V. I. Yanchevskii, G. L. Margilin, Torsion and the Brauer groups of local elliptic curves,
Algebra i Analiz, 1995, Volume 7, Issue 3, 200–239

Алгебра и анализ
Том 7 (1995), вып. 3

КРУЧЕНИЕ И ГРУППЫ БРАУЭРА ЛОКАЛЬНЫХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В. И. Янчевский, Г. Л. Марголин

В работе исследуется строение групп Брауэра эллиптических кривых, определенных над локальным полем нулевой характеристики. Кручение в таких группах описано в терминах кручения рациональных точек эллиптических кривых. Для подгрупп 2-кручения групп Брауэра недиадических эллиптических кривых получено представление их элементов неразветвленными алгебрами кватернионов.

§1. Введение

Пусть K — конечное расширение поля $\mathbf{Q}$. Строение группы Брауэра $\mathrm{Br}(K)$ поля K (и конечномерных центральных простых алгебр над K) может быть описано с помощью глобальной теории полей классов. Ситуация заметно усложняется при переходе к полям $K(X)$ K-рациональных функций K-определенных алгебраических многообразий X. Даже в случае кривых X отсутствует завершенное описание групп $\mathrm{Br}(K(X))$. Традиция локально-глобального принципа требует в этом случае предварительного описания групп $\mathrm{Br}(K_v(X_v))$ полей K_v-рациональных функций многообразий $X_v = X \times_K K_v$ (K_v — пополнение поля K относительно нетривиального абсолютного значения v). В случае комплексного архимедового v группа $\mathrm{Br}(K_v(X_v))$ в силу теоремы Тзена тривиальна, а в случае вещественного v она была подробно изучена в работах [1, 2] и [3]. Таким образом, основной интерес представляет изучение групп $\mathrm{Br}(K_v(X_v))$ для неархимедовых v. К сожалению, о строении групп $\mathrm{Br}(k(X))$, где k — конечное расширение поля $\mathbf{Q}_p$ и X — кривая, определенная над k, известно довольно мало. Известно, например, [4], что для произвольного поля F алгебраических функций одной переменной над k существует точная последовательность

$$\mathrm{Br}(F) \xrightarrow{\phi} \coprod_{\rho} \chi(G_\rho) \xrightarrow{\psi} \chi(G) \longrightarrow 0, \qquad (*)$$

где ρ — простой дивизор поля $F|k$, F_ρ — пополнение F относительно нормирования, связанного с дивизором ρ, $\overline{F}_\rho$ — поле вычетов F_ρ, k_s — алгебраическое замыкание поля k, $F_s = Fk_s$ и $G = \mathrm{Gal}(F_s|F) \cong \mathrm{Gal}(k_s|k)$, $G_\rho = \mathrm{Gal}(\overline{k}_s|\overline{F}_\rho)$ (по поводу гомоморфизмов ϕ и ψ см. [4]). Пусть $F = k(X)$ — поле рациональных функций

Ключевые слова: группа Брауэра кривой, группа Брауэра поля, локальное поле, эллиптическая кривая, группа рациональных точек, неразветвленная центральная простая алгебра.

неособой проективной алгебраической кривой X. Поскольку образ гомоморфизма ϕ ввиду точной последовательности $(*)$ известен, важное значение для описания группы $\mathrm{Br}(k(X))$ приобретает изучение его ядра, которое может быть отождествлено в этом случае с группой $\mathrm{Br}\,X$ кривой X (см. [5]) или с неразветвленной группой Брауэра $\mathrm{Br}_{nr}(k(X))$ поля $k(X)$ [6] классов конечномерных центральных простых и неразветвленных над $k(X)$ алгебр (по поводу определения неразветвленных алгебр см. §2). В дальнейшем мы для краткости используем обозначение $\mathrm{Br}\,X$, подразумевая под этим группу $\mathrm{Br}_{nr}(k(X))$.

В случае неособых коник C над k известно, что $\mathrm{Br}\,C \cong \mathrm{Br}(k)$, когда коника C обладает k-рациональной точкой, а в противном случае $\mathrm{Br}\,C$ является гомоморфным образом группы $\mathrm{Br}(k)$ с ядром порядка 2. Таким образом, в случае кривых X рода 0 имеется вполне удовлетворительное описание группы $\mathrm{Br}\,X$. Но уже в случае кривых X рода 1 о группах $\mathrm{Br}\,X$ почти ничего не известно. Целью настоящей работы является описание абстрактной структуры подгруппы ${}_m\mathrm{Br}\,X$ m-кручения группы $\mathrm{Br}\,X$, где m — число, взаимно простое с характеристикой поля $\overline{k}$, в случае, когда X — эллиптическая кривая, определенная над k. Кроме того, для группы ${}_2\mathrm{Br}\,X$ в работе получено представление всех ее элементов в виде кватернионных алгебр.

Содержание работы таково. В §2 собраны определения и сведения, а также вспомогательные результаты, необходимые в дальнейшем. В §3 приводится редукция проблемы описания групп Брауэра кривых над k к проблеме описания кручения в группе k-рациональных точек их якобианов. §4 посвящен получению списка минимальных уравнений Вейерштрасса для эллиптических кривых над k. Описанию кручения группы k-рациональных точек эллиптических кривых (и тем самым получению описания абстрактной структуры их групп Брауэра) посвящен §5 . Наконец, в заключительных параграфах получено представление всех элементов группы ${}_2\mathrm{Br}\,E$ кватернионными алгебрами для произвольной эллиптической кривой E над недиадическим полем k.

В заключение авторы выражают благодарность Ж.-Л. Колье-Телену, П. Зальбергеру, А.С. Меркурьеву и Ж.-П. Тиньолю за внимание, проявленное к работе.

§2. Предварительные сведения и вспомогательные результаты

Ниже будут использованы следующие обозначения. Для любой абелевой группы A, записываемой аддитивно, через ${}_nA$ (соответственно nA), мы будем обозначать ядро (соответственно образ) эндоморфизма умножения на n в группе A, а через A/n группу A/nA. В случае мультипликативной записи вместо nA мы будем писать A^n. Группа характеров группы A будет обозначаться через $\chi(A)$. Для всякого коммутативного кольца R с единицей через R^* обозначается группа обратимых в R элементов. Первообразным корнем ε_m степени m из единицы называется всякий элемент порядка m в R^*. Пусть F — поле и $\mathrm{char}\,F$ — его характеристика. Тогда если $\varepsilon_m \in F$, то, очевидно, m и $\mathrm{char}\,F$ взаимно просты. Пусть F_s — сепарабельное замыкание поля F. Группа Галуа расширения $F_s|F$ будет обозначаться через $G(F)$. Для всякого дискретного $G(F)$-модуля A через $H^i(F,A)$ будет обозначаться i-я группа когомологий $H^i(G(F),A)$. Символом $\mathrm{Br}(F)$ будем обозначать

группу Брауэра поля F — группу классов эквивалентности центральных простых F-алгебр, гомологическая интерпретация которых такова: $\mathrm{Br}(F) = H^2(F, F_s^*)$.

В дальнейшем нам потребуются некоторые специальные сведения о полях.

Конечные поля. Конечное поле из q элементов будет обозначаться через $\mathbf{F}_q$. Для всякого поля $\mathbf{F}_q$ нечетной характеристики подгруппа $(\mathbf{F}_q^*)^2$ является подгруппой индекса 2 в $\mathbf{F}_q^*$. Для $u \in \mathbf{F}_q^*$ положим $(u/q) = 1$, если $u \in (\mathbf{F}_q^*)^2$ и $(u/q) = -1$ в противном случае. Пусть элемент $u \in \mathbf{F}_q$ такой, что $u(u+1) \neq 0$. Мы будем говорить, что в группе $\mathbf{F}_q^*$ реализуется комбинация $(+,+)$, если u и $u+1$ — квадраты; $(-,-)$, если u и $u+1$ — не квадраты; $(+,-)$, если u — квадрат, а $u+1$ — не квадрат; и, наконец, $(-,+)$, если u — не квадрат, а $u+1$ — квадрат. Ниже нам потребуется следующее утверждение о реализуемости предыдущих комбинаций.

Лемма 1. *Пусть* $\mathrm{char}\,\mathbf{F}_q \neq 2$. *Тогда для произвольного* $q \geq 7$ *в группе* $\mathbf{F}_q^*$ *реализуются все комбинации. В группе* $\mathbf{F}_5^*$ *не реализуется только комбинация* $(+,+)$, *а в группе* $\mathbf{F}_3^*$ *реализуется только комбинация* $(+,-)$.

Доказательство. Справедливость леммы в случае полей $\mathbf{F}_3$ и $\mathbf{F}_5$ устанавливается непосредственной проверкой. Вначале докажем лемму в случае, когда $q = p$ простое число. Пусть $p \geq 7$. Рассмотрим последовательность $\{x_n\}$ такую, что $x_n = (n/p)$, $n = 1, 2, \ldots, p-2$. Тогда поскольку $x_1 = 1$ и не все элементы в $\mathbf{F}_q^*$ — квадраты, то, двигаясь от начала последовательности к ее концу, мы установим реализуемость комбинации $(+,-)$. Заметим далее, что последовательность $\{x_n\}$ не может совпадать с последовательностью $\{(-1)^{n+1}\}$. Действительно, тогда бы $x_4 = -1$, что не так. Значит, в $\mathbf{F}_q$ реализуется хотя бы одна из комбинаций $(+,+)$ и $(-,-)$. Пусть вначале $(-1/p) = -1$. Тогда если $(u/p) = ((u+1)/p) = 1$, то $((-u-1)/p) = ((-u)/p) = -1$, т.е. с комбинацией $(+,+)$ обязательно реализуется и комбинация $(-,-)$. Аналогично, если $(u/p) = ((u+1)/p) = -1$, то $((-u-1)/p) = ((-u)/p) = 1$. Предположим, что не реализуется комбинация $(-,+)$. Число элементов, являющихся квадратами и число элементов, не являющихся квадратами в $\mathbf{F}_q^*$, одинаково и равно $(p-1)/2$. Если в последовательности $\{x_n\}$ имеется число (-1) с номером, не превосходящим $(p-1)/2$, то, двигаясь в последовательности $\{x_n\}$ от начала к концу, обязательно найдем два соседних члена, реализующих комбинацию $(-,+)$. Если в последовательности $\{x_n\}$ числа (-1) нет, то $(2/p) = ((p-1)/2/p) = 1$. Но тогда $(-1/p) = (((p-1)/2)/p)(2/p) = 1$, что не так по предположению. Таким образом, комбинация $(-,+)$ реализуется. Пусть $(-1/p) = 1$. Если $(u/p) = 1, ((u+1)/p) = -1$, то $((-u-1)/p) = -1, ((-u)/p) = 1$ и комбинация $(-,+)$ реализуется. Далее, предположим, что не реализуется комбинация $(-,-)$. Тогда в последовательности $\{x_n\}$ за всяким числом (-1) следует число $(+1)$, а так как $x_1 = 1$, то в $\mathbf{F}_q^*$ число элементов, являющихся квадратами, оказывается большим числа элементов, не являющихся квадратами, что невозможно. Если в $\mathbf{F}_q^*$ не реализуется комбинация $(+,+)$, то так как $(1/p) = (4/p) = 1$, то должно быть $(2/p) = (3/p) = -1$ и $(-1/p) = (-4/p) = 1$, $(-2/p) = (-3/p) = -1$, причем $2 \neq -3$. Кроме того, после каждого числа (-1) в последовательности $\{x_n\}$ следует число $(+1)$. Вычеркнув из последовательности $\{x_n\}$ все числа $(+1)$ со следующими за ними непосредственно (-1), получим только одно число $(+1)$, соответствующее

элементу (-1) поля $\mathbf{F}_q$, и не менее двух (-1), соответствующих 3 и -2, что невозможно. Таким образом, лемма доказана для всех полей $\mathbf{F}_p$, где p — простое число и $p \geq 7$. Далее, если m — нечетное число, то все элементы, не являющиеся квадратами из $\mathbf{F}_q^*$, остаются таковыми в $\mathbf{F}_{q^m}^*$, и все комбинации в $\mathbf{F}_{p^m}^*$ реализуются при $p \geq 7$. Пусть теперь m — произвольное, $q = p^m$. Покажем, что в поле $\mathbf{F}_{q^2}^*$ все комбинации реализуются. Поскольку все элементы из $\mathbf{F}_q$, не являющиеся квадратами, становятся квадратами в $\mathbf{F}_{q^2}$, то в $\mathbf{F}_{q^2}^*$ реализуется комбинация $(+,+)$. Далее, существует элемент $\mu \in \mathbf{F}_{q^2}^* \setminus \mathbf{F}_q^*$ такой, что в смежном классе $\mu + \mathbf{F}_q$ лежат и квадраты, и элементы, квадратами не являющиеся. Действительно, пусть для любого $\mu \in \mathbf{F}_{q^2}^* \setminus \mathbf{F}_q^*$ в смежном классе $\mu + \mathbf{F}_q$ лежат только квадраты либо квадратов нет вообще. Рассмотрим элементы $\eta, \theta \in \mathbf{F}_{q^2}^* \setminus \mathbf{F}_q^*$, лежащие в различных смежных классах по $\mathbf{F}_q$. Элементы $\theta(\eta-\theta)^{-1}+1$ и $\theta(\eta-\theta)^{-1}$ лежат в одном смежном классе по $\mathbf{F}_q$, и потому

$$\left(\frac{\theta(\eta-\theta)^{-1}+1}{q^2}\right) = \left(\frac{\theta(\eta-\theta)^{-1}}{q^2}\right).$$

Откуда получаем

$$\begin{aligned}\left(\frac{\eta}{q^2}\right) &= \left(\frac{(\eta-\theta)+\theta}{q^2}\right) = \left(\frac{(\eta-\theta)(\theta(\eta-\theta)^{-1}+1)}{q^2}\right)\\ &= \left(\frac{\eta-\theta}{q^2}\right)\left(\frac{\theta(\eta-\theta)^{-1}}{q^2}\right)\\ &= \left(\frac{\theta}{q^2}\right).\end{aligned}$$

Следовательно, $(\eta/q^2) = (\theta/q^2)$. Так как по предположению все элементы из одного смежного класса $\mu + \mathbf{F}_q$ либо одновременно являются квадратами, либо одновременно не являются квадратами, то мы заключаем, что $\mathbf{F}_{q^2}^* \setminus \mathbf{F}_q^*$ состоит либо только из квадратов, либо только из элементов, не являющихся квадратами. Так как число элементов множества $\mathbf{F}_{q^2}^* \setminus \mathbf{F}_q^*$ равно q^2-q, и $q^2-q > (q^2-1)/2$, то получено противоречие. Следовательно, существует элемент $\mu \in \mathbf{F}_{q^2}^* \setminus \mathbf{F}_q^*$ такой, что в смежном классе $\mu + \mathbf{F}_q$ есть как квадраты, так и элементы, квадратами не являющиеся. Пусть для определенности элемент μ является квадратом. Рассмотрим последовательность $\{z_n\}$, определяемую формулой $z_n = (\mu + (n-1)/q^2)$, тогда $z_1 = 1$. Поскольку не все элементы из $\mu + \mathbf{F}_q$ — квадраты, то переходя каждый раз от члена z_n к члену z_{n+1}, мы убеждаемся, что существует такое i, что $z_i = 1$, а $z_{i+1} = -1$. Далее, ввиду того что для всех j $z_{j+p} = z_j$, мы заключаем, что реализуется также и комбинация $(-,+)$. Во множестве $\mathbf{F}_{q^2}^* \setminus \mathbf{F}_q^*$ квадратов больше, чем элементов, не являющихся квадратами, поэтому существует элемент, $\mu \in \mathbf{F}_{q^2}^* \setminus \mathbf{F}_q^*$ такой, что в смежном классе $\mu + \mathbf{F}_q$ квадратов больше половины, а тогда комбинация $(-,-)$ реализуется среди элементов этого смежного класса. Таким образом, лемма доказана для всех конечных полей $\mathbf{F}_q$, характеристика которых не меньше 7.

