V. A. Kolyvagin, D. Yu. Logachev, Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties,
Algebra i Analiz, 1989, Volume 1, Issue 5, 171–196

В. А. Колывагин, Д. Ю. Логачев

КОНЕЧНОСТЬ ГРУППЫ ШАФАРЕВИЧА–ТЭЙТА И ГРУППЫ РАЦИОНАЛЬНЫХ ТОЧЕК ДЛЯ НЕКОТОРЫХ МОДУЛЯРНЫХ АБЕЛЕВЫХ МНОГООБРАЗИЙ

Результат В. А. Колывагина о конечности групп Ш$(\mathbb{Q}, E)$ и $E(\mathbb{Q})$ для модулярной эллиптической кривой E, L-ряд которой не имеет 0 в точке $s = 1$, обобщается на случай модулярных абелевых многообразий произвольной размерности.

Первый автор в своей недавней работе [1] рассматривал модулярные эллиптические кривые E, определенные над полем $\mathbb{Q}$, L-ряд которых $L(E/\mathbb{Q}, s)$ не равен 0 в точке $s = 1$. Основной результат этой работы состоит в том, что если эта кривая E удовлетворяет некоторому дополнительному условию (которое, как анонсировали Бамп, Фридберг и Хофштейн [23], всегда выполняется), то ее группа Шафаревича–Тэйта Ш$(\mathbb{Q}, E)$ и группа рациональных точек (группа Морделла–Вейля) $E(\mathbb{Q})$ конечны. Тем самым достигнуто существенное продвижение в проблеме конечности группы Шафаревича–Тэйта, стоящей около 30 лет, и в доказательстве гипотезы Бёрча–Свиннертона-Дайера.

В настоящей работе этот результат обобщается на многомерный случай модулярных абелевых многообразий, т. е. на абелевы многообразия с вещественным умножением – факторы якобианов модулярных кривых (теорема 0.3).

Доказательство основной теоремы близко следует работе [1], обозначения, насколько возможно, согласованы. При этом в § 2, 3 настоящей работы часть доказательств по сравнению с доказательствами аналогичных утверждений в [1] упрощена, а никаких усложнений, вызванных тем, что мы рассматриваем многомерный случай, нет.

Укажем, какие результаты были получены ранее в доказательстве гипотезы конечности группы Шафаревича–Тэйта и гипотезы Берча–Свиннертона-Дайера. Пусть X – абелево многообразие, определенное над числовым полем F.

Ключевые слова: модулярные абелевы многообразия, группа Шафаервича–Тэйта, гипотеза Бёрча–Свиннертона-Дайера.

Определим $\mathrm{rk}\, X/F$ (ранг X/F) как ранг абелевой группы $X(F)$ и $L\text{-}\mathrm{rk}\, X/F$ (L-ранг X/F) как порядок нуля L-функции $L(X/F, s)$ многообразия X над полем F в точке $s=1$. Обозначим a_r коэффициент при $(s-1)^r$ в ряде Тейлора для $L(X/F, s)$ в точке $s=1$, и пусть $Ш = Ш(F, X)$ – группа Шафаревича–Тэйта многообразия X над полем F. Если группа Ш конечна, то $|Ш|$ будет обозначать ее порядок.

Гипотеза Бёрча–Свиннертона-Дайера утверждает:

(А) $\mathrm{rk}\, X/F = L\text{-}\mathrm{rk}\, X/F$;

(Б) $Ш(F, X)$ – конечная группа, и если $L\text{-}\mathrm{rk}\, X/F = r$, то $a_r = |Ш(F, X)| \cdot C$, где C – некоторый множитель, явно определяемый по многообразию X (см., например, [2]). Точный вид его нам не понадобится.

Для формулировки результатов, подтверждающих гипотезу Бёрча–Свиннертона-Дайера, удобно определить число $|Ш|^? = |Ш(F, X)|^? \stackrel{\text{def}}{=} a_r/C$ – гипотетический порядок Ш. Для многих эллиптических кривых числа a_r и C были найдены с большой степенью точности с помощью вычислений на компьютере. Найденное значение $|Ш|^?$ в пределах точности вычислений оказывалось целым и, более того, квадратом целого числа, что согласуется с результатами Касселса [3] и Тэйта [4]. В этих работах для абелева многообразия X, у которого существует главная поляризация (в частности, для эллиптической кривой), построена невырожденная альтернированная форма на $Ш(F, X)$, откуда несложно вывести, что если Ш конечна, то $|Ш|$ есть полный квадрат и $\sqrt{|Ш|} \cdot Ш = 0$. Известно, что для модулярной эллиптической кривой E с условием $L\text{-}\mathrm{rk}\, E/\mathbb{Q} = \mathrm{rk}\, E/\mathbb{Q} = 0$ мы имеем $|Ш|^? \in \mathbb{Q}^*$ ([5]).

Пусть E – эллиптическая кривая с комплексным умножением на мнимое квадратичное поле K. Коутс и Вайлс [6] доказали, что если поле K одноклассно и $L\text{-}\mathrm{rk}\, E/F = 0$, то и $\mathrm{rk}\, E/F = 0$ для $F = \mathbb{Q}$ или $F = K$. Рубин [7], используя идеи Коутса и Вайлса, доказал аналогичный результат для всех мнимых квадратичных полей K. Наконец, в работе [8] Рубин доказал при условии одноклассности K, что из условия $L\text{-}\mathrm{rk}\, E/K = 0$ следует конечность $Ш(K, E)$, построив тем самым первые примеры кривых с конечной группой Ш.

В работах Гросса и Цагира [9] и Колывагина [1, 10] рассматриваются любые модулярные эллиптические кривые, а не только кривые с комплексным умножением. Для такой кривой E Гросс и Цагир вывели формулу, выражающую высоту некоторых точек из $E(\mathbb{Q})$, а именно точек Хегнера, через производную функции $L(E, s)$ в точке $s=1$. В частности, они показали, что если $L\text{-}\mathrm{rk}\, E/\mathbb{Q} = 1$, то существуют точки Хегнера с ненулевой высотой, так что тогда $\mathrm{rk}\, E/\mathbb{Q} \geqslant 1$ (поскольку высота точки кручения равна 0).

Другое следствие формулы Гросса–Цагира таково. Пусть K – мнимое квадратичное поле и ${}^K E$ – скручивание кривой E над полем K. Тогда, если $L\text{-}\mathrm{rk}\, E/\mathbb{Q} = 1$, $L\text{-}\mathrm{rk}\, ({}^K E/\mathbb{Q}) = 0$ и $\mathrm{rk}\, E/K = 1$, то $|Ш(K, E)|^? \in \mathbb{Q}^{*2}$.

Результаты [8] существенно используются в [1] и настоящей работе.

Пусть N – кондуктор модулярной кривой E, и пусть запись $\Delta \equiv \square (4N)$ означает, что существует $a \in \mathbb{Z}$ такое, что $\Delta \equiv a^2 \bmod 4N$. Основной результат работы [1] –

Теорема 0.1. *Пусть выполнены условия:*

(1) $L\text{-}\mathrm{rk}\, E/\mathbb{Q} = 0$;

(2) *Существует поле* $K = \mathbb{Q}(\sqrt{\Delta})$, *где* $\Delta < 0$, Δ – *свободно от квадратов,* $\Delta \neq -1, -3$, $(\Delta, 2N) = 1$, $\Delta \equiv \square (4N)$, *и такое, что* $L\text{-}\mathrm{rk}\, ({}^K E/\mathbb{Q}) = 1$.

Тогда $E(\mathbb{Q})$ *и* $Ш(\mathbb{Q}, E)$ *конечны.*

Замечание 1. Приведенный выше результат Гросса и Цагира относился к эллиптической кривой E_1 с условиями $L\text{-}\mathrm{rk}\, (E_1) = 1$, $L\text{-}\mathrm{rk}\, ({}^K E_1) = 0$. В теореме 0.1, наоборот, рассматривается кривая E_2 с условиями $L\text{-}\mathrm{rk}\, (E_2) = 0$,

$L\text{-}\mathrm{rk}({}^{K}E_2) = 1$. Грубо говоря, $E_2 = {}^{K}E_1$ (операция скручивания кривой над полем K инволютивна).

Замечание 2. При доказательстве теоремы 0.1 вначале устанавливается существование числа D_0 такого, что $D_0 \cdot E(\mathbb{Q}) = 0, D_0 \cdot Ш(\mathbb{Q}, E) = 0$. Это число D_0 тесно связано с рациональным числом $\sqrt{|Ш(K,E)|}$?.

Замечание 3. Известно, что если $L\text{-}\mathrm{rk}\, E/\mathbb{Q} = 1$, то существует бесконечно много полей K таких, что $L\text{-}\mathrm{rk}({}^{K}E/\mathbb{Q}) = 0$ (см. [11]). Недавно Д. Бамп, С. Фридберг, Дж. Хофштейн [23] анонсировали результат о том, что из условия (1) теоремы 0.1 вытекает условие (2) для бесконечного множества значений Δ.

Основная теорема настоящей работы – теорема 0.3 – есть обобщение теоремы 0.1 на случай модулярных абелевых многообразий. Введем необходимые определения. Пусть E – модулярное абелево многообразие кондуктора N с вещественным умножением на поле U. Как само E, так и все его вещественные умножения определены над $\mathbb{Q}$. Пусть $L_U(E/\mathbb{Q}, s)$ – L-ряд многообразия E над $\mathbb{Q}$ относительно вещественного умножения на U (см., например, [12]). Как и в случае эллиптических кривых, определим $\mathrm{rk}_U(E/\mathbb{Q}) \stackrel{\mathrm{def}}{=} \dim_U(E(\mathbb{Q}) \otimes \mathbb{Q})$ и $L\text{-}\mathrm{rk}_U(E/\mathbb{Q})$ – порядок нуля $L_U(E/\mathbb{Q}, s)$ в точке $s = 1$.

Аналог части (A) гипотезы Бёрча–Свиннертона-Дайера таков:

$$L\text{-}\mathrm{rk}_U(E/\mathbb{Q}) = \mathrm{rk}_U(E/\mathbb{Q}). \tag{0.2}$$

Пусть K – мнимое квадратичное поле и ${}^{K}E$ – скручивание многообразия E над полем K, т. е. единственная $K/\mathbb{Q}$-форма E, определяемая нетривиальным гомоморфизмом $G(K/\mathbb{Q}) \to \{1, -1\} \subset \mathrm{Aut}\, E$. Это – также модулярное абелево многообразие с вещественным умножением на U.

Теорема 0.3. *Пусть выполнены условия:*

(1) $L\text{-}\mathrm{rk}_U(E/\mathbb{Q}) = 0$;

(2) *Существует поле* $K = \mathbb{Q}(\sqrt{\Delta})$, *где* $\Delta < 0$, Δ *свободно от квадратов,* $\Delta \neq -1, -3$, $(\Delta, 2N) = 1$, $\Delta \equiv \square\ (4N)$, *и такое, что* $L\text{-}\mathrm{rk}_U({}^{K}E/\mathbb{Q}) = 1$. *Тогда* $Ш(\mathbb{Q}, E)$ *и* $E(\mathbb{Q})$ *конечны.*

(Согласно [23], условие (2) следует из условия (1)).

В частности, для такого многообразия E справедлива формула (0.2).

Другие формулировки основной теоремы будут приведены в § 1. Теорема 1.3.2 сформулирована в терминах значений L-рядов модулярных форм. Применение основной теоремы работы [9] позволяет свести теорему 1.3.2 к теореме 1.3.3 с чисто алгебраической формулировкой.

Авторы благодарны М. В. Боровому и Ю. Г. Зархину за консультации по работе.

§ 1. Введение

В п. 1.2 даны определения группы Шафаревича–Тэйта и Зельмера, в п. 1.3 – определение модулярных абелевых многообразий, а также приведена формулировка основной теоремы в терминах L-рядов модулярных форм. Там же приведен общий план работы.

1.1. Обозначения. Для всякой абелевой группы A пусть A_D, A/D, A_{tors} и $A/_{\mathrm{tors}}$ обозначают соответственно ядро и коядро умножения на D, подгруппу кручения в A и фактор по ней. $|A|$ обозначает порядок группы A. Для кольца A группа его обратимых элементов обозначается A^*. Для произвольного поля L пусть $\bar{L}$ обозначает алгебраическое замыкание L и G_L – группу Галуа $G(\bar{L}/L)$.

Пусть X – коммутативная алгебраическая группа, определенная над полем L и L'/L – расширение Галуа. Группа точек X, определенных над полем L', обозначается $X(L')$. Группа когомологий Галуа $H^i(G(L'/L), X(L'))$ обозначается $H^i(L'/L, X)$, а для случая $L' = \bar{L}$ – просто $H^i(L, X)$.

1.2. Определение групп Шафаревича–Тэйта и Зельмера. Пусть X – абелево многообразие, определенное над числовым полем F. Элементы группы $H^1(F, X)$ классифицируют классы изоморфизма главных однородных пространств X' многообразия X (см., например, [13]). При этом X' представляет ненулевой элемент в $H^1(F, X)$ тогда и только тогда, когда $X'(F)$ пусто.

Пусть v – нормирование поля F и $\mathcal{F}_v$ – пополнение F в v. Существует естественное отображение локализации $j_v: H^1(F, X) \to H^1(\mathcal{F}_v, X)$; для главных однородных пространств оно соответствует переходу от X' к $X' \underset{F}{\times} \mathcal{F}_v$. Группа Шафаревича–Тэйта $Ш = Ш(F, X)$ есть, по определению, ядро отображения $H^1(F, X) \to \prod\limits_v H^1(\mathcal{F}_v, X)$, где произведение взято по множеству всех нормирований v поля F. Группа Ш периодична как подгруппа периодической группы $H^1(F, X)$.

Иными словами, главное однородное пространство X' лежит в Ш, если у него есть $\mathcal{F}_v$-точки над всеми пополнениями поля F. Группу Ш можно рассматривать как препятствие к выполнению принципа Хассе для X, т. е. $Ш = 0$ тогда и только тогда, когда принцип Хассе для X выполняется. В работах [8] и [10] приведены примеры кривых с $Ш = 0$.

