, очевидно, изоморфизм соответствующих римановых поверхностей, что и требовалось. $\square$

Как мы знаем из предыдущей лекции, эллиптическую кривую можно задать не только как $\mathbb{C}/L$, но и как риманову поверхность алгебраической функции вида $w^2=P(z)$, где P — кубический многочлен без кратных корней. Выясним, как k^2 выражается через корни этого многочлена. Для этого нужна небольшая подготовка.

Предложение 9.7. *Пусть $E=\mathbb{C}/L$ — эллиптическая кривая и f — мероморфная функция на E, имеющая двойной полюс в точке 0 и не имеющая других полюсов. Тогда имеем $f=\alpha\wp+\beta$, где $\alpha,\beta\in\mathbb{C}$ и $\alpha\neq0$.*

Доказательство. Подберем такое $\alpha \in \mathbb{C}^*$, что коэффициенты при z^{-2} в ряде Лорана в нуле у функций $\alpha\wp$ и f (рассматриваемых как эллиптические функции) совпадают. Тогда функция $g = \alpha\wp - f$ либо голоморфна на E, и тогда она является константой и доказательство закончено, либо имеет на E единственный простой полюс. Этот последний случай, однако, невозможен: если рассмотреть g как голоморфное отображение из E в $\overline{\mathbb{C}}$, то оно будет неразветвленным отображением степени 1 и тем самым изоморфизмом, при том что E и $\overline{\mathbb{C}}$ даже не гомеоморфны. $\square$

Следствие 9.8. *Пусть E и f — такие же, как в предложении 9.7. Тогда голоморфное отображение $f\colon E \to \overline{\mathbb{C}}$ разветвлено в точках второго порядка и только в них.* $\square$

Предложение 9.9. *Пусть X — эллиптическая кривая, заданная как риманова поверхность алгебраической функции с уравнением $w^2 = P(z)$, где P — кубический многочлен без кратных корней, и пусть $\{a_1, a_2, a_3\}$ — множество корней многочлена P. Тогда при подходящей нумерации точек второго порядка на X имеем $k^2 = (a_2 - a_3)/(a_1 - a_3)$.*

Доказательство. Пусть $X_0 = \{(z, w) \in \mathbb{C}^2 : w^2 = P(z) \neq 0\}$. Тогда, как мы знаем из лекции 6, $X_0 \subset X$; легко видеть, что функция $f\colon X_0 \to \mathbb{C}$, заданная правилом $(z, w) \mapsto z$, продолжается до мероморфной функции на X, имеющей единственный полюс (кратности 2) в точке, лежащей над ∞. Выберем изоморфизм $X \to \mathbb{C}/L$ так, чтобы эта точка перешла в нуль; тогда предложение 9.7 и следствие 9.8 показывают, что $f = \alpha\wp + \beta$, а точки $x_i = f^{-1}(a_i)$ — точки второго порядка. Теперь все вытекает из очевидного равенства

$$\frac{f(x_2) - f(x_3)}{f(x_1) - f(x_3)} = \frac{\wp(x_2) - \wp(x_3)}{\wp(x_1) - \wp(x_3)}. \quad \square$$

Следствие 9.10. *Пусть X_1 и X_2 — римановы поверхности алгебраических функций, заданных уравнениями $w^2 = P_1(z)$ и $w^2 = P_2(z)$ соответственно, где P_1 и P_2 — кубические многочлены без кратных корней. Тогда X_1 и X_2 изоморфны в том и только том случае, если корни многочленов P_1 и P_2*

можно занумеровать таким образом, что $(a_2 - a_3)/(a_1 - a_3) = (b_2 - b_3)/(b_1 - b_3)$, *где* $\{a_j\}$ — *корни* P_1 *и* $\{b_j\}$ — *корни* P_2. □

Следствие 9.11. *Отображение* $k^2\colon \widetilde{\mathfrak{L}} \to \mathbb{C} \setminus \{0, 1\}$ *сюръективно.*

Доказательство. Рассмотрите уравнение $w^2 = z(z-1)(z-a)$ для $a \in \mathbb{C} \setminus \{0, 1\}$. □

Теперь давайте освободим критерий, доставляемый следствием 9.10, от оговорки «с точностью до нумерации». Это уже делается элементарными рассуждениями.