Наконец, пусть $\operatorname{char} \mathbf{F}_q$ равна либо 3, либо 5. Доказательство для полей $\mathbf{F}_{q^2}$ в этом случае полностью аналогично доказательству в случае $\operatorname{char} \mathbf{F}_q \geq 7$. Предположим,

что $\mathbf{F}_q$ является расширением нечетной степени поля $\mathbf{F}_p$, где p есть 3 или 5. Если для произвольного $\mu \in \mathbf{F}_q^* \setminus \mathbf{F}_p^*$ смежный класс $\mu + \mathbf{F}_p$ состоит либо только из квадратов, либо квадратов не содержит вообще, то для произвольного $\eta \in \mathbf{F}_q^* \setminus \mathbf{F}_p^*$

$$\left(\frac{1+(\eta-1)^{-1}}{q^2}\right) = \left(\frac{\eta-1}{q^2}\right)$$

и

$$\begin{aligned}\left(\frac{\eta}{q^2}\right) &= \left(\frac{(\eta-1)+1}{q^2}\right) = \left(\frac{(\eta-1)(1+(\eta-1)^{-1})}{q^2}\right)\\ &= \left(\frac{\eta-1}{q^2}\right)\left(\frac{1+(\eta-1)^{-1}}{q^2}\right) = \left(\frac{\eta-1}{q^2}\right)^2\\ &= 1.\end{aligned}$$

Но равенство $(\eta/q^2) = 1$ для произвольного $\eta \in \mathbf{F}_q^* \setminus \mathbf{F}_p^*$ невозможно. Следовательно, существует элемент $\mu \in \mathbf{F}_q^* \setminus \mathbf{F}_p^*$ такой, что в смежном классе $\mu + \mathbf{F}_p$ содержатся как элементы-квадраты, так и элементы, квадратами не являющиеся, а тогда аналогично предыдущему в $\mathbf{F}_q^*$ реализуются комбинации $(+,-)$ и $(-,+)$. Если $\mu + \mathbf{F}_p$ — смежный класс, в котором есть и квадрат, и элемент, не являющийся квадратом, $\mu \in \mathbf{F}_q^* \setminus \mathbf{F}_p^*$, то, так как он содержит нечетное число элементов, заключаем, что хотя бы одна из комбинаций $(+,+)$, $(-,-)$ реализуется в $\mu + \mathbf{F}_p$. Пусть, например, комбинация $(+,+)$ реализуется, а комбинация $(-,-)$ — нет. Тогда в $\mu + \mathbf{F}_p$ квадратов больше половины, а так как в $\mathbf{F}_q^* \setminus \mathbf{F}_p^*$ количество элементов, являющихся квадратами, и количество элементов, квадратами не являющихся, одинаково, то в $\mathbf{F}_q^* \setminus (\mathbf{F}_p \bigcup (\mu + \mathbf{F}_p^*))$ квадратов больше, и потому существует элемент $\tau \in \mathbf{F}_q^* \setminus (\mathbf{F}_p \bigcup (\mu + \mathbf{F}_p^*))$ такой, что в классе $\tau + \mathbf{F}_p$ реализуется ситуация $(-,-)$. Аналогичное рассуждение применимо и в случае, когда в $\mu + \mathbf{F}_p$ реализуется комбинация $(-,-)$, но не реализуется $(+,+)$. Лемма доказана. •

Предложение 1. *Пусть* $s(x) = \alpha(x^2 + ax + b)$ *— многочлен из* $\mathbf{F}_q[x]$, *не имеющий кратных корней,* $q \geq 7$. *Тогда существуют элементы* $u, v \in \mathbf{F}_q$, *со свойством* $u \neq -a/2, v \neq 0$, *такие, что* $v^2 = \alpha(u^2 + au + b)$.

Доказательство. Положим $\Delta = a^2 - 4b$. Тогда

$$s(x) = -\frac{\alpha\Delta}{4}\left(\frac{-4}{\Delta}(x + a/2)^2 + 1\right).$$

Пусть вначале

$$\text{a)} \quad -\Delta \in (\mathbf{F}_q^*)^2, \ \alpha \in (\mathbf{F}_q^*)^2.$$

Тогда $-\alpha\Delta/4, -4/\Delta \in (\mathbf{F}_q^*)^2$. В силу леммы 1 существует элемент $c \in \mathbf{F}_q^*$ такой, что $c^2 + 1 = t^2, t \in \mathbf{F}_q^*$. Положим $u = -a/2 + \sqrt{-\Delta c^2/4}$. Тогда $s(u) = -\alpha\Delta t^2/4$ и достаточно положить $v = t\sqrt{-\alpha\Delta/4}$. Аналогично рассматриваются случаи

$$\text{b)} \quad -\Delta \in (\mathbf{F}_q^*)^2, \ \alpha \notin (\mathbf{F}_q^*)^2;$$

$$\text{c)} \quad -\Delta \notin (\mathbf{F}_q^*)^2, \ \alpha \in (\mathbf{F}_q^*)^2;$$

$$\text{d)} \quad -\Delta \notin (\mathbf{F}_q^*)^2, \ \alpha \notin (\mathbf{F}_q^*)^2.$$

Предложение доказано. •

Обозначим через $\mathbf{F}_q^*(\delta)$ множество специализаций многочлена $x^2+\delta$ ($\delta \in \mathbf{F}_q^*$), лежащих в $\mathbf{F}_q^*$, элементами из $\mathbf{F}_q^*$, q — нечетное.

Следствие 1. *Пусть $q \geq 7$. Тогда множество $\mathbf{F}_q^*(\delta)$ содержит как элементы, являющиеся квадратами, так и элементы, квадратами не являющиеся. Множество $\mathbf{F}_5^*(\delta)$ содержит элементы обоих типов, если $\delta \notin (\mathbf{F}_5^*)^2$ и только элементы, не являющиеся квадратами, если $\delta \in (\mathbf{F}_5^*)^2$. Множество $\mathbf{F}_3^*(\delta)$ пусто, если $\delta \notin (\mathbf{F}_3^*)^2$, и состоит из элемента, не являющегося квадратом, если $\delta \in (\mathbf{F}_5^*)^2$.*

Локальные поля нулевой характеристики. Всякое такое поле k является конечным расширением поля p-адических чисел $\mathbf{Q}_p$ и обладает нормированием v_k, являющимся однозначным продолжением стандартного нормирования поля $\mathbf{Q}_p$. Кольцо нормирования v_k обозначается через $A(k)$, его максимальный идеал — через $M(k)$, а его поле вычетов $A(k)/M(k)$ — через $\overline{k}$. Для всякого $a \in A(k)$ через $\overline{a}$ будет обозначаться образ a в $\overline{k}$ при естественном гомоморфизме $A(k)$ в $A(k)/M(k)$. Если $f(x)=\sum_{i=0}^n a_i x^i$ — многочлен с коэффициентами в $A(k)$, то $\overline{f}(x)$ будет обозначать многочлен $\sum_{i=0}^n \overline{a}_i x^i$. Простой элемент поля k — это произвольная образующая идеала $M(k)$. Поле k называется диадическим, если $\operatorname{char}\overline{k}=2$ и недиадическим в противном случае. С нормированием v_k также связана группа единиц $U(k)=A(k)^*$. Ее подгруппа $1+M(k)=\{1+a \mid a \in M(k)\}$ обладает свойством однозначности извлечения корня n-й степени. Точнее, имеет место

Предложение 2. *Пусть F — поле с гензелевым нормированием v, $M(F)$ — идеал нормирования v, а $\overline{F}$ — его поле вычетов. Пусть натуральное n взаимно просто с характеристикой поля $\overline{F}$. Тогда для всякого элемента $a \in 1+M(F)$ существует и единствен элемент $b \in 1+M(F)$ такой, что $b^n=a$.*

Таким образом, элемент $u \in U(k)$ тогда и только тогда является n-й степенью в k^*, когда $\overline{u} \in (\overline{k}^*)^n$ (n взаимно просто с $\operatorname{char}\overline{k}$). В частности, $u \in U(k)$ — квадрат в недиадическом поле тогда и только тогда, когда $\overline{u}$ — квадрат в $\overline{k}^*$.

В заключение зафиксируем $\alpha \in U(k) \setminus U(k)^2$ и простой элемент π поля k.

Нормирования и пополнения специальных полей алгебраических функций. Для произвольного поля F и трансцендентного над F элемента t через $F\langle t\rangle$ ниже будет обозначаться поле формальных степенных рядов от t с коэффициентами в F.

Пусть k — поле нулевой характеристики, $k[x]$ — кольцо многочленов от x с коэффициентами в k, $f(x)$ — многочлен из $k[x]$ без кратных корней, $k(x)$ — поле частных кольца $k[x]$ и $L=k(x)(\sqrt{f(x)})$. Тогда все нормирования поля $k(x)$, тривиальные над k, дискретны и могут быть двух типов: нормирования v_h, имеющие своими униформизующими унитарные неприводимые над k многочлены $h(x) \in k[x]$ и нормирование v_∞ с униформизующей x^{-1}. Пополнения поля $k(x)$ относительно этих нормирований будем обозначать соответственно через $k(x)_h$ и $k(x)_\infty$. Всякое нормирование поля $k(x)$, тривиальное на k, продолжается до нормирования поля L не более чем двумя способами, причем если таких продолжений два, то соответствующие пополнения k-изоморфны.

Через L_h (соответственно L_∞) будем обозначать либо пополнение L относительно единственного продолжения v_h (соответственно v_∞) до нормирования поля L, либо произвольное из двух пополнений этого поля относительно продолжений v_h (соответственно v_∞). Если θ — корень многочлена $h(x)$, то эти пополнения описываются следующим образом:

$$k(x)_h \cong k(\theta)\langle h(x)\rangle,$$

$$L_h \cong \begin{cases} k(\theta)(\sqrt{f(\theta)}), & \text{если } h(x) \text{ не делит } f(x), \\ k(\theta)\langle h(x)\rangle\big(\sqrt{g(\theta)h(x)}\big), & \text{если } f(x) = g(x)h(x), \end{cases}$$

$$k(x)_\infty \cong k\langle x^{-1}\rangle,$$

$$L_\infty \cong \begin{cases} k\langle x^{-1}\rangle(\sqrt{x^{-1}}) = k\langle\sqrt{x^{-1}}\rangle, & \text{если } f(x) \text{ имеет нечетную степень}, \\ k\langle x^{-1}\rangle, & \text{если } f(x) \text{ имеет четную степень}. \end{cases}$$

Нам понадобится явный вид указанных изоморфизмов. Для его получения заметим, что при каноническом эпиморфизме кольца нормирования дискретного нормирования v_h поля $k(x)$ на поле вычетов $k(\theta)$ элемент x переходит в θ. Соответствие $x \mapsto \theta$ определяет вложение $k(x)$ в свое v_h-пополнение $k(\theta)\langle h(x)\rangle$, причем образом $f(x)$ является $f(\theta)$ при $f(\theta) \neq 0$ и $g(\theta)h(x)$ при $f(x) = g(x)h(x)$. Это вложение продолжается до вложения поля L в алгебраическое замыкание поля $k(\theta)\langle h(x)\rangle$, и если образ L при этом вложении обозначить через L', то $L_h = k(x)_h L'$. Отсюда и получаются явные выражения для указанных изоморфизмов.

Эллиптические кривые. Ниже повсюду E обозначает определенную над полем k эллиптическую кривую, т.е. неособую проективную кривую рода 1 с k-рациональной точкой. Хорошо известно, что с точностью до k-изоморфизма кривая E может рассматриваться как замыкание в $\mathbf{P}^2$ некоторой неособой кубической кривой в $\mathbf{A}^2$, задаваемой уравнением вида

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in k,$$

называемым уравнением Вейерштрасса. Два уравнения Вейерштрасса задают одну и ту же кривую тогда и только тогда, когда получаются друг из друга заменой переменных вида

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t, \quad \text{где } u, r, s, t \in k,\ u \neq 0.$$

Кроме того, всякое уравнение Вейерштрасса, задающее неособую кубическую кривую в $\mathbf{P}^2$, задает эллиптическую кривую над k. Если $\operatorname{char} k \neq 2$, то замена переменной y на $(1/2)(y - a_1x - a_3)$ приводит вейерштрассово уравнение к виду

$$y^2 = 4x^3 + b_2x^2 + b_4x + b_6,$$

где

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

Положим также

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 - a_2 a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6,$$
$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27 b_6^2 + 9 b_2 b_4 b_6, \quad j = c_4^3/\Delta, \quad \text{если } \Delta \neq 0.$$

Условие $\Delta \neq 0$ эквивалентно неособости кривой, определяемой уравнением Вейерштрасса, так что для эллиптической кривой E всегда определен элемент $j \in k$, называемый ее j-инвариантом, причем две эллиптические кривые, определенные над k, k_s-изоморфны тогда и только тогда, когда их j-инварианты совпадают. Ниже нам потребуются выражения элементов c_4, c_6 и Δ в случае, когда кривая E задается уравнением $y^2 = x(x^2 + Ax + B)$:

$$c_4 = 16(A^2 - 3B), \qquad c_6 = 32A(2A^2 + 9B), \qquad \Delta = 16B^2(A^2 - 4B).$$

Пусть теперь k — локальное поле нулевой характеристики. Тогда, очевидно, E может быть задана уравнением Вейерштрасса, для которого $a_i \in A(k)$. Для всякого поля K, содержащего поле k, пусть $E(K)$ обозначает множество K-рациональных точек E. На множестве $E(K)$ может быть задана операция сложения, превращающая его в абелеву группу. Нейтральным элементом (нулем 0) относительно этой групповой операции является бесконечная точка. Далее, если $P_0 = (x_0, y_0) \in E)$, то $-P_0 = (x_0, -y_0 - a_1 x_0 - a_3)$, абсцисса точки $2P_0$ определяется формулой

$$x(2P_0) = \frac{x_0^4 - b_4 x_0^2 - 2b_6 x_0 - b_8}{4x_0^3 + b_2 x_0^2 + 2b_4 x_0 + b_6},$$

а для точек $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ таких, что $P_1 \neq \pm P_2$,

$$x(P_1 + P_2) = \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 + a_1\Big(\frac{y_2 - y_1}{x_2 - x_1}\Big) - a_2 - x_1 - x_2.$$

В частности, если уравнение кривой имеет вид $y^2 = x(x^2 + Ax + B)$, то $x(2P_0) = (x_0^2 - B)^2/(4y_0^2)$ при $y_0 \neq 0$ и $2P_0 = 0$ при $y_0 = 0$.

Естественный гомоморфизм $A(k) \longrightarrow A(k)/M(k) = \overline{k}$ позволяет по кривой E, заданной минимальным уравнением Вейерштрасса, определить редукцию этой кривой как кривую $\widetilde{E}$, определенную над $\overline{k}$ уравнением

$$y^2 + \overline{a}_1 xy + \overline{a}_2 y = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6.$$

Поскольку у каждой точки из $E(k) \subset \mathbf{P}^2(k)$ существуют однородные координаты, принадлежащие $A(k)$, то существует и однозначно определенное отображение редукции $R\colon E(k) \longrightarrow \widetilde{E}(\overline{k})$. Кривая $\widetilde{E}$, вообще говоря, не является эллиптической, поэтому естественно выделить в ней множество неособых точек $\widetilde{E}_{ns}(\overline{k})$, а в группе $E(k)$ подмножества

$$E_0(k) = \{\, P \in E(k) : R(P) \in \widetilde{E}_{ns}(\overline{k}) \,\},$$
$$E_1(k) = \{\, P \in E(k) : R(P) = 0 \,\}.$$

Нетрудно видеть, что с помощью отображения редукции групповая операция на $E(k)$ может быть перенесена на $\widetilde{E}_{ns}(\overline{k})$ и ограничение R на $E_0(k)$ является эпиморфизмом группы $E_0(k)$ на $\widetilde{E}_{ns}(\overline{k})$ с ядром E_k. Эллиптические кривые подразделяются на кривые с хорошей редукцией, когда $\widetilde{E}$ — эллиптическая кривая (что эквивалентно $v_k(\Delta) = 0$), и кривые с плохой редукцией, когда $\widetilde{E}$ не является эллиптической кривой. В последнем случае различают аддитивную редукцию, когда особенность $\widetilde{E}$ является точкой возврата и мультипликативную редукцию, когда особенность есть узловая точка. Мультипликативная редукция бывает двух типов: разложимая мультипликативная редукция, при которой обе касательные в особой точке определены над k и неразложимая в противном случае.

Наконец, нам потребуются некоторые сведения о группах $E_0(k)$, $E_1(k)$, $\widetilde{E}_{ns}(\overline{k})$ и $E(k)/E_0(k)$.

Предложение 3. *Если E — эллиптическая кривая над k, то в случае аддитивной редукции группа $\widetilde{E}_{ns}(\overline{k})$ изоморфна аддитивной группе $\overline{k}^+$ поля $\overline{k}$, а в случае мультипликативной редукции $\widetilde{E}_{ns}(\overline{k}) \cong \overline{k}^*$.*

Предложение 4. *Группа $E_1(k)$ является группой без кручения и, если m взаимно просто с $\operatorname{char}\overline{k}$, то $E_1(k)$ однозначно m-делима.*

Из последнего предложения без труда получается следующее утверждение:

Предложение 5. *Если $(m, \operatorname{char}\overline{k}) = 1$, то ${}_mE(k) \cong {}_m\widetilde{E}_{ns}(\overline{k})$.*

Теорема 1 (Кодаира-Нерон). *Пусть E — эллиптическая кривая над k с расщепимой мультипликативной редукцией. Тогда $E(k)/E_0(k)$ — циклическая группа порядка $v_k(\Delta) = -v_k(j)$. Во всех остальных случаях группа $E(k)/E_0(k)$ имеет порядок не больший чем 4.*

Ввиду дискретности v_k существует уравнение Вейерштрасса для E с коэффициентами из $A(k)$ с минимальным значением $v_k(\Delta)$. Всякое такое уравнение называется минимальным уравнением для E. Известно, что минимальное уравнение для E единственно с точностью до замены координат

$$x = u^2x' + r,\ \ y = u^3y' + u^2sx' + t, \quad \text{где} \quad u \in U(k),\ \ r, s, t \in A(k).$$

Причем при такой замене $\Delta = u^{12}\Delta'$. В недиадическом случае всегда имеется минимальное уравнение Вейерштрасса кривой E такое, что $a_1 = a_3 = 0$. Действительно, если минимальное уравнение Вейерштрасса таково, что хотя бы один из коэффициентов a_1, a_3 не равен нулю, то замена переменных $x = (1/2)x'$, $y = (1/2)y' - (a_1/4)x' - a_3/4$ приводит нас к уравнению

$$(y')^2 = (x')^3 + A(x')^2 + Bx' + C,$$

которое минимально ввиду $\Delta' = 2^{12}\Delta$. Если теперь $y^2 = x^3 + A_1x^2 + B_1x + C_1$ и $y^2 = x^3 + A_2x^2 + B_2x + C_2$ — два минимальных уравнения Вейерштрасса кривой E,

то ясно, что тип разложения многочленов $x^3+A_1x^2+B_1x+C_1$ и $x^3+A_2x^2+B_2x+C_2$ один и тот же, что позволяет нам после замены $x = x' - a$ различать три типа минимальных уравнений Вейерштрасса.

