Геометрия эллиптических кривых

Задача 1 (особые кубики). Пусть E/K — особая кубика в форме Вейерштрасса. Обозначим через E_{ns} множество неособых точек E.

a) Покажите, что E_{ns} является группой при стандартном определении операции с помощью касательных и секущих.

b) Пусть E имеет особую точку типа node и касательные $y = \alpha_i x + \beta_i$ в ней. Убедитесь, что, если $\alpha_1 \in K$, то $\alpha_2 \in K$ и $E_{ns}(K) \cong K^\times$.

c) В предположениях предыдущего пункта допустим, что $\alpha_1 \notin K$. Убедитесь, что $L = K(\alpha_1, \alpha_2)$ — квадратичное расширение K, $E_{ns}(L) \cong L^\times$ и $E_{ns}(K) \cong \{t \in L^\times \mid N_{L/K}(t) = 1\}$.

d) Пусть E имеет особую точку типа cusp. Покажите, что $E_{ns}(K) \cong K^+$ (поле K как группа по сложению).

Подсказка: в случае алгебраически замкнутого поля K можно воспользоваться отображениями $(x, y) \mapsto \frac{y-\alpha_1 x-\beta_1}{y-\alpha_2 x-\beta_2}$ для node'а и $(x, y) \mapsto \frac{x-x_0}{y-\alpha x-\beta}$ для cusp'а (x_0 — это x-координата особой точки, а $y = \alpha x + \beta$ — касательная в ней). Для упрощения вычислений особую точку можно перенести в $(0, 0)$.

Задача 2 (группа автоморфизмов). Пусть E/K — эллиптическая кривая, а $\mathrm{Aut}(E) = \mathrm{Aut}_{\bar K}(E)$ — группа её $\bar K$-автоморфизмов. Покажите, что

a) Если $j(E) \neq 0, 1728$, то $\mathrm{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$.

b) Пусть $\mathrm{char}\, K \neq 2, 3$. Тогда $\mathrm{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$, если $j(E) = 1728$, и $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$, если $j(E) = 0$.

c) Пусть $\mathrm{char}\, K = 3$, а $j(E) = 0 = 1728$. Тогда $\mathrm{Aut}(E) \cong \mathbb{Z}/3\mathbb{Z} \leftthreetimes \mathbb{Z}/4\mathbb{Z}$ (полупрямое произведение, в котором образующая $\mathbb{Z}/4\mathbb{Z}$ действует нетривиально на нормальную подгруппу $\mathbb{Z}/3\mathbb{Z}$, переводя каждый элемент в обратный ему).

d) Пусть $\mathrm{char}\, K = 2$, а $j(E) = 0 = 1728$. Тогда $\mathrm{Aut}(E) \cong SL_2(\mathbb{F}_3)$.

e) Пусть $m \geq 2$ взаимно просто с $\mathrm{char}\, K$. Не используя классификации групп автоморфизмов эллиптических кривых, докажите, что отображение $\mathrm{Aut}(E) \to \mathrm{Aut}(E[m])$ инъективно при $m \neq 2$ и имеет ядро $[\pm 1]$, когда $m = 2$.

Задача 3 (кривые рода 1). Пусть $C/\bar K$ — кривая рода 1. Для каждой точки $O \in C(\bar K)$ для эллиптической кривой (C, O) определен её j-инвариант $j(C, O)$.

a) Пусть (C, O) и (C', O') — кривые рода 1 с выбранными начальными точками. Предположим, что имеется такой изоморфизм кривых $\phi\colon C \longrightarrow C'$, что $\phi(O) = O'$. Докажите, что $j(C, O) = j(C', O')$.

Подсказка: j-инвариант, определённый через коэффициенты уравнения Вейерштрасса, не зависит от выбора уравнения.

b) Докажите, что для любых двух точек $O, O' \in C$ существует автоморфизм C, переводящий O в O'. Выведите отсюда, что $j(C, O) = j(C, O')$.

c) Пусть далее C — кривая рода 1, определённая над K. Докажите, что $j(C) \in K$.

d) Докажите, что C/K всегда изоморфна над $\bar K$ какой-то эллиптической кривой, определённой над K.