Предложение-определение 9.12. *Число*

$$j(L) = 256\,\frac{((k^2)^2 - k^2 + 1)^3}{(k^2)^2(k^2-1)^2} \tag{9.5}$$

называется j-инвариантом *эллиптической кривой* $E = \mathbb{C}/L$. *Это число обладает следующими свойствами:*

(1) $j(L)$ *не зависит от нумерации точек второго порядка.*

(2) *Эллиптические кривые* $E = \mathbb{C}/L$ *и* $E' = \mathbb{C}/L'$ *изоморфны тогда и только тогда, когда* $j(L) = j(L')$.

(3) *Отображение* $j\colon \mathfrak{L} \to \mathbb{C}$ *сюръективно.*

Замечание 9.13. Коэффициент 256 вводится для того, чтобы избавиться от коэффициентов в некоторых других формулах.

Доказательство. При перестановке номеров 1 и 2 происходит замена $k^2 \mapsto 1/k^2$, а при перестановке 2 и 3 будет $k^2 \mapsto 1 - k^2$. Легко видеть, что при таких заменах правая часть (9.5) не меняется, а так как (12) и (23) порождают всю группу S_3, утверждение (1) доказано. Далее, при остальных перестановках происходят, как легко видеть, замены $k^2 \mapsto 1/(1-k^2)$, $k^2 \mapsto k^2/(k^2-1)$ и $k^2 \mapsto (k^2-1)/k^2$; следовательно, данной элиптической кривой соответствует не более шести возможных значений k^2, причем легко убедиться, что при $k^2 \notin \left\{\frac{1 \pm i\sqrt{3}}{2}, \frac{1}{2}, 2, -1\right\}$ (или, что эквивалентно, при $j \notin \{0, 1728\}$) все эти шесть значений k^2 действительно различны. С другой стороны, ясно, что при данном $j \in \mathbb{C}$ существует не более шести значений k^2, удовлетворяющих условию (9.5), так что при $j \notin \{0, 1728\}$ утверждение (2) уже доказано, а при двух указанных значениях j прямым перебором проверяется, что число решений уравнения (9.5) относительно k^2 также равно числу возможных значений k^2, получаемых при перестановках точек, так что (2) доказано и в этом случае. Остается доказать (3), но это следует из предложения 9.11 и того очевидного факта, что уравнение (9.5) (относительно k^2) при любом $j \in \mathbb{C}$ имеет решение, отличное от нуля или единицы. $\square$

Напоследок опишем пространства $\widetilde{\mathcal{L}}/\mathbb{C}^*$ и $\mathcal{L}/\mathbb{C}^*$ более конкретно. Для начала обозначим через H верхнюю полуплоскость, через Γ — группу $SL_2(\mathbb{Z})$, и через $\Gamma(2)$ — подгруппу в Γ, состоящую из матриц, сравнимых по модулю 2 с единичной матрицей. Группа Γ действует на H по правилу $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : z \mapsto (az+b)/(cz+d)$. Если $g \in \Gamma$ и $z \in H$, то результат этого действия g на z будем обозначать gz.

Предложение 9.14. *Фактормножества $\mathcal{L}/\mathbb{C}^*$ и $\widetilde{\mathcal{L}}/\mathbb{C}^*$ находятся в естественном взаимно однозначном соответствии с фактормножествами H/Γ и $H/\Gamma(2)$ соответственно.*

Доказательство. Выбирая в решетке L базис $\langle \omega_1, \omega_2 \rangle$ таким образом, чтобы $\operatorname{Im}(\omega_2/\omega_1) > 0$, и умножая ее на ω_1^{-1}, получаем, что всякая решетка эквивалентна решетке с базисом $\langle 1, \tau \rangle$, где $\tau \in H$; два базиса $\langle 1, \tau \rangle$ и $\langle 1, \tau' \rangle$ определяют один и тот же элемент в $\mathcal{L}/\mathbb{C}^*$ тогда и только тогда, когда существуют такие $\lambda \in \mathbb{C}^*$ и $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, что

$$\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \lambda \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix},$$