1. Разложимый случай: $y^2 = x(x-e_1)(x-e_2)$, $e_1, e_2 \in A(k)$.

2. Полуразложимый случай: $y^2 = x(x^2+Ax+B)$, $A, B \in A(k)$ и многочлен $x(x^2+Ax+B)$ неприводим над k.

3. Неразложимый случай: $y^2 = x^3+Mx^2+Nx+P$, $M, N, P \in A(k)$ и многочлен x^3+Mx^2+Nx+P неприводим над k.

Ниже для определения специальных типов минимальных уравнений кривой E в недиадическом случае и описания групповой структуры множества $E(k)$ нам потребуется следующий упрощенный вариант алгоритма Тэйта [7] (вместе с соответствующими сведениями о группе $E(k)/E_0(k)$), описывающий переход от произвольного уравнения Вейерштрасса с коэффициентами в $A(k)$ к минимальному.

Итак, пусть $\operatorname{char}\overline{k} \neq 2$ и кривая E задана уравнением Вейерштрасса

$$y^2 = f(x), \tag{1}$$

где $f(x) = x^3+a_2x^2+a_4x+a_6$, $a_2, a_4, a_6 \in A(k)$ и $\Delta = -8(2a_2^2+a_4^2+64a_6^2-36a_2a_4a_6)$. Оказывается, что уравнение (1) минимально во всех нижеперечисленных случаях 1–6, за исключением случая $6c_4$. Рассмотрим эти случаи.

1. Если $\Delta \in U(k)$, то E — кривая с хорошей редукцией и $E(k)/E_0(k) = \langle 0\rangle$. Ниже $\Delta \notin U(k)$. В этом случае многочлен $\overline{f}(x)$ имеет кратный корень $\widetilde{u}$. Тогда замена $x' = x-u$, где $\overline{u} = \widetilde{u}$, показывает, что, не ограничивая общности, можно предполагать $a_4, a_6 \in M(k)$.
2. Пусть $a_2 \in U(k)$. Тогда E — кривая с мультипликативной редукцией и $E(k)/E_0(k) \cong \mathbf{Z}/m$. Ниже $a_2, a_4, a_6 \in M(k)$.
3. Если $v_k(a_6) = 1$, то $E(k)/E_0(k) = \langle 0\rangle$.
4. Пусть $\pi^2 | a_6$ и $v_k(a_4) = 1$. Тогда $E(k)/E_0(k) \cong \mathbf{Z}/2$.
5. Если $v_k(a_6) = 2$, $\pi^2 | a_4$, то $E(k)/E_0(k) \cong \mathbf{Z}/3$, если $\overline{a_6\pi^{-2}} \in (\overline{k}^*)^2$, и $E(k)/E_0(k) = \langle 0\rangle$ в противном случае.
6. Пусть π^3 делит a_6, π^2 делит a_4 и π делит a_2. Тогда с помощью замены переменных $x = \pi x'$, $y = \pi^2 y'$ мы приходим к уравнению

$$\pi(y')^2 = P(x'), \quad \text{где } P(x') = \frac{1}{\pi^3} f(\pi x'). \tag{2}$$

6a. Многочлен $\overline{P}(x)$ не имеет кратных корней. В этом случае $[E(k) : E_0(k)] = 1 + (\text{число корней } \overline{P}(x) \text{ в } \overline{k})$.

6b. Многочлен $\overline{P}(x)$ имеет двукратный корень. В этом случае индекс $[E(k) : E_0(k)]$ равен либо 2, либо 4.

6c. Если $\overline{P} = (x-\beta)^3$, $\beta \in \overline{k}$, то замена $x = x' - u$, $\overline{u} = \beta$ показывает, что, не ограничивая общности, можно считать, что $\beta = 0$. Откуда следует, что π^2 делит a_2, π^3 делит a_4 и π^4 делит a_6.

$6c_1$. Пусть $v_k(a_6) = 4$. Тогда $E(k)/E_0(k) \cong \mathbf{Z}/3$, при $\overline{a_6\pi^{-4}} \in (\overline{k}^*)^2$ и $E(k)/E_0(k) = \langle 0\rangle$ в противном случае.

$6c_2$. Если $\pi^5|a_6$ и $v_k(a_4)=3$, то $E(k)/E_0(k)\cong \mathbf{Z}/2$.

$6c_3$. Если $v_k(a_6)=5$, $\pi^4|a_4$, то $E(k)/E_0(k)=\langle 0\rangle$.

$6c_4$. При $\pi^6|a_6$ и $\pi^4|a_4$ уравнение (1) не является минимальным.

Ниже для определения структуры 3^n-кручения группы $E(k)$ нам потребуется следующее

Предложение 6. *Пусть E — эллиптическая кривая с аддитивной редукцией над локальным полем k. Тогда справедливы следующие утверждения.*

1. *Если k — недиадическое поле, то $[E(k):E_0(k)]=3$ тогда и только тогда, когда имеет место неразложимый случай и кривая E может быть задана минимальным уравнением вида $y^2=x^3+a_2x^2+a_4x+a_6$ с одним из следующих условий на коэффициенты:*

(i) $\pi|a_2$, $\pi^2|a_4$, $v_k(a_6)=2$ *и* $a_6\in(k^*)^2$,

(ii) $\pi^2|a_2$, $\pi^3|a_4$, $v_k(a_6)=4$ *и* $a_6\in(k^*)^2$.

2. *Если k — диадическое поле, то $[E(k):E_0(k)]=3$ тогда и только тогда, когда кривая E может быть задана минимальным уравнением вида $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ с одним из следующих условий на коэффициенты:*

(i) $\pi|a_1$, $v_k(a_3)=1$, $\pi|a_4$, $\pi^2|a_6$, $\pi^3|(a_2a_3^2-a_4^2)$ *и многочлен* $x^2+\overline{a_3\pi^{-1}}x+\overline{a_6\pi^{-2}}$ *имеет корни в* $\overline{k}$,

(ii) $\pi|a_1$, $\pi^2|a_3$, $\pi^3|a_4$, $\pi^4|a_6$ *и многочлен* $x^2+\overline{a_3\pi^{-1}}x+\overline{a_6\pi^{-2}}$ *имеет в* $\overline{k}$ *различные корни.*

Доказательство. Из приведенного выше упрощенного варианта алгоритма Тэйта для недиадического поля k непосредственно следует, что $[E(k):E_0(k)]=3$ только в двух случаях:

a) имеет место случай 5 (в нумерации, приведенной в алгоритме) вместе с ограничением $\overline{a_6\pi^{-2}}\in(k^*)^2$, что в точности приводит к условию 1 (i), либо

b) имеет место случай $6c_1$ вместе с ограничением $\overline{a_6\pi^{-4}}\in(k^*)^2$, что приводит к условию 1 (ii).

Рассмотрим теперь случай диадического поля k. Воспользуемся для этого общим алгоритмом Тэйта [7], из которого немедленно вытекает, что в случае аддитивной редукции $[E(k):E_0(k)]=3$ тогда и только тогда, когда имеет место один из следующих двух случаев (в обозначениях [7])

a) случай IV со следующим дополнительным условием многочлен $x^2+\overline{a_3\pi^{-1}}x+\overline{a_6\pi^{-2}}$ имеет корни в $\overline{k}$, либо

b) случай IV* и многочлен $x^2+\overline{a_3\pi^{-2}}x+\overline{a_6\pi^{-4}}$ имеет корни в $\overline{k}$.

Для получения необходимых и достаточных условий на коэффициенты минимальных уравнений, соответствующих случаям IV и IV*, частично повторим алгоритм Тэйта.

В силу того что редукция плохая, можно предполагать, что $\pi|a_3$, $\pi|a_4$ и $\pi|a_6$.

Аддитивность редукции влечет условие $\pi|b_2$, что в диадическом случае эквивалентно $\pi|a_1$.

Случай, обозначенный символом Кодаиры II, не имеет места, а потому $\pi^2|a_6$.

Случай III исключаем, накладывая условие $\pi^3|b_8$, что равносильно $\pi^3|(a_2a_3^2-a_4^2)$. Тогда IV реализуется в том и только том случае, когда $\pi^3|b_8$ или $v(a_3)=1$.

Пусть теперь $\pi^2|a_3$. Тогда можно предполагать, что $\pi|a_1, \pi|a_2, \pi^2|a_3, \pi^2|a_4$ и $\pi^3|a_6$.

Опуская не интересующие нас случаи I_0^* и I_ν^*, получаем, что многочлен $x^3+\overline{a_2\pi^{-1}}x^2+\overline{a_4\pi^{-2}}x+\overline{a_6\pi^{-3}}$ имеет трехкратный корень. Тогда, не ограничивая общности, можно предполагать, что $\pi^2|a_2, \pi^3|a_4$ и $\pi^4|a_6$.

Наконец, для выделения случая IV* накладываем условие: многочлен $x^2+\overline{a_3\pi^{-2}}x+\overline{a_6\pi^{-3}}$ имеет различные корни. •

Ниже нам потребуются следующие сведения об алгебрах кватернионов.

Определение 1. Алгеброй кватернионов над полем F называется четырехмерная алгебра над F с базисом $\{1,u,v,t\}$ и определяющими соотношениями для элементов базиса:

A) $1\cdot u=u\cdot 1=u$, $1\cdot v=v\cdot 1=v$, $1\cdot t=t\cdot 1=t$;

B) $u^2=a$, $v^2=b$, $t^2=-ab$; $a,b\in F^*$;

C) *элементы u, v, t попарно антикоммутируют между собой.*

Такая алгебра обозначается через $(a,b\mid F)$ либо через

$$\left(\frac{a,b}{F}\right).$$

Хорошо известно, что $(a,b\mid F)$ — центральная простая алгебра над F и, следовательно, по теореме Веддербарна является либо центральным над F телом, либо изоморфна (над F) полной матричной алгебре над полем F. Если $(a,b\mid F)$ изоморфна полной матричной алгебре над F, то мы будем кратко писать $(a,b|F)\sim 1$. Вообще, если центральная простая алгебра A над полем F F-изоморфна полной матричной алгебре над F, то мы называем A тривиальной и пишем $A\sim 1$. Приведем теперь ряд свойств алгебр кватернионов, необходимых нам в дальнейшем.

1.
$$\left(\frac{a,b}{F}\right)\otimes_F\left(\frac{a,c}{F}\right)\cong M_2\left(\left(\frac{a,bc}{F}\right)\right),$$

где $M_2((a,bc\mid F))$ — полная матричная алгебра над F-алгеброй $(a,bc\mid F)$.

2.
$$\left(\frac{a,b}{F}\right)\sim 1 \quad \text{тогда и только тогда, когда} \quad b\in N_{F(\sqrt{a})F}(F(\sqrt{a})^*).$$

В частности,

$$\left(\frac{a,1}{F}\right)\sim 1,\qquad \left(\frac{a,c^2}{F}\right)\sim 1,\qquad \left(\frac{a,b}{F}\right)\sim\left(\frac{-ab,b}{F}\right).$$

3. Если L — расширение поля F, то
$$\left(\frac{a,b}{F}\right)\otimes_F L\cong\left(\frac{a,b}{L}\right).$$

4. Если k — локальное поле, то группа ${}_2\mathrm{Br}(k)$ состоит из двух элементов, представителями которых могут быть алгебры $(\pi, 1 \mid k)$ и $(\pi, \alpha \mid k)$. Для произвольной алгебры $(a, b \mid k)$ и произвольного квадратичного расширения L поля k

$$\left(\frac{a,b}{k}\right) \otimes_k L \sim 1.$$

Напомним, что для произвольного поля формальных степенных рядов $F\langle y\rangle$ алгебра кватернионов над $F\langle y\rangle$ называется неразветвленной (над $F\langle y\rangle$), если она имеет вид $(a, b \mid k) \otimes_F F\langle y\rangle$. Далее, если E — эллиптическая кривая, определенная над k, A — алгебра кватернионов над $k(E)$, то A называется неразветвленной над $k(E)$, если для произвольного дискретного тривиального над k нормирования v поля $k(E)$ и его пополнения $k(E)_v$ алгебра $A \otimes_{k(E)} k(E)_v$ неразветвлена над $k(E)_v$. Наконец, если $k(E)$ — квадратичное расширение поля рациональных функций $k(x)$, то для проверки неразветвленности над $k(E)$ алгебры $(f(x), g(x) \mid k(E))$, где $f(x), g(x) \in k[x]$, достаточно проверить неразветвленность алгебр $(f(x), g(x) \mid k(E)_v)$ для тех нормирований v, которые продолжают нормирования поля k, соответствующие неприводимым делителям $f(x)$ и $g(x)$, а также для нормирования, соответствующего бесконечной точке.

§3. Кручение групп Брауэра кривых и их якобианов

Пусть k — локальное поле, C — гладкая абсолютно неприводимая проективная кривая, определенная над k. Предположим также, что множество k-рациональных точек кривой C непусто. Хорошо известна следующая точная последовательность (см., например, [5]):

$$0 \longrightarrow \mathrm{Pic}(C) \longrightarrow H^0(k, \mathrm{Pic}(\overline{C})) \longrightarrow \mathrm{Br}(k) \xrightarrow{\alpha} \mathrm{Br}\, C \longrightarrow H^1(k, \mathrm{Pic}(\overline{C})) \longrightarrow H^3(k, k^*).$$

Так как порядок ядра гомоморфизма α совпадает с индексом кривой C, (который, в свою очередь, равен наибольшему общему делителю степеней k-рациональных дивизоров на C), то наличие у кривой C k-рациональной точки влечет тривиальность индекса C и тем самым инъективность α. С учетом локальности k (см. [8]) $H^3(k, k^*) = 0$. Таким образом, имеем точную последовательность

$$0 \longrightarrow \mathrm{Br}(k) \longrightarrow \mathrm{Br}\, C \longrightarrow H^1(k, \mathrm{Pic}(\overline{C})) \longrightarrow 0.$$

Пусть n — натуральное число, $n > 1$. Переход к n-кручению в предыдущей последовательности с учетом n-делимости $\mathrm{Br}(k)$ дает нам точную последовательность

$$0 \longrightarrow {}_n\mathrm{Br}\, k \longrightarrow {}_n\mathrm{Br}\, C \longrightarrow {}_nH^1(k, \mathrm{Pic}(\overline{C})) \longrightarrow 0. \tag{3}$$

Короткая точная тройка

$$0 \longrightarrow \mathrm{Pic}^0(\overline{C}) \longrightarrow \mathrm{Pic}(\overline{C}) \longrightarrow \mathbf{Z} \longrightarrow 0$$

порождает следующую точную последовательность:

$$H^0(k,\mathrm{Pic}(\overline{C})) \xrightarrow{\deg} H^0(k,\mathbf{Z}) \longrightarrow H^1(k,\mathrm{Pic}^0(\overline{C})) \longrightarrow H^1(k,\mathrm{Pic}(\overline{C})) \longrightarrow H^1(k,\mathbf{Z}).$$

Так как $H^1(k,\mathbf{Z}) = 0$ и гомоморфизм deg сюръективен (ввиду непустоты множества k-рациональных точек кривой C), то

$$H^1(k,\mathrm{Pic}^0(\overline{C})) \cong H^1(k,\mathrm{Pic}(\overline{C})).$$

Обозначим через J_C якобиево многообразие кривой C. Тогда G-модули $\mathrm{Pic}^0(\overline{C})$ и J_C изоморфны, и поэтому

$$H^1(k,\mathrm{Pic}(\overline{C})) \cong H^1(k,J_C).$$

В силу двойственности Шафаревича–Тэйта (см. [9]) группа $H^1(k,J_C)$ канонически изоморфна группе характеров $\chi(\widehat{J}_C(k))$, где $\widehat{J}_C$ — многообразие, двойственное J_C. Поскольку J_C — якобиево многообразие, то $\widehat{J}_C$ k-изоморфно J_C. Откуда следует, что

$$ {}_nH^1(k,\mathrm{Pic}(\overline{C})) \cong {}_n\chi(J_C(k)). \tag{4}$$

В свою очередь

$$ {}_n\chi(J_C(k)) \cong \mathrm{Hom}(J_C(k),\mathbf{Z}/n) \cong \mathrm{Hom}(J_C(k)/n,\mathbf{Z}/n) \cong J_C(k)/n. \tag{5}$$

(Последний изоморфизм ввиду конечности $J_C(k)/n$). В силу (3), (4), (5) получаем короткую точную последовательность

$$0 \longrightarrow {}_n\mathrm{Br}(k) \longrightarrow {}_n\mathrm{Br}\,C \longrightarrow J_C(k)/n \longrightarrow 0.$$

Поскольку группа ${}_n\mathrm{Br}(k)$ циклическая и имеет порядок n, то справедливо предложение

Предложение 7. ${}_n\mathrm{Br}\,C \cong \mathbf{Z}/n \oplus J_C(k)/n$.

Следствие 2. $|{}_n\mathrm{Br}\,C| = n|{}_nJ_C(k)||\overline{k}|^{v_k(n)}$.

Действительно, из предложения следует, что $|{}_n\mathrm{Br}\,C| = n|J_C(k)/n|$ и, кроме того, $|J_C(k)/n| = n|{}_nJ_C(k)||\overline{k}|^{v_k(n)}$ (см. [10]).

§4. Минимальные уравнения Вейерштрасса эллиптических кривых над недиадическими полями

Ниже поле k локальное и $\mathrm{char}\,\overline{k} \neq 2$. Нашей целью является получение списка минимальных уравнений для всех эллиптических кривых над k.

