

Эллиптические кривые

1. Обобщённая форма Вейерштрасса.

Вычисления в этом пункте основаны на теореме Римана-Роха. Пусть X - гладкая кривая над полем k рода g , D - дивизор на X , определённый над k . Обозначим $L(D)$ линейное подпространство в $k(X)$, состоящее из рациональных функций f таких, что $\operatorname{div}(f) + (D) \geq 0$, а через $|D|$ его проективизацию, находящуюся во взаимнооднозначном соответствии с множеством всех эффективных дивизоров, линейно эквивалентных D (это так называемая полная линейная система). $L(D)$ конечномерно, его размерность обозначим $l(D)$, она зависит только от класса линейной эквивалентности дивизора D . Пусть K - канонический класс дивизоров (т.е. класс эквивалентности дивизора любого дифференциала на X - последние образуют одномерное пространство над $k(X)$). Тогда

$$l(D) - l(K - D) = 1 - g + \deg D.$$

Если линейная система $|D|$ не имеет базисных точек (то есть на кривой не существует точки P , содержащейся в носителях всех дивизоров из $|D|$), то выбор базиса $f_1, \dots, f_{l(D)}$ в пространстве $L(D)$ определяет морфизм $X \rightarrow \mathbf{P}^{l(D)-1}$ (образ точки P будет иметь однородные координаты $f_1(P) : \dots : f_{l(D)}(P)$; если $P \in \operatorname{supp} D$, то для вычисления образа P надо помножить элементы базиса на соответствующую степень локального параметра).

- Лемма. 1) Если $\deg D \geq 2g - 1$, то $\dim |D| = \deg D - g$
2) Если $\deg D \geq 2g$, то $|D|$ не имеет базисных точек
3) Если $\deg D \geq 2g + 1$, то $|D|$ определяет регулярное вложение.

Действительно, из условия 1) следует, что $\deg(K - D) < 0$, а значит, в классе $(K - D)$ нет эффективных дивизоров (в этом случае дивизор D называется неспециальным),. Если выполнено условие 2) и существует базисная точка P (то есть все дивизоры из $|D|$ её содержат), то $L(D) = L(D - P)$, а это противоречит 1). Наконец, если выполнено 3), то $\forall P \in X$ никакая точка Q не является базисной для линейной системы $|D - P|$, а следовательно, в $L(D)$ содержится функция, равная нулю в P , но не равная ему в Q , в частности, при $Q = P$ имеющая в P нуль ровно первого порядка. Это означает, что степень морфизма, задаваемого линейной системой $|D|$, равна 1 и все точки образа простые.

Теорема - определение. Эллиптическая кривая E задается одним из эквивалентных определений:

- 1) Неособая кривая степени 3 в $\mathbf{P}^2(k)$ вместе с точкой $O \in E(k)$.
- 2) То же, но при этом O - точка перегиба.
- 3) Кривая E в $\mathbf{P}^2(k)$ (при условии, что она неособа), заданная уравнением $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$.
- 4) Неособая проективная кривая E рода 1 вместе с точкой $O \in E(k)$.

Доказательство. 1) $\Rightarrow$ 4 следует из формулы присоединения для рода плоской кривой степени d : $g = \frac{(d-1)(d-2)}{2}$.

3) $\Rightarrow$ 2 очевидно (точка $0 : 1 : 0$ является точкой перегиба). На самом деле, если $\text{char}(k) \neq 2$, то точки перегиба на кривой любой степени можно вычислить и непосредственно, добавляя к уравнению кривой $F(X, Y, Z) = 0$ условие равенства нулю гессиана - определителя, составленного из вторых частных производных F по координатам. Для кривой степени 3 это условие также имеет степень 3, поэтому на ней есть 9 точек перегиба (можно проверить, что при $\text{char}(k) \neq 3$ все они однократны), но при $k \neq \bar{k}$ они не обязательно определены над k .

4) $\Rightarrow$ 3. При $g = 1$ по теореме Римана-Роха $l(D) = \deg D$ для любого дивизора D . Поэтому $L(O)$ состоит из констант, $L(2(O)) = \langle 1, x \rangle$, $L(3(O)) = \langle 1, x, y \rangle$, при этом функции x и y имеют в O полюса порядка, соответственно, 2 и 3. Поскольку x^2 имеет там полюс порядка 4, x^2 не может линейно выражаться через $1, x$ и y , поэтому $L(4(O)) = \langle 1, x, y, x^2 \rangle$. Аналогично $L(5(O)) = \langle 1, x, y, x^2, xy \rangle$. Функции $1, x, y, x^2, xy, x^3, y^2$ все лежат в пространстве $L(6(O))$, размерность которого равна 6, поэтому они должны быть линейно зависимы, причем коэффициенты при x^3 и y^2 должны быть ненулевыми, так как только эти две функции имеют в (O) полюс шестого порядка. Домножая при необходимости x или y на константу, мы получим (в неоднородной форме) уравнение из 3). По п.3 предыдущей леммы линейная система $|3(O)|$ определяет регулярное вложение $E \rightarrow \mathbf{P}^2(k)$, которое в координатах при $P \neq O$ задается формулой $P \rightarrow x(P) : y(P) : 1$, а точка O переходит в $xt^3(O) : yt^3(O) : t(O)^3 = 0 : 1 : 0$, где t - локальный параметр в O ■