Для изучения группы Ш полезна группа Зельмера $S_D(F, X)$ многообразия X. Она определяется так. Пусть $D > 0$ – целое число и

$$0 \to X_D \to X \xrightarrow{D} X \to 0 \tag{1.2.1}$$

– точная последовательность G_F-модулей, происходящая из умножения X на D. Для каждого нормирования v поля F рассмотрим коммутативную диаграмму

$$\begin{array}{ccccccc} 0 \to & X(F)/D & \to & H^1(F, X_D) & \to & H^1(F, X)_D & \to 0 \\ & \downarrow & & \downarrow j_v & & \downarrow & \\ 0 \to & X(\mathcal{F}_v)/D & \xrightarrow{\alpha} & H^1(\mathcal{F}_v, X_D) & \to & H^1(\mathcal{F}_v, X)_D & \to 0 \end{array}$$

с точными строками. Ее верхняя строка происходит из точной когомологической последовательности для (1.2.1), а вертикальные стрелки – отображения локализации.

По определению, группа Зельмера

$$S_D(F, X) = \left\{ t \in H^1(F, X_D) \mid \forall v \; j_v(t) \in \operatorname{im} \alpha \right\}.$$

Очевидно, существует точная последовательность

$$0 \to X(F)/D \to S_D(F, X) \to Ш(F, X)_D \to 0.$$

Группа $S_D(F, X)$ – конечная D-периодическая группа. Это – промежуточный результат, получаемый при стандартном доказательстве теоремы Морделла–Вейля (см., например, [14]).

Начиная с этого места, введем такое соглашение. Будем считать, что $D = l^n$, где l – простое. Мы будем рассматривать переменные $m_k(l)$ – целые неотрицательные числа, зависящие только от l, и такие, что для любого индекса k $m_k(l) = 0$ для почти всех простых l.

Л е м м а 1.2.2. *Пусть X удовлетворяет следующему условию:*

(1.2.3). *Для любого простого l существует число $m_1(l)$ такое, что для любого $n > 0$ и $D = l^n$ мы имеем $l^{m_1(l)} \cdot S_D(F, X) = 0$.*

Тогда $X(F)$ и $Ш(F, X)$ конечны, и для $D_0 = \prod_l l^{m_1(l)}$ мы имеем $D_0 \cdot Ш(F, X) = 0$.

Д о к а з а т е л ь с т в о. Если $l^{m_1(l)} \cdot S_D(F, X) = 0$, то $\forall\, l, n\ D_0 \times \times Ш(F, X)_{l^n} = 0$. Но $Ш(F, X)$ – периодическая группа, т. е. $Ш(F, X) = \sum_l (\cup_n Ш(F, X)_{l^n})$. Отсюда $D_0 \cdot Ш(F, X) = 0$, т. е. $Ш(F, X) = Ш(F, X)_{D_0}$. Эта группа конечна как фактор-группа $S_{D_0}(F, X)$.

Если $X(F)$ бесконечна, то в ней есть прямое слагаемое, изоморфное Z, а в $X(F)/D$ – прямое слагаемое, изоморфное Z/D. Оно не может аннулироваться числом D_0 при $D > D_0$ – противоречие.

Таким образом, для доказательства теоремы 0.3 достаточно доказать, что для многообразия E, удовлетворяющего ее условию, выполнено свойство 1.2.3.

1.3. В этом пункте будет дано определение модулярных абелевых многообразий, приведены другие формулировки основной теоремы и указан общий план работы.

Фиксируем число $N > 0$ (кондуктор). Конгруэнц-подгруппа $\Gamma_0(N)$ – это подгруппа $SL_2(Z)$, состоящая из матриц $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ таких, что $c \equiv 0 \bmod N$. Она действует на верхней полуплоскости H и на верхней полуплоскости, объединенной с параболическими точками $\overline{H} = H \cup \{i\,\infty\} \cup \{Q\}$. Факторпространство $X = X_0(N) = \Gamma_0(N) \backslash \overline{H}$ можно рассматривать как неособую проективную алгебраическую кривую, определенную над Q (см., например, [12]). Обозначим естественную проекцию $\overline{H}$ на X через π. При этом $\pi(H) \subset X$, и точки из $\pi(H)$ параметризует изогении эллиптических кривых $A \to A'$ с ядром, изоморфным Z/N. Если $z \in H$, то точке $\pi(z) \in X$ соответствует изогения $C/\langle z, 1\rangle \to C/\langle z, 1/N\rangle$, где $\langle a, b\rangle$ – решетка в C, порожденная числами a и b.

Отображение $z \to -\frac{1}{Nz}$ – это инволюция H, обозначаемая w_N. Она согласована с действием $\Gamma_0(N)$ на H и может быть продолжена с $\pi(H)$ на X; соответствующую инволюцию на X обозначим $w_{N,X}$.

Пусть $S_2(N)$ – пространство параболических форм веса 2 относительно $\Gamma_0(N)$ и $f \in S_2(N)$ – нормализованная новая форма, собственная относительно операторов Гекке. Это значит, что если $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ и T_m – m-й оператор Гекке, то $a_1 = 1$ и $T_m(f) = a_m \cdot f$. Определим $L_f(s)$ – L-ряд формы f – формулой $L_f(s) = \sum_{n=1}^{\infty} a_n / n^s$. Эта функция аналитически продолжается на всю комплексную плоскость и удовлетворяет функциональному уравнению, связывающему $L_f(s)$ и $L_f(2-s)$.

Инволюция w_N может быть определена также и на $S_2(N)$. Форма f собственна относительно w_N, и если g –порядок нуля $L_f(s)$ в точке $s = 1$, то

$$w_N(f) = -(-1)^g \cdot f \qquad (1.3.1)$$

(см., например, [12], теорема 3.66).

Пусть U – поле, порожденное над Q всеми числами a_n. U – конечное вполне вещественное расширение Q. Обозначим $d = \dim [U:\mathrm{Q}]$. По форме f можно построить (см., например, [12]) единственное с точностью до изогении простое d-мерное абелево многообразие E – фактор якобиана кривой X – с вещественным умножением на U. Оно называется модулярным абелевым многообразием, соответствующим форме f. Обозначим J якобиан кривой X и $\lambda : J \to E$ – проекцию J на E.

Более подробные сведения о конструкции многообразия E нам понадобятся лишь при доказательстве предложения 2.3.5 и леммы 2.3.7 и будут там приведены.

Как само многообразие E, так и все его вещественные умножения определены над Q. Согласно обобщенной гипотезе Вейля, наоборот, всякое такое простое абелево многообразие является модулярным. Эта гипотеза доказана для абелевых многообразий СМ-типа.

В частном случае $d = 1$ мы имеем $U = \mathrm{Q}$ и E – просто эллиптическая кривая, определенная над Q. В работе [1] рассматривался именно этот случай.

Функция $L_U(E/\mathrm{Q}, s)$ – L-ряд многообразия E относительно вещественного умножения на U – совпадает с функцией $L_f(s)$ (см. [12]).

Пусть теперь $K = \mathrm{Q}(\sqrt{\Delta})$, где $\Delta < 0$, – мнимое квадратичное поле и $\chi_K : \mathbb{Z} \to \{\pm 1; 0\}$ – квадратичный характер поля K. Положим $f_{(K)}(z) \overset{\text{def}}{=} \overset{\text{def}}{=} \sum_{n=1}^{\infty} a_n \chi_K(n) e^{2\pi i n z}$. Тогда $f_{(K)} \in S_2(N')$ для некоторого N'. Пусть ${}^K E$ – скручивание многообразия E относительно поля K. Это – также модулярное абелево многообразие, кондуктор которого – делитель N'. С точностью до конечного числа эйлеровых множителей

$$L_U({}^K E/\mathrm{Q}, s) = L_{f_{(K)}}(s)$$

$$\text{и} \quad L_U(E/K, s) = L_U(E/\mathrm{Q}, s) \cdot L_U({}^K E/\mathrm{Q}, s).$$

Сформулируем основной результат работы в терминах значений L-рядов модулярных форм:

Теорема 1.3.2. *Пусть f и E те же, что и выше, и выполнены условия:*

(1) $L_f(1) \neq 0$;

(2) *существует поле $K = \mathrm{Q}(\sqrt{\Delta})$, где $\Delta < 0$, Δ свободно от квадратов, $\Delta \neq -1, -3$, $(\Delta, 2N) = 1$, $\Delta \equiv \square (4N)$, и такое, что порядок нуля функции $L_{f_{(K)}}(s)$ в точке $s = 1$ равен 1.*

Тогда для любого простого числа l существует $m_1(l)$ такое, что $\forall\, n > 0$ и $D = l^n$,

$$l^{m_1(l)} \cdot S_D(\mathrm{Q}, E) = 0.$$

По лемме 1.2.2 отсюда следует, что $E(\mathrm{Q})$ и $Ш(\mathrm{Q}, E)$ конечны.

Приведем основные шаги доказательства теоремы 1.3.2. Мы фиксируем форму f, поле K, числа l, n и $D = l^n$ из условия теоремы; для любого индекса k вместо $m_k(l)$ будем писать просто m_k.

В п. 2.1 формулируются хорошо известные свойства модулярных абелевых многообразий, которые будут использованы в работе. Далее, в § 2, определяются точки Хегнера на кривой X и многообразии E, в частности, строится некоторая точка Хегнера $y \in E(K)$, играющая важную роль в работе. Приведены формулы действия операторов Гекке и элементов группы Галуа на точки Хегнера.

Пусть $\bar{y}$ – образ y в $E(K)/_{\text{tors}}$ и σ – инволюция $E(K)$, происходящая из автоморфизма комплексного сопряжения поля K.

Из условия (1) теоремы 1.3.2 мы выведем предложение 2.3.9: $\sigma(\bar{y}) = -\bar{y}$.

Из условий (1) и (2) теоремы 1.3.2 как непосредственное следствие результатов Гросса и Цагира мы выведем предложение 2.3.5: $y \neq 0$.

Остальная часть работы – это доказательство следующей теоремы:

Теорема 1.3.3. *Пусть точка Хегнера $y \in E(K)$, определенная в п. 2.3, такова, что $\sigma(\bar{y}) = -\bar{y}$ и $\bar{y} \neq 0$. Тогда существует такое m_1, что $\forall\, n$ $l^{m_1} S_D(\mathbb{Q}, E) = 0$.*

С учетом сказанного выше из теоремы 1.3.3 вытекает основная теорема.

В п. 3.1 напоминаются свойства спаривания Вейля $[\cdot, \cdot]: E_D \otimes E_D \to (\mathbb{C}^*)_D$ и (для числового поля P) спаривания Тэйта $<\cdot, \cdot>: S_D(P, E) \otimes H^1(P, E)_D \to (\mathrm{Br}\, P)_D$ на абелевых многообразиях. В п. 3.3 для каждого D определяется некоторое подмножество Ω_D множества всех простых чисел; его непустота доказана в лемме 5.2.

Для всякого $p \in \Omega_D$ явно строится элемент $c_p \in H^1(K, E)_D$, обладающий следующим свойством (лемм 3.3.3):

Существует ненулевое кратное Ac_p, где $A \in \mathbb{Z}$, элемента c_p такое, что для любого нормирования v поля K, кроме нормирования $v = p$, его локализация в $H^1(\mathcal{K}_v, E)_D$ равна 0.

Из леммы 3.3.3 следует, что

$$\forall\, s \in S_D(K, E) \quad <s, Ac_p> = 0. \tag{1.3.4}$$

Остальная часть § 3 – это вывод формулы, аналогичной формуле (1.3.4), но такой, в которой участвует спаривание Вейля, а не спаривание Тэйта. Для этого определяется отображение e_p: $S_D(K, E) \to E_D$.

Пусть s – произвольный элемент из $S_D(\mathbb{Q}, E)$ и s_K – его образ в $S_D(K, E)$. Из формулы (1.3.4) выводится предложение 3.4.7:

Существует такой элемент x – ненулевое кратное образа y при отображении $E(K) \to S_D(K, E)$, что $\forall\, s \in S_D(\mathbb{Q}, E)$ $[e_p(s_K), e_p(x)] = 1$.

На E_D, как и на $E(K)$, есть инволюция σ. Из предложения 2.3.9 следует, что $\sigma(e_p(x)) = -e_p(x)$ (см. формулу 3.4.6). Кроме того, $\sigma(e_p(s_K)) = e_p(s_K)$ (см. формулу 3.4.8).

Неформально смысл утверждений § 4 и 5 таков. В группах E_D и $S_D(K, E)$ есть l-адическая метрика: элемент близок к 0, если он аннулируется малой степенью l. В § 4 доказано, что из предложения 3.4.7 и формул (3.4.6), (3.4.8) следует, что $e_p(s_K)$ и $e_p(x)$ не могут быть оба далеки от 0.

В § 5 устанавливается, насколько отображение e_p сохраняет свойство близости к 0 в $S_D(K, E)$ и E_D. Грубо говоря, для любого конечного множества $s_1, \ldots, s_a$ элементов $S_D(K, E)$ есть такое множество $P \subset \Omega_D$ простых чисел,

что всякий s_i, $i = 1, \ldots, \alpha$ близок к 0 в $S_D(K, E)$ тогда и только тогда, когда $\forall_{p \in P}\ e_p(s_i)$ близок к 0 в E_D. (Нам потребуется лишь случай $\alpha = 2$, $s_1 = s_K$, $s_2 = x$). Из этого выводится, что s_K и X не могут быть оба далеки от нуля. Из предложения 2.3.5 несложно вывести, что при большом n элемент x далек от 0 (предложение 5.12), откуда следует, что произвольный элемент $s \in S_D(\mathrm{Q}, E)$ близок к 0, что и доказывает основную теорему.

§ 2. Определение и свойства точек Хегнера на X и E

В п. 2.1 будут приведены хорошо известные свойства модулярных абелевых многообразий; их доказательства в основном можно найти в [12].

