Слабая теорема Морделла–Вейля и главные однородные пространства

Задача 1° (явный m-спуск). Пусть E/K — эллиптическая кривая над полем алгебраических чисел K и пусть $E[m] \subset E(K)$. Докажите следующее:

a) Существует билинейной спаривание $b\colon E(K)/mE(K) \times E[m] \to K(S,m)$, определяемое соотношением $e_m(\delta_E(P), T) = \delta_K(b(P,T))$. Здесь e_m — спаривание Вейля, $\delta_m\colon E(K) \to H^1(G_K, E[m])$ и $\delta_K\colon K^\times \to H^1(G_K, \mu_m)$ — связывающие гомоморфизмы, $K(S,m) = \{b \in K^\times/(K^\times)^m \mid \mathrm{ord}_v(b) \equiv 0 \mod m \text{ для } v \notin S\}$, а S— множество нормирований, содержащее все архимедовы нормирования, простые плохой редукции для E и простые, делящие m.

b) Спаривание из (a) невырождено слева.

c) Спаривание может быть вычислено следующим образом. Для $T \in E[m]$ возьмём такие функции $f_T, g_T \in K(E)$, что $\mathrm{div}(f_T) = m(T) - m(O)$ и $f_T \circ [m] = g_T^m$ (их существование следует из определения спаривания Вейля). Тогда $b(P,T) = f_T(P) \mod (K^\times)^m$ для всех $P \neq O, T$. Как вычислить $b(P,T)$ при $P = O, T$?

d) Пусть T_1, T_2 — базис $E[m]$, тем самым зафиксировано отождествление $H^1(G_K, E[m]; S) = K(S,m) \times K(S,m)$. Тогда уравнения $b_1 z_1^m = f_{T_1}(P)$, $b_2 z_2^m = f_{T_2}(P)$ вместе с условием $P \in E$ задают главное однородное пространство, соответствующее коциклу (b_1, b_2).

Подсказка: изоморфизм E с однородным пространством, определённый над $\bar{K}$, переводит P в $[m]P$, а $z_1 = b_1^{-1/m} g_{T_1}(P)$, $z_2 = b_2^{-1/m} g_{T_2}(P)$.

e) Для $m = 2$ и эллиптической кривой $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$ можно взять $f_T = x - e$, если $T = (e, 0)$. Таким образом, мы получаем инъективный инъективный гомоморфизм $E(K) \to K(S,2) \times K(S,2)$:

$$P = (x,y) \mapsto \begin{cases} (x-e_1, x-e_2), & \text{если } x \neq e_1, e_2, \\ \left(\frac{e_1-e_3}{e_1-e_2}, e_1 - e_2\right), & \text{если } x = e_1, \\ \left(e_2 - e_1, \frac{e_2-e_3}{e_2-e_1}\right), & \text{если } x = e_2, \\ (1,1), & \text{если } x = \infty. \end{cases}$$

Это утверждение можно доказать и непосредственно, что даёт простое доказательство конечности $E(K)/2E(K)$ (см. Кнапп "Эллиптические кривые").

f) Уравнение соответствующих главных однородных пространств при $m = 2$ будет $b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1$, $b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1$. Таким образом, $P \in E(K)/2E(K)$ тогда и только тогда, когда эти уравнения имеют решение $(z_1, z_2, z_3) \in K^\times \times K^\times \times K$. Если такое решение есть, то $P = (b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3)$.

Задача 2 (явный ϕ-спуск). Пусть $\phi\colon E/K \to E'/K$ — изогения степени m эллиптических кривых, определённая над числовым полем K. Предположим, что $E[\phi] \subset E(K)$. Докажите следующее:

a) Существует невырожденное слева билинейной спаривание $b\colon E'(K)/\phi(E(K)) \times E'[\hat{\phi}] \to K(S,m)$, определяемое соотношением $e_\phi(\delta_\phi(P), T) = \delta_K(b(P,T))$. Здесь e_ϕ — обобщённое спаривание Вейля (см. листок 3, задача 10), а $\delta_\phi\colon E'(K) \to H^1(G_K, E[\phi])$ и $\delta_K\colon K^\times \to H^1(G_K, \mu_m)$ — связывающие гомоморфизмы.

