# Лекция 8. 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 $\mathcal{L}$. Если $L \in \mathcal{L}$ и $\lambda \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$, то через $\lambda L$ обозначим решетку, полученную умножением на $\lambda$ 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 предполагать в дальнейшем.

**Предложение 8.1.** *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 $\lambda$), предположим, что $\varphi\colon E \to E'$ — изоморфизм (считаем, что $\varphi(0) = 0$). Поднимем отображение $\varphi$ 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 $\varphi$ равна 1, имеем $\lambda L = L'$. $\square$

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

Пусть $L \in \mathcal{L}$ и $n \geqslant 2$ — целое число. Тогда ряд $\sum_{u \in L\setminus\{0\}} (1/u^{2k})$ абсолютно сходится (эти ряды называются *рядами Эйзенштейна*). Сумма этого ряда обозначается $G_k$ (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 7.4.

**Предложение 8.2.** *Эллиптическая кривая $E = \mathbb{C}/L$ изоморфна римановой поверхности алгебраической функции, заданной уравнением*

$$w^2 = 4z^3 - g_2 z - g_3, \tag{8.1}$$

*где $g_2 = 60G_2$, $g_3 = 140G_3$.*

*Доказательство.* Разложим каждое из слагаемых вида $1/(z-u)^2 - 1/u^2$ в выражении для функции $\wp$ 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

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{k+1}z^{2k} = \frac{1}{z^2} + 3G_2z^2 + 5G_3z^4 + \dots . \tag{8.2}$$

Отсюда получаем:

$$\begin{aligned}
\wp'(z) &= -\frac{2}{z^3} + 6G_2z + 20G_3z^3 + \dots, \\
(\wp'(z))^2 &= \frac{4}{z^6} - \frac{24G_2}{z^2} - 80G_3 + \dots, \qquad (8.3)\\
\wp(z) - e_i &= \frac{1}{z^2} - e_i + 3G_2z^2 + 5G_3z^4 + \dots, \\
4\prod_i(\wp(z) - e_i) &= \frac{4}{z^6} - \frac{4(e_1+e_2+e_3)}{z^4} + \frac{4(e_1e_2+e_1e_3+e_2e_3)+36G_2}{z^2} + \\
&\quad + (-4e_1e_2e_3 - 24G_2(e_1+e_2+e_3) + 60G_3) + \dots . \qquad (8.4)
\end{aligned}$$

Сравнивая коэффициенты при одинаковых степенях $z$ в (8.3) и (8.4), получаем последовательно $e_1+e_2+e_3 = 0$, $4(e_1e_2+e_1e_3+e_2e_3) = -60G_2$, $4e_1e_2e_3 = 140G_3$. Теперь все следует из предложения 7.4. □

**Замечание 8.3.** 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 $G_3$. См. главу VII книги Ж.-П. Серра «Курс арифметики» (М.: «Мир», 1972).

Уравнение (8.1) называется *уравнением эллиптической кривой в нормальной форме Вейерштрасса.*

И функция $\wp$, и коэффициенты в уравнении (8.1) 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 $(\frac{1}{2}L)/L$; дадим в связи с этим следующее (необщепринятое)

**Определение 8.4.** *Оснащенной решеткой* называется пара из решетки $L \subset \mathbb{C}$ и нумерации на множетсве ненулевых элементов в $(\frac{1}{2}L)/L$. *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 $\widetilde{\mathcal{L}}$. Ввиду предложения 8.1 множество классов изоморфизма оснащенных эллиптических кривых естественно отождествляется с пространством орбит $\widetilde{\mathcal{L}}/\mathbb{C}^*$. Ясно, что $e_1$, $e_2$ и $e_3$ являются функциями из $\widetilde{\mathcal{L}}$ в $\mathbb{C}$ и что при $\widetilde{L} \in \widetilde{\mathcal{L}}$ и $\lambda \in \mathbb{C}^*$ имеем $e_j(\lambda\widetilde{L}) = \lambda^{-2}e_j(\widetilde{L})$.