2. Групповой закон.

Мы будем пользоваться вариантом 4) определения. Пусть P и Q - не обязательно различные точки на E . Степень дивизора $D = (P) + (Q) - (O)$ равна 1, поэтому по п.1) леммы из предыдущего пункта $\dim |D| = 0$, а это означает, что существует

единственный эффективный дивизор, линейно эквивалентный D . Поскольку $\deg D = 1$, этот дивизор имеет вид (R) , где R - точка. Будем считать эту точку суммой точек P и Q . Аналогично, точка $-P$ соответствует единственному эффективному дивизору в классе $2(O) - (P)$.

Отображение $P \rightarrow cl((P)-(O))$, которое ставит в соответствие точке P класс линейной эквивалентности дивизора $(P)-(O)$, является биекцией множества точек на множество классов дивизоров степени 0. Действительно, дивизоры (P) и (Q) не могут лежать в одном классе эквивалентности по указанной лемме, а если $\deg D = 0$, то точка P такая, что $(P) \sim D + (O)$, однозначно восстанавливается по той же причине. Из определения в предыдущем абзаце сразу следует, что это отображение переводит сумму точек в сумму классов дивизоров, и поэтому операция суммирования определяет структуру абелевой группы на точках кривой E .

Теперь нужно доказать, что так определенный групповой закон является "алгебраическим". Для этого понадобится

Лемма. Пусть P и Q - точки на E (возможно, совпадающие). Тогда существует алгебраическая инволюция $\sigma : E \rightarrow E$ такая, что $\sigma(P) = Q$ и при этом $\forall R \in E$ $(R) + (\sigma(R)) \sim (P) + (Q)$.

Действительно, $\deg((P) + (Q)) = 2$, поэтому по п.2 леммы из предыдущего пункта линейная система $| (P) + (Q) |$ не имеет базисных точек и определяет морфизм $E \rightarrow \mathbf{P}^1$, который имеет степень 2 и сепарабелен, поскольку чисто несепарабельный морфизм не меняет род кривой. Сепарабельный морфизм степени 2 является накрытием Галуа, и в качестве σ можно взять единственный элемент группы Галуа.

Теорема. Отображения $P, Q \rightarrow P + Q : E \times E \rightarrow E$ и $R \rightarrow -R : E \rightarrow E$ являются морфизмами.

Доказательство. По лемме, примененной к точкам $P = Q = O$, $(\sigma(R)) + (R) \sim 2(O)$, откуда $-R = \sigma(R)$. Далее нетрудно видеть, что при вложении $E \rightarrow \mathbf{P}^2$, определяемом линейной системой $|3(O)|$, точку $-P - Q$ можно вычислить, как третью точку пересечения кривой E с прямой, проходящей через P и Q . Действительно, дивизоры, получающиеся как пересечения различных прямых в $\mathbf{P}^2$ с кривой E , очевидно, линейно эквивалентны, а бесконечноудаленная прямая трехкратно пересекается с E в точке O , поэтому если R - искомая третья точка пересечения, то $(P) + (Q) + (R) \sim 3(O)$, а из этого следует, что $R = -P - Q$. Ясно, что координаты R задаются рациональными функциями от координат P и Q и что рациональное отображение $(P, Q) \mapsto R$ всюду определено ■

Пример. Точки порядка 2. Точка P имеет порядок $2 \Leftrightarrow 2(P) \sim 2(O)$. Следовательно, все точки порядка 2 являются точками ветвления сепарабельного морфизма $E \rightarrow \mathbf{P}^1$ степени 2, заданного линейной системой $|2(O)|$, который уже упоминался в лемме. По формуле Гурвица $2g(E) - 2 = 2(2g(\mathbf{P}^1) - 2) + \sum_P v_P(\mathcal{D}_P)$, где P пробегает точки ветвления, а $\mathcal{D}_P$ - локальная дифферента. Если $\text{char}(k) \neq 2$, то ветвление может быть только слабым, а значит, в любой точке ветвления $v_P(\mathcal{D}_P) = e_P - 1 = 1$. Поэтому точек ветвления ровно 4, а значит, группа точек второго порядка $E_2(\bar{k})$ изоморфна $\mathbf{Z}/(2) \oplus \mathbf{Z}/(2)$ (координаты точек второго порядка не обязаны лежать в k).