b) Для $T \in E[\hat{\phi}]$ возьмём такие функции $f_T \in K(E')$ и $g_T \in K(E)$, что $\mathrm{div}(f_T) = m(T) - m(O)$ и $f_T \circ \phi = g_T^m$. Тогда $b(P,T) = f_T(P) \mod (K^\times)^m$ для всех $P \neq O, T$.

c) Запишите уравнение однородного пространства, соответствующего элементу $b \in K(S,m)$.

d) В частности, если $\deg(\phi) = 2$ и $E'[\hat{\phi}] = \{O, T\}$, то $b(P,T) = x(P) - x(T) \mod (K^\times)^2$ и мы получаем формулы для спуска с использованием 2-изогений, обсуждавшиеся на лекциях.

Задача 3. Посчитайте $E(\mathbb{Q})/2E(\mathbb{Q})$ для следующих эллиптических кривых:
$a^\circ)\, y^2 = x(x-1)(x+3)$; $b^\circ)\, y^2 = x(x-12)(x-36)$;
$c^\circ)\, y^2 = x^3 + 6x^2 + x$; $d^\circ)\, y^2 = x^3 + 14x^2 + x$; $e^\circ)\, y^2 = x^3 + 9x^2 - x$;
$f^*)\, y^2 + y = x^3 - x$.

Задача 4°. Пусть E/K — эллиптическая кривая, определённая над полем характеристики $\neq 2, 3$. Зафиксируем уравнение Вейерштрасса для E/K и, в предположении, что $j(E) \neq 0, 1728$, определим $\gamma(E/K) = -c_4/c_6 \in K^\times/(K^\times)^2$.

a) Докажите, что $\gamma(E/K)$ не зависит от выбора уравнения Вейерштрасса для E/K.

b) Пусть E'/K — другая эллиптическая кривая с $j(E) \neq 0, 1728$. Докажите, что E и E' изоморфны над K тогда и только тогда, когда $j(E) = j(E')$ и $\gamma(E/K) = \gamma(E'/K)$.

c) Если $j(E) = j(E') \neq 0, 1728$, докажите, что E и E' изоморфны над полем $K\left(\sqrt{\frac{\gamma(E/K)}{\gamma(E'/K)}}\right)$.

Задача 5. Пусть K — поле характеристики 2 и E/K — кривая с $j(E) \neq 0$, задаваемая уравнением Вейерштрасса $y^2 + xy = x^3 + a_2x^2 + a_6$. Пусть $\xi \in H^1(G_K, \mathrm{Aut}(E)) = \mathrm{Hom}(G_K, \mathbb{Z}/2\mathbb{Z})$ и L/K — квадратичное расширение, отвечающее характеру ξ. Пусть L/K, являющееся расширением Артина–Шрайера, порождается корнем многочлена $t^2 - t - D = 0$, $D \in K$. Докажите, что скрутка E посредством ξ задаётся уравнением $y^2 + xy = x^3 + (a_2 + D)x^2 + a_6$.

Задача 6. Пусть E/K и E'/K — эллиптические кривые над (не обязательно совершенным) полем K. Предположим, что $j(E) = j(E')$. Докажите, что E и E' изоморфны над сепарабельным расширением L поля K, степень которого делит 24. Если $j(E) \neq 0, 1728$, докажите, что L может быть выбрано имеющим степень 2.

Задача 7. Пусть E/K — эллиптическая кривая, $\xi \in H^1(G_K, \mathrm{Aut}(E))$ и пусть E_ξ — скрутка E, отвечающая ξ. Пусть $v \in M_K$ — неархимедово нормирование, в котором E имеет хорошую редукцию. Докажите, что E_ξ имеет хорошую редукцию в v, если и только если коцикл ξ неразветвлён в v.

Подсказка: если характеристика поля вычетов не равна 2 *или* 3, *можно использовать явные уравнения, в общем случае используйте критерий Нерона–Огга–Шафаревича.*

Задача 8. Пусть E/K — эллиптическая кривая, $D \in K^\times$, $L = K(\sqrt{D})$ — квадратичное расширение, и пусть E_D/K — соответствующая квадратичная скрутка E. Докажите, что $\mathrm{rk}E(L) = \mathrm{rk}E(K) + \mathrm{rk}E_D(K)$.