Теорема 2. *Пусть E — эллиптическая кривая над k, для которой имеет место разложимый случай. Тогда минимальное уравнение кривой E содержится в следующем списке, причем все уравнения из списка минимальны для задаваемых ими кривых.*

E имеет хорошую *редукцию.* $y^2 = x(x-e_1)(x-e_2)$, $e_1, e_2 \in A(k)$, $\overline{e_1 e_2} \neq 0$, $\overline{e_1} \neq \overline{e_2}$.

E имеет плохую *редукцию.* $a, b \in U(k)$.

I$_1$. $y^2 = x(x+\alpha)(x-\pi^m a)$, $m > 0$ (*редукция неразложимая мультипликативная*).

I$_2$. $y^2 = x(x+1)(x-\pi^m a)$, $m > 0$ (*редукция разложимая мультипликативная*).

II. $y^2 = x(x-\pi a)(x-\pi b)$, $a \neq b$ (*аддитивная редукция*).

III. $y^2 = x(x-\pi a)(x-\pi^m b)$, $m > 1$ (*аддитивная редукция*).

Доказательство. Воспользуемся алгоритмом Тэйта. Как отмечалось выше, E обладает минимальным уравнением $(y')^2 = (x')^3 + A(x')^2 + Bx' + C$. Поскольку мы рассматриваем разложимый случай, то k является полем разложения многочлена в правой части уравнения. Положив $x = x' - s$, где s — один из его корней, можем без ограничения общности считать, что кривая E обладает минимальным уравнением вида

$$y^2 = x(x-e_1)(x-e_2). \tag{6}$$

В случае хорошей редукции немедленно получаем $\bar{e}_1\bar{e}_2 \neq 0$ и $\bar{e}_1 \neq \bar{e}_2$. Всюду далее E обладает плохой редукцией. Тогда, не ограничивая общности, можно считать, что $\bar{e}_2 = 0$ и

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

где $a_2 = -(e_1+e_2)$, $a_4 = e_1e_2$, $a_6 = 0$ и $\pi | a_4$. Если $\bar{e}_1 \neq 0$, то $v_k(a_2) = 0$ и имеет место мультипликативная редукция. В случае $-e_1 \in (k^*)^2$ с помощью замены $x = x'(-e_1)$ приходим к уравнению

$$y^2 = x(x+1)(x-\pi^m a), \quad m > 0, \ a \in U(k),$$

и редукция E разложимая мультипликативная. Пусть $-e_1 \notin (k^*)^2$. Тогда замена $x = -\alpha e_1 x'$ дает уравнение

$$y^2 = x(x+\alpha)(x-\pi^m a), \quad m > 0, \ a \in U(k)$$

и редукция E неразложимая мультипликативная.

При $\bar{e}_1 = 0$, $\pi | a_2$ и редукция E аддитивная. Так как $a_6 = 0$, то случаи 3, 5 из алгоритма Тэйта не реализуются. Далее, $b_8 = -e_1e_2$ и $\pi^3 | b_8$, тогда не реализуется случай 4. В случае 6 рассмотрим многочлен $\overline{P}(T) = T(T - \overline{e_1\pi^{-1}})(T - \overline{e_2\pi^{-1}})$. Для 6a будем иметь уравнение

$$y^2 = x(x-\pi a)(x-\pi b), \quad a, b \in U(k), \ \bar{a} \neq \bar{b}.$$

В случае 6b имеются три возможности:

α) $e_1\pi^{-1}, e_1\pi^{-1} \in U(k)$, $\overline{e_1\pi^{-1}} = \overline{e_1\pi^{-1}}$;

β) $e_1\pi^{-1} \in U(k)$, $e_2\pi^{-1} \in M(k)$;

γ) $e_1\pi^{-1} \in M(k)$, $e_2\pi^{-1} \in U(k)$.

В первом случае замена $x' = x - e_1$ приводит нас к уравнению вида III. В случаях β) и γ) мы изначально имеем уравнение вида III. Ввиду $a_6 = 0$ не реализуются случаи $6c_1$ и $6c_3$. Теорема доказана. •

Теорема 3. *Пусть E — эллиптическая кривая над k, для которой имеет место полуразложимый случай, $a, b, c \in U(k)$. Тогда минимальное уравнение кривой E содержится в следующем списке, причем все уравнения из списка минимальны для задаваемых ими кривых и относятся к полуразложимому случаю.*

E имеет хорошую *редукцию.* $y^2 = x(x^2+tx+n)$, $t, n \in A(k)$, $\overline{t}^2 - 4\overline{n} \notin (\overline{k}^*)^2 \cup \{0\}$.

E имеет плохую *редукцию. Различаем два случая:*

A. *E имеет* аддитивную *редукцию.*

A.a)

1. $y^2 = x(x^2 + \pi^m ax + \pi b)$, $m > 0$;
2. $y^2 = x(x^2 + \pi b)$;
3. $y^2 = x(x^2 + \pi^m ax + \pi^3 b)$, $m > 1$;
4. $y^2 = x(x^2 + \pi^3 b)$.

A.b) $b \notin (k^*)^2$.

1. $y^2 = x(x^2 + \pi^m ax + \pi^2 b)$, $m > 1$, $-1 \in (k^*)^2$;
2. $y^2 = x(x^2 + \pi ax + \pi^2 b)$, $a^2 - 4b \notin (k^*)^2 \cup \{0\}$;
3. $y^2 = x(x^2 + \pi^2 b)$, $-1 \in (k^*)^2$.

A.c) $b \in (k^*)^2$.

1. $y^2 = x(x^2 + \pi^2 b)$, $-1 \notin (k^*)^2$;
2. $y^2 = x(x^2 + \pi^m ax + \pi^2 b)$, $m > 1$, $-1 \notin (k^*)^2$;
3. $y^2 = x(x^2 + \pi ax + \pi^2 b)$, $\overline{a} - 4\overline{b} \notin (\overline{k}^*)^2 \cup \{0\}$;
4. $y^2 = x(x^2 + \pi ax + \pi^2 b)$, $a/\sqrt{b} = 2 + \pi^{2r} c$, $r > 0$, $c \notin (k^*)^2$.

A.d) $y^2 = x(x^2 + \pi ax + \pi^2 b)$, $a/\sqrt{b} = 2 + \pi^{2r+1} c$, $r \geq 0$, $c\sqrt{b} \notin (k^*)^2$.

A.e) $y^2 = x(x^2 + \pi ax + \pi^2 b)$, $a/\sqrt{b} = 2 + \pi^{2r+1} c$, $r \geq 0$, $c\sqrt{b} \in (k^*)^2$.

M. *E имеет* мультипликативную *редукцию.*

$$y^2 = x((x + a)^2 + \pi^s bx), \quad s > 0.$$

M.a) $s = 2m+1$, *редукция разложимая, если и только если* $-a \in (k^*)^2$.

M.b) $s = 2m$, $-a \notin (k^*)^2$, $-b \in (k^*)^2$, *редукция неразложимая.*

M.c) $s = 2m$, $-1 \in (k^*)^2$, $a \in (k^*)^2$, $b \notin (k^*)^2$, *редукция разложимая.*

M.d) $s = 2m$, $-1 \notin (k^*)^2$, $a \notin (k^*)^2$, $b \in (k^*)^2$, *редукция разложимая.*

В случаях A.c) 4, A.d) *и* A.e) *элемент $\sqrt{b}$ выбирается таким образом, что* $\overline{a/\sqrt{b}} = 2$.

Доказательство. Кривая E обладает минимальным уравнением $y^2 = (x')^3 + A(x')^2 + Bx' + C$, $A, B, C \in A(k)$. В полуразложимом случае $(x')^3 + A(x')^2 + Bx' + C = (x' - \mu)((x')^2 + \nu x' + \tau)$. Тогда замена $x = x' - \mu$ приводит уравнение кривой E к виду

$$y^2 = x(x^2 + tx + n), \tag{7}$$

где $t, n \in A(k)$ и многочлен $x^2 + tx + n$ неприводим над k ($a_2 = t$, $a_4 = n$, $a_6 = 0$, $b_8 = -n^2$).

В случае хорошей редукции дискриминант $\overline{t}^2 - 4\overline{n} \notin (\overline{k}^*)^2 \cup \{0\}$.

Рассмотрим случай плохой редукции. Многочлен $x^2 + tx + n$ должен иметь двукратный корень $\beta \in \overline{k}$.

Пусть вначале $\beta = 0$. Тогда редукция аддитивная. В силу $a_6 = 0$ случаи 3 и 5 из алгоритма Тэйта не реализуются. Если $v_k(n) = 1$, то имеет место случай 4 и уравнение (7) приобретает либо вид $y^2 = x(x^2 + \pi^m ax + \pi b)$, либо вид $y^2 = x(x^2 + \pi b)$.

Пусть $\pi^2 | n$. Тогда для уравнения (7) обязан реализоваться один из случаев 6a–6c$_3$. Рассмотрим многочлен $\overline{P}(x) = x^3 + \overline{t\pi^{-1}}x^2 + \overline{n\pi^{-2}}x$. В случае 6a $v_k(n) = 2$, и потому $n = \pi^2 b$. Поскольку многочлен $x^2 + \overline{t\pi^{-1}}x + \overline{n\pi^{-2}}$ не имеет кратных корней, то $(\overline{\pi^{-1}t})^2 \neq 4\overline{b}$. В случае $\pi^2 | t$ это всегда имеет место и уравнение (7) приобретает один из двух видов:

$$y^2 = x(x^2 + \pi^m ax + \pi^2 b), \quad m > 1,$$
$$y^2 = x(x^2 + \pi^2 b).$$

Если $t = \pi a$, то условие $\overline{a}^2 \neq 4\overline{b}$ приводит нас либо к случаю A.c)3, либо к случаю A.b)2. Заметим, что в случае 6b алгоритма Тэйта нуль не является двукратным корнем. В противном случае многочлен $\overline{P}(x)/x$ разлагался бы на два взаимно простых множителя. Таким образом, $n = \pi^2 b$ и $x^2 + \overline{t\pi^{-1}}x + \overline{n\pi^{-2}} = (x - r)^2$, $r \neq 0$. Откуда следует, что $t = \pi a$ и уравнение (7) приобретает вид

$$y^2 = x(x^2 + \pi ax + \pi^2 b),$$

причем $b \in (k^*)^2$, так как $b = \gamma^2$ и $\overline{a}^2 = 4\overline{b}$. Заметим, наконец, что случаи 6c$_1$, 6c$_3$ не реализуются ввиду $a_6 = 0$, а случай 6C$_2$ дает A.α)3, A.α)4.

Рассмотрим случай $\beta \neq 0$. Так как $x^2 + \overline{t}x + \overline{n} = (x - \beta)^2$, то $\overline{n} = \beta^2$. Следовательно, существует элемент $a \in U(k)$ такой, что $n = a^2$. Поскольку $\overline{t} = 2\overline{a}$, то $t = 2a + \pi^s b$, $s > 0$. Заметим, что $t \neq 2a$ ввиду неприводимости над k многочлена $x^2 + tx + n$. Таким образом, уравнение (7) может быть переписано в виде

$$y^2 = x((x + a)^2 + \pi^s bx), \quad s > 0.$$

В заключение заметим, что другие ограничения на элементы a, b, c, имеющиеся в списке, связаны либо с разбиением на необходимые нам в дальнейшем случаи, либо с неприводимостью многочлена $x^2 + tx + n$. •

Наконец, рассмотрим неразложимый случай. Справедлива следующая

Лемма 2. *Пусть* $f(x) = x^3 + tx^2 + \pi^l bx + \pi^m c$, *где* $b, c \in U(k)$, $t \in M(k)$ *и* $m \geq 2l > 0$. *Тогда* $f(x)$ — *приводимый над* k *многочлен.*

Доказательство. Покажем, что $f(x)$ имеет корень в k, воспользовавшись методом Ньютона. Имеем $f'(x) = 3x^2 + 2tx + \pi^l bx$. Если $m > 2l$, то $v_k(f(0)) > 2v_k(f'(0))$, так как $v_k(f(0)) = m$, а $v_k(f'(0)) = l$. Значит, $f(x)$ имеет корень в k. Пусть $m = 2l$ и $\mu = -cb^{-1}\pi^l$. Тогда $v_k(f(\mu)) = v_k((-cb^{-1})^3\pi^{3l} + t(cb^{-1})^2\pi^{2l}) > 2l$. С другой стороны, $v_k(3(cb^{-1})^2\pi^{2l} + 2(-cb^{-1})\pi^l t + \pi^l b) = l$. Откуда $v_k(f(\mu)) > 2v_k(f'(\mu))$, и потому $f(x)$ снова имеет корень в k. •

Докажем теперь следующее утверждение.

Теорема 4. *Пусть E — эллиптическая кривая над k, для которой имеет место неразложимый случай, $a, b \in U(k) \cup \{0\}$, $c \in U(k)$, $r, l, m \geq 0$. Тогда E обладает минимальным уравнением вида $y^2 = f(x)$, где $f(x) = x^3 + \pi^r a x^2 + \pi^l b x + \pi^m c$, которое содержится в следующем списке, причем все уравнения минимальны для задаваемых ими кривых и относятся к неразложимому случаю.*

i) *E имеет* хорошую *редукцию. Многочлен $\overline{f}(x)$ неприводим над $\overline{k}$.*

ii) *E имеет* аддитивную *редукцию. Тогда $r, l, m > 0$, $y^2 = f(x)$ и выполнено одно из условий* 1–5.

1. $m = 1$.
2. $m = 2$, *причем* $b = 0$, *либо* $l \geq 2$.
3. $m = 3$, *причем имеет место условие* ($b = 0$, *либо* $l \geq 2$) *и многочлен* $x^3 + \overline{\pi^{r-1}} a x^2 + \overline{\pi^{l-2}} b x + \overline{c}$ *неприводим над* $\overline{k}$.
4. $m = 4$, *причем выполнены следующие два условия*:
   a) $a = 0$, *либо* $r \geq 2$,
   b) $b = 0$, *либо* $l \geq 3$,
5. $m = 5$, *причем выполнены следующие два условия*:
   a) $a = 0$, *либо* $r \geq 2$,
   b) $b = 0$, *либо* $l \geq 4$.

Доказательство. Пусть $y^2 = x^3 + a_2 x^2 + a_4 x + a_6$ — минимальное уравнение Вейерштрасса для E. Положим $a_2 = \pi^r a$, $a_4 = \pi^l b$, $a_6 = \pi^m c$, где $r, l, m \geq 0$ и $a, b, c \in U(k) \cup \{0\}$. Поскольку для E имеет место неразложимый случай, то, очевидно, $c \in U(k)$. Таким образом, минимальное уравнение для E может быть записано в виде $y^2 = f(x)$ при подходящих $r, l, m \geq 0$ и $a, b \in U(k) \cup \{0\}$, $c \in U(k)$. Ввиду неприводимости $f(x)$ над k многочлен $\overline{f}(x)$ либо неприводим над $\overline{k}$, либо имеет вид $(x - \delta)^3$ при подходящем $\delta \in \overline{k}$. В первом случае E обладает хорошей редукцией и случай i) рассмотрен. Во втором редукция E аддитивная. Тогда, не ограничивая общности, можно считать, что $r, l, m > 0$ и уравнение $y^2 = f(x)$ относится к одному из случаев в алгоритме Тэйта. Принадлежность к случаям 3–5 приводит к следующим ограничениям на m, l, b.

3. $m = 1$.
4. $m \geq 2, l = 1, b \in U(k)$.
5. $m = 2$ и либо $b = 0$, либо $l \geq 2$.

В случае 6 $m \geq 3$ и $\pi^2 | \pi^l b$, т.е. $l \geq 2$ либо $b = 0$. Далее, многочлен $P(x) = 1/\pi^3 f(\pi x)$ неприводим над k (в силу неприводимости $f(x)$), поэтому $\overline{P}$ либо неприводим над $\overline{k}$, либо имеет в $\overline{k}$ трехкратный корень. Таким образом, случай 6b для уравнения $y^2 = f(x)$ не реализуется. В случае 6a многочлен $\overline{P}(x)$ должен быть неприводимым, а так как при $m > 3$ $\overline{P}(x)$ делится на x, то должно быть $m = 3$. Рассмотрим теперь ограничения, возникающие в случае 6c. Тогда многочлен $\overline{P}(x)$ имеет трехкратный корень β. В этом случае замена $x' = x - u$, где u — прообраз β в k, позволяет, не ограничивая общности, считать, что $m \geq 4$, и реализуются оба условия: a) $a = 0$ либо $r \geq 2$, b) $b = 0$ либо $l \geq 3$. Далее, если для уравнения $y^2 = f(x)$ реализуется возможность $6c_1$, то $m = 4$. Если имеет место $6c_2$, то $m \geq 4$, $l = 3$ и выполняется условие: $a = 0$ либо $r \geq 2$. Наконец, если имеет место $6c_3$, то $m = 5$ и выполнены

следующие два условия: а) $a = 0$ либо $r \geq 2$, b) $b = 0$ либо $l \geq 4$. Ясно, что минимальность уравнения $y^2 = f(x)$ влечет нереализуемость условия $6c_4$. Таким образом, в случае аддитивной редукции нами получены следующие ограничения на коэффициенты уравнения:

α) $m = 1$, $r > 0$, $l > 0$.
β) $m = 2$, $r > 0$, $l > 0$.
γ) $m = 3$, $r > 0$ и $l = 1$, $b \in U(k)$ либо выполнены следующие условия:
  а) $b = 0$ либо $l \geq 2$,
  b) многочлен $\overline{P}(x)$ неприводим над $\overline{k}$.
δ) $m = 4$, $r > 0$ и $l = 1$, $b \in U(k)$ либо выполнены следующие условия:
  а) $a = 0$ либо $r \geq 2$,
  b) $b = 0$ либо $l \geq 3$.
σ) $m = 5$, $r > 0$ и
  σ_1) $b = 0$ и выполнено условие: $a = 0$ либо $r \geq 2$.
  σ_2) $b \in U(k)$, $l = 1$.
  σ_3) $b \in U(k)$, $l \geq 2$ и выполнено условие: $a = 0$ либо $r \geq 2$.