или, что эквивалентно, $\tau' = g\tau$, чем доказано первое утверждение. Заметим теперь, что выбрать нумерацию ненулевых элементов группы $\left(\frac{1}{2}L\right)/L$ — то же самое, что выбрать базис в $\left(\frac{1}{2}L\right)/L$, рассматриваемом как двумерное векторное пространство над полем $\mathbb{Z}/2\mathbb{Z}$; преобразование $g \in \Gamma$ сохраняет эту нумерацию тогда и только тогда, когда матрица $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ индуцирует тождественное отображение на этом пространстве, а это как раз и означает, что $g \in \Gamma(2)$, что доказывает второе утверждение. $\square$

В свете доказанного предложения можно рассматривать k^2 и j как функции на H; расписывая определения, немедленно получаем, что эти функции голоморфны.

Следствие 9.15. *Отображение* $k^2\colon H \to \mathbb{C} \setminus \{0,1\}$ *сюръективно, и* $k^2(z_1) = k^2(z_2)$ *тогда и только тогда, когда* $z_1 = gz_2$ *для некоторого* $g \in \Gamma(2)$.

Отображение $j\colon H \to \mathbb{C}$ *сюръективно, и* $j(z_1) = j(z_2)$ *тогда и только тогда, когда* $z_1 = gz_2$ *для некоторого* $g \in \Gamma$.

Об эллиптических кривых можно сказать еще очень многое, но мы на этом остановимся.

Приложение: k^2 как универсальное накрытие

В этом приложении мы докажем следующий факт:

Предложение 9.16. *Отображение* $k^2\colon H \to \mathbb{C} \setminus \{0,1\}$ *является накрытием.*

Следствие 9.17. *Универсальное накрытие комплексной плоскости с двумя выколотыми точками изоморфно верхней полуплоскости и единичному кругу.*

Доказательство следствия. Комплексная плоскость с двумя выколотыми точками изоморфна $\mathbb{C} \setminus \{0,1\}$, а верхняя полуплоскость односвязна. □

Основная часть доказательства предложения будет состоять в анализе действия $\Gamma(2)$ на верхней полуплоскости; функция k^2 вступит в игру только под конец.

Начнем с простых замечаний. Ясно, что из всех элементов группы $SL_2(\mathbb{R})$ только I и $-I$, где I обозначает единичную матрицу, индуцируют тождественный автоморфизм верхней полуплоскости. Если теперь отфакторизовать $SL_2(\mathbb{R})$ по подгруппе, состоящей из I и $-I$, то получится группа (обозначаемая $PSL_2(\mathbb{R})$), которая действует на H, как говорят, «эффективно»: всякий неединичный элемент индуцирует нетождественное преобразование. Поскольку $\{I, -I\} \subset \Gamma(2)$, можно и $\Gamma(2)$ отфакторизовать по группе $\{I, -I\}$; получится группа $\Gamma(2)/\{I, -I\}$

(никакого специального обозначения для нее мы вводить не будем), являющаяся дискретной подгруппой в $PSL_2(\mathbb{R})$.

Теперь введем следующее общее определение:

Определение 9.18. Пусть Γ — абстрактная группа, действующая гомеоморфизмами на топологическом пространстве X. Тогда говорят, что это действие *свободно,* если стабилизатор всякой точки $x \in X$ состоит только из единичного элемента; если действие группы Γ на X свободно, то говорят, что это действие *разрывно,* если у всякой точки $x \in X$ существует такая окрестность $V \ni x$, что для всех элементов $\gamma \in \Gamma$, отличных от единичного, имеем $\gamma(V) \cap V = \varnothing$.

(Что такое разрывное действие, не являющееся свободным, мы определять не будем.)

Наша ближайшая цель — показать, что описанное выше действие группы $\Gamma(2)/\{I, -I\}$ на верхней полуплоскости разрывно и свободно; если это будет сделано, мы сможем завершить доказательство с помощью простых и чисто формальных рассуждений.