2.1. Рассмотрим модулярное абелево многообразие E как комплексный тор: $E = V/L$, где V – C-векторное пространство, а L – решетка в V. Для $u \in U$ отображение вещественного умножения на u обозначим $\varphi(u)$; это – эндоморфизм пространства V такой, что $\varphi(u)(L) \subset \mathrm{Q}L$. Множество таких u, что $\varphi(u)(L) \subset L$, есть порядок $R \subset U$; для $u \in R$ $\varphi(u)$ есть эндоморфизм абелева многообразия E, определенный над Q.

Максимальный порядок поля U обозначим O. Для произвольного E (напомним, что E определено однозначно лишь с точностью до изогении) не обязательно $R = O$. Однако, по ([15], § 7.1, предл. 7), существует изогения $\alpha: E \to E'$ со следующими свойствами:

1) E' и α определены над Q;

2) $\mathrm{End}\, E' \supset O$;

3) всякий элемент из O, рассматриваемый как эндоморфизм E', определен над Q.

Так как свойство конечности $Ш(\mathrm{Q}, E)$ и $E(\mathrm{Q})$ – инвариант относительно Q-изогений, то, заменяя, если надо, E на E', мы можем считать, что $R = O$.

На E существует поляризация Λ такая, что инволюция Розати относительно Λ тождественна на O (см. [12], § 7.6).

Напомним, что проекция $\tilde{H}$ на X обозначается через π, а проекция J на E – через λ. Обозначим $j: X \to E$ естественное вложение кривой X в ее якобиан, выбранное так, что $j(\pi(i\infty)) = 0 \in J$. Инволюция $w_{N, X}$ продолжается до инволюции $w_{N, J}$ на J. Так как $w_{N, X}(\pi(i\infty)) = \pi(0)$, то $\forall\, x \in X$,

$$j(w_{N, X}(x)) = w_{N, J}(j(x)) + j(\pi(0)). \tag{2.1.1}$$

Из условия (1) теоремы 1.3.2 и формулы 1.3.1 следует, что $w_N(f) = -f$. Отсюда следует, что

$$\lambda \circ w_{N, J} = -\lambda \tag{2.1.2}$$

(надо рассмотреть действие $w_{N, J}$ на $H^{1,0}(J)$ и $H^{1,0}(E)$).

Из (2.1.1) и (2.1.2) следует формула

$$\lambda \circ j \circ w_{N, X}(x) = -\lambda \circ j(x) + \lambda \circ j \circ \pi(0). \tag{2.1.3}$$

Далее в работе p будет обозначать простое число такое, что $p \nmid N\Delta l$. На X определено соответствие Гекке $T_{p, X}$, которое продолжается до отображения

$T_{p,J}$ на J. Соответствие $T_{p,X}$ и отображение $T_{p,J}$ определены над Q. При этом коэффициент Фурье $a_p \in O$ и

$$\varphi(a_p) \circ \lambda = \lambda \circ T_{p,J} \tag{2.1.4}$$

(см. [12], теорема 7.14).

Зафиксируем теперь какое-либо продолжение нормирования p на поле $\bar{\mathrm{Q}}$ и будем обозначать редукцию по нему знаком $\sim$. Многообразия X, J, E, соответствие $T_{p,X}$ и отображения $T_{p,J}$ и $\varphi(a_p)$ имеют хорошую редукцию в точке p. По теореме Эйхлера–Шимуры на $\tilde{X}$ имеет место равенство соответствий

$$\tilde{T}_{p,X} = \mathrm{fr} + \mathrm{fr}', \tag{2.1.5}$$

где fr – эндоморфизм Фробениуса на $\tilde{X}$, рассматриваемый как соответствие, а fr' – двойственное соответствие (см. [12, 16]). В $\mathrm{End}\tilde{J}$ имеет место равенство

$$\tilde{T}_{p,J} = \mathrm{fr} + \mathrm{fr}', \tag{2.1.6}$$

где fr' – отображение, происходящее из соответствия fr' на $\tilde{X}$; при этом

$$\mathrm{fr} \circ \mathrm{fr}' = p \cdot 1_{\mathrm{End}\,J}. \tag{2.1.7}$$

Из (2.1.6), (2.1.7) и (2.1.4) следует, что в $\mathrm{End}\,\tilde{E}$ выполнено равенство

$$\mathrm{fr}^2 - \varphi(a_p) \cdot \mathrm{fr} + p = 0, \tag{2.1.8}$$

где fr – эндоморфизм Фробениуса на $\tilde{E}$.

Положим $O_l = O \otimes \mathrm{Z}_l$. Для всякого $k > 0$ E_{l^k} – свободный O/l^k-модуль ранга 2, и модуль Тэйта $T_l(E)$ многообразия E – свободный O_l-модуль ранга 2 (см. [12], § 7.6). Эндоморфизм fr на $\tilde{E}$ действует на O_l-модуль $T_l(\tilde{E})$, и его характеристический многочлен равен $T^2 - a_p T + p$, где T – независимая переменная (см. [12], доказательство теоремы 7.24). Это уточняет формулу (2.1.8).

2.2. Содержание остальной части § 2, а также § 3 настоящей работы идейно следует работе [1]. Постоянное различие – использование вещественного умножения $\varphi(a_p) \in \mathrm{End}\,E$ вместо умножения на $a_p \in \mathrm{Z}$ в случае эллиптической кривой E. Однако из-за невозможности дать удобные ссылки многие доказательства будут здесь приведены.

Пусть точка $x \in X$ соответствует изогении эллиптических кривых $A \to A'$ с ядром, изоморфным Z/N. По определению, x – точка Хегнера, если A и A' – кривые СМ-типа и кольца комплексного умножения у них совпадают. Основная теорема теории комплексного умножения позволяет определить, как действует на точки Хегнера группа Галуа.

Пусть p – либо простое число такое, что p инертно в $K \nmid p \mid ND$, либо $p = 1$. Обозначим O_K кольцо целых поля K и $O_p = \mathrm{Z} + pO_K$ – порядок в K. Множество собственных O_p-идеалов в K (это – такие решетки в K, кольцо множителей которых есть O_p) образует группу; ее фактор по группе главных O_p-идеалов обозначается $\mathrm{Cl}(K, p)$. Для $p > 1$ определим абелево расширение

K_p/K (кольцевое поле классов кондуктора p) и изоморфизм θ: Cl $(K, p) \to$ $\to G(K_p/K)$ следующим образом. Обозначим I_K группу иделей поля K. Если v – нормирование K, то $\mathcal{K}_v$ будет обозначать пополнение K, а $\mathcal{U}_v$ – его группу единиц. Так как p инертно в K, можно рассматривать p как нормирование поля K. Его поле вычетов равно $\mathbf{F}_{p^2}$, так что существует эпиморфизм β: $\mathcal{U}_p \to \mathbf{F}_{p^2}^*$. Обозначим $\mathcal{U}_p^{\text{ring}} = \beta^{-1}(\mathbf{F}_p^*)$, где $\mathbf{F}_p^* \hookrightarrow \mathbf{F}_{p^2}^*$ – обычное вложение. Тогда расширение K_p/K соответствует идельной подгруппе

$$I_{K,p}^{\text{ring}} \overset{\text{def}}{=} \left(\prod_{v \neq p,\infty} \mathcal{U}_v\right) \cdot \mathcal{K}_\infty^* \cdot \mathcal{U}_p^{\text{ring}} \cdot K^*.$$

Существует естественный изоморфизм Cl $(K, p) \to I_K/I_{K,p}^{\text{ring}}$, и его композиция с изоморфизмом взаимности $I_K/I_{K,p}^{\text{ring}} \to G(K_p/K)$ дает нам θ.

Для $p = 1$ мы имеем $O_1 = O_K$ и Cl $(K, 1) =$ Cl (K) – группа классов идеалов поля K. Обозначим $h = |\text{Cl}(K)|$. Положим K_1 – гильбертово поле классов поля K. Если $p > 1$, то, так как p инертно в K, нормирование p вполне распадается в расширении K_1/K. Кроме того, $K_p \supset K_1$, и расширение K_p/K_1 вполне разветвлено в нормированиях, лежащих над p. Из сформулированных выше условий на p и Δ (напомним, что $\Delta \neq -1, -3$) следует, что для $p > 1$ $G(K_p/K_1) = \mathcal{U}_p/\mathcal{U}_p^{\text{ring}} = \mathbf{F}_{p^2}^*/\mathbf{F}_p^* = \mathbf{Z}/(p+1)$ (см. [1], предл. 5).

Из того, что $\Delta \equiv \square(4N)$, следует, что в O_K есть такой идеал i_1, что $O_K/i_1 = \mathbf{Z}/N$ (см. [9]). Положим $i_p = i_1 \cap O_p$. Пусть a – собственный O_p-идеал. Обозначим $\{a, i_p\}$ точку на X, соответствующую изогении $\mathbf{C}/a \to$ $\to \mathbf{C}/i_p^{-1}a$. $\{a, i_p\}$ – точка Хегнера.

Лемма 2.2.1. *$\{a, i_p\}$ зависит лишь от класса идеала a в группе* Cl (K, p). *Если $\{a_1, i_p\} = \{a_2, i_p\}$, то классы идеалов a_1 и a_2 в группе* Cl (K, p) *совпадают.* ●

Обозначим σ автоморфизм комплексного сопряжения поля $\mathbf{C}$, а также его ограничение на любое расширение Галуа P поля $\mathbf{Q}$ с фиксированным вложением $P \hookrightarrow \mathbf{C}$. Автоморфизм σ действует на X и E.

Следующая лемма показывает, как действуют автоморфизмы на точки Хегнера.

Лемма 2.2.2.

(1) *Для собственного O_p-идеала a $\{a, i_p\} \in X(K_p)$.*

(2) *Пусть b – собственный O_p-идеал и $\bar{b}$ – его класс в* Cl (K, p). *Тогда* $\theta(\bar{b})(\{a, i_p\}) = \{ab^{-1}, i_p\}$.

(3) $\sigma(\{a, i_p\}) = \{\sigma(a), \sigma(i_p)\}$.

(4) $w_{N,X}(\{a, i_p\}) = \{ai_p, \sigma(i_p)\}$.

Доказательство. См. [9], II, § 1. ●

Обозначим $z_p = \{O_p, i_p\}$. По лемме 2.2.2, (1) $z_p \in X(K_p)$, в частности, $z_1 \in X(K_1)$. Далее мы будем считать, что $p > 1$.

2.3. Предложение 2.3.1. $T_{p,X}(z_1) = \sum_{g \in G(K_p/K_1)} g(z_p)$ (*равенство дивизоров на X*).

Доказательство. Из коммутативности диаграммы

$$\begin{array}{ccc} \mathbf{C}/O_K & \to & \mathbf{C}/i_1^{-1} \\ \downarrow & & \downarrow \\ \mathbf{C}/O_p & \to & \mathbf{C}/i_p^{-1} \end{array}$$

где вертикальные стрелки – изогении с ядром $\mathbf{Z}/p$, следует, что $z_p \in$ $\in \operatorname{Supp} T_{p,X}(z_1)$. Так как $T_{p,X}$ – соответствие, определенное над $\mathbf{Q}$ и $z_1 \in X(K_1)$, то $\forall g \in G(K_p/K_1)$ $g(z_p) \in \operatorname{Supp} T_p(z_1)$. Из леммы 2.2.2 (2) и леммы 2.2.1 следует, что точки $g(z_p)$ различны для всех $g \in G(K_p/K_1)$. Так как $\dim K_p/K_1 = \deg T_{p,X}(z_1) = p+1$, мы получаем равенство дивизоров. •

Напомним, что отображение редукции $\bmod p$ мы обозначаем знаком $\sim$. Точнее, зафиксируем $\bar{p}$ – продолжение нормирования p на поле $\bar{\mathbf{Q}}$; оно определяет отображение $\sim: X(\bar{\mathbf{Q}}) \to \tilde{X}(\bar{\mathbf{F}}_p)$.

Предложение 2.3.2. $\operatorname{fr}(\tilde{z}_1) = \tilde{z}_p$, *где* fr – *отображение Фробениуса на* $\tilde{X}$.

Доказательство. Из (2.1.5) и предложения 2.3.1 следует, что для произвольного $g \in G(K_p/K_1)$ (в частности, для единичного элемента) либо $\operatorname{fr}(\tilde{z}_1) = \widetilde{g(z_p)}$, либо $\operatorname{fr}(\widetilde{g(z_p)}) = \tilde{z}_1$. Так как поля вычетов полей K_p и K_1 в точке p – это $\mathbf{F}_{p^2}$, то эти две возможности совпадают. •

Определим следующие точки Хегнера на J и E:

$$y_p = \lambda \circ j(z_p) \in E(K_p);\ y_1 = \lambda \circ j(z_1) \in E(K_1);$$

$$y = N_{K_1/K}(y_1) \in E(K);\ c = j(z_1) \in J(K_1);$$

$$c_1 = N_{K_1/K}(c) \in J(K).$$

Точки c и c_1 нам будут нужны лишь при доказательстве предложения 2.3.5.

Следствие 2.3.3. $N_{K_p/K_1}(y_p) = \varphi(a_p)(y_1)$.

Доказательство. Следует из предложения 2.3.1 и (2.1.4). •

Следствие 2.3.4. $\tilde{y}_p = \operatorname{fr}(\tilde{y}_1)$.

Доказательство. Следует из предложения 2.3.2. •

Обозначим $\bar{y}$ образ y в $E(K)/_{\text{tors}}$.

Предложение 2.3.5. $\bar{y} \neq 0$.

Доказательство. Этот результат вытекает из основной теоремы работы [9] (по существу он приводится в этой работе без доказательства, см. гл. V, конец § 2), требуется лишь тщательная проверка определений.

Рассмотрим формулу (6.3), гл. I, [9]:

$$L'(f, \chi, 1) = a \cdot \hat{h}(c_{\chi, f}). \tag{2.3.6}$$

Здесь χ – характер группы $\operatorname{Cl}(K)$; мы будем использовать формулу (2.3.6) лишь в случае $\chi = \mathbf{1}$ – тождественный характер. Функция $L(f, \chi, s)$ определена формулой (5.4), гл. I, [9]; в случае $\chi = 1$ она равна $L_f(s) \cdot L_{f_{(K)}}(s)$, так что из условий (1) и (2) теоремы 1.3.2 следует, что $L'(f, \mathbf{1}, 1) \neq 0$. Число a не равно 0;

его точное значение для нас несущественно. Элемент $c_{1,f} \in J(K) \otimes \mathbf{C}$; это – f-изотипическая компонента элемента c_1. (Она собственна относительно операторов Гекке T_m с собственными значениями a_m. Точное определение будет приведено ниже). Наконец, $\hat{h}$ – функция Нерона–Тэйта на $J(K)$, продолженная на $J(K) \otimes \mathbf{C}$ по эрмитовой линейности.