Точки третьего порядка также просто описываются - это точки перегиба. При $\text{char}(k) \neq 3$ их ровно 9, и $E_3(\bar{k}) \simeq \mathbf{Z}/(3) \oplus \mathbf{Z}/(3)$. Позже мы увидим, что аналогичное утверждение верно для группы точек любого порядка, не делящегося на $\text{char}(k)$.

Справедливо также утверждение, отчасти обратное к доказанной выше теореме: если $f : (E, O) \rightarrow (E', O')$ - морфизм эллиптических кривых, переводящий O в O' , то он является гомоморфизмом групп. Действительно, $P + Q = R \Rightarrow (P) + (Q) \sim (R) + (O) \Rightarrow (f(P)) + (f(Q)) \sim (f(R)) + (f(O)) \Rightarrow f(P) + f(Q) = f(R)$ (на самом деле тот факт, что морфизм переводит линейно эквивалентные дивизоры в линейно эквивалентные, не вполне очевиден, но мы опустим доказательство).

3. Эллиптические кривые над $\mathbf{C}$.

Пусть L - решётка в $\mathbf{C}$. Определим $\wp$ -функцию Вейрштрасса формулой

$$\wp_L(z) = \sum_{w \in L, w \neq 0} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) + \frac{1}{z^2}.$$

Элементарно проверяется, что ряд сходится абсолютно и равномерно на компактах, не содержащих точек решетки, и определяет инвариантную относительно сдвигов на векторы решётки мероморфную функцию, голоморфную вне точек решетки L . Её производная

$$\wp'_L(z) = -2 \sum_{w \in L} \frac{1}{(z-w)^3}.$$

Разложение Лорана функции $\wp_L(z)$ в нуле имеет вид

$$\wp_L(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) \gamma_{2k+2}(L) z^{2k},$$

где $\gamma_n(L) \stackrel{\text{def}}{=} \sum_{w \in L, w \neq 0} \frac{1}{w^n}$ (ряд сходится абсолютно при четных $n \geq 4$ и равен нулю

при нечетных n ; ср. с определением ряда Эйзенштейна). Соответственно,

$$\wp'_L(z) = -\frac{2}{z^3} + \sum_{k=1}^{\infty} 2k(2k+1)\gamma_{2k+2}(L)z^{2k-1}$$

Функция $\wp_L(z)$ является четной, а $\wp'_L(z)$ нечетной.

С точностью до прибавления функций, обращающихся в 0 в $z = 0$, $\wp_L(z) = \frac{1}{z^2}$, $\wp_L(z)^3 = \frac{1}{z^6} + 9\gamma_4(L)\frac{1}{z^2} + 15\gamma_6(L)$, $\wp_L(z)^2 = \frac{4}{z^6} - 24\gamma_4(L)\frac{1}{z^2} - 80\gamma_6(L)$.

Следовательно, функция $\wp_L'^2 - 4\wp_L^3 + 60\gamma_4(L)\wp_L + 140\gamma_6(L)$ инвариантна относительно сдвигов на векторы L , обращается в нуль при $z = 0$, а значит, и во всех точках L , и тем самым всюду голоморфна. Следовательно, она тождественно равна нулю, и мы видим, что функции $\wp_L$ и $\wp'_L$ связаны уравнением (оно называется уравнением Вейерштрасса), которое является практически частным случаем уравнения из п.1 (в аффинной форме). Чтобы убедиться в том, что кривая, задаваемая этим уравнением, эллиптическая, достаточно проверить её невырожденность.

Пусть $g_2 = 60\gamma_4(L)$, а $g_3 = 140\gamma_6(L)$ (это традиционные обозначения). Кривая, в аффинной форме задаваемая уравнением $y^2 = 4x^3 - g_2x - g_3$, в бесконечной точке всегда невырождена, а на $\mathbf{C}^2$ не имеет особых точек тогда и только тогда, когда $\Delta \neq 0$, где Δ - дискриминант кубического полинома в правой части. $\Delta = g_2^3 - 27g_3^2 = 16 \prod_{i \neq j} (e_i - e_j)^2$, а e_i - корни полинома. Из предыдущего раздела мы знаем, что модулярная форма $\Delta(z)$ нигде не обращается в нуль. Решетка L подобна решетке $\langle z, 1 \rangle$ при некотором z , и наш дискриминант отличается от $\Delta(z)$ умножением на ненулевую константу.