Сначала установим, что действие свободно; это, очевидно, эквивалентно следующему предложению:

Лемма 9.19. *Если $g \in \Gamma(2)$ — элемент, отличный от $\pm I$, то $gz \neq z$ для всех $z \in H$.*

Доказательство. Пусть $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$; тогда $gz = z$ в том и только том случае, когда z является корнем уравнения

$$cz^2 + (d-a)z - b = 0.$$

Если c отлично от нуля, то это квадратное уравнение имеет корень в H тогда и только тогда, когда его дискриминант отрицателен. Поскольку $ad - bc = 1$, этот дискриминант равен $D = (a-d)^2 + 4bc = (a+d)^2 - 4$, а поскольку a и d нечетны, неравенство $D < 0$ возможно только при $d = -a$; записывая условие, что определитель нашей матрицы равен единице, получаем, что $-a^2 - bc = 1$; так как числа b и c четны, отсюда следует, что $a^2 \equiv -1 \pmod 4$, а это невозможно.

Если же $c = 0$, то наше уравнение может иметь мнимые корни только тогда, когда $b = 0$ и $a = d$, т. е. когда $g = \pm I$. $\square$

Для доказательства разрывности нам придется совершить небольшой экскурс в теорию топологических групп. Напомним, что топологическая группа — это группа G, являющаяся топологическим пространствам и обладающая тем свойством, что отображения $G \times G \to G$ и $G \to G$, задающие умножение и взятие обратного элемента, являются непрерывными; в частности, $SL_2(\mathbb{R})$ и $PSL_2(\mathbb{R})$ (с естественной топологией) являются топологическими группами. Когда говорят, что топологическая группа G действует на топологическом пространстве X, то всегда подразумевают, что отображение $G \times X \to X$, задающее действие, является непрерывным.

Определение 9.20. Говорят, что действие топологической группы G на топологическом пространстве X является *собственным*, если отображение $\varphi\colon G \times X \to X \times X$, действующее по формуле $(g, x) \mapsto (gx, x)$, обладает тем свойством, что для всякого компактного подмножества $K \subset X \times X$ множество $\varphi^{-1}(K) \subset G \times X$ также является компактным.

Теперь сформулируем следующее общее утверждение о действиях топологических групп:

Предложение 9.21. *Пусть топологическая группа G действует на локально компактном метризуемом*[3] *пространстве X. Предположим, что это действие собственно. Если теперь $\Gamma \subset G$ — такая замкнутая дискретная подгруппа в G, что естественное действие Γ на X свободно, то это действие группы Γ будет и разрывно.*

Доказательство. Рассуждая от противного, предположим, что действие группы Γ разрывным не является. Тогда существуют точка $x \in X$, последовательность точек $\{x_n \in X\}$ и последовательность $\{\gamma_n\}$, состоящая из неединичных элементов группы Γ, обладающие тем свойством, что $\lim x_n = x$ и $\lim \gamma_n x_n = x$. Так как X локально компактно, можно, не ограничивая общности, считать, что все x_n и $\gamma_n x_n$ лежат в некотором компактном множестве $K \ni x$. Следовательно, для всех n имеем

[3]На самом деле метризуемости можно не требовать.

$(\gamma_n, x_n) \in \varphi^{-1}(K \times K)$, где $\varphi\colon G \times X \to X \times X$ — отображение, о котором идет речь в определении 9.20. Поскольку действие G на X собственно, множество $\varphi^{-1}(K \times K)$ компактно, и тем самым у последовательности $\{(\gamma_n, x_n)\}$ имеется сходящаяся подпоследовательность. Изменив обозначения, будем считать, что сходится сама последовательность $\{(\gamma_n, x_n)\}$. Поскольку подгруппа $\Gamma \subset G$ замкнута и дискретна, из этого следует, что для всех достаточно больших n имеем $\gamma_n = \gamma$, где $\gamma \in \Gamma$ — некоторый фиксированнный неединичный элемент. Стало быть, $\lim \gamma x_n = x$, но так как $\lim x_n = x$, отсюда вытекает, что $\gamma x = x$, а это противоречит тому, что действие группы Γ свободно. □

Вооружившись предложением 9.21, продолжим:

Предложение 9.22. *Действие* $\Gamma(2)/\{\pm I\}$ *на верхней полуплоскости является разрывным.*

Доказательство. Ввиду предложений 9.19 и 9.21 нам достаточно показать, что действие $PSL_2(\mathbb{R})$ на верхней полуплоскости является собственным.