Таким образом, из формулы (2.3.6) следует, что $\hat{h}(c_{1,f}) \neq 0$, а значит, и $c_{1,f} \neq 0$. Заметим, что $y = \lambda(c_1)$.

Тем самым предложение 2.3.5 вытекает из следующей леммы.

Лемма 2.3.7. *Пусть элемент $\tau \in J(K)$ таков, что $\tau_f \neq 0$. Тогда $\lambda(\tau) \notin E(K)_{\text{tors}}$.*

Доказательство. Напомним конструкцию многообразия E. Обозначим $S_2(N)_{\mathbf{Q}}$ подпространство $S_2(N)$, состоящее из форм с рациональными коэффициентами Фурье. Тогда $\dim_{\mathbf{Q}}(S_2(N)_{\mathbf{Q}}) = \dim_{\mathbf{C}} S_2(N)$, так что $S_2(N) = (S_2(N)_{\mathbf{Q}}) \otimes \mathbf{C}$. Пространство $S_2(N)_{\mathbf{Q}}$ инвариантно относительно операторов Гекке T_m. Пусть $\mathbf{T} \subset \mathrm{End}_{\mathbf{Q}}(S_2(N)_{\mathbf{Q}})$ – подалгебра, порожденная в $\mathrm{End}_{\mathbf{Q}}(S_2(N)_{\mathbf{Q}})$ всеми операторами T_m (см., например, [9], гл. 5, § 1). Вложение $T \hookrightarrow \mathrm{End}_{\mathbf{Q}}(S_2(N)_{\mathbf{Q}})$ определяет вложение $\psi_J : \mathbf{T} \to \mathrm{End}^0 J$, где $\mathrm{End}^0 J = \mathrm{End}\, J \otimes \mathbf{Q}$. Алгебра $\mathbf{T}$ разлагается на полупростую S и нильпотентную R части: $\mathbf{T} = S + R$. Алгебра S есть прямая сумма числовых полей: $S = \sum_{i=1}^{r} S_i$. Пусть e_i – единица в поле S_i.

Так как форма f собственна относительно операторов Гекке, можно определить эпиморфизм $\alpha : \mathbf{T} \to U$ задаваемой формулой: $\forall\, t \in \mathbf{T}\ \ t(f) = \alpha(t) \cdot f$. Ясно, что $\alpha(R) = 0$ и среди полей S_i существует одно S_{i_0} такое, что $\alpha : S_{i_0} \to U$ – изоморфизм и $\alpha(S_i) = 0$ для $i \neq i_0$.

Представим многообразие J как комплексный тор: $J = W/M$, где W – $\mathbf{C}$-векторное пространство (W комплексно сопряжено $S_2(N)$ в $H^1(X, \mathbf{C})$), а M – решетка в W. Существует естественное вложение $\psi_W : \mathbf{T} \to \mathrm{End}\, W$. Положим $V = \mathrm{im}\, \psi_W(e_{i_0})$ и разложим отображение $\psi_W(e_{i_0}) : W \to W$ на эпиморфизм $\lambda_W : W \to V$ и мономорфизм $i_W : V \to W$. Ясно, что $M \cap V$ – решетка в V. Так как f – новая форма, из теории Аткина–Ленера следует, что $\dim V = d$. По определению, модулярное абелево многообразие E есть V/L, где L – некоторая решетка в V, соизмеримая с $M \cap V$. Существуют ненулевые константы $c_\lambda, c_i \in \mathbf{Z}$ такие, что отображения векторных пространств $c_\lambda \lambda_W, c_i i_W$ индуцируют отображения абелевых многообразий $\lambda : J \to E$, $i : E \to J$, так что

$$i \circ \lambda = c_\lambda c_i \psi_J(e_{i_0}). \tag{2.3.8}$$

Для всякого $t \in \mathbf{T}$ отображение $\psi_J(t)$ определено на группе $J(K) \otimes \mathbf{Q}$. Если $(\psi_J(e_{i_0}))(\tau) \neq 0$, то из (2.3.8) следует, что и $\lambda(\tau) \notin E(K)_{\text{tors}}$. Однако элемент τ_f может быть получен из $(\psi_J(e_{i_0}))(\tau)$ с помощью следующей общей конструкции.

Пусть A – произвольный $\mathbf{Q}$-модуль, и пусть дано вложение алгебр $\delta : U \to \mathrm{End}_{\mathbf{Q}} A$. Вложение δ продолжается до вложения $\delta_{\mathbf{C}} : U \to \mathrm{End}_{\mathbf{C}}(A \otimes \mathbf{C})$. Пусть $\eta_1 = \mathrm{id}, \eta_2, \ldots, \eta_d$ – все вложения $U \to \bar{\mathbf{Q}}$. Легко доказать, что $\forall\, a \in A$ однозначно определены элементы $a_{\eta_1}, \ldots, a_{\eta_d} \in A \otimes \mathbf{C}$ с такими свойствами:

1) $\sum_{i=1}^{d} a_{\eta_i} = a \otimes 1$;

2) $\forall\, u \in U \quad (\delta_{\mathbf{C}}(u))(a_{\eta_i}) = \eta_i(u) \cdot a_{\eta_i}$

(т. е. элемент a_{η_i} – собственный относительно операторов из U).

Положим $A = J(K) \otimes \mathbf{Q}$ и $\delta(u) = \psi_J(a^{-1}(u))$. По определению, $\tau_f = [(\psi_J(e_{i_0}))(\tau)]_{\eta_1}$. Значит, если $\tau_f \neq 0$, то и $(\psi_J(e_{i_0}))(\tau) \neq 0$, и $\lambda(\tau) \notin E(K)_{\text{tors}}$. •

Предложение 2.3.9. $\sigma(\bar{y}) = -\bar{y}$.

Доказательство (см. также [1], с. 531–532). Пусть C – множество представителей элементов группы $\mathrm{Cl}(K)$ в группе всех идеалов поля K.

$$\sigma(y) = \sigma(N_{K_1/K}(\lambda \circ j(\{O_K, i\}))) =$$

$$= \sum_{g \in G(K_1/K)} \lambda \circ j(\sigma g(\{O_K, i\})) \quad \text{(так как } \lambda \text{ и } j \text{ определены над } \mathbf{Q})$$

$$= \sum_{a \in C} \lambda \circ j(\sigma(\{a, i\})) \quad \text{(по лемме 2.2.2, (2))}$$

$$= \sum_{a \in C} \lambda \circ j(\{a, \sigma(i)\}) \quad \text{(по лемме 2.2.2, (3))}$$

$$= \sum_{a \in C} \lambda \circ j(w_{N,\ X}(\{a \cdot \sigma(i), i\})) \quad \text{(по лемме 2.2.2, (4))}$$

$$= \sum_{a \in C} -\lambda \circ j(\{a \cdot \sigma(i), i\}) + h \cdot \lambda \circ j(\pi(0)) \quad \text{(по (2.1.3))}$$

$$= -y + h \cdot \lambda \circ j(\pi(0)).$$

По теореме Манина–Дринфельда $j(\pi(0))$ – точка конечного порядка на J, т. е. $\sigma(\bar{y}) = -\bar{y}$. •

§ 3. Определение элемента c_p; доказательство предложения 3.4.7

3.1. Напомним определения и свойства спариваний Вейля и Тэйта для абелевых многообразий (см. [17, 18]). Пусть A – абелево многообразие, определенное над полем P, μ_D – множество корней из 1 степени D в $\bar{P}^*$ и ξ_D – первообразный корень. Пусть Λ – поляризация многообразия A; спаривание Вейля $[\cdot, \cdot] : A_D \otimes A_D \to \mu_D$ определено относительно поляризации Λ. Оно кососимметрично, согласовано с действием группы Галуа и редукцией. Пусть $\varphi_\Lambda : A \to \check{A}$ – отображение поляризации (здесь $\check{A}$ – двойственное к A абелево многообразие). Тогда ядро спаривания Вейля (т. е. множество таких $a \in A_D$, что $\forall\, b \in A_D\ [a, b] = 1$) есть $\mathrm{Ker}\,\varphi_\Lambda \cap A_D$, т. е. его порядок ограничен независимо от D. Обозначим $m_2 = \mathrm{ord}_l(|\mathrm{Ker}\,\varphi_\Lambda|)$, и пусть $D' = D \cdot l^{m_2}$.

Лемма 3.1.1. *Существуют $a, b \in A_{D'}$ такие, что $[a, b] = \xi_{D'}$.*

Доказательство. Пусть $\varphi_\Lambda|_{A_{D'}} : A_{D'} \to \check{A}_{D'}$ – ограничение φ_Λ на $A_{D'}$. Так как спаривание Вейля между $A_{D'}$ и $\check{A}_{D'}$ не вырождено, то существуют $a \in A_{D'}$, $b' \in \check{A}_{D'}$ такие, что $[a, b'] = \xi_{D'}$. Так как $(|\mathrm{Coker}\,(\varphi_\Lambda|_{A_{D'}})|) \mid l^{m_2}$,

то $l^{m_2}b' \in \operatorname{im}\varphi_\Lambda|_{A_{D'}}$, т. е. $b \in A_{D'}$ такой, что $\varphi_\Lambda(b) = l^{m_2}b'$. Тогда $[a, b] = \xi_D$. •

Если P – p-адическое поле, то определено локальное спаривание Тэйта $<\cdot, \cdot>: A(P)/D \otimes H^1(P, A)_D \to (\operatorname{Br} P)_D \xrightarrow{\sim} \frac{1}{D}\mathbf{Z}/\mathbf{Z}$. Если P – числовое поле, то определено глобальное спаривание Тэйта $<\cdot, \cdot> : Ш_D(P, A) \otimes H^1(P, A)_D \to \to (\operatorname{Br} P)_D$. Так как спаривание Тэйта определяется через спаривание Вейля, оно зависит от выбора поляризации Λ.

Глобальное спаривание Тэйта согласовано с локальным. Пусть P – числовое поле, v – его нормирование, $\mathfrak{P}_v$ – пополнение и $j_v : P \to \mathfrak{P}_v$ – отображение пополнения. Обозначим через j_v также отображения локализации $(\operatorname{Br} P)_D \to \to (\operatorname{Br} \mathfrak{P}_v)_D$, $H^1(P, A)_D \to H^1(\mathfrak{P}_v, A)_D$ и $Ш_D(P, A) \to A(\mathfrak{P}_v)/D$ (существующее по определению группы Зельмера). Тогда $\forall s \in Ш_D(\mathfrak{P}, A)$, $\forall a \in \in H^1(P, A)_D$ $<j_v(s), j_v(a)> = j_v(<s, a>)$.

3.2. Сформулируем лемму о связи между спариваниями Вейля и Тэйта. Пусть $\mathcal{K}$ – p-адическое поле с нормированием v, $\mathcal{L}$ – его циклическое вполне разветвленное расширение степени D, E – произвольное абелево многообразие, определенное над $\mathcal{K}$ и k – поле вычетов поля $\mathcal{K}$.

Пусть выполнены условия:

$$\begin{aligned} &1)\ E \text{ имеет хорошую редукцию в } v; \\ &2)\ \operatorname{ord}_v(D) \neq 0 \ (\text{т. е. } l \neq \mathrm{p}); \\ &3)\ E_D \subset E(\mathcal{K}). \end{aligned} \tag{3.2.1}$$

Тогда $\widetilde{E}_D \subset \widetilde{E}(k)$. Пусть далее $R \in E(\mathcal{L})$ – такой элемент, что $N_{\mathcal{L}/\mathcal{K}}(R) = 0$, и пусть $\widetilde{R}$ – его редукция. Так как $\mathcal{L}/\mathcal{K}$ – вполне разветвленное расширение, то из $N_{\mathcal{L}/\mathcal{K}}(R) = 0$ следует, что $\widetilde{R} \in \widetilde{E}_D$. Обозначим $R' \in \check{H}^{-1}(\mathcal{L}/\mathcal{K}, E)$ проекцию R при отображении $\operatorname{Ker}(N_{\mathcal{L}/\mathcal{K}}(E)) \to \check{H}^{-1}(\mathcal{L}/\mathcal{K}, E)$. Пусть α – образующая $H^2(\mathcal{L}/\mathcal{K}, \mathbf{Z})$ и $r = R' \cup \alpha \in H^1(\mathcal{L}/\mathcal{K}, E) \hookrightarrow H^1(\mathcal{K}, E)_D$.

Определим отображение $e_v = e_{v,\mathcal{K}} : E(\mathcal{K})/D \to \widetilde{E}_D$ следующим способом. Пусть $\operatorname{red} : E(\mathcal{K})/D \to \widetilde{E}(k)/D$ – отображение редукции; из условий (3.2.1) следует, что red – изоморфизм. Пусть $\delta : \widetilde{E}(k)/D \to H^1(k, \widetilde{E}_D) = \operatorname{Hom}(G_k, \widetilde{E}_D)$ – связывающий гомоморфизм в когомологической точной последовательности. Наконец, пусть $\omega : \operatorname{Hom}(G_k, \widetilde{E}_D) \to \widetilde{E}_D$ – образ фробениуса, т. е. для $\chi \in \operatorname{Hom}(G_k, \widetilde{E}_D)$ $\omega(\chi) = \chi(\mathrm{fr})$, где $\mathrm{fr} \in G_k$ – автоморфизм Фробениуса поля k. Положим $e_v = \omega \circ \delta \circ \operatorname{red}$.

Заметим, что e_v – изоморфизм. Действительно, ω и red – изоморфизмы, δ – вложение. Но так как $\widetilde{E}(k)$ – конечная группа, то $|\widetilde{E}(k)/D| = |\widetilde{E}_D|$.