Заметим, что в минимальном уравнении вида $y^2 = f(x)$ допустимо $m \geq 6$, однако, как будет показано ниже, в этом случае многочлен $f(x)$ приводим над k.

Для завершения доказательства отберем из приведенных выше минимальных уравнений те, которые соответствуют неразложимому случаю. В случае α) $f(x)$ неприводим над k, поскольку является многочленом Эйзенштейна. В случае β) если $l = 1$ и $b \in U(k)$, то f приводим в силу леммы 2. Если же $b = 0$ либо $l \geq 2$, то f неприводим над k. Действительно, если f имеет корень $\mu \in k$, то $\mu = \pi^s e, e \in U(k), s > 0$. Тогда $\pi^{3s}e^3 + \pi^{r+2s}ae^2 + \pi^{l+s}be = -\pi^2 c$. Невозможность последнего равенства устанавливается сравнением порядков его левой и правой частей. В случае γ) при $b \in U(k), l = 1$ $f(x)$ приводим над k в силу леммы 2. Если же $b = 0$ либо $l \geq 2$, но $\overline{P}(x)$ неприводим над $\overline{k}$, то и $P(x)$ неприводим над k, а, следовательно, и $f(x)$ неприводим над k. В случае δ) если $b \in U(k)$ и $l = 1, 2$, то многочлен $f(x)$ приводим над k в силу леммы 2. Пусть далее $b = 0$ либо $l \geq 3$. Рассмотрим многочлен $P(x)$. Если $r \geq 2$ либо $a = 0$, то $P(x)$ — многочлен Эйзенштейна. Тогда $f(x)$ неприводим над k. Если же $a \in U(k)$ и $r = 1$, то $\overline{P}(x) = x^2(x + \overline{a})$. Следовательно, $P(x)$ а с ним и $f(x)$ приводимы над k. Рассмотрим случай σ). Если $b \in U(k)$ и $l = 1, 2$, то в силу леммы 2 $f(x)$ приводим над k. Пусть теперь $b = 0$ либо $l \geq 3$. Многочлен $P(x)$ в этом случае имеет вид $x^3 + \pi^{r-1}ax^2 + \pi^{l-2}bx + \pi^2 c$. Если $b \in U(k), l = 3$, то $f(x)$ приводим над k. Если же $b = 0$ либо $l \geq 4$, то рассуждение, применявшееся при рассмотрении случая β), показывает, что $P(x)$, а вместе с ним и $F(x)$ неприводимы над k.

В заключение покажем, что при $m \geq 6$ не существует минимального уравнения вида $y^2 = f(x)$ с неприводимым над k многочленом $f(x)$. Действительно, если такое уравнение существует, то должно быть $b = 0$ либо $l \geq 4$, так как в противном случае $f(x)$ приводим над k в силу леммы 2. Далее, если $a = 0$ либо $r \geq 2$, то замена $x = \pi^2 x'$, $y = \pi^3 y'$ приводит к уравнению с дискриминантом меньшего порядка. Следовательно, $a \in U(k)$ и $r = 1$. Но тогда $\overline{P}(x) = x^2(x + \overline{a})$, что влечет приводимость над k $P(x)$, а, следовательно, и $f(x)$. •

§5. Кручение локальных эллиптических кривых

Пусть k — локальное поле, m — натуральное число, взаимно простое с $\operatorname{char}\overline{k}$. Ясно, что для описания группы ${}_mE(k)$ достаточно описать группы ${}_{p^n}E(k)$, где p — простое число, не равное $\operatorname{char}\overline{k}$.

Далее d будет обозначать минимальное из чисел n и показателя максимальной степени p, делящей порядок группы $\overline{k}^*$, $c=(p^n, v_k(j(E)))$, $v_k(j(E)\neq 0$ и

$$r=\min_{0<i\leq c}\{\,i\in\mathbf{Z}\mid \overline{u}^{i/c}\in\overline{k}^*\,\},\quad \text{где } \overline{u}=\overline{j(E)\pi^{-v_k(j(E))}}.$$

Описание группы ${}_{p^n}E(k)$ дается следующими двумя теоремами.

Теорема 5. *Пусть k — локальное недиадическое поле, E — эллиптическая кривая, определенная над k, p — простое число, взаимно простое с $\operatorname{char}\overline{k}$. Тогда имеют место следующие утверждения.*

G. *Если E — кривая с хорошей редукцией, то*

$$ {}_{p^n}E(k)\cong {}_{p^n}\widetilde{E}(\overline{k}).$$

A. *Пусть E — кривая с аддитивной редукцией. Тогда имеют место следующие утверждения.*

A1. *При $p>3$*

$$ {}_{p^n}E(k)\cong\langle 0\rangle.$$

A2. *Если имеют место разложимый либо полуразложимый случаи, то*

$$ {}_{3^n}E(k)\cong\langle 0\rangle.$$

A3. *Если имеет место неразложимый случай, то*

$$ {}_{3^n}E(k)\cong\mathbf{Z}/3,\ \textit{если}\ [E(k):E_0(k)]=3$$

и

$$ {}_{3^n}E(k)\cong\langle 0\rangle\ \textit{в противном случае}.$$

A4. *В разложимом случае*

$$ {}_{2^n}E(k)={}_2E(k)\cong(\mathbf{Z}/2)^2.$$

A5. *В полуразложимом случае*

$$ {}_2E(k)\cong\mathbf{Z}/2,$$

а при $n\geq 2$

$$ {}_{2^n}E(k)\cong\begin{cases}\mathbf{Z}/2 & \textit{в случаях A.a)–A.d)},\\ \mathbf{Z}/4 & \textit{в случае A.e)}.\end{cases}$$

А6. *В неразложимом случае*

$$_{2^n}E(k) \cong \langle 0 \rangle.$$

М. *Пусть E — кривая с мультипликативной редукцией. Тогда*

М.1. *В разложимом случае при неразложимой редукции*

$$_{p^n}E(k) \cong \begin{cases} \mathbf{Z}/p^d & \text{при } p > 2, \\ \mathbf{Z}/2^d \oplus \mathbf{Z}/2 & \text{при } p = 2. \end{cases}$$

М.2. *В полуразложимом случае при неразложимой редукции*

$$_{p^n}E(k) \cong \begin{cases} \mathbf{Z}/p^d & \text{при } p > 2 \text{ или нечетном } m, \\ \mathbf{Z}/2^d & p = 2,\ m \text{ четное и } 2^n \text{ делит } |\overline{k}^*|, \\ \mathbf{Z}/2^{d+1} & p = 2,\ m \text{ четное и } 2^n \text{ не делит } |\overline{k}^*|. \end{cases}$$

М.3. *В разложимом и полуразложимом случаях при разложимой редукции*

$$_{p^n}E(k) \cong \langle \mu_{p^n} \rangle \oplus \mathbf{Z}/(c/r),$$

где $\langle \mu_{p^n} \rangle$ — группа корней степени p^n из 1, лежащих в k.

Замечание 1. В силу утверждения G теоремы изучение p^n-кручения группы $E(k)$ сводится к изучению соответствующего кручения редуцированной кривой над конечным полем, информация о которой может быть найдена в [11, 12] либо в [13].

Доказательство теоремы предварим рядом вспомогательных утверждений.

Лемма 3. *Если $(m, \operatorname{char} \overline{k}) = 1$, то ограничение гомоморфизма редукции R на $_mE_0(k)$ есть изоморфизм $_mE_0(k)$ на $_m\widetilde{E}_0(\overline{k})$.*

Доказательство. $\operatorname{Ker} R = E_1(k) \cap {}_mE_0(k) = {}_mE_1(k) = \langle 0 \rangle$. Пусть $\widetilde{Q} \in {}_m\widetilde{E}_{ns}(\overline{k})$. В силу сюръективности ограничения R на $E_0(k)$ существует точка Q_0 такая, что $\overline{Q}_0 = \widetilde{Q}$. Далее, $\overline{mQ_0} = m\overline{Q}_0 = m\widetilde{Q} = 0$, значит, $mQ_0 \in E_1(k)$, и потому $mQ_0 = Q_1' \in E_1(k)$.Тогда существует единственная точка $Q_1 \in E_1(k)$ такая, что $Q_1' = mQ_1$. Следовательно, $mQ_0 = mQ_1$, что влечет $Q_0 - Q_1 \in {}_mE_0(k)$. Положив $Q = Q_0 - Q_1$, будем иметь $\overline{Q} = \overline{Q}_0 = \widetilde{Q}$. Таким образом, ограничение R на $_mE_0(k)$ сюръективно. Инъективность утверждается в [14]. •

Предложение 8. *Если E — эллиптическая кривая с разложимой мультипликативной редукцией, то существует элемент $q \in M(k)$ такой, что E изоморфна кривой Тэйта E_q с уравнением*

$$y^2 + xy = x^3 + a_4x + a_6,$$

где

$$a_4 = -5\sum_{n\geq 1} n^3q^n/(1-q^n), \qquad a_6 = -\frac{1}{2}\sum_{n\geq 1}(7n^5 + 5n^3)q^n/(1-q^n),$$

причем

$$j(E) = \frac{1}{q} + 744 + 196884q + \dots,$$

в частности,

$$v_k(q) = -v_k(j(E)), \qquad \overline{q\pi^{-v_k(q)}} = (\overline{j(E)\pi^{-v_k(j(E))}})^{-1}.$$

Кроме того, абелевы группы $E_q(k)$ и $k^*/\langle q\rangle$, где $\langle q\rangle$ — подгруппа в k^*, порожденная элементом q, изоморфны.

По поводу доказательства см. [15], с. 356.

Предложение 9. *Если E — кривая с неразложимой мультипликативной редукцией, то*

$$[E(k) : E_0(k)] = \begin{cases} 1, & \text{если } v_k(\Delta(E)) \text{ нечетно,} \\ 2, & \text{если } v_k(\Delta(E)) \text{ четно.} \end{cases}$$

По поводу этого предложения см. [15], с. 266.

Предложение 10. *Если E обладает аддитивной редукцией, то $[E(k) : E_0(k)] \leq 4$, причем если поле k недиадическое и имеет место разложимый или полуразложимый случай, то $[E(k) : E_0(k)] \neq 3$.*

Доказательство. Первое утверждение есть часть утверждения теоремы Кодаиры—Нерона, а второе связано с информацией о группе $E(k)/E_0(k)$, помещенной в упрощенном варианте алгоритма Тэйта. •

Ниже p — простое число и $(p, \operatorname{char}\overline{k}) = 1$, E — произвольная эллиптическая кривая, определенная над k.

Предложение 11. *Пусть s — натуральное число. Тогда*

$${}_{p^s}E(k) \cong E(k)/p^s, \qquad {}_{p^s}\operatorname{Br} E \cong {}_{p^s}\operatorname{Br}(k) \oplus {}_{p^s}E(k).$$

Доказательство. Существует m такое, что для всякого $n > m$ ${}_{p^n}E(k) = {}_{p^m}E(k)$. Тогда для произвольного $n \geq m$ и $e \in {}_{p^n}E(k)$ положим $\phi_n(e) = e + p^nE(k)$, $\phi_n\colon {}_{p^n}E(k) \longrightarrow ({}_{p^n}E(k) + p^nE(k))/p^nE(k)$. Так как ${}_{p^{n+1}}E(k) = {}_{p^n}E(k)$, то ${}_{p^{n+1}}E(k) \cap p^nE(k) = \langle 0\rangle$. Действительно, если $x \in {}_{p^n}E(k) \cap p^nE(k)$, то $p^nx = 0$ и $x = p^ny$, $y \in E(k)$. Тогда $p^{2n}y = 0$ и $y \in {}_{p^{2n}}E(k)$. Но ${}_{p^{2n}}E(k) = {}_{p^n}E(k)$, и поэтому $p^ny = 0$, т.е. $x = 0$. Таким образом, ϕ_n — инъективный гомоморфизм. Сюръективность ϕ_n вытекает из того, что

$$({}_{p^n}E(k) + p^nE(k))/p^nE(k) \cong {}_{p^n}E(k)/(p^nE(k) \cap {}_{p^n}E(k))$$

и порядки групп ${}_{p^n}E(k)$ и $E(k)/p^n$ совпадают. Поэтому ϕ_n — изоморфизм. Тогда, так как $({}_{p^n}E(k) + p^nE(k))/p^nE(k) \in E(k)/p^n$, получаем ${}_{p^n}E(k) \cong E(k)/p^n$ и в силу предложения 7

$${}_{p^n}\operatorname{Br} E \overset{\theta_n}{\cong} {}_{p^n}\operatorname{Br}(k) \oplus {}_{p^n}E(k).$$

Пусть теперь $1 \leq n \leq m$. Рассмотрим $x \in {}_{p^n}\mathrm{Br}\, E$, то $p^n\theta_m(x) = 0$. Если $\theta_m(x) = a + b$, $a \in {}_{p^m}\mathrm{Br}(k)$, $b \in {}_{p^m}E(k)$, то $p^n a = 0$ и $p^n b = 0$. Последнее означает, что $\theta_m({}_{p^n}\mathrm{Br}\, E) \subset {}_{p^n}\mathrm{Br}(k) \oplus {}_{p^n}E(k)$. Обратное включение очевидно и, таким образом, второе утверждение предложения доказано. Доказательство первого утверждения вытекает из второго и предложения 7. •

Лемма 4. *Пусть E — эллиптическая кривая с аддитивной редукцией и $p > 3$. Тогда* ${}_{p^n}E(k) = \langle 0\rangle$.

Доказательство. Поскольку $([E(k) : E_0(k)], p) = 1$, то в силу теоремы Кодаиры—Нерона ${}_{p^n}E(k) = {}_{p^n}E_0(k) \cong {}_{p^n}\widetilde{E}_{ns}(\overline{k})$ (последний изоморфизм в силу леммы 3). Но ввиду аддитивности редукции $\widetilde{E}(\overline{k}) \cong \overline{k}^+$. Поскольку аддитивная группа $\overline{k}^+$ поля $\overline{k}$ имеет тривиальное p^n-кручение, лемма доказана. •

Предложение 12. *Пусть E — эллиптическая кривая с аддитивной редукцией, причем* $\mathrm{char}\,\overline{k} \neq 3$. *Тогда если* $[E(k) : E_0(k)] = 3$, *то* ${}_{3^n}E(k) \cong \mathbf{Z}/3$, *в противном случае* ${}_{3^n}E(k) = \langle 0\rangle$.

Доказательство. Пусть вначале $[E(k):E_0(k)] = 3$. Поскольку группа $E_1(k)$ 3-делима и $E_1(k) \subset E_0(k)$, то $E_1(k) \subset 3E_0(k)$. Далее, $3E_0(k)/E_1(k)$ — подгруппа $E_0(k)/E_1(k) \cong \widetilde{E}_{ns}(k) \cong \overline{k}^+$. Так как $E_0(k)/3E_0(k)$ — гомоморфный образ группы $E_0(k)/E_1(k)$ порядка, взаимно простого с 3 и $E_0(k)/3E_0(k)$ — группа, порядок которой равен 3^m для подходящего m, то $m = 0$ и $E_0(k) = 3E_0(k)$. Так как $3E(k) \subset E_0(k)$ и $E_0(k) = 3E_0(k) \subset 3E(k)$, то $E_0(k) = 3E(k)$. Пусть теперь $x \in E(k) \setminus E_0(k)$. Из равенства $[E(k) : E_0(k)] = 3$ следует, что $3x \in E_0(k)$. Но $E_0(k) = 3E_0(k)$, поэтому $3x = 3e_0$ для некоторого $e_0 \in E_0(k)$. Таким образом, $x - e_0 \in {}_3E(k)$, причем $x - e_0 \neq 0$. Следовательно, ${}_3E(k) \neq \langle 0\rangle$. Далее, если $x_1, x_2 \in {}_3E(k)$ и $x_1 - x_2 \in E_0(k)$, то $x_1 - x_2 \in {}_3E_0(k)$, поэтому $x_1 = x_2$. Таким образом, различные элементы из ${}_3E(k)$ содержатся в различных смежных классах по $E_0(k)$, а так как ${}_3E(k_s) \cong (\mathbf{Z}/3)^2$ и $[E(k) : E_0(k)] = 3$, то ${}_3E(k) \cong \mathbf{Z}/3$. Обратно, если $[E(k) : E_0(k)] \neq 3$, то 3 взаимно просто с $[E(k) : E_0(k)]$ и в силу того, что ${}_3E_0(k) = \langle 0\rangle$, ${}_3E(k) = \langle 0\rangle$. •

Следствие 3. *Пусть E — эллиптическая кривая с аддитивной редукцией, а также* $\mathrm{char}\,\overline{k} \neq 2, 3$ *и имеет место разложимый либо полуразложимый случай. Тогда* ${}_3E(k) = \langle 0\rangle$.

Доказательство. В силу предложения 6 $([E(k) : E_0(k)], 3) = 1$. •

Описание 2-примарного кручения таково.

