Лекция 8. Эллиптические функции

На этой лекции мы докажем, в числе прочего, что всякая эллиптическая кривая является римановой поверхностью некоторой алгебраической функции.

Пусть $L \subset \mathbb{C}$ — решетка с базисом $\langle \omega_1, \omega_2 \rangle$ и $E = \mathbb{C}/L$ — соответствующая эллиптическая кривая. По предложению 5.8 непостоянных голоморфных функций на E нет; будем искать мероморфные функции. Ясно, что мероморфная функция на E — это то же самое, что двоякопериодическая мероморфная функция на $\mathbb{C}$, имеющая числа ω_1 и ω_2 своими периодами; такие двоякопериодические мероморфные функции называются *эллиптическими функциями*.

Предложение-определение 8.1. *Ряд*

$$\frac{1}{z^2} + \sum_{u \in L \setminus \{0\}} \Big(\frac{1}{(z-u)^2} - \frac{1}{u^2} \Big) \tag{8.1}$$

*сходится абсолютно и равномерно на любом компактном подмножестве в $\mathbb{C} \setminus L$ к мероморфной функции, обозначаемой $\wp(z)$ и называемой $\wp$-*функцией Вейерштрасса*. Функция $\wp$ является четной и удовлетворяет тождеству $\wp(z+u) = \wp(z)$ при всех $u \in L$. В каждой точке решетки L функция $\wp$ имеет полюс второго порядка, а других полюсов у нее нет. Главная часть ряда Лорана функции $\wp$ в нуле имеет вид $1/z^2$.*

Доказательство. Пусть $K \subset \mathbb{C} \setminus L$ — компакт и $z \in K$. Тогда имеем $|z-u| \sim |u|$ при $u \in L$, $|u| \to \infty$, причем эта эквивалентность равномерна по $z \in K$. Следовательно, имеем

$$\Big| \frac{1}{(z-u)^2} - \frac{1}{u^2} \Big| = \frac{|z| \cdot |z-2u|}{|u|^2 \cdot |z-u|^2} = O\Big(\frac{1}{|u|^3}\Big)$$

(O равномерно по $z \in K$), откуда утверждение о сходимости следует с очевидностью. Стало быть, $\wp$ голоморфна на $\mathbb{C} \setminus L$; тождество $\wp(-z) = \wp(z)$ немедленно следует из возможности переставлять члены в абсолютно сходящемся ряде.

Ввиду равномерной сходимости ряда (8.1) на компактах его можно почленно продифференцировать; если сделать это, получится формула

$$\wp'(z) = -2\sum_{u\in L}\frac{1}{(z-u)^3}, \tag{8.2}$$

где ряд сходится абсолютно и равномерно на компактах в $\mathbb{C}\setminus L$; из абсолютной сходимости ряда (8.2) немедленно следует, что $\wp'(z+u) = \wp'(z)$ при любом $u \in L$; следовательно, для всякого $u \in L$ имеем $\wp(z+u) - \wp(u) = C$, где $C \in \mathbb{C}$ — константа. Ввиду четности $\wp$ имеем теперь

$$\wp(-u/2) = \wp(u/2) = \wp(-u/2+u) = \wp(-u/2) + C,$$

откуда $C = 0$, что доказывает тождество $\wp(z+u) = \wp(z)$ при $u \in L$. Утверждения о полюсах функции $\wp$ следуют с очевидностью из всего доказанного выше. □

Следствие 8.2. *Функция $\wp'$ мероморфна на $\mathbb{C}$, нечетна и двоякопериодична с периодами ω_1 и ω_2; она имеет полюсы порядка 3 во всех точках решетки, а других полюсов не имеет; главная часть ряда Лорана функции $\wp'$ в нуле имеет вид $(-2/z^3)$.* □

Эллиптическую кривую $E = \mathbb{C}/L$ можно рассматривать как группу по сложению (факторгруппу аддитивной группы $\mathbb{C}$); очевидно, как группа она изоморфна $(\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z})$; стало быть, E имеет ровно четыре точки второго порядка: образы точек 0, $\omega_1/2$, $\omega_2/2$ и $(\omega_1+\omega_2)/2$.

Коль скоро функции $\wp$ и $\wp'$ двоякопериодичны с периодами ω_1 и ω_2, их можно рассматривать как мероморфные функции на E, то есть как голоморфные отображения из E в $\overline{\mathbb{C}}$.