Л е м м а 3.2.2. *В приведенных выше обозначениях* $\forall s \in E(\mathcal{K})/D$

$$<s, r> = [e_v(s), \widetilde{R}] \cup \alpha. \tag{3.2.3}$$

(*Мы рассматриваем здесь* $[e_v(s), \widetilde{R}]$ *как элемент из* $H^0(G_{\mathcal{K}}, \overline{\mathcal{K}}^*)$).

Д о к а з а т е л ь с т в о. По существу эта лемма совпадает с предложением 8 из [1]. Тот факт, что в нашем случае рассматриваются

произвольные (не обязательно одномерные) абелевы многообразия, не влияет на доказательство. •

3.3. Пусть Ω_D – множество простых чисел p, удовлетворяющих следующим условиям:

$$\begin{aligned} &(1)\ p \nmid N\Delta; \\ &(2)\ p \text{ инертно в } K; \\ &(3)\ p \equiv -1 \bmod D; \\ &(4)\ a_p/D \in O. \end{aligned} \tag{3.3.1}$$

Его непустота будет доказана в лемме 5.2. Фиксируем $p \in \Omega_D$. Обозначим $\mathcal{K}_p$ пополнение поля K в нормировании p.

Лемма 3.3.2.

(а) $\tilde{E}_D \subset \tilde{E}(\mathbf{F}_{p^2})$;

(б) $E_D \subset E(\mathcal{K}_p)$.

Доказательство. Из равенства $\mathrm{fr}^2 - \varphi(a_p/D) \cdot D \cdot \mathrm{fr} + p = 0$ (см. 2.1.8) и условий (3), (4) из (3.3.1) следует, что на $\tilde{E}_D$ $\mathrm{fr}^2 = 1$, откуда получаем (а); (б), очевидно, следует из (а). •

Так как $G(K_p/K_1) = \mathbf{Z}/(p+1)$ и $D/(p+1)$, существует поле L_p такое, что $K_p \supset L_p \supset K_1$ и $G(K_p/L_p) = \mathbf{Z}/((p+1)/D)$, $G(L_p/K_1) = \mathbf{Z}/D$.

Положим $R_p = N_{K_p/L_p}(y_p) - \varphi(a_p/D)(y_1) \in E(L_p)$. Из следствия 2.3.3 сразу получаем: $N_{L_p/K_1}(R_p) = 0$.

Как и в п. 3.2, рассмотрим образующую $\alpha \in H^2(L_p/K_1, \mathbf{Z})$, определим $R'_p \in \check{H}^{-1}(L_p/K_1, E)$ как проекцию R_p и $r_p = R'_p \cup \alpha \in H^1(L_p/K_1, E) \hookrightarrow$ $\hookrightarrow H^1(K_1, E)_D$. Положим $c_p = N_{K_1/K}(r_p) \in H^1(L_p/K, E)_D \hookrightarrow H^1(K, E)_D$.

Пусть ν – нормирование поля K. Как и в п. 3.1, обозначим $j_\nu : K \to \mathcal{K}_\nu$ отображение пополнения поля K и отображения локализации в когомологиях. Пусть $N(K)$ – множество всех нормирований поля K.

Лемма 3.3.3. *Существует число* $A \neq 0$ *такое, что* $\forall\, \nu \in N(K)$, *кроме* $\nu = p$, $j_\nu(Ac_p) = 0$.

Доказательство. Так как $c_p \in H^1(L_p/K, E)$, а расширение L_p/K неразветвлено вне p, то $\forall\, \nu \neq p$ $j_\nu(c_p) \in H^1(\mathcal{K}_\nu^{\mathrm{nr}}/\mathcal{K}_\nu, E)$, где $\mathcal{K}_\nu^{\mathrm{nr}}$ – максимальное неразветвленное расширение поля $\mathcal{K}_\nu$. Но эта группа равна 0, если E имеет хорошую редукцию в точке ν, и аннулируется некоторым числом A_ν для прочих ν (см. [19]). Тогда $A = \prod_\nu A_\nu$. •

Следствие 3.3.4. $\forall\, s \in S_D(K, E)$ $\langle j_p(s), j_p(Ac_p)\rangle = 0$.

Доказательство. $\langle s, Ac_p\rangle \in (\mathrm{Br}\, K)_D$. $\forall\, \nu \in N(K)$, кроме $\nu = p$, $j_\nu(\langle s, Ac_p\rangle) = \langle j_\nu(s), j_\nu(Ac_p)\rangle = 0$. Обозначим, как обычно, $\mathrm{inv}: \mathbf{Br}\,\mathcal{K}_\nu \to \mathbf{Q}/\mathbf{Z}$ – канонический изоморфизм группы Брауэра локального поля. Так как $\forall\, b \in \mathrm{Br}\, K$ $\sum_\nu \mathrm{inv}(j_\nu(b)) = 0$, то и для $\nu = p$ $j_p(\langle s, Ac_p\rangle) = 0$. Но $j_p(\langle s, Ac_p\rangle) = \langle j_p(s), j_p(Ac_p)\rangle$. •

3.4. Применим теперь лемму 3.2.2, чтобы в формулировке следствия 3.3.4 перейти от спаривания Тэйта к спариванию Вейля. Расширим определение

отображения e_v из п. 3.2 на случай числового поля P. Пусть E – абелево многообразие над полем P и v – нормирование P. Пусть $\mathcal{P}_v$ и j_v те же, что и в п. 3.1, и E как многообразие над $\mathcal{P}_v$ удовлетворяет условиям (3.2.1). Тогда если $s \in S_D(P, E)$ и $j_v(s) \in E(\mathcal{P}_v)/D$ – его локализация, определен элемент $e_{v, \mathcal{P}_v}(j_v(s)) \in \widetilde{E}_D$. Положим $e_{v,P}(s) = e_{v, \mathcal{P}_v}(j_v(s))$.

Пусть $v_1, \ldots, v_h$ – продолжения нормирования p с поля K на поля K_1, L_p и K_p (очевидно, p вполне распадается в K_1/K, а K_p/K_1 вполне разветвлено в v_i (см. п. 2.2)). Пополнение L_p в точке v_i обозначим через $\mathcal{L}_p$, а K_p – через $(\mathcal{K}_p)_p$ (они не зависят от i), а отображения пополнения $K_1 \to \mathcal{K}_p$, $L_p \to \mathcal{L}_p$, $K_p \to (\mathcal{K}_p)_p$ и соответствующие им отображения локализации в когомологиях обозначим через j_{v_i}. Ясно, что поля вычетов полей $\mathcal{K}_p$, $\mathcal{L}_p$ и $(\mathcal{K}_p)_p$ равны $\mathbf{F}_{p^2}$.

Пусть теперь $s \in S_D(\mathbf{Q}, E) \hookrightarrow H^1(\mathbf{Q}, E_D)$. Его ограничение в $S_D(K, E) \hookrightarrow \hookrightarrow H^1(K, E_D)$ обозначим s_K. Для каждого $i = 1, \ldots, h$ применим лемму 3.2.2 к расширению $\mathcal{L}_p/\mathcal{K}_p$, нормированию v_i, многообразию E (согласно лемме 3.3.2, оно удовлетворяет условиям 3.2.1), элементам $j_p(s_K) \in E(\mathcal{K}_p)/D$ и $j_{v_i}(R_p) \in E(\mathcal{L}_p)$. Обозначим $\mathrm{red}_i : E(K_p) \to \widetilde{E}(\mathbf{F}_{p^2})$ композицию отображения пополнения $j_{v_i} : E(K_p) \to E((\mathcal{K}_p)_p)$ и отображения редукции относительно нормирования $v_i : E((\mathcal{K}_p)_p) \to \widetilde{E}(\mathbf{F}_{p^2})$. В таких обозначениях формула (3.2.3) принимает вид

$$\langle j_p(s_K), j_{v_i}(r_p) \rangle = [e_{p,K}(s_K), \mathrm{red}_i(R_p)] \cup a. \qquad (3.4.1)$$

Для элементов $y_1 \in E(K_1)$, $y \in E(K)$ обозначим через $\check{y}_1$, $\check{y}$ их образы в $E(K_1)/D$, $E(K)/D$. Так как $E(K_1)/D \hookrightarrow S_D(K_1, E)$, определен элемент $e_{v_i, K_1}(\check{y}_1) \in \widetilde{E}_D$.

Далее fr будет означать автоморфизм Фробениуса поля $\mathbf{F}_p$. Так как $\widetilde{E}$ определено над $\mathbf{F}_p$, то fr действует на $\widetilde{E}$.

Лемма 3.4.2. $\mathrm{red}_i(R_p) = -\mathrm{fr}^{-1}(e_{v_i, K_1}(\check{y}_1))$.

Доказательство. Найдем сначала $\mathrm{red}_i(R_p)$. Так как $R_p = N_{K_p/L_p}(y_p) - \varphi(a_p/D)(y_1)$, то $\mathrm{red}_i(R_p) = [(p+1)/D] \cdot \mathrm{red}_i(y_p) - \varphi(a_p/D)(\mathrm{red}_i(y_1))$ (расширение K_p/L_p вполне разветвлено, так что на редукции норма сводится к умножению на $\dim K_p/L_p = (p+1)/D$). Пусть $t \in \widetilde{E}$ – такой элемент, что $Dt = \mathrm{red}_i(y_1)$. Так как по следствию 2.3.4

$$\forall\, i \quad \mathrm{red}_i(y_p) = \mathrm{fr}(\mathrm{red}_i(y_1)),$$

то

$$\mathrm{red}_i(R_p) = (p+1)\,\mathrm{fr}(t) - \varphi(a_p)(t) =$$

$$= \mathrm{fr}^{-1}[(p+1)\,\mathrm{fr}^2(t) - \varphi(a_p)(\mathrm{fr}(t))] =$$

$$= \mathrm{fr}^{-1}(p(\mathrm{fr}^2(t) - t)) = -\mathrm{fr}^{-1}(\mathrm{fr}^2(t) - t) \qquad \text{(по 2.1.8)}$$

(так как $\mathrm{fr}^2(t) - t \in \widetilde{E}_D$, а $p \equiv -1 \bmod D$).

Найдем теперь $e_{v_i, K_1}(\check{y}_1)$. Рассмотрим диаграмму

$$\begin{array}{ccc} E(K_1) & \xrightarrow{\mathrm{red}_i} & \widetilde{E}(\mathbf{F}_{p^2}) \\ \downarrow & & \downarrow \\ E(K_1)/D & \xrightarrow{\mathrm{red}_i} & \widetilde{E}(\mathbf{F}_{p^2})/D \xrightarrow{\delta} H^1(\mathbf{F}_{p^2}, \widetilde{E}_D) \xrightarrow{\omega} \widetilde{E}_D, \end{array}$$

где вертикальные отображения – естественные проекции, а δ и ω – те же, что и в п. 3.2. По определению, $e_{v_i, K_1}(\check{y}_1) = \omega \circ \delta \circ \mathrm{red}_i(\check{y}_1)$. Учитывая, что $Dt = \mathrm{red}_i(y_1)$, по определению связывающего гомоморфизма δ мы имеем $\omega \circ \delta \circ \mathrm{red}_i(\check{y}_1) = \mathrm{fr}^2(t) - t$ (так как автоморфизм Фробениуса в группе $G_{\mathbf{F}_{p^2}}$ есть fr^2). •

Так как множество нормирований $v_1, \ldots, v_h$ есть главное однородное пространство над группой Галуа $G(K_1/K)$, мы имеем

$$\sum_{i=1}^{h} j_{v_i}(r_p) = j_p(c_p) \tag{3.4.3}$$

и

$$\sum_{i=1}^{h} e_{v_i, K_1}(\check{y}_1) = e_{p, K}(\check{y}) \tag{3.4.4}$$

(мы рассматриваем $\check{y} \in E(K)/D$ как элемент $S_D(K, E)$).

Суммируя (3.4.1) по всем i, мы получаем с учетом леммы 3.4.2 и формул (3.4.3) и (3.4.4):

$$\langle j_p(s_K), j_p(c_p) \rangle = [e_{p, K}(s_K), -\mathrm{fr}^{-1}(e_{p, K}(\check{y}))] \cup \alpha. \tag{3.4.5}$$

Заметим теперь, что при отображении редукции $E(K) \to \widetilde{E}(\mathbf{F}_{p^2})$ автоморфизм σ на $E(K)$ переходит в автоморфизм fr на $\widetilde{E}(\mathbf{F}_{p^2})$. По предложению 2.3.9 существует число $B \neq 0$ такое, что $\sigma(By) = -By$; легко видеть, что тогда $\mathrm{fr}(e_{p, K}(B\check{y})) = -e_{p, K}(B\check{y})$.

Положим $x = AB\check{y}$, где A из леммы 3.3.3. Умножим равенство (3.4.5) на AB; по следствию 3.3.4 левая часть станет равна 0. Так как

$$\mathrm{fr}(e_{p, K}(x)) = -e_{p, K}(x), \tag{3.4.6}$$

а $\cup$-умножение на α – изоморфизм, мы получаем

Предложение 3.4.7. $\forall s \in S_D(\mathbf{Q}, E) \quad [e_{p, K}(s_K), e_{p, K}(x)] = 1$. •

При этом так как s_K – образ элемента $s \in S_D(\mathbf{Q}, E)$ при отображении ограничения $s_D(\mathbf{Q}, E) \to S_D(K, E)$, то

$$\mathrm{fr}(e_{p, K}(s_K)) = e_{p, K}(s_K). \tag{3.4.8}$$

§ 4. Некоторые вспомогательные утверждения

Всюду в дальнейшем мы фиксируем произвольный элемент $s \in S_D(\mathbf{Q}, E)$. Элементы $s_K \in S_D(K, E) \hookrightarrow H^1(K, E_D)$ и $x \in E(K)/D \hookrightarrow S_D(K, E) \hookrightarrow \hookrightarrow H^1(K, E_D)$ будут почти всюду одинаково входить в наши рассуждения, поэтому мы обозначим $s_1 = s_K$, $s_2 = x$, и индекс i будет всюду принимать значения 1, 2. В этом параграфе мы покажем, что из предложения 3.4.7 и равенств (3.4.6), (3.4.8) следует, что элементы $e_{p,K}(s_i)$ не могут быть оба далеки от 0 в $\widetilde{E}_D$ (см. п. 1.3).