Для начала заметим, что действие $PSL_2(\mathbb{R})$ на верхней полуплоскости изоморфно в очевидном смысле действию группы конформных автоморфизмов диска $\Delta = \{z \in \mathbb{C} : |z| < 1\}$, так что достаточно доказать собственность действия этой последней. Как мы помним, автоморфизмы Δ имеют вид

$$g_{\theta,a} : z \mapsto e^{i\theta}\frac{z-a}{1-\overline{a}z},$$

где $\theta \in \mathbb{R}$, $|a| < 1$. Группу таких дробно-линейных преобразований обозначим через G. Ясно, что достаточно проверить, что компактны все множества вида $\varphi^{-1}(K_1 \times K_2) \subset \subset G \times \Delta$, где $K_1, K_2 \subset \Delta$ — компактные подмножества и $\varphi\colon G \times \Delta \to \Delta \times \Delta$ — отображение из определения 9.20. Поскольку $\varphi^{-1}(K_1 \times K_2)$, очевидно, замкнуто в $G \times \Delta$, нам достаточно показать, что существует такое число $\varepsilon > 0$, что $|a| \leqslant 1 - \varepsilon$, как только $(g_{\theta,a}, w) \in \varphi^{-1}(K_1 \times K_2)$. Предположим противное; тогда существуют такие последовательности $\{a_n\}$, $\{\theta_n\}$, $\{z_n\}$, что $z_n \in K_2$, $g_{\theta_n,a_n}(z_n) \in K_1$, и при этом $\lim a_n = a$, где $|a| = 1$. Поскольку K_2 компактно, мы можем (выбрав подходящую подпоследовательность) считать, что $\lim z_n = z \in K_2$. Теперь заметим, что

$$\lim |g_{\theta_n,a_n}(z_n)| = \lim \left|\frac{z_n - a_n}{1-\overline{a_n}z}\right| = \left|\frac{z-a}{1-\overline{a}z}\right| = \left|\frac{z-a}{1-z/a}\right| = |-a| = 1$$

(так как $|a| = 1$, имеем $\overline{a} = 1/a$). Однако же $g_{\theta_n,a_n}(z_n) \in K_1$ и тем самым числа $|g_{\theta_n,a_n}(z_n)|$ отграничены от единицы — противоречие. $\square$

Теперь мы можем наконец завершить доказательство предложения 9.16. Из того, что $\Gamma(2)/\{\pm I\}$ разрывно и свободно действует на H, с помощью стандартных и хорошо известных рассуждений выводится, что естественное отображение $H \to H/(\Gamma(2)/\{\pm I\})$ является накрытием, а также что на $H/(\Gamma(2)/\{\pm I\})$ (или, что то же самое, $H/\Gamma(2)$) можно ввести структуру римановой поверхности, относительно которой это отображение будет голоморфно (подобно тому, как мы в лекции 5 ввели структуру римановой поверхности на эллиптической кривой). При этом отображение k^2 индуцирует, ввиду следствия 9.15, голоморфное и взаимно однозначное отображение $\widetilde{k^2}\colon H/\Gamma(2) \to \mathbb{C} \setminus \{0,1\}$; значит, это отображение неразветвлено и тем самым является изоморфизмом, что и утверждалось.

Лекция 10. Теорема Римана об отображении

Вся эта лекция будет посвящена доказательству следующей теоремы, называемой теоремой Римана об отображении:

Теорема 10.1. *Всякое односвязное открытое множество $U \subset \mathbb{C}$, отличное от самого $\mathbb{C}$, изоморфно диску* $\Delta = \{z \in \mathbb{C} : |z| < 1\}$.

Для удобства введем следующее классическое

Определение 10.2. Голоморфная функция $f\colon W \to \mathbb{C}$ на открытом множестве $W \subset \mathbb{C}$ называется *однолистной*, если отображение f взаимно однозначно.