Предложение 8.3. *Функция $\wp$, рассматриваемая как голоморфное отображение из E в $\overline{\mathbb{C}}$, имеет степень 2, а функция $\wp'$ — степень 3. Отображение $\wp\colon E \to \overline{\mathbb{C}}$ разветвлено с индексом два в точках второго порядка и неразветвлено в остальных точках. Если $\wp(a_1) = \wp(a_2)$, где $a_1, a_2 \in E$, то $a_2 = \pm a_1$ (если рассматривать a_1 и a_2 как комплексные числа, это запишется как $a_2 \equiv \pm a_1 \pmod{L}$). Если $a \in C$ — число, соответствующее точке второго порядка, отличной от нуля, то $\wp'(a) = 0$. Если $\wp'(z) = 0$, то z сравнимо по модулю L с $\omega_1/2$, $\omega_2/2$ или $(\omega_1+\omega_2)/2$.*

Доказательство. Если рассматривать $\wp$ и $\wp'$ как голоморфные отображения из E в $\overline{\mathbb{C}}$, то предложение 8.1 и следствие 8.2 показывают, что $\wp^{-1}(\{\infty\}) = \wp'^{-1}(\{\infty\}) = \{0\}$, причем индекс ветвления в нуле равен двум для $\wp$ и трем для $\wp'$; ввиду предложения 7.1 отсюда следуют утверждения про степени. Если $a \in \mathbb{C}$ — число, соответствующее точке второго порядка на E, то $a \equiv -a \pmod L$, откуда ввиду четности $\wp$ получаем тождество $\wp(a+z) = \wp(-a-z) = \wp(a-z)$; дифференцируя это равенство по z при $z=0$, получаем $\wp'(a) = -\wp'(a)$, откуда $\wp'(a) = 0$. Стало быть, отображение $\wp$ разветвлено во всех точках второго порядка, причем индекс ветвления не может быть больше двух ввиду предложения 7.1, поскольку $\deg\wp = 2$. Далее, из доказанных равенств следует, что все три точки второго порядка, кроме нуля, содержатся в множестве $\wp'^{-1}(0)$; поскольку $\deg\wp' = 3$, ничего другого в этом множестве содержаться не может (и отображение $\wp'$ в этих точках неразветвлено), так что у отображения $\wp$ нет других точек ветвления, кроме точек второго порядка, а у функции $\wp'$ нет других нулей на $\mathbb{C}$, кроме сравнимых с $\omega_1/2$, $\omega_2/2$ или $(\omega_1+\omega_2)/2$, причем эти нули просты. Если, наконец, $\wp(a_1) = \wp(a_2)$ и $a_1 \neq a_2$ на E, то обе эти точки лежат в $\wp^{-1}(b)$, где $b = \wp(a_1) = \wp(a_2) \in \overline{\mathbb{C}}$; поскольку имеем также $\wp(-a_1) = b$ ввиду четности $\wp$, то $-a_1 = a_2$ (если $-a_1 = a_1$, то a_1 — точка второго порядка, отображение $\wp$ в ней разветвлено и $a_2 = a_1$). Все доказано. $\square$

Положим $e_1 = \wp(\omega_1/2)$, $e_2 = \wp((\omega_1+\omega_2)/2)$, $e_3 = \wp(\omega_2/2)$. Заметим, что числа e_1, e_2 и e_3 различны: если значения $\wp$ в каких-то двух из этих точек совпадают и равны, скажем, $c \in \mathbb{C}$, то, рассматривая $\wp$ как голоморфное отображение из E в $\overline{\mathbb{C}}$, получаем, что $\wp^{-1}(c)$ содержит две разные точки ветвления, что невозможно, так как $\deg\wp = 2$.

Предложение 8.4. *Функции $\wp$ и $\wp'$ связаны тождеством*

$$(\wp'(z))^2 = 4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3). \tag{8.3}$$

Доказательство. И левая, и правая часть (8.3) — мероморфные функции на E, имеющие полюсы порядка 6 в точке 0 и нигде больше и обращающиеся в нуль в остальных точках второго порядка (и левая, и правая часть — с кратностью 2) и нигде больше. Следовательно, их отношение — голоморфная функция на E, то есть константа. Поскольку «старший» (с наиболее отрицательной степенью z) член ряда Лорана в нуле и у левой, и у правой части имеет вид $4/z^6$, эта константа равна единице. $\square$

Предложение 8.5. *Эллиптическая кривая E изоморфна римановой поверхности алгебраической функции, заданной уравнением*