Напомним, что отображение редукции определяет изоморфизм $E_D \to \widetilde{E}_D$, перестановочный со спариванием Вейля, переводящий отображение $\sigma : E_D \to E_D$ в отображение $\mathrm{fr} : \widetilde{E}_D \to \widetilde{E}_D$. Подгруппу элементов $a \in E_D$ таких, что $\sigma(a) = a$, обозначим E_D^+, а таких, что $\sigma(a) = -a$, обозначим E_D^-. Вещественное умножение на U превращает E_D в O-модуль и в O/D-модуль; для $u \in O$ или $u \in O/D$, $a \in E_D$ их произведение обозначим просто ua. „Идеал" будет обозначать целый идеал поля U; множество идеалов упорядочивается отношением делимости: $I_1 I_2 \geqslant I_1$. Для $a \in O$ (a) обозначает главный идеал aO, а для $a \in O/D$ (a) обозначает прообраз в O идеала $a \cdot O/D$ при эпиморфизме $O \to O/D$.

Если в формулировках утверждений или в их доказательствах будет встречаться не определенная раньше переменная m_i с каким-либо индексом, то тем самым (как часть утверждения) предполагается ее существование.

Следующее предложение аналогично предложению 9 из [1].

Предложение 4.1. *Пусть* $\omega_1 \in E_D^+$, $\omega_2 \in E_D^-$ *такие, что* $\forall\, r \in O$ $[r\omega_1, \omega_2] = 1$. *Тогда существуют идеалы* I_1, I_2 *такие, что* $I_1 I_2 \leqslant (Dl^{m_3})$ *и* $I_i \omega_i = 0$.

Следствие 4.2. *Существуют идеалы* I_1, I_2 *такие, что* $I_1 I_2 \leqslant (Dl^{m_3})$ *и* $I_i e_{p,K}(s_i) = 0$.

Вывод 4.2 из 4.1. Достаточно взять ω_1, ω_2 такими, что $\widetilde{\omega}_i = e_{p,K}(s_i)$. Тогда $\omega_1 \in E_D^+$, $\omega_2 \in E_D^-$; из (3.4.7) следует, что $\forall\, r \in O$ $[r\omega_1, \omega_2] = 1$. •

Доказательство предложения 4.1. E_D – свободный O/D-модуль ранга 2 (см. [12], § 7.6). Пусть b_1, b_2 – базис E_D над O/D, и пусть $\sigma(b_i) = u_{i1} b_1 + u_{i2} b_2$, где $u_{ij} \in O/D$. Тогда $u_{11} + u_{22} = 0$ в O/D, так как характеристический многочлен автоморфизма fr в $\widetilde{E}_D$ есть $T^2 - a_p T + p = T^2 - 1$ в O/D, где T – независимая переменная.

Лемма 4.3. *Существует элемент* $a_1 = r_1 b_1 + r_2 b_2 \in E_D^+$, *где* $r_1, r_2 \in O/D$ *такие, что* $\min((r_1), (r_2)) \leqslant (l^{m_4})$.

Доказательство. Будем искать a_1 в виде

$$a_1 = x_1(b_1 + \sigma(b_1)) + x_2(b_2 + \sigma(b_2)) =$$

$$= ((u_{11} + 1)x_1 + u_{21} x_2) b_1 + (u_{12} x_1 + (u_{22} + 1) x_2)\, b_2 .$$

Обозначим $\begin{pmatrix} u_{11}+1 & u_{12} \\ u_{21} & u_{22}+1 \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$.

Лемма свелась к такой задаче на вычисления в кольце O/D: пусть $t_{ij} \in O/D$ такие, что $t_{11} + t_{22} = 2$. Тогда существуют $x_1, x_2 \in O/D$ такие, что

$$\min((t_{11}x_1 + t_{21}x_2), (t_{12}x_1 + t_{22}x_2)) \leqslant l^{m_4}.$$

Пусть $\lambda_1, \ldots, \lambda_k$ – простые идеалы в O, лежащие над l, они же – простые идеалы в O/D. Положим $m_{5j} = \operatorname{ord}_{\lambda_j}(2)$.

Выберем произвольное $j = 1, \ldots, k$. Если $\operatorname{ord}_{\lambda_j}(t_{11}) \leqslant m_{5_j}$, то положим

$$x_1 \equiv 1 \bmod \lambda_j, \quad x_2 \equiv 0 \bmod \lambda_j^{m_{5j}+1}. \tag{4.4}$$

Если $\operatorname{ord}_{\lambda_j}(t_{11}) > m_{5j}$, то $\operatorname{ord}_{\lambda_j}(t_{22}) \leqslant m_{5j}$, и в этом случае положим

$$x_1 \equiv 0 \bmod \lambda_j^{m_{5j}+1}, \quad x_2 \equiv 1 \bmod \lambda_j. \tag{4.5}$$

При таком выборе x_1, x_2

$$\min[\operatorname{ord}_{\lambda_j}(t_{11}x_1 + t_{21}x_2), \operatorname{ord}_{\lambda_j}(t_{12}x_1 + t_{22}x_2)] \leqslant m_{5j}.$$

Существуют x_1, x_2, удовлетворяющие сравнениям (4.4) либо (4.5) для всех j; полученное a_1 удовлетворяет условию леммы. Ясно, что для $l = 2$ $m_4 = 1$, для $l \neq 2$ $m_4 = 0$. ●

Лемма 4.6. $|E_D^+| \leqslant D^d l^{m_6}$.

Доказательство. Заметим, что $[E_D^+, E_D^+] \subset \{1, -1\}$ и $[E_D^-, E_D^-] \subset \{1, -1\}$. Действительно, спаривание Вейля перестановочно с действием группы Галуа. Пусть $a, b \in E_D^+$ или $a, b \in E_D^-$. Тогда $[a, b] = [\sigma(a), \sigma(b)] = [\widetilde{\sigma(a)}, \widetilde{\sigma(b)}] = [\operatorname{fr}(\tilde{a}), \operatorname{fr}(\tilde{b})] = [\tilde{a}, \tilde{b}]^p = [\tilde{a}, \tilde{b}]^{-1} = [a, b]^{-1}$, так как $p \equiv -1 \bmod D$. Значит, $[a, b]^2 = 1$.

Для $a \in E_D^+$ рассмотрим характер $\chi(a) \in \operatorname{Hom}(E_D^-, \mathbf{C}^*)$, определенный формулой $(\chi(a))(b) = [a, b]$. Тогда $\chi: E_D^+ \to \operatorname{Hom}(E_D^-, \mathbf{C}^*)$ – гомоморфизм. Если $\chi(a) = 0$, то $4a \in \operatorname{Ker}\varphi_\Lambda$. ($\varphi_\Lambda$ – отображение из E в двойственное многообразие, соответствующее поляризации Λ (см. п. 3.1)). Действительно, $[4a, b] = [a, 4b] = [a, 2(b + \sigma(b))] \cdot [a, 2(b - \sigma(b))] = [a, b + \sigma(b)]^2 \cdot [a, 2(b - \sigma(b))] = 1$, так как $b + \sigma(b) \in E_D^+$, $b - \sigma(b) \in E_D^-$. Значит, $|\operatorname{Ker}\chi| \leqslant 4^{2d}|\operatorname{Ker}\varphi_\Lambda|$, т. е.

$$|E_D^+| \leqslant 4^{2d} l^{m_2} |E_D^-|. \tag{4.7}$$

Так как $E_D^+ \cap E_D^- \subset E_2$, то из формулы $|E_D^+ + E_D^-| \cdot |E_D^+ \cap E_D^-| = |E_D^+| \cdot |E_D^-|$ следует, что $|E_D^+| \cdot |E_D^-| \leqslant 2^{2d} D^{2d}$. Отсюда и из (4.7) получаем $|E_D^+| \leqslant 2^{3d} l^{m_{2/2}} \cdot D^d$, откуда следует существование m_6. ●

Определим отображение $\alpha: O/D \to E_D^+$ следующим образом: $\alpha(u) = ua_1$, где a_1 из леммы 4.3. Если $\alpha(u) = 0$, то $ur_1 = ur_2 = 0$, откуда следует, что $ul^{m_4} = 0$ в O/D. Сравнивая порядки O/D и E_D^+, получаем, что $|\operatorname{Coker}\alpha| \leqslant l^{m_7}$, где $m_7 = dm_4 + m_6$. Значит,

$$\forall\, a \in E_D^+ \;\; \exists\, u \in O/D \text{ такой, что } ua_1 = l^{m_7}a. \tag{4.8}$$

Заметим теперь, что в предыдущих рассуждениях можно всюду заменить E_D^+ на E_D^-; существует элемент $a_2 \in E_D^-$, удовлетворяющий аналогу леммы 4.3 для E_D^-, и для него выполнен аналог формулы 4.8:

$$\forall\, a \in E_D^- \;\; \exists\, u \in O/D \text{ такой, что } ua_2 = l^{m_7}a. \tag{4.8'}$$

Рассмотрим ω_1, ω_2 из условия предложения, и пусть $l^{m_7}\omega_i = t_i a_i$, где $t_i \in O/D$. Покажем, что $l^{m_7}t_1t_2a_1 \in \operatorname{Ker}\chi$, т. е. $\forall\, c \in E_D^-$ $[l^{m_7}t_1t_2a_1,\, c] = 1$. Действительно, пусть $l^{m_7}c = ua_2$. Тогда, так как инволюция Розати тождественна на U,

$$[l^{m_7}t_1t_2a_1,\, c] = [t_1t_2a_1,\, l^{m_7}c] = [t_1t_2a_1,\, ua_2] =$$

$$= [ut_1a_1,\, t_2a_2] = [l^{m_7}u\omega_1,\, l^{m_7}\omega_2] = 1,$$

по условию предложения. Таким образом, $4l^{m_7}t_1t_2a_1 \in \operatorname{Ker}\varphi_\Lambda$, и $4l^{m_2+m_7}t_1t_2a_1 = 0$ и $4l^{m_2+m_4+m_7}t_1t_2 = 0$ в O/D. Значит,

$$(t_1t_2) \geqslant (Dl^{-m_7-m_4-m_2}\cdot 4^{-1}). \tag{4.9}$$

Положим $I_i = (Dl^{m_7})/(t_i)$. Покажем, что $I_i\omega_i = 0$. Пусть $u \in I_i$. Так как $(D) \geqslant (t_i)$, то $u = l^{m_7}u_1$, где $u_1 \in (D)/(t_i)$. Если $\bar{u}_1$ – образ элемента u_1 в O/D, то $\bar{u}_1t_i = 0$. Но $u\omega_i = l^{m_7}u_1\omega_i = \bar{u}_1t_ia_i = 0$.

Далее, $I_1I_2 = (D^2l^{2m_7})/(t_1)(t_2) \leqslant (D^2l^{2m_7})/(t_1t_2) \leqslant (D^2l^{2m_7})/(Dl^{-m_7-m_4-m_2}4^{-1}) = (Dl^{3m_7+m_4+m_2}\cdot 4)$. Отсюда следует существование m_3. ●

§ 5. Конец доказательства

В этом параграфе мы выясним, насколько отображение $e_{p,K}$ сохраняет отношение близости к 0 в группах $S_D(K, E)$ и $\widetilde{E}_D$ (см. п. 1.3). Сначала $\forall\, a \in S_D(K, E)$ мы определим элемент $a_V \in \operatorname{Hom}(\Gamma, \widetilde{E}_D)$, где Γ – некоторая группа Галуа, и покажем, что $e_{p,K}(a)$ есть значение гомоморфизма a_V на некотором элементе $\gamma \in \Gamma$ (лемма 5.3). Отсюда будет следовать, что элементы $(s_i)_V(\gamma)$ не могут быть оба далеки от 0; при этом, выбирая различные $p \in \Omega_D$, мы будем получать разные γ (следствие 5.4).

Следующий шаг – показать, что сами элементы $(s_i)_V$ не могут быть оба далеки от 0 (предложение 5.7). Затем мы покажем, что отсюда следует, что сами элементы s и x не могут быть оба далеки от 0 (следствие 5.11) и, наконец, что элемент x далек от 0 (предложение 5.12), откуда будет следовать, что элемент s близок к 0, что нам и нужно.

Дадим точные определения. Напомним, что $D' = Dl^{m_2}$, и рассмотрим поле $V = K(E_{D'})$. Пусть $\operatorname{res}: H^1(K, E_D) \to H^1(V, E_D)$ – отображение ограничения.

Рассмотрим s_i как элементы $H^1(K, E_D)$ и обозначим $s_{iV} = \mathrm{res}(s_i)$. Тогда $s_{iV} \in H^1(V, E_D) = \mathrm{Hom}(G_V, E_D)$, так что можно рассматривать элементы s_{iV} как гомоморфизмы из G_V в E_D. Расширение поля V, соответствующее $\mathrm{Ker}\, s_{iV}$, обозначим W_i и обозначим W композит W_1 и W_2. Обозначим также $G(W/V) = H$, $G(W_i/V) = H_i$. Таким образом, $s_{iV} \in \mathrm{Hom}(H, E_D)$.

Лемма 5.1. *$W/\mathbf{Q}$ – расширение Галуа.*

Доказательство. Достаточно показать, что для $i = 1, 2$ $W_i/\mathbf{Q}$ – расширение Галуа. Так как $s_{iV} \in \mathrm{res}(H^1(K, E_D))$, то W_i/K – расширение Галуа. Рассмотрим элемент $\sigma \in G(K/\mathbf{Q})$. Так как $\sigma(s_1) = s_1$, $\sigma(s_2) = -s_2$, то действие σ сохраняет расширения W_i/K. •

Рассмотрим некоторое вложение $W \hookrightarrow \mathbf{C}$ и обозначим $\sigma \in G(W/\mathbf{Q})$ ограничение автоморфизма комплексного сопряжения на поле W.

Пусть $\eta \in H$ – произвольный элемент. Положим $g = \eta\sigma$, тогда $g^2 \in H$. Обозначим g_i образ g^2 при эпиморфизме $H \to H_i$.