Невырожденность кривой можно проверить и непосредственно.

Пусть f - эллиптическая функция (по определению, это означает, что f - мероморфная функция на $\mathbf{C}$, инвариантная относительно сдвигов на векторы решетки L). Если Π - фундаментальный параллелограмм L , граница которого не содержит нулей и полюсов f , то справедливы равенства:

$$1) \sum_{P \in \Pi} \text{ord}_P f = 0; 2) \sum_{P \in \Pi} (\text{ord}_P f)P \equiv 0 \pmod{L}; 3) \sum_{P \in \Pi} \text{res}_P f = 0.$$

Доказательство сразу получается интегрированием по границе Π , соответственно, $d \log f$, $z d \log f$ и df .

Функция $\wp'_L$ имеет тройные полюса в точках L и больше полюсов не имеет. Она L - инвариантна и нечетна и поэтому обращается в нуль в точках $w_1/2, w_2/2$ и $w_3/2 = (w_1 + w_2)/2$, где (w_1, w_2) - какой-нибудь базис L . Из свойства 1) предыдущего абзаца

следует, что все эти нули простые и больше нулей (по модулю L) у $\wp'_L$ нет. Далее, по определению $\wp_L(w_i/2) = e_i$, следовательно, функция $\wp_L(z) - e_i$ обращается в точке $z = w_i/2$ в нуль, причем этот нуль двойной (ибо $\wp'_L(w_i/2) = 0$), а значит, других нулей у этой функции нет (она мероморфна с двойными полюсами только в точках L). Это показывает, что все e_i различны и ещё раз подтверждает невырожденность кривой.

Проведенные вычисления позволяют легко проверить, что поле эллиптических функций для решетки L алгебраически порождается функциями $\wp_L$ и $\wp'_L$. Пусть f - такая функция. Её можно представить в виде суммы чётной и нечётной, так что можно считать, что f - чётна, и достаточно проверить, что она есть рациональная дробь от $\wp_L$. Рассмотрим функцию $g(z) \stackrel{\text{def}}{=} \prod (\wp_L(z) - \wp_L(u_i))^{m_i}$. Здесь точки u_i пробегают полный набор представителей $\bmod L$ нулей и полюсов функции f , но из каждой пары противоположных по знаку представителей выбирается только один, а если представитель лежит в L , то он вообще не учитывается. Показатели m_i суть порядки f в u_i , но при этом если $2u_i \in L$, то порядок считается с кратностью $1/2$. Легко видеть, что дивизоры функций f и g совпадают вне L , а значит, и с учетом точек L тоже (поскольку дивизор функции должен иметь нулевую степень). Это означает, что поделив f на g , мы получим эллиптическую функцию с нулевым дивизором, то есть константу.

Естественная проекция $\pi : \mathbf{C} \rightarrow E(\mathbf{C})$, где E - эллиптическая кривая, построенная выше по решетке L , является сюръективным гомоморфизмом групп с ядром L . Действительно, при любом $c \in \mathbf{C}$ функция $\wp_L(z) - c$ имеет по модулю L один или два нуля, в последнем случае нули имеют вид $z = u$ и $z = -u$, и они простые, так что нечётная функция $\wp'_L(z)$ принимает в них разные значения. Это доказывает, что отображение $\mathbf{C}/L \rightarrow E(\mathbf{C})$ взаимнооднозначно (0 при этом переходит в бесконечноудаленную точку O). Условие $P + Q = R$ на $E(\mathbf{C})$ эквивалентно условию $(P) + (Q) \sim (R) + (O)$, которое, в свою очередь, эквивалентно существованию эллиптической функции f такой, что $\text{div}(f) = (\pi^{-1}(P)) + (\pi^{-1}(Q)) - (\pi^{-1}(R) - (0)) \bmod L$, и утверждение о гомоморфности теперь следует из свойства 2) тремя абзацами выше.

В заключение отметим, что на кривой E , заданной уравнением $y^2 = 4x^3 - g_2x - g_3$, x -координата суммы P_3 точек P_1 и P_2 задается уравнением $x_3 = -x_1 - x_2 + \frac{1}{4} \left(\frac{y_1 - y_2}{x_1 - x_2} \right)^2$ при $P_1 \neq P_2$ и уравнением $x_3 = -2x_1 + \frac{1}{4} \left(\frac{6x_1^2 - g_3/2}{y_1} \right)^2$ при $P_1 = P_2$, а точка $-P$ получается из точки P изменением знака y -координаты.