$$w^2 = 4(z - e_1)(z - e_2)(z - e_3). \tag{8.4}$$

Доказательство. Обозначим через X компактную риманову поверхность, соответствующую алгебраической функции с уравнением (8.4), и пусть $E_0 \subset E$ — подмножество, получаемое удалением из E точек второго порядка, а X_0 — подмножество в $\mathbb{C}^2$, состоящее из точек, координаты которых удовлетворяют уравнению (8.4), причем $z \notin \{e_1, e_2, e_3\}$. Легко видеть, что X_0 — это то самое множество, которое было обозначено через X_0 в предыдущей лекции, причем X получается добавлением к X_0 четырех точек, лежащих над e_1, e_2, e_3 и ∞. Определим отображение $\varphi_0 \colon E_0 \to X_0$ по формуле $z \mapsto (\wp(z), \wp'(z))$ (то, что $\varphi_0(E_0) \subset X_0$, следует из соотношения (8.3)). Ясно, что отображение φ_0 голоморфно. Покажем, что оно является биекцией E_0 на X_0. В самом деле, если $\wp(a_1) = \wp(a_2)$, причем $a_1, a_2 \in E_0$, то $a_1 = \pm a_2$ ввиду предложения 8.3; поскольку ввиду нечетности функции $\wp'$ имеем $\wp'(-a_1) = -\wp'(a_1)$, причем $\wp'(a_1) \neq 0$, так как a_1 не является точкой второго порядка (см. то же предложение 8.3), случай $a_1 = -a_2$ исключается; тем самым доказана инъективность отображения φ_0. Если $(z, w) \in X_0$, то, очевидно, $z = \wp(a) = \wp(-a)$ для некоторого $a \in E$ (так как отображение $\wp \colon E \to \overline{\mathbb{C}}$ сюръективно); из формулы (8.3) и нечетности функции $\wp'$ теперь следует, что либо $\wp'(a)$, либо $\wp'(-a)$ равно w, так что φ_0 и сюръективно. Итак, $\varphi_0 \colon E_0 \to X_0$ — голоморфная биекция и, стало быть, изоморфизм. Продолжим теперь отображение φ_0 до отображения $\varphi \colon E \to X$ следующим образом: переведем нуль в точку римановой поверхности X, лежащую над ∞, а точку второго порядка $a \neq 0$ — в точку, лежащую над $\wp(a)$. Легко видеть, что отображение $\varphi\colon E \to X$ непрерывно (следовательно, по теореме Римана об устранимой особенности оно голоморфно) и биективно, так что φ — изоморфизм. Все доказано. $\square$

Предложение 8.5 можно обратить:

Предложение 8.6. *Риманова поверхность алгебраической функции, заданной уравнением*

$$w^2 = c(z - \lambda_1)(z - \lambda_2)(z - \lambda_3), \tag{8.5}$$

где $c \neq 0$, а числа λ_1, λ_2 и λ_3 различны, является эллиптической кривой.

Доказательство. Начнем с важного определения.

Определение 8.7. *Голоморфной* 1*-формой* (классический термин: *дифференциал первого рода*; мы будем говорить просто «голоморфная форма») на римановой поверхности X называется комплексная дифференциальная форма степени 1 на X, которую в локальных координатах можно записать в виде $\omega = f\,dz$, где функция f голоморфно зависит от локальной координаты z.

Сделаем два простых замечания к этому определению. Во-первых, если функция замены координат $z = z(w)$ голоморфна, то имеем $f(z)\,dz = f(z(w))z'(w)\,dw$ (см. предложение 1.3), так что форма, записываемая в одной из систем координат в виде $f\,dz$, где f голоморфна, будет записываться в таком виде и в *любой* системе координат. Во-вторых, всякая голоморфная форма будет обязательно замкнута (предложение 1.3 (5)), так что ее интегралы по двум гомологичным 1-цепям совпадают.

Пусть теперь X — риманова поверхность алгебраической функции, заданной уравнением (8.5). Обозначим правую часть этого уравнения через $P(z)$. Легко видеть, что естественное отображение $p\colon X \to \overline{\mathbb{C}}$ имеет степень 2 и разветвлено с индексом 2 ровно в четырех точках, лежащих над λ_1, λ_2 и λ_3 и бесконечностью; обозначим эти точки a_1, a_2, a_3 и $\overline{\infty}$. Отсюда немедленно следует, что X гомеоморфна тору (иными словами, род X равен единице). Проще всего убедиться в этом с помощью формулы

Римана–Гурвица: если обозначить род поверхности X через g, то $2g-2=2\cdot(-2)+4\cdot(2-1)=0$.

Теперь построим на X голоморфную форму ω, нигде не обращающуюся в нуль (существование такой формы на компактной римановой поверхности — характеристическое свойство эллиптических кривых: см. задачу 66 на с. 130). Именно, пусть $X_0=X\setminus\{a_1,a_2,a_3,\overline{\infty}\}$ и $X'=X\setminus\overline{\infty}$. На X' определены голоморфные функции z и w; положим $\omega=dz/w$ на X_0; ясно, что эта голоморфная форма не обращается в нуль на X_0; утверждается, что ее можно продолжить на все X. В самом деле, в точке a_j в качестве локальной координаты можно выбрать w (поскольку $w^2=P(z)$ и $P(z)$ можно выбрать в качестве локальной координаты на $\overline{\mathbb{C}}$ в окрестности λ_j); так как из соотношения (8.5) следует, что $2w\,dw=P'(z)\,dz$ на X, имеем $dz/w=2\,dw/P'(z)$, и так как $P'(\lambda_j)\neq 0$ (корень λ_j — не кратный), получаем, что форма dz/w продолжается до голоморфной в окрестности точки a_j. Осталось посмотреть на окрестность точки $\overline{\infty}$; в этой точке можно выбрать такую локальную координату t, что $z=1/t^2$, $w=h(t)/t^3$, где функция h голоморфна и не обращается в нуль в нуле (так как h — одна из ветвей $\sqrt{c(1-t^2\lambda_1)(1-t^2\lambda_2)(1-t^2\lambda_3)}$). Отсюда получаем, что $dz=-2\,dt/t^3$ и $\omega=dz/w=-2\,dt/h(t)$, так что ω продолжается и в $\overline{\infty}$ и не обращается там в нуль.