Задача 9 (групповая структура на WC**).** Пусть E/K — эллиптическая кривая над совершенным полем K и пусть C_1/K и C_2/K — однородные пространства для E/K.

a) Докажите, что существует однородное пространство C_3/K для E/K и морфизм $\phi\colon C_1 \times C_2 \to C_3$, определённый над K и такой, что для всех $p_1 \in C_1, p_2 \in C_2$ и $P_1, P_2 \in E$ имеем $\phi(p_1 + P_1, p_2 + P_2) = \phi(p_1, p_2) + P_1 + P_2$.

Подсказка: $C_3 = C_1 \times C_2/$(*диагональное действие* E).

b) Докажите, что C_3 однозначно определено с точностью до эквивалентности однородных пространств.

c) Покажите, что $\{C_1\} + \{C_2\} = \{C_3\}$ в смысле суммы в $\mathrm{WC}(E/K)$.

Задача 10 (геометрическая интерпретация $H^1(K, E[m])$). Назовём m-накрытием пару $(C, \alpha)/K$, состоящую из главного однородного пространства для E и регулярного отображения $\alpha\colon C \to E$ (определённого над K), удовлетворяющую условию: найдется такое $w_1 \in C(\bar{K})$, что $\alpha(w_1 + P) = mP$ для всех $P \in E(\bar{K})$. Морфизм $(C, \alpha) \to (C', \alpha')$ m-накрытий есть такой морфизм $\phi\colon C \to C'$ главных однородных пространств, что $\alpha = \alpha' \circ \phi$.

a) Покажите, что имеется естественная биекция между множеством m-накрытий и $H^1(K, E[m])$.

b) Придумайте аналогичную интерпретацию $H^1(K, E[\phi])$ для изогении $\phi\colon E \to E'$.

Задача 11° (кривые рода 1 и однородные пространства). Пусть C/K — кривая рода один над совершенным полем.

a) Докажите, что существует такая эллиптическая кривая E/K, что C — однородное пространство для E.

Подсказка: используйте задачу 3 из листка 3, чтобы показать, что $C \in \mathrm{Twist}(E/K)$. Затем найдите такой элемент $\{\xi\} \in H^1(G_K, \mathrm{Aut}(E))$, что C является однородным пространством для скрутки E посредством ξ.

b) Докажите, что E единственна с точностью до K-изоморфизма.

Задача 12 (группа Пикара главного однородного пространства). Пусть C/K — однородное пространство для эллиптической кривой E/K. Выберем точку $p_0 \in C$ и рассмотрим отображение $\mathrm{sum}\colon \mathrm{Div}^0(C) \to E$, при котором $\sum n_i(p_i) \mapsto \sum [n_i](p_i - p_0)$. Докажите, что

a) Существует точная последовательность $1 \to \bar{K}^\times \to \bar{K}(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \xrightarrow{\mathrm{sum}} E \to 0$.

b) Отображение суммирования не зависит от выбора точки p_0.

c) Отображение суммирования коммутирует с естественным действием группы Галуа G_K на $\mathrm{Div}^0(C)$ и E, а значит индуцирует изоморфизм G_K-модулей $\mathrm{sum}\colon \mathrm{Pic}^0(C) \xrightarrow{\sim} E$. В частности, $\mathrm{Pic}^0_K(C) \cong E(K)$.

Эта конструкция имеет важное обобщение — по кривой C можно аналогичным образом построить её якобиан, являющийся абелевым многообразием размерности, равной роду C.

Задача 13. Пусть E/K — эллиптическая кривая над совершенным полем K.

a) Докажите, что существует естественное действие $\mathrm{Aut}_K(E)$ на $\mathrm{WC}(E/K)$, определённое для $\alpha \in \mathrm{Aut}_K(E)$ и $\{C/K, \mu\} \in \mathrm{WC}(E/K)$ по правилу $\{C/K, \mu\}^\alpha = \{C/K, \mu \circ (1 \times \alpha)\}$ (т.е. берем ту же кривую, но определяем новое действие E на C по правилу $\mu^\alpha(p, P) = \mu(p, \alpha(P))$).

b) Обратно, если $\{C/K, \mu\}$ и $\{C/K, \mu'\}$ — элементы в $\mathrm{WC}(E/K)$, докажите, что найдется такой $\alpha \in \mathrm{Aut}_K(E)$, что $\mu' = \mu \circ (1 \times \alpha)$.

c) Заключите, что для данной кривой C/K рода один существует только конечное множество неэквивалентных способов сделать из C/K однородное пространство. В частности, если $j(C) \neq 0, 1728$, то число способов не больше двух.