Задача 4 (многочлены деления). Пусть E/K задаётся уравнением Вейерштрасса

$$E\colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

и пусть b_2, b_4, b_6, b_8 — выражения от a_i, определённые в прошлом листке (для простоты можно сначала предполагать, что $\mathrm{char}\, K \neq 2, 3$, и уравнение имеет вид $y^2 = x^3 + Ax + B$.) Определим многочлены деления $\psi_m \in \mathbb{Z}[a_1, \ldots, a_6, x, y]$ начальными значениями

$$\psi_1 = 1, \quad \psi_2 = 2y + a_1 x + a_3, \quad \psi_3 = 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8,$$

$$\psi_4 = \psi_2 \cdot (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),$$

и далее индуктивно по формулам:

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \qquad \text{если } m \geq 2,$$

$$\psi_2\psi_{2m} = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2, \quad \text{если } m \geq 3.$$

Определим далее многочлены ϕ_m и ω_m следующим образом:

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \quad 4y\omega_m = \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.$$

a) Докажите, что при нечётном (соответственно, чётном) m многочлены ψ_m, ϕ_m и $y^{-1}\omega_m$ (соответственно, $(2y)^{-1}\psi_m\phi_m$ и ω_m) принадлежат $\mathbb{Z}[a_1, \ldots, a_6, x, (2y + a_1x + a_3)^2]$.
Таким образом, заменяя $(2y+a_1x+a_3)^2$ на $4x^3+b_2x^2+2b_4x+b_6$, мы можем считать каждую из этих величин многочленом из $\mathbb{Z}[a_1, \ldots, a_6, x]$.

b) Покажите, что, как многочлены от x, ψ_m, ϕ_m имеют старший член x^{m^2} и $m^2x^{m^2-1}$ соответственно.

c) Докажите, что при $\Delta \neq 0$ (т. е. E — эллиптическая кривая) $\phi_m(x)$ и $\psi_m(x)$ — взаимно простые многочлены в $K[x]$.

d) В предположении, что $\Delta \neq 0$, докажите, что для любой точки $P = (x_0, y_0) \in E$ справедливо равенство $[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right)$.

e) Докажите, что отображение $[m]\colon E \longrightarrow E$ имеет степень m^2.

f) Докажите, что функция $\psi_n \in K(E)$ имеет дивизор $\operatorname{div}(\psi_n) = \sum\limits_{T \in E[n]} (T) - n^2(O)$. Таким образом, ψ_n обращается в ноль в точности в нетривиальных точках n-кручения и имеет соответствующий полюс в O.

Задача 5 (точки порядка 3). Пусть $\operatorname{char} K \neq 2, 3$, E/K — эллиптическая кривая с однородным уравнением Вейерштрасса $F(X_0, X_1, X_2) = X_1^2X_2 - X_0^3 - AX_0X_2^2 - BX_2^3 = 0$, $x = \frac{X_0}{X_2}$ и $y = \frac{X_1}{X_2}$ — соответствующие аффинные координаты. Пусть $P \in E$.

a) Докажите, что $[3]P = O$ тогда и только тогда, когда касательная к E в точке P пересекает E только в P.

b) Выведите, что $[3]P = O$ равносильно обращению в ноль определителя гессиана $\left(\frac{\partial F}{\partial X_iX_j}(P)\right)$.

c) Докажите, что $E[3]$ состоит из девяти точек.

Задача 6 (вложения кривых). Пусть C — гладкая кривая рода g и $n \geq 2g + 1$ — целое число. Выберем базис $\{f_0, \ldots, f_m\}$ в $\mathcal{L}(n(P_0))$ и определим отображение

$$\phi = [f_0, \ldots, f_m]\colon C \longrightarrow \mathbb{P}^m.$$

a) Докажите, что образ $C' = \phi(C)$ — кривая в $\mathbb{P}^m$.

b) Докажите, что отображение $\phi\colon C \longrightarrow C'$ имеет степень 1.

c*) Докажите, что C' — гладкая и что $\phi\colon C \longrightarrow C'$ — изоморфизм.

Задача 7 (эллиптические кривые в $\mathbb{P}^3$). Пусть E/K — эллиптическая кривая, заданная уравнением Вейерштрасса.

a) Покажите, что $\phi :: E \to \mathbb{P}^3$, $\phi = [1, x, y, x^2]$ изоморфно отображает E на пересечение квадратичных поверхностей в $\mathbb{P}^3$.

b) Выведите из этого, что, если $H \subset \mathbb{P}^3$ — плоскость, то $H \cap \phi(E)$ состоит из 4 точек (считая кратности). Убедитесь, что $\phi(O) = [0, 0, 0, 1]$ и плоскость $T_0 = 0$ пересекает $\phi(E)$ в единственной точке $\phi(O)$ с кратностью 4.

c) Пусть $P, Q, R, S \in E$. Докажите, что $P + Q + R + S = O$ тогда и только тогда, когда $\phi(P)$, $\phi(Q)$, $\phi(R)$, $\phi(S)$ лежат в одной плоскости (т. е. существует такая плоскость H, что с учётом кратностей пересечение $H \cap E$ состоит из точек $\phi(P)$, $\phi(Q)$, $\phi(R)$, $\phi(S)$).

d) Пусть $P \in E$. Покажите, что $[4]P = O$ тогда и только тогда, когда существует такая плоскость $H \subset \mathbb{P}^3$, что $H \cap \phi(E) = P$.