Поскольку поверхность X гомеоморфна тору, ее первая группа гомологий $H_1(X,\mathbb{Z})$ изоморфна $\mathbb{Z}\oplus\mathbb{Z}$; пусть γ_1,γ_2 — образующие этой группы. Обозначим через $L\subset\mathbb{C}$ подгруппу, состоящую из чисел $\int_\gamma\omega$ для всевозможных $\gamma\in H_1(X,\mathbb{Z})$; эта подгруппа порождена числами $u_1=\int_{\gamma_1}\omega$ и $u_2=\int_{\gamma_2}\omega$.

Лемма 8.8. *Числа u_1 и u_2 линейно независимы над $\mathbb{R}$.*

Доказательство леммы. Предположим противное; тогда группа L содержится в некоторой прямой; умножая ω на ненулевое комплексное число α, можно добиться того, что эта прямая будет совпадать с вещественной осью.

Пусть $\pi\colon\tilde X\to X$ — универсальное накрытие; введем на $\tilde X$ структуру римановой поверхности, индуцированную с X. Выберем точки $x_0\in X$ и $\tilde x_0\in\pi^{-1}(x_0)$ и определим голоморфную функцию $\tilde{\varphi}\colon \tilde{X} \to \mathbb{C}$ по формуле $x \mapsto \int_{\tilde{x}_0}^{x} (\alpha\pi^*\omega)$ (интегрирование ведется по кривой, соединяющей x_0 и x; ввиду односвязности $\tilde{X}$ от выбора кривой интеграл не зависит). В силу нашего выбора числа α мнимая часть интеграла от $\alpha\omega$ по любому циклу на X равна нулю, так что $\operatorname{Im}\tilde{\varphi}(x) = \operatorname{Im}\tilde{\varphi}(x')$ при $\pi(x) = \pi(x')$. Следовательно, функция $x \mapsto \operatorname{Im}\tilde{\varphi}(x)$ пропускается через компактное пространство X и тем самым достигает наибольшего значения на $\tilde{X}$; по принципу максимума отсюда следует, что $\tilde{\varphi}$ — константа, и, следовательно, $\pi^*\omega = 0$, что нелепо. □

Итак, мы доказали, что $L \subset \mathbb{C}$ — решетка. Определим теперь голоморфное отображение $\varphi\colon X \to \mathbb{C}/L$ по формуле $x \mapsto \int_{x_0}^{x} \omega \bmod L$ (при замене пути интегрирования к интегралу прибавится элемент из L, так что отображение определено корректно). Поскольку ω нигде не обращается в нуль, отображение φ неразветвлено и, следовательно, является накрытием; так как отображение $\varphi_*\colon \pi_1(X, x_0) \to \pi_1(\mathbb{C}/L, \varphi(x_0)) \cong L$ имеет вид $\gamma \mapsto \int_\gamma \omega$, получаем, что по построению группы L отображение φ^* сюръективно. Следовательно, φ — голоморфный гомеоморфизм и тем самым изоморфизм. □

Замечание 8.9. К доказательству предложения 8.6 ведет следующий ход мыслей. Мы хотим представить риманову поверхность X в виде $\mathbb{C}/L$, для чего хотелось бы, чтобы отображение $p\colon X \to \overline{\mathbb{C}}$ было похоже на функцию $\wp$, также дающую разветвленное накрытие над $\overline{\mathbb{C}}$ степени два с ветвлением в четырех точках. Однако же функция $\wp$ удовлетворяет дифференциальному уравнению (8.3); стало быть, чтобы найти наш аналог $\wp$, надо решить дифференциальное уравнение

$$(z')^2 = c(z-\lambda_1)(z-\lambda_2)(z-\lambda_3), \tag{8.6}$$

что мы и сделали, интегрируя форму

$$dz/\sqrt{c(z-\lambda_1)(z-\lambda_2)(z-\lambda_3)}.$$

Во избежание недоразумений отметим, что решение уравнения (8.6) не обязательно является именно $\wp$-функцией, хотя и тесно с ней связано (подробнее об этом — на следующей лекции).