Задача 14° (WC над конечными полями). Пусть $C/\mathbb{F}_q$ — кривая рода один. Возьмём любую точку $C(\bar{\mathbb{F}}_q)$ в качестве нулевой, чтобы сделать из C эллиптическую кривую. Пусть $\phi\colon C \to C$ — отображение Фробениуса степени q на C.

a) Докажите, что существует такие $f \in \mathrm{End}(C)$ и $P_0 \in C(\bar{\mathbb{F}}_q)$, что $\phi(P) = f(P) + P_0$.

b) Докажите, что f несепарабельно и заключите, что существует такая точка $P_1 \in C(\bar{\mathbb{F}}_q)$, что $(1 - f)(P_1) = P_0$.

c) Докажите, что $\phi(P_1) = P_1$ и, следовательно, $P_1 \in C(\mathbb{F}_q)$.

d) Пусть $E/\mathbb{F}_q$ — эллиптическая кривая. Докажите, что $\mathrm{WC}(E/\mathbb{F}_q) = 0$.

Задача 15° (WC над $\mathbb{R}$). a) Докажите, что $\mathrm{WC}(E/\mathbb{R}) = \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{если } \Delta(E) > 0, \\ 0, & \text{если } \Delta(E) < 0. \end{cases}$

b) В предположении, что $\Delta(E) > 0$, найдите уравнение для однородного пространства, представляющего нетривиальный элемент $\mathrm{WC}(E/\mathbb{R})$ в терминах уравнения Вейерштрасса для $E/\mathbb{R}$.

Задача 16. Пусть E/K — эллиптическая кривая, $m \geq 2$ — целое число, и $E[m] \subset E(K)$. Пусть v — неархимедово простое, не делящее m. Докажите, что отображение ограничения $\mathrm{WC}(E/K)[m] \to \mathrm{WC}(E/K_v)[m]$ сюръективно.

Подсказка: покажите, что отображение сюръективно на группах $H^1(\cdot, E[m])$.

Задача 17 (индекс и период в WC**).** E/K — эллиптическая кривая над совершенным полем K, и C/K — однородное пространство для E. Периодом C называется порядок C в $\mathrm{WC}(E/K)$, а индексом C — наименьшая степень такого расширения L/K, что $C(L) \neq \emptyset$ (например, период равен единице тогда и только тогда, когда индекс равен единице).

a) Докажите, что период есть такое наименьшее целое $m \geq 1$, что существует точка $p \in C$ со свойством $p^\sigma - p \in E[m]$ для всех $\sigma \in G_K$.

b) Докажите, что индекс равен наименьшей степени положительных дивизоров из $\mathrm{Div}_K(C)$.

c) Докажите, что период делит индекс.

d) Докажите, что период и индекс имеют одинаковое множество простых делителей.

e^*) Приведите пример с $K = \mathbb{Q}$, показывающий, что период может быть строго меньше индекса.

f^*) Пусть C/K — такая кривая рода 1 над числовым полем, что $C(K_v) \neq \emptyset$ для всех v. Покажите, что отображение $\mathrm{Div}_K(C) \to \mathrm{Pic}_K(C)$ сюръективно.

Подсказка: воспользуйтесь тем, что $H^1(G_K, \bar{K}(C)^\times) = 0$ *(теорема Нётер) и утверждение о том, что элемент из* $H^2(G_K, \bar{K}^\times)$ *тривиален тогда и только тогда, когда он тривиален в* $H^2(G_{K_v}, \bar{K}_v^\times)$ *для всех* $v \in M_K$ *(теорема Брауэра–Хассе-Нётер).*

g^*) Докажите, что если K — числовое поле и C/K представляет нетривиальный элемент из $Ш(E/K)$, то период и индекс равны.

Подсказка: используйте пункты a, b, c, f.

h^*) Пусть $K/\mathbb{Q}_p$ — конечное расширение. Докажите, что период и индекс равны.