Лемма 5. *Пусть E — эллиптическая кривая с аддитивной редукцией,* $\mathrm{char}\,\overline{k} \neq 2$. *Тогда*

$$ {}_2E(k) \cong \begin{cases} \langle 0\rangle, & \textit{в неразложимом случае,} \\ \mathbf{Z}/2, & \textit{в полуразложимом случае,} \\ \mathbf{Z}/2 \oplus \mathbf{Z}/2, & \textit{в разложимом случае.} \end{cases} $$

Доказательство хорошо известно.

Лемма 6. *Пусть E — эллиптическая кривая с аддитивной редукцией,* $\operatorname{char}\overline{k} \neq 2$. *Тогда для любого* $n \geq 2$ ${}_{2^n}E(k) = {}_4E(k)$.

Доказательство. Действительно, если $x \in {}_{2^n}E(k) \setminus {}_4E(k)$, $n > 2$, то $[E(k):E_0(k)]x \neq 0$ и $[E(k):E_0(k)]x \in {}_{2^n}E_0(k)$, что невозможно в силу аддитивности редукции. •

Таким образом, описание 2-примарного кручения в случае кривых с аддитивной редукцией сводится к описанию 4-кручения.

Лемма 7. *В условиях предыдущей леммы в разложимом и полуразложимом случае*

$$ {}_4E(k) \cong \begin{cases} {}_2E(k), & \text{если } E(k)/E_0(k) \ncong \mathbf{Z}/4, \\ \mathbf{Z}/4, & \text{если } E(k)/E_0(k) \cong \mathbf{Z}/4. \end{cases} $$

В неразложимом случае ${}_4E(k) = \langle 0 \rangle$.

Доказательство. Пусть $E(k)/E_0(k) \ncong \mathbf{Z}/4$ и $x \in {}_4E(k) \setminus {}_2E(k)$. Пусть также $y = [E(k):E_0(k)]x$. По теореме Кодаиры—Нерона $[E(k):E_0(k)] \leq 4$, поэтому $y \neq 0$. Но $y \in E_0(k)$ и $4y = 0$. В силу тривиальности группы ${}_4E_0(k)$ приходим к противоречию. Пусть теперь $E(k)/E_0(k) \cong \mathbf{Z}/4$. Тогда, рассуждая аналогично доказательству предложения 12, получим $E_0(k) = 4E_0(k) = 4E(k)$. Далее, пусть $x \in E(k) \setminus E_0(k)$ такой, что $x + E_0(k)$ — образующая группы $E(k)/E_0(k)$. Пусть $e = 4x$, $e \in E_0(k)$. Ввиду $E_0(k) = 4E_0(k)$ $e = 4e_0$, $e_0 \in E_0(k)$. Следовательно, $4(x - e_0) = 0$, $x - e_0 \neq 0$ и $x - e_0 \in {}_4E(k)$. Заметим, что $2(x - e_0) \neq 0$. Далее, аналогично доказательству предложения 12 устанавливается, что любые два различных элемента из ${}_4E(k)$ лежат в различных смежных классах по $E_0(k)$, и потому ${}_4E(k) \ncong \mathbf{Z}/4 \oplus \mathbf{Z}/4$, что влечет ${}_4E(k) \cong \mathbf{Z}/4$. •

Предложение 13. *Пусть E — эллиптическая кривая над недиадическим полем k и с аддитивной редукцией, причем имеет место полуразложимый случай. Тогда*

$$ {}_4E(k) \cong \begin{cases} {}_2E(k), & \text{в случаях A.a)-A.d)}, \\ \mathbf{Z}/4, & \text{в случае A.e)}. \end{cases} $$

Доказательство. Пусть минимальное уравнение E имеет вид $y^2 = x(x^2 + Ax + B)$. Если $Q \in {}_4E(k) \setminus {}_2E(k)$, то $2Q \in {}_2E(k) \setminus \{0\}$. Значит, $2Q = (0,0)$ и $x(2Q) = 0$. С другой стороны, $x(2Q) = (x(Q) - B)^2/(4y(Q)^2)$. Откуда $B \in (k^*)^2$. В случаях A.a) и A.b) теоремы $B \notin (k^*)^2$, следовательно, в этих случах ${}_4E(k) = {}_2E(k)$. Далее, $x(Q)(x(Q)^2 + Ax(Q) + B) \in (k^*)^2$, и так как $x(Q)^2 = B$, то $A + 2x(Q) \in (k^*)^2$. Ясно, что одновременное выполнение двух условий

$$ x(Q)^2 = B \quad A + 2x(Q) \in (k^*)^2 $$

необходимо и достаточно для того, чтобы $Q \in {}_4E(k) \setminus {}_2E(k)$. В случаях A.c)–A.e) $B = \pi^2 b$, $b \in U(k)^2$, значит, $v_k(x(Q)) = 1$, и потому $v_k(A) = 1$, т.е. $A = \pi a$, $a \in U(k)$ (в противном случае $v_k(A + 2x(Q)) = 1$, что противоречит $A + 2x(Q) \in (k^*)^2$).

Поэтому для уравнений A.c)1–A.c)2 ${}_4E(k) = {}_2E(k)$. $x(Q) = \pm\pi\sqrt{b}$. Необходимое и достаточное условие того, что $Q \in {}_4E(k) \setminus {}_2E(k)$, примет вид

$$\pi(a + 2\sqrt{b}) \in (k^*)^2 \quad \text{или} \quad \pi(a - 2\sqrt{b}) \in (k^*)^2.$$

Поэтому $\overline{a}^2 - 4\overline{b} = 0$ и в случае A.c)3 ${}_4E(k) = {}_2E(k)$. В оставшихся случаях фиксируем элемент $\sqrt{b}$ так, чтобы $\overline{a/\sqrt{b}} = 2$. Тогда $a + 2\sqrt{b} = 4\sqrt{b} + \pi^m c\sqrt{b}$ ($m = 2r$ в уравнении A.c)4 и $m = 2r + 1$ в случаях A.d), A.e)). Тогда $v_k(\pi(4\sqrt{b} + \pi^m c\sqrt{b})) = 1$ и $\pi(4\sqrt{b} + \pi^m c\sqrt{b}) \notin (k^*)^2$. Во втором случае $\pi(a - 2\sqrt{b}) = \pi^{m+1}c\sqrt{b}$. Последнее выражение является квадратом в k^* тогда и только тогда, когда имеет место случай A.e). •

Предложение 14. *Пусть E — эллиптическая кривая над недиадическим полем k с аддитивной редукцией, причем имеет место разложимый случай. Тогда*

$$ {}_4E(k) \cong {}_2E(k).$$

Доказательство. Если утверждение предложения не имеет места, то ${}_4E(k) \cong \mathbf{Z}/4$. С другой стороны, ${}_2E(k) \subset {}_4E(k)$ и ${}_2E(k) \cong \mathbf{Z}/2 \oplus \mathbf{Z}/2$. •

Опишем теперь примарное кручение в случае, когда кривая E имеет мультипликативную редукцию. В этой ситуации, как показывает лемма Гензеля, могут иметь место лишь разложимый или полуразложимый случаи.

Предложение 15. *Пусть E — эллиптическая кривая с неразложимой мультипликативной редукцией, заданная уравнением $y^2 = x(x + \alpha)(x - a\pi^m)$, $a \in U(k)$, $\alpha \in U(k) \setminus U(k)^2$, $m > 0$. Тогда*

$$ {}_{p^n}E(k) \cong \begin{cases} \mathbf{Z}/p^d, & \text{при } p \neq 2, \\ \mathbf{Z}/2^d \oplus \mathbf{Z}/2, & \text{при } p = 2. \end{cases}$$

Доказательство. Положим $x^2 + Ax + B = (x + \alpha)(x - a\pi^m)$. Тогда дискриминант Δ уравнения $y^2 = x(x^2 + Ax + B)$ равен $16b^2(A^2 - 4B) \in (k^*)^2$, поэтому $v_k(\Delta) = 2r$. Тогда в силу предложения 9 $[E(k) : E_0(k)] = 2$. Далее, поскольку точка второго порядка $(0,0) \in E(k) \setminus E_0(k)$, то $E(k) = E_0(k) \oplus \langle(0,0)\rangle$. Тогда для нечетного p

$$ {}_{p^n}E(k) = {}_{p^n}E_0(k) \oplus {}_{p^n}\langle(0,0)\rangle \cong {}_{p^n}\overline{k}^* \cong \mathbf{Z}/p^d.$$

Если же $p = 2$, то

$$ {}_{2^n}E(k) = {}_{2^n}E_0(k) \oplus {}_{2^n}\langle(0,0)\rangle \cong {}_{p^n}\overline{k}^* \oplus \mathbf{Z}/2 \cong \mathbf{Z}/p^d \oplus \mathbf{Z}/2. \quad \bullet$$

Предложение 16. *Пусть E — эллиптическая кривая с неразложимой мультипликативной редукцией, заданная уравнением $y^2 = x((x+a)^2 + \pi^m c x)$, $a, c \in U(k)$, $m > 0$, $-a \notin (k^*)^2$ (случай полуразложимый). Тогда*

$$ {}_{p^n}E(k) \cong \begin{cases} \mathbf{Z}/p^d, & \text{при } p > 2 \text{ либо } m \text{ нечетном}, \\ \mathbf{Z}/2^d, & \text{при } p = 2,\ m \text{ четном и } 2^n \text{ делит } |\overline{k}^*|, \\ \mathbf{Z}/2^{d+1}, & \text{при } p = 2,\ m \text{ четном и } 2^n \text{ не делит } |\overline{k}^*|. \end{cases} $$

Доказательство. Пусть сначала p нечетное. Если $Q \in {}_{p^n}E(k)$, то $Q = (p^n+1)Q$. Так как $[E(k) : E_0(k)] = 1$ либо 2 и число $p^n + 1$ четное, то $(p^n+1)Q \in E_0(k)$, а значит, и $Q \in E_0(k)$. Таким образом, ${}_{p^n}E(k) = {}_{p^n}E_0(k) \cong {}_{p^n}\overline{k}^* \cong \mathbf{Z}/p^d$.

Если $p = 2$ и m нечетно, то число $v_k(\Delta(E))$ также нечетно и ввиду предложения 9 $E(k) = E_0(k)$. В силу мультипликативности редукции снова ${}_{p^n}E(k) \cong \mathbf{Z}/2^d$. Пусть далее $p = 2$ и m четно. Тогда $[E(k) : E_0(k)] = 2$, что влечет $2E(k) \subset E_0(k)$. Как уже отмечалось выше, при $(2, \operatorname{char}\overline{k}) = 1$ порядки групп ${}_2E(k)$ и $E(k)/2$ совпадают, тогда из включений $2E(k) \subset E_0(k) \subset E(k)$ следует, что $E_0(k) = 2E(k)$. Значит, умножение на 2 в группе $E(k)$ является сюръективным гомоморфизмом на $E_0(k)$, что обеспечивает 2-делимость любого элемента из $E_0(k)$. Тогда ясно, что умножение на 2 сюръективно отображает ${}_{2^{n+1}}E(k)$ на ${}_{p^n}E_0(k)$ с ядром $\langle 0, (0,0)\rangle$. Значит, $|{}_{2^n}E(k)| = 2|{}_{2^{n-1}}E_0(k)|$ для произвольного $n \geq 2$. С другой стороны,

$$ |{}_{2^n}E_0(k)| = \begin{cases} 2|{}_{2^{n-1}}E_0(k)|, & \text{если } 2^n \text{ делит } |\overline{k}^*|, \\ |{}_{2^{n-1}}E_0(k)|, & \text{если } 2^n \text{ не делит } |\overline{k}^*|. \end{cases} $$

Поэтому $|{}_{2^n}E(k)| = |{}_{2^n}E_0(k)|$, если 2^n делит $|\overline{k}^*|$ и $|{}_{2^n}E(k)| = 2|{}_{2^n}E_0(k)|$, если 2^n не делит $|\overline{k}^*|$. В первом случае ввиду ${}_{2^n}E_0(k) \subset {}_{2^n}E(k)$, имеем ${}_{2^n}E(k) = {}_{2^n}E_0(k) \cong \mathbf{Z}/2^d$. Во втором случае ввиду 2^n не делит $|\overline{k}^*|$, имеем ${}_{2^n}E_0(k) = {}_{2^{n-1}}E_0(k)$, откуда получается сюръективность гомоморфизма умножения на 2, действующего из ${}_{2^n}E(k)$ в ${}_{2^n}E_0(k)$. Деля пополам образующую группы ${}_{2^n}E_0(k)$ (которая изоморфна $\mathbf{Z}/p^d$), получаем элемент порядка 2^{d+1}, что и завершает доказательство предложения. •

Наконец, рассмотрим случай разложимой мультипликативной редукции.

Лемма 8. *Пусть $q = u\pi^s$, $u \in U(k)$, $s > 0$, $(m, \operatorname{char}\overline{k}) = 1$. Тогда*

$$ {}_m(k^*/\langle q\rangle) \cong \langle \mu_m \rangle \oplus \mathbf{Z}/((m,s)/d), $$

где $\langle \mu_m \rangle$ — группа корней степени m из 1, лежащих в k, μ_m — ее образующая, и $d = \min_{0<i\leq(m,s)}\{\, i \in \mathbf{Z} \mid u^{i/(m,s)} \in k \,\}$.

Замечание 2. Условие $u^{i/(m,s)} \in k$ означает существование в k корня многочлена $x^m - u^{mi/(m,s)}$.

Доказательство. Сначала покажем, что условие $u^{j/(m,s)} \in k$ выполнено тогда и только тогда, когда d делит j. Действительно, если d делит j, то условие, очевидно,

выполняется. Пусть теперь $u^{j/(m,s)} \in k$, но d не делит j. Тогда для $\delta = (d, j)$, $\delta < d$. Существуют $r, t \in \mathbf{Z}$ такие, что $rd + tj = \delta$. Следовательно, $u^{\delta/(m,s)} = (u^{d/(m,s)})^r \cdot (u^{j/(m,s)})^t \in k$, что противоречит минимальности d. В частности, d делит (m, s).

Пусть $x = v\pi^n$, $v \in U(k)$, $n \in \mathbf{Z}$ и $v\pi^n + \langle q \rangle \in {}_m(k^*/\langle q \rangle)$. Тогда $v^m \pi^{nm} = u^l \pi^{ls}$ для некоторого $l \in \mathbf{Z}$. Откуда $mn = sl$ и $v^m = u^l$. Далее, s делит mn тогда и только тогда, когда $s/(m, s)$ делит $mn/(m, s)$. Для выполнения последнего условия необходимо и достаточно, чтобы $s/(m, s)$ делило n, что эквивалентно существованию $i \in \mathbf{Z}$ такого, что $n = si/(m, s)$. Таким образом, элемент $v\pi^n + \langle q \rangle$ принадлежит группе ${}_m(k^*/\langle q \rangle)$ тогда и только тогда, когда $n = si/(m, s)$ и $v^m = u^{mi/(m,s)}$ для некоторого $i \in \mathbf{Z}$. Из замечания, сделанного перед доказательством леммы 8 теперь следует, что группа ${}_m(k^*/\langle q \rangle)$ состоит из смежных классов вида $v\pi^n + \langle q \rangle$, где $n = sdj/(m, s)$ и $v^m = u^{mdj/(m,s)}$, $j = 0, 1, \ldots, (m, s)/d - 1$. Условие $v^m = u^{mdj/(m,s)}$ эквивалентно условию $v = \mu_m^r u^{dj/(m,s)}$ при подходящем $r \in \mathbf{Z}$. Зафиксируем элемент $u^{d/(m,s)} \in k$. Тогда нетрудно видеть, что

$$ {}_m(k^*/\langle q \rangle) \cong \langle \mu_m \rangle \oplus \langle u^{d/(m,s)} \pi^{ds/(m,s)} \rangle, $$

что и завершает доказательство леммы. •

Предложение 17. *Пусть E — эллиптическая кривая с разложимой мультипликативной редукцией и r, c — числа из формулировки теоремы. Тогда*

$$ {}_{p^n}E(k) \cong \langle \mu_{p^n} \rangle \oplus \mathbf{Z}/(c/r). $$

Доказательство. В силу предложения 8 кривая E изоморфна над k некоторой кривой Тэйта E_q. Тогда ${}_{p^n}E(k) \cong {}_{p^n}(k^*/\langle q \rangle)$. Пусть $q = u\pi^s$. Воспользуемся предыдущей леммой:

$$ {}_{p^n}E(k) \cong \langle \mu_{p^n} \rangle \oplus \langle u^{d/(p^n,s)} \pi^{ds/(p^n,s)} \rangle. $$

В силу предложения 8 $s = -v_k(j(E_q)) = -v_k(j(E))$, $\overline{u} = (\overline{j(E)\pi^s})^{-1}$. •

Теперь доказательство теоремы немедленно вытекает из лемм 4–7 и предложений 12–17.

Описание p-примарного кручения в диадическом случае дается следующим утверждением.

Теорема 6. *Пусть k — локальное поле, $\operatorname{char} \overline{k} = 2$, E — эллиптическая кривая, определенная над k, p — нечетное простое число. Тогда имеют место следующие утверждения.*

G_2. *Если E — кривая с хорошей редукцией, то*

$$ {}_{p^n}E(k) \cong {}_{p^n}\widetilde{E}(\overline{k}). $$

A_2. *Если E — кривая с аддитивной редукцией, то при $p > 3$*

$$ {}_{p^n}E(k) = \langle 0 \rangle, $$

а при $p = 3$

$$ {}_{3^n}E(k) \cong \mathbf{Z}/3, \quad \textit{если} \quad [E(k) : E_0(k)] = 3, $$

и

$$ {}_{3^n}E(k) \cong \langle 0 \rangle \quad \textit{в противном случае.} $$

M_2. *Если* E *— кривая с мультипликативной редукцией, то в случае неразложимой редукции*

$$ {}_{p^n}E(k) \cong \mathbf{Z}/p^d, $$

а в случае редукции разложимой

$$ {}_{p^n}E(k) \cong \langle \mu_{p^n} \rangle \oplus \mathbf{Z}/(c/r), $$

где числа d, r *и* c *определяются также, как и в теореме* 5.