**Определение 8.5.** Функция $k^2\colon \widetilde{\mathcal{L}} \to \mathbb{C} \setminus \{0,1\}$ 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 $\widetilde{L} \in \widetilde{\mathcal{L}}$. Стало быть, $k^2$ зависит только от оснащенной эллиптической кривой. На самом деле значение $k^2$ оснащенную эллиптическую кривую полностью определяет:

**Предложение 8.6.** *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 7.5, 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 8.7.** *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 $\alpha \neq 0$.*

*Доказательство.* Подберем такое $\alpha \in \mathbb{C}^*$, что коэффициенты при $z^{-2}$ в ряде Лорана в нуле у функций $\wp$ и $\alpha f$ (рассматриваемых как эллиптические функции) совпадают. Тогда функция $g = \wp - \alpha f$ 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 8.8.** *Пусть $E$ и $f$ — такие же, как в предложении 8.7. Тогда голоморфное отображение $f\colon E \to \overline{\mathbb{C}}$ разветвлено в точках второго порядка и только в них.* $\square$

**Предложение 8.9.** *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 $X_0 = \{(z, w) \in \mathbb{C}^2 \mid w^2 = P(z) \neq 0\}$. Тогда, как мы знаем из лекции 6, $X_0 \subset X$; легко видеть, что функция $f\colon X_0 \to \mathbb{C}$, заданная правилом $(z, w) \to z$, продолжается до мероморфной функции на $X$, имеющей единственный полюс (кратности 2) в точке, лежащей над $\infty$. Выберем изоморфизм $X \to \mathbb{C}/L$ так, чтобы эта точка перешла в ноль; тогда предложение 8.7 и следствие 8.8 показывают, что $f = \alpha\wp + \beta$, а точки $x_i = f^{-1}(a_i)$ — точки второго порядка. Теперь все вытекает из очевидного равенства $(f(x_2) - f(x_3))/(f(x_1) - f(x_3)) = (\wp(x_2) - \wp(x_3))/(\wp(x_1) - \wp(x_3))$. $\square$

**Следствие 8.10.** *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 $P_2$.* $\square$

**Следствие 8.11.** *Отображение* $k^2\colon \widetilde{\mathcal{L}} \to \mathbb{C} \setminus \{0,1\}$ *сюръективно.*

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

Теперь давайте освободим критерий, доставляемый следствием 8.10, от оговорки «с точностью до нумерации». Это уже делается элементарными рассуждениями.

**Предложение-определение 8.12.** *$j$-инвариантом эллиптической кривой $E = \mathbb{C}/L$ называется число*

$$j(L) = 256\frac{((k^2)^2 - k^2 + 1)^3}{(k^2)^2(k^2-1)^2}. \tag{8.5}$$

*Число $j(L)$ обладает следующими свойствами:*

(1) *Число $j(L)$ 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 $j\colon \mathcal{L} \to \mathbb{C}$ сюръективно.*

**Замечание 8.13.** 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 (8.5) 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 $k^2 \notin \{\frac{1\pm i\sqrt{3}}{2}, \frac{1}{2}, 2, -1\}$ (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 (8.5), так что при $j \notin \{0, 1728\}$ утверждение (2) уже доказано, а при двух указанных значениях $j$ прямым перебором проверяется, что число решений уравнения (8.5) 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 8.11 и того очевидного факта, что уравнение (8.5) (относительно $k^2$) при любом $j \in \mathbb{C}$ имеет решение, отличное от нуля или единицы. $\square$

Напоследок опишем более конкретно пространства $\widetilde{\mathcal{L}}/\mathbb{C}^*$ и $\mathcal{L}/\mathbb{C}^*$. Для начала обозначим через $H$ верхнюю полуплоскость, через $\Gamma$ — группу $Sl_2(\mathbb{Z})$, и через $\Gamma(2)$ — подгруппу в $\Gamma$, состоящую из матриц, сравнимых по модулю 2 с единичной матрицей. Группа $\Gamma$ 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 8.14.** *Фактормножества $\mathcal{L}/\mathbb{C}^*$ и $\widetilde{\mathcal{L}}/\mathbb{C}^*$ находятся в естественном взаимно-однозначном соответствии с фактормножетсвами $H/\Gamma$ 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 на $\omega_1^{-1}$, 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 $\frac{1}{2}L/L$ — то же самое, что выбрать базис в $\frac{1}{2}L/L$, 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 8.15.** *Голоморфное 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 $g \in \Gamma(2)$.*

*Голоморфное 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.