e) Покажите, что, если $\operatorname{char} K \neq 2$, то имеется ровно 16 таких точек, что $[4]P = O$.

f) Пусть $\operatorname{char} K \neq 2$. Покажите, что существует линейная замена переменных над $\bar{k}$, приводящая уравнения E в $\mathbb{P}^3$ к виду $T_0^2 + T_2^2 = T_0T_3$, $T_1^2 + \alpha T_2^2 = T_2T_3$. Для каких α данная кривая неособая? Какой её j-инвариант?

g) Используя модель из предыдущего пункта, выведите явные формулы для $-P$, $P_1 + P_2$ и $[2]P$ (в координатах в $\mathbb{P}^3$).

Задача 8* (эллиптические кривые в $\mathbb{P}^n$). Пусть E/K — эллиптическая кривая. Выберем базис $f_1, \ldots, f_m$ в $\mathcal{L}(m(O))$. Для $m \geq 3$ из задачи про вложения кривых следует, что отображение $\phi = [f_1, \ldots, f_m] \colon E \longrightarrow \mathbb{P}^{m-1}$ — изоморфизм E на её образ.

a) Покажите, что $\phi(E)$ — кривая степени m, то есть, что пересечение $\phi(E)$ и гиперплоскости состоит из m точек, считая кратности.

Подсказка: Найдите гиперплоскость, пересекающую $\phi(E)$ в единственной точке $\phi(O)$ и покажите, что это пересечение кратности m.

b) Пусть $P_1, \ldots, P_m \in E$. Докажите, что $P_1 + \ldots + P_m = O$ тогда и только тогда, когда $\phi(P_1), \ldots, \phi(P_m)$ лежат в гиперплоскости (если какие-то P_i совпадают, то гиперплоскость обязана пересекать $\phi(E)$ с большими кратностями в соответствующих точках).

c) Пусть $P \in E$. Докажите, что $[m]P = O$ тогда и только тогда, когда существует такая гиперплоскость $H \subset \mathbb{P}^{m-1}$, что $H \cap \phi(E) = P$. При $\operatorname{char} K > m$, докажите, что таких точек ровно m^2. Используйте это, чтобы заключить, что $\deg[m] = m^2$.

Задача 9 (факторизация по группе автоморфизмов). Пусть $C/\bar{K}$ — гладкая кривая, а Φ — конечная группа автоморфизмов C. Элементы $\alpha \in \Phi$ действуют на $\bar{K}(C)$ следующим образом: $\alpha^*(f) = f \circ \alpha$, где $f \in \bar{K}(C)$.

a) Докажите, что существует единственная гладкая кривая $C'/\bar{K}$ и такой конечный сепарабельный морфизм $\phi \colon C \longrightarrow C'$, что $\phi^*\bar{K}(C') = \bar{K}(C)^\Phi$, где $\bar{K}(C)^\Phi$ обозначает подполе в $\bar{K}(C)$, инвариантное относительно всех элементов Φ.

b) Пусть $P \in C$. Докажите, что $e_\phi(P) = \#\{\alpha \in \Phi \mid \alpha(P) = P\}$.

c) Выразите род C' через род C, количество элементов в Φ через число неподвижных точек элементов из Φ.

d*) Предположим, что C определена над K и что Φ — $G_{\bar{K}/K}$-инвариантна (т. е. для всех $\alpha \in \Phi$ и всех $\sigma \in G_{\bar{K}/K}$ имеем $\alpha^\sigma \in \Phi$). Докажите, что можно подобрать C' и ϕ из пункта a) так, чтобы они были определены над K. Докажите, что C' единственна с точностью до изоморфизма над K.

Задача 10. Пусть E_1/K и E_2/K — эллиптические кривые и пусть $\phi \colon E_1 \longrightarrow E_2$ — изогения степени m, определённая над K, где m взаимно просто с $\operatorname{char} K$, если $\operatorname{char} K > 0$.

a) Аналогично тому, что было на лекции, постройте спаривание $e_\phi \colon \ker\phi \times \ker\hat{\phi} \longrightarrow \mu_m$.

b) Докажите, что e_ϕ билинейно, невырождено и инвариантно относительно действия группы Галуа.

c) Докажите, что, если $\psi \colon E_2 \longrightarrow E_3$ — другая изогения, то $e_{\psi\circ\phi}(P, Q) = e_\psi(\phi(P), Q)$ для всех $P \in \ker(\psi \circ \phi)$ и $Q \in \ker(\hat{\psi})$.