Напомним, что для неразветвленного нормирования π поля W, лежащего над простым числом p поля $\mathbf{Q}$, определен элемент $\mathrm{fr}\,\pi \in G(\mathcal{W}_\pi/\mathbf{Q}_p) \to G(W/\mathbf{Q})$, где $\mathcal{W}_\pi$ – пополнение W в π. По теореме Чеботарева существуют такие π и p, что $\mathrm{fr}\,\pi = g$ и $p \nmid N\Delta$. Ограничение нормирования π на V и W_i будем обозначать $\pi|_V$ и $\pi|_{W_i}$ соответственно.

Лемма 5.2. *Определенное таким образом число p удовлетворяет условиям* (3.3.1).

Доказательство. Достаточно использовать то, что $\mathrm{fr}(\pi|_V) = \sigma$. Так как $g|_K = \sigma$, то p инертно в K. Так как $g|_V = \sigma$, то пополнение V в точке π есть $\mathcal{K}_p$; значит, $E_{D'} \subset E(\mathcal{K}_p)$ и $\widetilde{E}_{D'} \subset \widetilde{E}(\mathbf{F}_{p^2})$.

Пусть теперь $a, b \in E_{D'}$ такие, что $[a, b] = \xi_D$ (см. лемму 3.1.1). Тогда $[\sigma(a), \sigma(b)] = \sigma(\xi_D) = \xi_D^{-1}$. Но $[\sigma(a), \sigma(b)] = [\overline{\sigma(a)}, \overline{\sigma(b)}] = [\mathrm{fr}(\tilde{a}), \mathrm{fr}(\tilde{b})] = \xi_D^p$, откуда $p + 1 \equiv 0 \bmod D$. Для любого $a \in \widetilde{E}_D$ мы имеем $\mathrm{fr}^2 a - \varphi(a_p)\,\mathrm{fr}\, a + pa = 0$ и $\mathrm{fr}^2 a = a$. Отсюда $\varphi(a_p)\,\mathrm{fr}\, a = 0$, т. е. отображение $\varphi(a_p)$ равно 0 на $\widetilde{E}_D$, а значит и на E_D. Таким образом, $\varphi(a_p)/D \in \mathrm{End}\, E$, откуда $a_p/D \in O$. •

Лемма 5.3. $e_{p,K}(s_i) = \overline{s_{iV}(g_i)}$.

Доказательство. Следует из определений. Обозначим вложение $G(\mathcal{W}_\pi/\mathbf{Q}_p) \hookrightarrow G(W/\mathbf{Q})$ через τ, и пусть $\mathrm{fr} \in G(\mathcal{W}_\pi/\mathbf{Q}_p)$ – автоморфизм Фробениуса. Тогда $\tau(\mathrm{fr}) = g$. Обозначим пополнение поля W_i в точке $\pi|_{W_i}$ через $\mathcal{W}_{i\pi}$ и вложение $G(\mathcal{W}_{i\pi}/\mathcal{K}_p) \hookrightarrow G(W_i/V) = H_i$ через τ'; тогда $\mathrm{fr}^2 \in G(\mathcal{W}_{i\pi}/\mathcal{K}_p)$ и $\tau'(\mathrm{fr}^2) = g_i$.

Рассмотрим коммутативную диаграмму

$$
\begin{array}{ccccccc}
S_D(K, E) & \hookrightarrow & H^1(K, E_D) & \xrightarrow{\mathrm{res}} & H^1(V, E_D) & \xrightarrow{\sim} & \mathrm{Hom}(G_V, E_D) \\
\downarrow j_p & & \downarrow j_p & \swarrow j_\pi & & & \\
E(\mathcal{K}_p)/D & \xrightarrow{\delta} & H^1(\mathcal{K}_p, E_D) & \xrightarrow{\sim} & \mathrm{Hom}(G_{\mathcal{K}_p}, E_D) & \hookleftarrow & \mathrm{Hom}(G(\mathcal{K}_p^{\mathrm{nr}}/\mathcal{K}_p), E_D) \\
\downarrow \mathrm{red} & & & & & \swarrow & \\
\widetilde{E}(\mathbf{F}_{p^2})/D & \xrightarrow{\delta} & H^1(\mathbf{F}_{p^2}, \widetilde{E}_D) & \xrightarrow{\sim} & \mathrm{Hom}(G_{\mathbf{F}_{p^2}}, \widetilde{E}_D) & \xrightarrow{\omega} & \widetilde{E}_D
\end{array}
$$

где red, δ, ω — те же, что и в п. 3.2, а α индуцировано вложением τ'. Мы имеем $s_{iV} \in \mathrm{Hom}(H_i, E_D)$ и $[\alpha(s_{iV})](\mathrm{fr}^2) = s_{iV}(g_i)$. Но по коммутативности, $[\alpha(s_{iV})](\mathrm{fr}^2) = e_{p,K}(s_i)$, по определению $e_{p,K}$. •

Следствие 5.4. *$\forall\, \eta \in H$ существуют идеалы I_1, I_2 такие, что $I_1 I_2 \leqslant (Dl^{m_3})$ и $I_i s_{iV}(g_i) = 0$.* •

Следующая лемма показывает, что можно переставить кванторы $\forall\, \eta\ \exists\ I_1, I_2$.

Лемма 5.5. *Пусть A — абелева группа, B_1, B_2 — O/D-модули, $\alpha_i : A \to B_i$ $(i = 1, 2)$-гомоморфизмы и P — идеал. Пусть $\forall\, a \in A$ существуют идеалы I_1, I_2 такие, что $I_1 \alpha_1(a) = I_2 \alpha_2(a) = 0$ и $I_1 I_2 \leqslant P$. Тогда $\exists\ I_1, I_2\ \forall a\ I_1 \alpha_1(a) = I_2 \alpha_2(a) = 0$ и $I_1 I_2 \leqslant P$.*

Доказательство. Пусть $\lambda_1, \ldots, \lambda_k$ — простые идеалы, лежащие в O над l. Кольцо O/D есть прямая сумма колец O/D_j, $j = 1, \ldots, k$, где D_j — некоторая степень λ_j. Легко видеть, что достаточно доказать лемму, заменив кольцо O/D на O/D_j. Для $b \in B_1$ или $b \in B_2$ $\mathrm{Ann}\, b$ — идеал в O/D_j. Для $i = 1, 2$ пусть $a_i \in A$ таково, что $\mathrm{Ann}\, \alpha_i(a_i) \geqslant \mathrm{Ann}\, \alpha_i(a)$ $\forall\, a \in A$. Обозначим $J_i = \mathrm{Ann}\, \alpha_i(a_i)$. Если $J_1 J_2 \leqslant P$, то лемма доказана. Пусть $J_1 J_2 > P$. При $a = a_2$ из условия леммы следует, что $\mathrm{Ann}\, \alpha_1(a_2) < J_1$, а при $a = a_1$ — что $\mathrm{Ann}\, \alpha_2(a_1) < J_2$. Но тогда $\mathrm{Ann}\, \alpha_1(a_1 + a_2) = J_1$, $\mathrm{Ann}\, \alpha_2(a_1 + a_2) = J_2$, и условие $J_1 J_2 > P$ противоречит условию леммы при $a = a_1 + a_2$. •

Следствие 5.6. *Существуют идеалы I_1, I_2 такие, что $I_1 I_2 \leqslant (Dl^{m_3})$ и $\forall\, \eta \in H, g = \eta\sigma$, $I_i s_{iV}(g_i) = 0$.* •

Предложение 5.7. *Существуют идеалы I_1, I_2 такие, что $I_1 I_2 \leqslant (Dl^{m_3})$ и $I_i s_{iV} = 0$.*

Доказательство. Автоморфизм σ действует на O/D-модулях $H^1(K, E_D)$ и $H^1(V, E_D) = \mathrm{Hom}(G_V, E_D)$. Формулы этого действия таковы. Если $\alpha \in \mathrm{Hom}(G_V, E_D)$, $\eta \in G_V$, то $(\sigma(\alpha))(\eta) = \sigma(\alpha(\sigma(\eta)))$, где $\sigma(\eta) = \sigma\eta\sigma$.

Лемма 5.8. $\forall\, \eta \in H$ $(1 + \sigma)(s_{1V}(\eta)) = s_{1V}(g_1)$, $(1 - \sigma)(s_{2V}(\eta)) = s_{2V}(g_2)$.

Доказательство. Так как $\sigma(s_1) = s_1$, $\sigma(s_2) = -s_2$, то $s_{iV}(g_i) = s_{iV}(\eta\sigma\eta\sigma) = s_{iV}(\eta) + s_{iV}(\sigma\eta\sigma) = s_{iV}(\eta) + \sigma((\sigma(s_{iV}))(\eta)) = s_{iV}(\eta) \pm \pm \sigma(s_{iV}(\eta)) = (1 \pm \sigma)(s_{iV}(\eta))$ (знак „+" для $i = 1$, знак „−" для $i = 2$). •

Обозначим $\Lambda_i = s_{iV}(H_i) \subset E_D$. Из леммы 5.8 вытекает, что для идеалов I_1, I_2 из следствия 5.6 мы имеем $I_1(1 + \sigma)\Lambda_1 = 0$, $I_2(1 - \sigma)\Lambda_2 = 0$. Положим $\Lambda_1' = I_1\Lambda_1$, $\Lambda_2' = I_2\Lambda_2$. Тогда $\Lambda_1' \subset E_D^-$, $\Lambda_2' \subset E_D^+$.

Обозначим $G = G(V/\mathbf{Q})$. Группа G действует на O/D-модуль E_D. Нетрудно видеть, что подмодули Λ_i, Λ_i' G-инвариантны. Действительно, $\Lambda_i = \mathrm{im}\, s_{iV}$, но s_{1V} G-инвариантен, а для $g \in G$ $g(s_{2V}) = s_{2V}$, если $g \in G(V/K)$, и $g(s_{2V}) = -s_{2V}$, если $g \notin G(V/K)$.

Лемма 5.9. *Если $e \in E_D$ – такой элемент, что орбита $G(e)$ содержится либо в E_D^+, либо в E_D^-, то $l^{m_9} e = 0$.*

Доказательство этой леммы будет приведено ниже; закончим доказательство предложения 5.7.

Из леммы 5.9 следует, что $l^{m_9}\Lambda_1' = l^{m_9}\Lambda_2' = 0$, т. е. $(I_i \cdot l^{m_9})\,\Lambda_i = 0$, а значит, и $(I_i l^{m_9})\,s_{iV} = 0$. Идеалы $I_i l^{m_9}$ удовлетворяют условию предложения, при этом $m_8 = 2m_9 + m_3$. •

Предложение 5.10. *Рассмотрим отображения ограничения* $\operatorname{res}_{K/\mathbf{Q}}: H^1(\mathbf{Q}, E_D) \to H^1(K, E_D)$ *и* $\operatorname{res}_{V/K}: H^1(K, E_D) \to H^1(V, E_D)$. *Тогда* $l^{m_{10}} \operatorname{Ker} \operatorname{res}_{K/\mathbf{Q}} = 0$, $l^{m_{11}} \operatorname{Ker} \operatorname{res}_{V/K} = 0$.

Доказательство этого предложения также будет приведено ниже.

Следствие 5.11. *Существуют идеалы I_1, I_2 такие, что $I_1 I_2 \leqslant (Dl^{m_{12}})$ и $I_1 s = 0$, $I_2 x = 0$.*

Доказательство. Рассмотрим идеалы I_1, I_2 из предложения 5.7; тогда $l^{m_{10}+m_{11}} I_1 s = l^{m_{11}} I_2 x = 0$. Идеалы $I_1 \cdot l^{m_{10}+m_{11}}$, $I_2 l^{m_{11}}$ удовлетворяют условию следствия, при этом $m_{12} = m_8 + m_{10} + 2m_{11}$. •

Покажем теперь, что элемент $x \in S_D(K, E)$ „далек от 0". Это легко следует из предложения 2.3.5.

Предложение 5.12. *Если I_2 – такой идеал, что $I_2 x = 0$, то $I_2 \geqslant (Dl^{-m_{13}})$.*

Доказательство. Достаточно доказать, что если $r \in O$ – такой элемент, что $r\,ABy \in D \cdot E(K)$, то $r \in (Dl^{-m_{13}})$ (A, B – те же, что в конце §3). Рассмотрим U-модуль $E(K) \otimes \mathbf{Q}$; $E(K)/_{\text{tors}} \subset E(K) \otimes \mathbf{Q}$. Существует базис $e_1, \ldots, e_a$ U-модуля $E(K) \otimes \mathbf{Q}$ такой, что координаты любого элемента из $E(K)/_{\text{tors}}$ в этом базисе целые. Пусть $ABy = \Sigma a_j e_j$, $a_j \in O$. Так как $r \cdot ABy \in DE(K)$, то $\Sigma r a_j e_j = D \cdot \Sigma b_j e_j$, где $b_j \in O$. Хоть один из элементов a_j, скажем a_1, не равен 0; значит, $r a_1 \in (D)$. Отсюда, очевидно, следует существование m_{13}. •

Закончим доказательство основной теоремы. Так как $I_1 I_2 \leqslant (Dl^{m_{12}})$ и $I_2 \geqslant (Dl^{-m_{13}})$, то $I_1 \leqslant (l^{m_{12}+m_{13}})$. Так как $I_1 s = 0$, то и $l^{m_{12}+m_{13}} s = 0$. Но s – произвольный элемент $S_D(\mathbf{Q}, E)$. Теорема доказана.

Доказательство леммы 5.9. Эту лемму можно доказать, используя теорему об образе l-адического представления $\rho_l: G_{\mathbf{Q}} \to GL_2(O_l)$. Однако можно использовать лишь утверждение, аналогичное теореме 2.1, гл. IV, [20] (с. 118), являющееся первым шагом доказательства теоремы об образе l-адического представления. А именно по элементу e мы построим набор $\mathbf{Q}$-изогений. $E \to E_b$. По аналогии с леммой 2.1, гл. IV, [20] (с. 119) мы докажем, что многообразия E_b попарно неизоморфны, откуда по теореме Фалтингса будет следовать ограниченность порядка множества этих изогений, а из нее – утверждение леммы.