Доказательство. Справедливость G_2, A_2 вытекает соответственно из лемм 3 и 4. В случае неразложимой мультипликативной редукции доказательство совпадает с соответствующим рассуждением из доказательства предложения 16. В случае разложимой мультипликативной редукции все следует из предложения 17. •

§6. Группа ${}_2\mathrm{Br}\, E$. Случай хорошей редукции

В этом параграфе k обозначает недиадическое локальное поле нулевой характеристики. Сохраняются также все обозначения предыдущих параграфов. Для эллиптической кривой E, определенной над k и обладающей хорошей редукцией, мы приведем список кватернионных алгебр, представляющих все элементы группы ${}_2\mathrm{Br}\, E$. Для этого зафиксируем простой элемент π поля k и единицу α кольца целых поля k, которая не является квадратом. Тогда справедлива следующая теорема представления.

Теорема 7. *Пусть* E *— эллиптическая кривая с хорошей редукцией, определенная над* k. *Тогда группа* ${}_2\mathrm{Br}\, E$ *представляется следующими алгебрами кватернионов:*

- *В разложимом случае*

$$ \left[\left(\frac{\pi, 1}{k(E)}\right)\right], \quad \left[\left(\frac{\pi, \alpha}{k(E)}\right)\right], \quad \left\{\left[\left(\frac{\pi, x - e_i}{k(E)}\right)\right]\right\}_{i=1,2,3}, \quad \left\{\left[\left(\frac{\pi, \alpha(x - e_i)}{k(E)}\right)\right]\right\}_{i=1,2,3}, $$

  где $e_3 = 0$.

- *В полуразложимом случае*

$$ \left[\left(\frac{\pi, 1}{k(E)}\right)\right], \quad \left[\left(\frac{\pi, \alpha}{k(E)}\right)\right], \quad \left[\left(\frac{\pi, x}{k(E)}\right)\right], \quad \left[\left(\frac{\pi, \alpha x}{k(E)}\right)\right]. $$

- *В неразложимом случае*

$$ \left[\left(\frac{\pi, 1}{k(E)}\right)\right], \quad \left[\left(\frac{\pi, \alpha}{k(E)}\right)\right]. $$

Доказательство теоремы предварим двумя утверждениями.

Лемма 9. *Пусть* $[(f,g \mid k(E))] \in \mathrm{Br}(k(E))$ *и кривая* E *определяется уравнением* $y^2 = x(x^2+ax+b)$. *Тогда, если* f *— унитарный многочлен из* $k[x]$, *то* $(f,g \mid k(E))_\infty$ *— тривиальная алгебра над* $k(E)_\infty$.

Доказательство. Положим $z = 1/x$. Тогда $k(E) = k(z)\left(\sqrt{z(1+az+bz^2)}\right)$. Поле $k(E)_\infty$ в бесконечной точке изоморфно полю $k\langle z\rangle\left(\sqrt{z(1+az+bz^2)}\right)$, которое, очевидно, совпадает с $k\langle z\rangle(\sqrt{z})$. Далее, $f(x) = f(1/z)$. Унитарность $f(x)$ влечет тогда, что многочлен $\widetilde{f}(z) = f(1/z)((\sqrt{z})^{\deg f})^2$ имеет вид $1 + zP(z)$, где $P(z) \in k[z]$ и, следовательно, $\widetilde{f}(z) = c^2$ для подходящего $c \in k\langle z\rangle(\sqrt{z})$. Тогда имеем

$$\left(\frac{f,g}{k(E)}\right)_\infty \cong \left(\frac{c^2,\widetilde{g}}{k(E)_\infty}\right),$$

где $\widetilde{g}$ — образ g при изоморфизме $k(E)_\infty$ и $k\langle z\rangle(\sqrt{z})$. Откуда и вытекает утверждение леммы. •

Следствие 4. *В условиях леммы* 9

$$\left(\frac{f,g}{k(E)}\right) \ncong \left(\frac{\pi,\alpha}{k(E)}\right).$$

Действительно, $(\pi,\alpha|k(E))_\infty \cong (\pi,\alpha|k\langle z\rangle(\sqrt{z}))$. Последняя алгебра нетривиальна и потому ввиду леммы 9 не изоморфна алгебре $(f,g \mid k(E))_\infty$. Откуда и вытекает справедливость следствия. •

Обратимся теперь к доказательству теоремы.

Доказательство. Справедливость теоремы в неразложимом случае вытекает из неразветвленности и неизоморфности тривиальной и числовой алгебр, а также из того факта, что $|_2\mathrm{Br}\, E| = 2$ (предложение 11).

Таким образом, в рассмотрении нуждаются только разложимый и полуразложимый случаи. Ввиду неразветвленности над $k(E)$ алгебры $(\pi,\alpha|k(E))$ для доказательства неразветвленности (над $k(E)$) алгебр из формулировки теоремы достаточно установить неразветвленность алгебр $(\pi, x-e_i \mid k(E))$, $i=1,2,3$ в разложимом случае и алгебры $(\pi, x \mid k(E))$ в полуразложимом. Заметим вначале для этого, что все перечисленные алгебры тривиальны при расширении поля скаляров до $k(E)_\infty$ и, следовательно, неразветвлены над $k(E)_\infty$. Таким образом, алгебра $(\pi, x-e_i \mid k(E))$ может ветвиться разве что в точке, определяемой многочленом $x-e_i$.

$$\left(\frac{\pi,x-e_i}{k(E)_{x-e_i}}\right) = \left(\frac{\pi,\frac{y^2}{(x-e_j)(x-e_k)}}{k(E)_{x-e_i}}\right) = \left(\frac{\pi,(x-e_j)(x-e_k)}{k(E)_{x-e_i}}\right) = \left(\frac{\pi,(e_i-e_j)(e_i-e_k)}{k(E)_{x-e_i}}\right),$$

где индексы i, j, k все различны. Очевидно, что последняя алгебра неразветвлена над полем $k(E)_{x-e_i}$. Следовательно, алгебры $(\pi, x-e_i \mid k(E))$, $i=1,2,3$ неразветвлены над $k(E)$. В полуразложимом случае будем иметь для алгебры $(\pi, x \mid k(E))$ в точке x:

$$\left(\frac{\pi,x}{k(E)_x}\right) = \left(\frac{\pi,\frac{y^2}{x^2+ax+b}}{k(E)_x}\right) = \left(\frac{\pi,x^2+ax+b}{k(E)_x}\right) = \left(\frac{\pi,b}{k(E)_x}\right).$$

Следовательно, и алгебра $(\pi, x|k(E))$ также неразветвлена над $k(E)$. Покажем теперь, что все алгебры, кроме первой из списка в формулировке теоремы, нетривиальны. Заметим прежде всего, что замена $z = x - e_i$ позволяет представить алгебру $(\pi, x-e_i|k(E))$ в виде $(\pi, z|k(E))$, а кривую E задать уравнением $y^2 = z(z^2+mz+n)$, где многочлен $z^2+\overline{m}z+\overline{n}$ имеет различные корни. Пусть теперь $\overline{X}$ — кривая над $\overline{k}$, заданная уравнением $V^2 = \overline{\alpha}(\overline{\alpha}^2U^4+\overline{m\alpha}U^2+\overline{n})$. Отметим, что ввиду предыдущего замечания многочлен $\overline{\alpha}(\overline{\alpha}^2U^4+\overline{m\alpha}U^2+\overline{n})$ не имеет кратных корней, и потому $\overline{X}$ — гладкая кривая над $\overline{k}$. В силу неравенства Вейля тогда для достаточно большого нечетного простого p кривая $\overline{X}$ имеет рациональную точку $(\overline{\delta}, \overline{\gamma})$ над $\mathbf{F}_{|\overline{k}|^p}$ (либо это имеет место уже для $p = 1$). Пусть теперь L — неразветвленное расширение k степени p. Тогда гладкая точка $(\overline{\delta}, \overline{\gamma})$ поднимается до L-рациональной точки (δ, γ) кривой X, определенной над L уравнением $V^2 = \alpha(\alpha^2U^4+m\alpha U^2+n)$. Таким образом, $\alpha\delta^2(\alpha^2\delta^4+m\alpha\delta^2+n) \in (k(\alpha\delta^2)^*)^2$. Обозначим теперь через $f(z)$ минимальный многочлен элемента $\alpha\delta^2$ над k. Тогда

$$k(E)_{f(z)} \cong k(\alpha\delta^2)\big(\sqrt{\alpha\delta^2(\alpha^2\delta^4+m\alpha\delta^2+n)}\big)\langle\mu\rangle,$$

где μ — простой элемент поля $k(E)_{f(z)}$. Поэтому $k(E)_{f(z)} \cong k(\alpha\delta^2)\langle\mu\rangle$, причем $k(\alpha\delta^2) = k$, либо $[k(\alpha\delta^2) : k] = p$. Откуда следует

$$\left(\frac{\pi, z}{k(E)_{f(z)}}\right) \cong \left(\frac{\pi, \alpha\delta^2}{k(E)_{f(z)}}\right) \cong \left(\frac{\pi, \alpha}{k(\alpha\delta^2)\langle\mu\rangle}\right) \cong \left(\frac{\pi, \alpha}{k\langle\mu\rangle}\right) \otimes_{k\langle\mu\rangle} k(\alpha\delta^2)\langle\mu\rangle.$$

Так как степень расширения $k(\alpha\delta^2)\langle\mu\rangle \mid k\langle\mu\rangle$ равна p или 1, а алгебра $(\pi, \alpha \mid k\langle\mu\rangle)$ нетривиальна, то нетривиальна и алгебра $(\pi, z \mid k(E)_{f(z)})$ а с ней и алгебра $(\pi, z \mid k(E)) = (\pi, x - e_i \mid k(E))$. Аналогичное рассуждение применимо и для алгебры $(\pi, x \mid k(E))$ в полуразложимом случае.

Обратимся теперь к полуразложимому случаю. Алгебры $(\pi, x|k(E))$ и $(\pi, \alpha|k(E))$ нетривиальны и в силу следствия к лемме 9 не изоморфны. Откуда следует, что алгебра $(\pi, \alpha x|k(E))$ также нетривиальна и не изоморфна ни одной из алгебр $(\pi, \alpha|k(E))$, $(\pi, x \mid k(E))$, что завершает доказательство теоремы для полуразложимого случая, поскольку элементы $[(\pi, 1 \mid k(E))]$, $[(\pi, \alpha \mid k(E))]$, $[(\pi, x \mid k(E))]$, $[(\pi, \alpha x \mid k(E))]$, очевидно, образуют группу порядка 4.

В разложимом случае элементы, перечисленные в формулировке теоремы, образуют группу (чтобы убедиться в этом, достаточно использовать соотношение $(x-e_i)y^2 = (x-e_i)^2(x-e_j)(x-e_k)$, где индексы i, j, k все различны). Таким образом, достаточно показать, что все эти алгебры попарно не изоморфны над $k(E)$. Поскольку элементы группы $\mathrm{Br}(k(E))$, соответствующие этим алгебрам, имеют порядок, не превосходящий 2, то для этого в свою очередь достаточно показать, что все они, исключая алгебру $(\pi, 1 \mid k(E))$, нетривиальны. Для алгебр $(\pi, \alpha \mid k(E))$ и $(\pi, x-e_i \mid k(E))$, $i = 1, 2, 3$, это уже показано. Что касается алгебр $(\pi, \alpha(x-e_i) \mid k(E))$, то

$$\left(\frac{\pi, \alpha(x-e_i)}{k(E)}\right) \sim \left(\frac{\pi, \alpha}{k(E)}\right) \otimes_{k(E)} \left(\frac{\pi, x-e_i}{k(E)}\right).$$

Но так как ввиду следствия к лемме 9 алгебры $(\pi, \alpha \mid k(E))$ и $(\pi, x - e_i \mid k(E))$ не $k(E)$-изоморфны, то последнее тензорное произведение, а с ним и алгебра $(\pi, \alpha(x - e_i) \mid k(E))$ нетривиальны. •

§7. Группа ${}_2\mathrm{Br}\,E$. Разложимый случай плохой редукции

Здесь мы рассмотрим разложимый случай кривой E с плохой редукцией. В этом случае ввиду теоремы 2 кривая E изоморфна над k одной из кривых, задаваемых уравнениями следующих типов. Пусть $a, b \in U(k)$.

I_1. $y^2 = x(x+\alpha)(x-\pi^m a)$, $m > 0$.
I_2. $y^2 = x(x+1)(x-\pi^m a)$, $m > 0$.
II. $y^2 = x(x-\pi a)(x-\pi b)$, $\overline{a} \neq \overline{b}$.
III. $y^2 = x(x-\pi a)(x-\pi^m b)$, $m > 1$.

Описание группы ${}_2\mathrm{Br}\,E$ в этих обозначениях дается следующим утверждением.

Теорема 8. *Пусть E — эллиптическая кривая, заданная над k одним из приведенных выше уравнений. Тогда в случае I_1 группа ${}_2\mathrm{Br}\,E$ представляется элементами*

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\ \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\ \left[\left(\frac{\pi,x}{k(E)}\right)\right],\ \left[\left(\frac{\pi,\alpha x}{k(E)}\right)\right],$$
$$\left[\left(\frac{\pi,x+\alpha}{k(E)}\right)\right],\ \left[\left(\frac{\alpha,\alpha(x+\alpha)}{k(E)}\right)\right],\ \left[\left(\frac{\pi,x-\pi^m a}{k(E)}\right)\right],\ \left[\left(\frac{\pi,\alpha(x-\pi^m a)}{k(E)}\right)\right].$$

В случае I_2 группа ${}_2\mathrm{Br}\,E$ представляется элементами

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\ \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\ \left[\left(\frac{\pi,x}{k(E)}\right)\right],\ \left[\left(\frac{\pi,\alpha x}{k(E)}\right)\right],$$
$$\left[\left(\frac{\alpha,x}{k(E)}\right)\right],\ \left[\left(\frac{\alpha,\pi x}{k(E)}\right)\right],\ \left[\left(\frac{\pi\alpha,x}{k(E)}\right)\right],\ \left[\left(\frac{\pi\alpha,\alpha x}{k(E)}\right)\right].$$

В случаях II и III группа ${}_2\mathrm{Br}\,E$ представляется элементами

$$\left[\left(\frac{\alpha,1}{k(E)}\right)\right],\ \left[\left(\frac{\alpha,\pi}{k(E)}\right)\right],\ \left[\left(\frac{\alpha,x}{k(E)}\right)\right],\ \left[\left(\frac{\alpha,x-\pi a}{k(E)}\right)\right],$$
$$\left[\left(\frac{\alpha,\pi(x-\pi a)}{k(E)}\right)\right],\ \left[\left(\frac{\alpha,\pi x}{k(E)}\right)\right],\ \left[\left(\frac{\alpha,x-\pi^m b}{k(E)}\right)\right],\ \left[\left(\frac{\alpha,\pi(x-\pi^m b)}{k(E)}\right)\right]$$

(где $m = 1$ в случае II и $m > 1$ в случае III).