Задача 11 (другое определение спаривания Вейля). Пусть E — эллиптическая кривая. Определим спаривание $\tilde{e}_m \colon E[m] \times E[m] \longrightarrow \mu_m$ следующим образом: пусть $P, Q \in E[m]$, выберем дивизоры с непересекающимися носителями D_P и D_Q в $\operatorname{Div}^0(E)$, сумма

точек из которых равна P и Q соответственно. Поскольку P и Q имеют порядок m, существуют такие функции $f_P, f_Q \in \bar{K}(E)$, что $\operatorname{div}(f_P) = mD_P$ и $\operatorname{div}(f_Q) = mD_Q$. Определим $\tilde{e}_m(P,Q) = \frac{f_P(D_Q)}{f_Q(D_P)}$.

a) Докажите, что $\tilde{e}_m(P,Q)$ определено корректно, то есть его значения зависят только от P и Q и не зависят от различных выборов D_P, D_Q, f_P и f_Q.

Подсказка: используйте закон взаимности Вейля из листка 1.

b) Докажите, что $\tilde{e}_m(P,Q) \in \mu_m$.

c) Докажите, что $\tilde{e}_m = e_m$, где e_m — спаривание Вейля, определённое на лекции.

Задача 12 (двойственные изогении в произвольной характеристике). Пусть E/K — эллиптическая кривая, $\operatorname{char} K \neq 2$.

a) Используя явные формулы, докажите, что отображение удвоения $[2]\colon E \longrightarrow E$ имеет степень 4. Выведите отсюда, что $\deg[2^n] = 4^n$ для всех $n \geq 1$.

b) Докажите, что $\#E[2^n] = 4^n$ для всех $n \geq 1$ (здесь мы используем предположение, что $\operatorname{char} K \neq 2$). Заключите, что $E[2^n] \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ для всех $n \geq 1$.

c) Проверьте, что доказательство существования двойственных изогений справедливо в любой характеристике.

d) Предположим, что m — число, для которого известно, что $\#E[m] = m^2$. Покажите, что этого достаточно, чтобы доказать существование и основные свойства спаривания Вейля $e_m\colon E[m] \times E[m] \to \mu_m$.

e) Пусть $\phi\colon E_1 \longrightarrow E_2$ и $\psi\colon E_1 \longrightarrow E_2$ — изогении эллиптических кривых. Пусть $m = 2^n$, так что мы знаем существование спаривания Вейля e_m на E_1 и E_2. Пусть $T_1 \in E_1[m]$ и $T_2 \in E_2[m]$ — точки m-деления. Используя свойства спаривания Вейля, докажите, что

$$e_m\left(T_1, \widehat{(\phi+\psi)}(T_2)\right) = e_m\left(T_1, \hat{\phi}(T_2) + \hat{\psi}(T_2)\right).$$

Используйте невырожденность спаривания Вейля, чтобы заключите, что $\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$.

f) Получите, что $\widehat{[m]} = [m]$ и $\deg[m] = m^2$ для всех целых m.

g) Пусть m — целое число и $m \neq 0$ в K. Докажите, что $\#E[m] = m^2$ и заметьте, что пункт d) даёт существование и основные свойства спаривания Вейля.

h) Если $\operatorname{char} K = 2$, докажите прямым вычислением, что $\deg[3] = 9$. Проделайте предыдущие пункты упражнения, заменяя 2^n на 3^n.

Задача 13. Пусть E/K — эллиптическая кривая с комплексным умножением над K, то есть такая, что $\operatorname{End}_K(E)$ строго больше, чем $\mathbb{Z}$. Докажите, что для всех простых $l \neq \operatorname{char} K$ действие $G_{\bar{K}/K}$ на модуле Тейта $T_l(E)$ абелево (т. е. образ $G_{\bar{K}/K}$ в $\mathrm{GL}_2(\mathbb{Q}_l)$ — коммутативная подгруппа).

Подсказка: Используйте тот факт, что эндоморфизмы из $\operatorname{End}_K(E)$ *коммутируют с действием* $G_{\bar{K}/K}$ *на* $T_l(E)$.

Задача 14*. Пусть E/K — эллиптическая кривая и предположим, что $\mathcal{K} = \operatorname{End}(E) \otimes \mathbb{Q}$ — алгебра кватернионов.

a) Докажите, что, если $p \neq \infty$ и $p \neq \operatorname{char} K$, то $\mathcal{K}$ расщепляется в p, т.е. $\mathcal{K} \otimes \mathbb{Q}_p \cong \mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$.

b) Заключите, что $\operatorname{char} K > 0$.

c) Докажите, что $\mathcal{K}$ — единственная алгебра кватернионов (некоммутативная алгебра с делением размерности 4), разветвленная (т. е. не расщепляющаяся) в ∞ и $\operatorname{char} K$ и больше нигде.

d) Докажите, что $\operatorname{End}(E)$ — максимальный порядок в $\mathcal{K}$ (в отличие от числовых полей, в алгебрах кватернионов может быть более одного максимального порядка).