Можно считать, что $e \in E_D^+$, в случае $e \in E_D^-$ доказательство аналогично. Докажем вначале существование m_9 для каждого l. Пусть a_1 – то же, что и в лемме 4.3. Положим $J = \operatorname{Ann} a_1 = \{u \in O \mid ua_1 = 0\}$. Тогда $J \geqslant (Dl^{-m_4})$, $\alpha: O/J \to E_D$ – вложение и $G(l^{m_7} e) \subset \alpha(O/J)$ (см. (4.8) и ее вывод). O-модуль, порожденный $G(l^{m_7} e)$, обозначим через M, $\alpha^{-1}(M)$ – через I_M

(I_M — идеал в O/J), а прообраз I_M в O — через J_M. Пусть $J = J_M \cdot \prod_{i=1}^{k} (\lambda_i)^{c_i}$. Фиксируем произвольное i и для каждого b, $1 \leqslant b \leqslant c_i$, рассмотрим идеал $J \cdot (\lambda_i)^{-b}$. Его образ в O/J обозначим через I_b, а $\alpha(I_b)$ — через K_b. I_b и K_b изоморфны $O/(\lambda_i)^b$ как O-модули.

K_b инвариантен относительно G. Действительно, все идеалы в O/J главные, так что $\exists\, j$ такой, что $I_b = j \cdot I_M$. Тогда $K_b = j \cdot M$.

Пусть $\tau_b : E \to E_b$ — изогения с ядром K_b. Из инвариантности K_b следует, что τ_b и E_b определены над $\mathbf{Q}$. Покажем, что E_{b_1} и E_{b_2} неизоморфны над $\mathbf{Q}$, если $b_1 \neq b_2$ и $h \mid b_2$.

Действительно, пусть $\chi : E_{b_1} \to E_{b_2}$ — $\mathbf{Q}$-изоморфизм. Так как $h \mid b_2$, то $(\lambda_i)^{b_2}$ — главный идеал, обозначим его образующую через γ. Изогения $\varphi(\gamma) : E \to E$ пропускается через τ_{b_2}, т. е. существует $\mathbf{Q}$-изогения $\tau_0 : E_{b_2} \to E$ с ядром, изоморфным $O/(\lambda_i)^{b_2}$ как O-модуль. Композиция $\tau_0 \circ \chi \circ \tau_{b_1} : E \to E$ определена над $\mathbf{Q}$, а значит, совпадает с одним из отображений $\varphi(u)$, $u \in O$ (комплексные умножения E, если они существуют, определены не над $\mathbf{Q}$). Но $\operatorname{Ker} \varphi(u) = (O/u)^2$, а $\operatorname{Ker} \tau_0 \circ \chi \circ \tau_{b_1}$ есть расширение модуля $O/(\lambda_i)^{b_1}$ при помощи модуля $O/(\lambda_i)^{b_2}$. Из теоремы о модулях над дедекиндовым кольцом легко следует, что при $b_1 \neq b_2$ никакой такой O-модуль неизоморфен $(O/u)^2$. Противоречие.

Пусть C — число (конечное по теореме Фалтингса) различных многообразий, $\mathbf{Q}$-изогенных E. Тогда $\forall\, i \;\; c_i \leqslant hC$, т. е. $l^{m_7 + hC} e = 0$.

Докажем теперь, что для почти всех l $m_9 = 0$. Можно ограничиться теми l, для которых $m_7 = 0$. Пусть для каких-либо двух значений l, обозначим их l' и l'', $m_9 \neq 0$. Рассуждая, как и выше, построим $\mathbf{Q}$-изогении $\tau' : E \to E'$, $\tau'' : E \to E''$ с ядрами, O-изоморфными O/λ', O/λ'' соответственно (λ', λ'' — некоторые простые идеалы, лежащие над l', l'' соответственно). Тогда E' и E'' неизоморфны над $\mathbf{Q}$. Действительно, пусть $\chi : E' \to E''$ — $\mathbf{Q}$-изоморфизм. Пусть γ — образующая главного идеала λ''^h. Существует изогения $\tau_0'' : E'' \to E$ такая, что $\tau_0'' \circ \tau'' = \varphi(\gamma)$. Изогения $\tau_0'' \circ \chi \circ \tau' : E \to E$ определена над $\mathbf{Q}$, т. е. равна $\varphi(u)$ для некоторого $u \in O$. $\operatorname{Ker} \tau_0'' \circ \chi \circ \tau'$ есть расширение модуля O/λ' при помощи модуля $(O/\lambda''^h)^2/(O/\lambda'')$. Но никакой такой модуль неизоморфен $(O/u)^2$.

Таким образом, из теоремы Фалтингса об изогениях следует, что существует лишь конечное множество таких l, для которых $m_9 \neq 0$. •

Доказательство предложения 5.10. Назовем порядок группы, зависящей от n, универсально ограниченным, если он ограничен одной константой для всех n. $\operatorname{Ker} \operatorname{res}_{K/\mathbf{Q}} = H^1(K/\mathbf{Q}, E(K)_D)$. Эта группа равна 0, если $l \neq 2$. Так как $E(K)_D \subset E(K)_{\text{tors}}$, то $|E(K)_D|$, а значит, и $|H^1(K/\mathbf{Q}, E(K)_D)|$ универсально ограничен. Это доказывает существование m_{10}.

Докажем теперь существование m_{11}. Идея доказательства — та же, что и в хорошо известном случае $d = 1$. Обозначим $G_0 = G(V/K)$; тогда $\operatorname{Ker} \operatorname{res}_{V/K} = H^1(G_0, E_D)$. Докажем сначала, что для почти всех l эта группа равна 0. По теореме Серра [21, 22] существует число M, не зависящее от l, такое, что образ l-адического представления $\rho_l : G_K \to GL_2(O_l)$ содержит $\mathbf{Z}_l^{*M} \cdot I$, где I — единичная матрица. Если $m_2 = 0$, т. е. $D = D'$, то ограничение ρ_l на E_D

есть вложение $G_0 \to GL_2(O/D)$, и $G_0 \supset (\mathbf{Z}/D)^{*M}$. Обозначим $Y = (\mathbf{Z}/D)^{*M}$ и для целого a, $1 \leqslant a \leqslant n$, положим $\Gamma_a = \{x \in (\mathbf{Z}/D)^* \mid x \equiv 1 \bmod l^a\}$. Если $l - 1 > M$, то группа Y циклична, содержит Γ_1 и строго больше Γ_1. Это значит, что Y действует на E_D без неподвижных точек, т. е. $(E_D)^Y = 0$. Так как E_D конечна, то ее индекс Эрбрана равен 1, так что и $H^1(Y, E_D) = 0$. Из точной последовательности ограничения и инфляции для $G_0 \supset Y$ следует, что $H^1(G_0, E_D) = 0$.

Покажем теперь существование m_{11} для каждого l. Ограничение l-адического представления ρ_l на $E_{D'}$ определяет вложение $G_0 \hookrightarrow \mathrm{GL}_2(O/D')$, и $G_0 \supset \supset (\mathbf{Z}/D')^{*M}$. Группа $(\mathbf{Z}/D')^{*M}$ действует на E_D умножением на соответствующее целое число. Очевидно, $(\mathbf{Z}/D')^{*M} \supset \Gamma_a$ для некоторого a, не зависящего от n. Группа Γ_a циклична (в случае $l = 2$ возьмем $a \geqslant 2$). Обозначим $\mathrm{GL}_2(O_l)_a = \{x \in \mathrm{GL}_2(O_l) \mid x \equiv I \bmod l^a\}$, $\mathrm{GL}_2(O/D')_a = \{x \in \mathrm{GL}_2(O/D') \mid x \equiv I \bmod l^a\}$ и положим $Y = G_0 \cap \mathrm{GL}_2(O/D')_a$.

Из точных последовательностей ограничения и инфляции для $G_0 \supset Y \supset \Gamma_a$ следует, что достаточно доказать универсальную ограниченность для $|H^1(\Gamma_a, E_D)|$, $|H^1(Y/\Gamma_a, (E_D)^{\Gamma_a})|$, $|H^1(G_0/Y, (E_D)^Y)|$. Очевидно, $(E_D)^{\Gamma_a} = (E_D)^Y = E_{l^a}$. Так как группа E_D конечна, то ее индекс Эрбрана равен 1, и $|H^1(\Gamma_a, E_D)| \leqslant$ $\leqslant |(E_D)^{\Gamma_a}| = l^{2ad}$, т. е. универсально ограничен. Так как $G_0/Y \subset \mathrm{GL}_2(O/D')/\mathrm{GL}_2(O/D')_a$, то $|G_0/Y|$, а значит, и $|H^1(G_0/Y, (E_D)^Y)|$ универсально ограничен.

Так как Y действует на $(E_D)^{\Gamma_a}$ тривиально, то $H^1(Y/\Gamma_a, (E_D)^{\Gamma_a}) =$ $= \mathrm{Hom}(Y/\Gamma_a, E_{l^a}) \subset \mathrm{Hom}(Y, E_{l^a}) = \mathrm{Hom}(Y/Y^{l^a}, E_{l^a})$, где Y^{l^a} – нормальный делитель, порожденный элементами x^{l^a} для $x \in Y$. Нам осталось показать, что $|Y/Y^{l^a}|$ универсально ограничен.

Обозначим Σ образ l-адического представления $\rho_l : G_K \to \mathrm{GL}_2(O_l)$ и $\Sigma_a = \Sigma \cap \mathrm{GL}_2(O_l)_a$. Очевидно, существует эпиморфизм $\Sigma_a/(\Sigma_a)^{l^a} \to Y/Y^{l^a}$, поэтому достаточно показать, что $\Sigma_a/(\Sigma_a)^{l^a}$ – конечная группа.

Группа Σ_a – компактная подгруппа $\mathrm{GL}_2(O_l)$. Отображение возведения в степень l^a на группе Σ_a имеет ненулевой дифференциал в точке 1, откуда следует, что группа $(\Sigma_a)^{l^a}$ содержит Σ_a-открытую окрестность 1, а значит, и сама открыта в Σ_a. Отсюда вытекает конечность $\Sigma_a/(\Sigma_a)^{l^a}$. •

Список литературы

[1] *Колывагин В. А.* Конечность $E(\mathbf{Q})$ и Ш$(E, \mathbf{Q})$ для подкласса кривых Вейля // Изв. АН СССР. Сер. мат. *1988*. Т. 52, № 3. С. 522–540.

[2] *Тэйт Дж.* О гипотезах Бёрча–Свиннертона-Дайера и их геометрическом аналоге // Математика. *1968*. Т. 12, № 6. С. 41–55.

[3] *Cassels J. W. S.* Arithmetic on curwes of genus 1. IV: Proof of the Hauptvermutung // J. reine und angew. Math. *1962*. Bd 211. S. 95–112.

[4] *Tate J.* Duality theorems in Galois cohomology over number fields // Proc. Intern. Congr. Math. Stockholm. *1962*. P. 288–295.

[5] *Mazur B., Swinnerton-Dyer H. P. F.* Arithmetic of Weil curves // Invent. Math. *1974*. Vol. 25, N 1. P. 1–61.

[6] *Coates J., Wiles A.* On the conjecture of Birch and Swinnerton-Dyer // Invent. Math. *1977.* Vol. 39, N 3. P. 223–251.
[7] *Rubin K.* Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer // Invent. Math. *1981.* Vol. 64, N 3. P. 445–470.
[8] *Rubin K.* Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication // Invent. Math. *1987.* Vol. 89, N 3. P. 527–560.
[9] *Gross B. H., Zagier D. B.* Heegner points and derivatives of L-series // Invent. Math. *1986.* Vol. 84, N 2. P. 225–320.
[10] *Колывагин В. А.* О группах Морделла–Вейля и Шафаревича–Тэйта для эллиптических кривых Вейля // Изв. АН СССР. Сер. мат. *1988.* Т. 52, № 6. С. 1154–1180.
[11] *Waldspurger J.-L.* Sur les coefficients de Fourier des formes modulaires de poinds demi-entier // J. Math. Pures Appl. *1981.* Vol. 60, N 4. P. 375–484.
[12] *Шимура Г.* Введение в арифметическую теорию автоморфных функций. М.: Мир, *1971.*
[13] *Серр Ж.-П.* Когомологии Галуа. М.: Мир, *1968.*
[14] *Манин Ю. И.* Теорема Морделла–Вейля. Приложение к [17].
[15] *Shimura G., Taniyama Y.* Complex multiplication of abelian varieties... // Rubl. Math. Soc. Japan. *1961.* N 6.
[16] *Swinnerton-Dyer H. P. F., Birch B.* Elliptic curves and modular functions // Modular functions of variable. IV. Lecture notes in Math. *1975.* N. 476. P. 2–32.
[17] *Мамфорд Д.* Абелевы многообразия. М.: Мир, *1971.*
[18] *Касселс Дж.* Диофантовы уравнения со специальным рассмотрением эллиптических кривых // Математика. *1968.* Т. 12, № 2. С. 3–48.
[19] *Манин Ю. И.* Круговые поля и модулярные кривые // Успехи мат. наук. *1971.* Т. 26, № 6. С. 7–71.
[20] *Серр Ж.-П.* Абелевы l-адические представления и эллиптические кривые. М.: Мир, *1973.*
[21] *Serre J.-P.* Resume des cours de 1984–1985 // Annuaire du College de France. Paris, *1985.*
[22] *Serre J.-P.* Resume des cours de 1985–1986 // Annuaire du College de France. Paris, *1986.*
[23] *Bump D., Friedberg S., Hoffstein J.* A nonvanishing theorem for derivatives of automorphic L-functions with applications to elliptic curves // Bull. Amer. Math. Soc. 1989. Vol. 21, N 1. P. 89–93.

Математический институт им. В. А. Стеклова АН СССР
117966, ГСП-1, Москва, ул. Вавилова, 42

Хабаровское отделение
Института прикладной математики
Дальневосточного отделения АН СССР
680063, Хабаровск, ул. Ким Ю Чена, 65

Поступило 10 июля 1988 г.