Доказательство. Рассмотрим вначале случай I. Соотношение $y^2 = x(x+b)(x-\pi^m a)$, где $b \in U(k)$ позволяет способом, аналогичным способу, приведенному в доказательстве теоремы 7, установить, что элементы, перечисленные в случае I, образуют подгруппу порядка, делящего 8. Покажем неразветвленность соответствующих кватернионных алгебр. Алгебры $(\pi, 1 \mid k(E))$ и $(\pi, \alpha \mid k(E))$ неразветвлены над $k(E)$. Для точки, определяемой многочленом x, будем иметь $k(E)_x \cong k\langle x\rangle(\sqrt{x(x+b)(x-\pi^m a)}) \cong k\langle x\rangle(\sqrt{-ab\pi^m x})$. Тогда, если $u \in k^*$, то

$$\left(\frac{u,x}{k(E)_x}\right) \cong \left(\frac{u,-ab\pi^m}{k(E)_x}\right),$$

и потому алгебры $(\pi, x \mid k(E))$ и $(\alpha, x \mid k(E))$ неразветвлены над $k(E)_x$, а так как в силу леммы 9 эти алгебры неразветвлены над $k(E)_\infty$, то они неразветвлены и над $k(E)$. Аналогично над $k(E)_\infty$ неразветвлены и алгебры $(\pi, x+b \mid k(E))$ и $(\pi, x-\pi^m a \mid k(E))$. Покажем, что эти алгебры неразветвлены соответственно в точках, определяемых многочленами $x+b$ и $x-\pi^m a$. Действительно,

$$\begin{aligned} k(E)_{x+b} &\cong k\langle x+b\rangle\big(\sqrt{(x+b)(-b)(-b-\pi^m a)}\big) \\ &\cong k\langle x+b\rangle(\sqrt{x+b}), \\ k(E)_{x-\pi^m a} &\cong k\langle x-\pi^m a\rangle(\sqrt{ab\pi^m)x\pi^m a)}). \end{aligned}$$

Откуда

$$\left(\frac{\pi, x+b}{k(E)_{x+b}}\right) \cong \left(\frac{\pi, \pi(\sqrt{x+b})^2}{k(E)_{x+b}}\right) \sim 1, \left(\frac{\pi, x-\pi^m a}{k(E)_{x-\pi^m a}}\right) \cong \left(\frac{\pi, ab\pi^m}{k(E)_{x-\pi^m a}}\right).$$

Таким образом, алгебры $(\pi, x+b|k(E))$ и $(\pi, x-\pi^m a|k(E))$ неразветвлены над $k(E)$. Далее, так как все алгебры, указанные в случае I теоремы, подобны тензорным произведениям алгебр, неразветвленность которых уже доказана, то установлена неразветвленность над $k(E)$ всех алгебр из этого случая. Покажем теперь, что все эти алгебры, кроме первой, нетривиальны. Обозначим через L неразветвленное расширение степени 3 поля k. В силу леммы 1 существует такой элемент $\widetilde{v} \in \overline{L}^*$, что $\widetilde{v} \notin (\overline{L}^*)^2$, $\widetilde{v}+1 \in (\overline{L}^*)^2$, если $b \in (\overline{k}^*)^2$, и $\widetilde{v} \in (\overline{L}^*)^2, \widetilde{v}+1 \notin (\overline{L}^*)^2$, если $b \notin (\overline{k}^*)^2$. Положим $\widetilde{u} = \overline{b}\widetilde{v}/\overline{a}$, u — прообраз $\widetilde{u}$ в L и $\theta = \alpha u^2$. Обозначим через $f(x)$ минимальный многочлен элемента θ над k. Тогда

$$k(E)_{f(x)} \cong k(\theta)\langle f(x)\rangle\big(\sqrt{\theta(\theta+b)(\theta-\pi^m a)}\big) = k(\theta)\langle f(x)\rangle(\sqrt{\theta+b}).$$

Покажем теперь, что элемент $\theta+b \in (k(\theta)^*)^2$. Действительно, $\theta+b = \alpha u^2 - b$, последний же элемент ввиду недиадичности L является квадратом в L^* тогда и только тогда, когда $\overline{\alpha}\widetilde{u}^2 + \overline{b} \in (\overline{L}^*)^2$. Но $\overline{\alpha}\widetilde{u}^2 + \overline{b} = \overline{b}\widetilde{v} + \overline{b} = \overline{b}(\widetilde{v}+1) \in (\overline{L}^*)^2$. Таким образом, $\theta+b \in (L^*)^2$, а так как L имеет над k либо степень 1, либо 3, то $\theta+b \in (k(\theta)^*)^2$. Следовательно, $k(E)_{f(x)} \cong k(\theta)\langle f(x)\rangle$ и потому степень $[k(E)_{f(x)} : k\langle f(x)\rangle]$ равна либо 1, либо 3. Тогда

$$\left(\frac{\pi, x}{k(E)_{f(x)}}\right) = \left(\frac{\pi, \theta}{k(E)_{f(x)}}\right) = \left(\frac{\pi, \alpha}{k(E)\langle f(x)\rangle}\right) \otimes_{k\langle f(x)\rangle} k(\theta)\langle f(x)\rangle.$$

В силу последнего замечания о степени $[k(E)_{f(x)} : k\langle f(x)\rangle]$ последняя алгебра нетривиальна над $k(E)_{f(x)}$ тогда и только тогда, когда $(\pi, \alpha \mid k(E)\langle f(x)\rangle)$ нетривиальна над $k\langle f(x)\rangle$. Но нетривиальность этой алгебры известна, и потому $(\pi, x|k(E)_{f(x)})$ нетривиальна, а, следовательно, нетривиальна и алгебра $(\pi, x \mid k(E))$. Если положить $z = x - \pi^m a$, то алгебра $(\pi, x-\pi^m a \mid k(E))$ представляется в виде $(\pi, z|k(E))$, и кривая E задается теперь уравнением $y^2 = z(z+\pi^m a)(x+(b+\pi^m a))$, т.е. мы приходим к уже разобранному случаю, и потому $(\pi, x-\pi^m a|k(E))$ нетривиальна.

Заметим, что $(\pi, \alpha \mid k(E)) \ncong (\pi, x \mid k(E))$ ввиду следствия к лемме 9, поэтому $(\pi, \alpha x \mid k(E))$ — нетривиальная алгебра. Это же рассуждение показывает, что алгебры $(\pi, \alpha(x - \pi^m a) \mid k(E))$, $(\pi, \alpha(x + b) \mid k(E))$ также нетривиальны.

Докажем, что в случае $b \notin (k^*)^2$ алгебра $(\pi, x + b \mid k(E))$ нетривиальна. Для этого рассмотрим алгебру $(\pi, x + b \mid k(E)_x)$:

$$\left(\frac{\pi, x+b}{k(E)_x}\right) = \left(\frac{\pi, x+b}{k\langle x\rangle(\sqrt{-ab\pi^m x})}\right) \cong \left(\frac{\pi, b + (-ab\pi^m x)/(-ab\pi^m)}{k\langle x\rangle(\sqrt{-ab\pi^m x})}\right) \cong \left(\frac{\pi, b}{k\langle\sqrt{-ab\pi^m x}\rangle}\right).$$

Последняя алгебра нетривиальна ввиду $b \notin (k^*)^2$, поэтому нетривиальна и алгебра $(\pi, x + b \mid k(E)_x)$. Теперь аргументы, аналогичные уже указанным в доказательстве теоремы 7, показывают, что в случае I, $b \notin (k^*)^2$ алгебры, приведенные в формулировке теоремы, попарно не $k(E)$-изоморфны и потому соответствующие элементы из списка различны. Поскольку их количество совпадает с порядком группы ${}_2\mathrm{Br}(E)$, то случай I, $b \notin (k^*)^2$ полностью рассмотрен. Аналогично предыдущему, для завершения доказательства случая I достаточно установить нетривиальность алгебр

$$\left(\frac{\alpha, x}{k(E)}\right), \quad \left(\frac{\alpha, \pi x}{k(E)}\right), \quad \left(\frac{\pi\alpha, x}{k(E)}\right), \quad \left(\frac{\pi\alpha, \alpha x}{k(E)}\right) \quad \text{при} \quad b \in u(k)^2.$$

Для алгебры $(\alpha, x \mid k(E))$ рассмотрим два случая: $m = 1$ и $m > 1$. В первом случае

$$\left(\frac{\alpha, x}{k(E)_x}\right) = \left(\frac{\alpha, -\pi ab}{k\langle x\rangle(\sqrt{-\pi abx})}\right) = \left(\frac{\pi, \alpha}{k\langle\sqrt{-\pi abx}\rangle}\right)$$

и ясно, что последняя алгебра нетривиальна. В случае $m > 1$ будем иметь

$$\left(\frac{\alpha, x}{k(E)_{x-\pi}}\right) = \left(\frac{\alpha, \pi}{k\langle x - \pi\rangle(\sqrt{\pi(\pi - \pi^m a)(\pi + b)})}\right) = \left(\frac{\alpha, \pi}{k\langle x - \pi\rangle(\sqrt{b})}\right) = \left(\frac{\alpha, \pi}{k\langle x - \pi\rangle}\right).$$

Последняя алгебра снова нетривиальна, а поэтому $(\alpha, x \mid k(E))$ нетривиальна для любого $m \geq 1$. Далее,

$$\left(\frac{\alpha, \pi x}{k(E)_\infty}\right) \cong \left(\frac{\alpha, \pi z}{k\langle z\rangle(\sqrt{z^{-1}(z^{-1} - \pi^m a)(z^{-1} + b)})}\right) \cong \left(\frac{\alpha, \pi z}{k\langle\sqrt{z}\rangle}\right) \cong \left(\frac{\alpha, \pi}{k\langle\sqrt{z}\rangle}\right),$$

и потому $(\alpha, \pi x \mid k(E))$ — нетривиальная алгебра. Случаи II, III — аналогично. •

§8. Группа ${}_2\mathrm{Br}\,E$. Полуразложимый случай аддитивной редукции

В случае, когда кривая E имеет аддитивную редукцию, группа ${}_2\mathrm{Br}\,E$ описывается следующим утверждением.

Теорема 9. *Пусть E — эллиптическая кривая над недиадическим полем k с аддитивной редукцией. Тогда группа ${}_2\mathrm{Br}\,E$ представляется следующими элементами.*
В случае A.a):

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,x}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,\pi x}{k(E)}\right)\right].$$

В случае A.b):

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,x}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha x}{k(E)}\right)\right].$$

В случае A.c):

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],$$
$$\left[\left(\frac{\pi\sqrt{b}g(u)u,\, x-\pi\sqrt{b}u}{k(E)}\right)\right],\quad \left[\left(\frac{\pi\sqrt{b}g(u)u,\, \alpha(x-\pi\sqrt{b}u)}{k(E)}\right)\right],$$

где $g(x)\in k[x]$ *и*

$$g(x)=\begin{cases} x^2+1 & \text{в случаях A.c)1–A.c)2,}\\ x^2+\dfrac{a}{\sqrt{b}}x+1 & \text{в случаях A.c)3–A.c)4,}\end{cases}$$

а элемент u *подчинен условиям*

$$u\in u(k), g(u)\in U(k)\setminus U(k)^2 \quad \text{в случаях A.c)1–A.c)3,}$$

и

$$u=-1+\pi^r w,\ w\in U(k),\ w^2-c\in U(k)\setminus U(k)^2 \quad \text{в случае A.c)4.}$$

В случае A.d):

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,x+\pi\sqrt{b}}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,\alpha\pi(x+\pi\sqrt{b})}{k(E)}\right)\right].$$

В случае A.e):

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,x}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,\pi x}{k(E)}\right)\right].$$

Доказательство. Поскольку порядок группы ${}_2\mathrm{Br}\,E$ равен 4, и $(\pi,1\mid k(E))$, $(\pi,\alpha\mid k(E))$ — два различных ее элемента, то для представления всех ее элементов достаточно указать нетривиальную, неразветвленную и не изоморфную $(\pi,\alpha\mid k(E))$

алгебру. Пусть вначале кривая задается уравнением $y^2 = x(x^2 + \pi^m a x + \pi^t b)$, где $a \in U(k) \cup \{0\}$, $b \in U(k)$, $m > 0$, $t = 1, 2, 3$. В случае нечетного t рассмотрим алгебру $(\alpha, x \mid k(E))$. Тогда

$$\left(\frac{\alpha, x}{k(E)_x}\right) \cong \left(\frac{\alpha, \pi^t b}{k\langle\sqrt{\pi^t b x}\rangle}\right) \cong \left(\frac{\alpha, \pi}{k\langle\sqrt{\pi^t b x}\rangle}\right).$$

Следовательно, алгебра $(\alpha, x \mid k(E))$ нетривиальна и неразветвлена. Она не изоморфна алгебре $(\pi, \alpha \mid k(E))$ ввиду следствия к лемме 9. В случае $t = 2$, $b \notin (k^*)^2$ рассмотрим алгебру $(\pi, x \mid k(E))$. Тогда

$$\left(\frac{\pi, x}{k(E)_x}\right) \cong \left(\frac{\pi, b}{k\langle\sqrt{bx}\rangle}\right),$$

и потому алгебра $(\pi, x \mid k(E))$ нетривиальна и неразветвлена. Снова по следствию к лемме 9 она неизоморфна числовой алгебре.

Если кривая E не задается уравнением указанного выше типа, то ее уравнение имеет вид $y^2 = x(x^2 + \pi^m a x + \pi^2 b)$, где $a \in U(k) \cup \{0\}$, $b \in U(k)^2$, $m > 0$.

Замена простого элемента π на элемент $\nu = \pi\sqrt{b}$ позволяет переписать эти уравнения в виде

$$y^2 = x(x^2 + \nu^2),$$
$$y^2 = x(x^2 + \nu^m \widetilde{a} x + \nu^2), \quad \text{где } \widetilde{a} = a/(\sqrt{b})^m.$$

Выделим следующие случаи задания E, соответствующие списку минимальных уравнений для E:

A) $y^2 = x(x^2 + \nu^2)$, $-1 \notin (k^*)^2$;
B) $y^2 = x(x^2 + \nu^m \widetilde{a} x + \nu^2)$, $m > 1$, $-1 \notin (k^*)^2$;
C) $y^2 = x(x^2 + \nu \widetilde{a} x + \nu^2)$, $\overline{\widetilde{a}^2} \neq 4$;
D) $y^2 = x(x^2 + \nu \widetilde{a} x + \nu^2)$, $\widetilde{a} = 2 + \nu^{2r} c$, $c \in U(k) \setminus U(k)^2$;
F) $y^2 = x(x^2 + \nu \widetilde{a} x + \nu^2)$, $\widetilde{a} = 2 + \nu^{2r+1} c$, $c \in U(k)$.

Пусть многочлен $g(x)$ — многочлен из формулировки теоремы. Покажем, что в каждом из случаев A), B), C), D) существует элемент $u \in U(k)$ такой, что алгебра $(\nu u g(u), x - \nu u \mid k(E))$ нетривиальна, неразветвлена и не изоморфна числовой алгебре (над полем $k(E)$). Рассмотрим сначала случаи A), B), C). Ввиду неприводимости $\overline{g}(x)$ и леммы 1 существует элемент $\widetilde{u} \in \overline{k}^*$ такой, что $\overline{g}(\widetilde{u}) \in \overline{k}^* \setminus (\overline{k}^*)^2$. Обозначим через u прообраз $\widetilde{u}$ в k. Тогда $g(u) \in U(k) \setminus U(k)^2$. Следовательно,

$$\left(\frac{\nu u g(u), x - \nu u}{k(E)_x}\right) \cong \left(\frac{\nu u g(u), -\nu u}{k\langle x\rangle\left(\sqrt{x g(u)}\right)}\right) \cong \left(\frac{\nu u g(u), -\nu u}{k\left\langle\sqrt{x g(u)}\right\rangle}\right),$$

и потому алгебра $(\nu u g(u), x - \nu u \mid k(E))$ нетривиальна. Пусть теперь $|\overline{k}| \leq 7$. Тогда в случаях A), B) $\overline{k} = \mathbf{F}_3$ (поскольку $-1 \in (\mathbf{F}_5^*)^2$). Тогда в силу леммы 1 существует

$\widetilde{u} \in \mathbf{F}_3^*$ такой, что $g(u) \in \mathbf{F}_3^* \setminus (\mathbf{F}_3^*)^2$. Если u — прообраз $\widetilde{u}$ в k, то алгебра $(\nu u g(u), x - \nu u \mid k(E))$ снова нетривиальна. В случае C) имеем

$$x^2 + \overline{\widetilde{a}}x + 1 = \left(x + \frac{\overline{\widetilde{a}}}{2}\right)^2 + \left(\frac{-\overline{\widetilde{a}}^2 + 4}{4}\right).$$

Если $\overline{k} = \mathbf{F}_3$, то $-\overline{\widetilde{a}} + 4 \in (\mathbf{F}_3^*)^2$, и потому существует $\widetilde{u} \in \mathbf{F}_3^*$ такой, что $(\widetilde{u} + \overline{\widetilde{a}}/2)^2 + ((-\overline{\widetilde{a}}^2 + 4)/4) \in \mathbf{F}_3^* \setminus (\mathbf{F}_3^*)^2$. Тогда прообраз $\widetilde{u}$ в k — искомый элемент u. В случае $\overline{k} = \mathbf{F}_5$ $((-\overline{\widetilde{a}}^2 + 4)/4) \in (\mathbf{F}_5^*)^2$ и по следствию к лемме 1 снова существует $\widetilde{u}$ такой, что $\widetilde{u}^2 + \overline{\widetilde{a}}u + 1 \in (\overline{k}^*)^2$, а тогда прообраз u элемента $\widetilde{u}$ в k искомый. Таким образом, установлено существование элемента u из $U(k)$ такого, что алгебра $(\nu u g(u), x - \nu u \mid k(E))$ нетривиальна. Заметим, что она неразветвлена. Действительно, ввиду леммы 9 достаточно установить неразветвленность алгебры $(\nu u g(u), x - \nu u \mid k(E)_{x-\nu u})$. Последняя же алгебра действительно неразветвлена:

$$\left(\frac{\nu u g(u), x - \nu u}{k(E)_{x-\nu u}}\right) \cong \left(\frac{\nu u g(u), x - \nu u}{k\langle x - \nu u\rangle(\sqrt{\nu u g(u)})}\right) \cong \left(\frac{\pi, 1}{k\langle x - \nu u\rangle(\sqrt{\nu u g(u)})}\right).$$

Ввиду следствия к лемме 9 алгебра $(\nu u g(u), x - \nu u \mid k(E))$ не изоморфна числовой алгебре, и тем самым завершено рассмотрение случаев A), B), C).

Рассмотрим случай D). Покажем, что в $\overline{k}^*$ существует элемент $\widetilde{v}$ такой, что $(\widetilde{v}^2 - \overline{c}/\overline{b}^r) \in \overline{k}^* \setminus (\overline{k}^*)^2$. Действительно, все вытекает из следствия к лемме с учетом $c \notin (k^*)^2$. Пусть теперь v — прообраз $\widetilde{v}$ в k и $u = -1 + \nu^r v$. Тогда ввиду выбора u алгебра $(\nu u g(u), x - \nu u \mid k(E))$ неразветвлена и не изоморфна числовой алгебре. Теперь для того чтобы завершить доказательство теоремы для случая D) полагаем $w = (\sqrt{b})^r v$.

Наконец, рассмотрим случай F). Пусть вначале $c \notin (k^*)^2$. Подберем $u \in U(k)$ таким образом, чтобы алгебра $(\alpha, x - u\nu \mid k(E)_{x-u\nu})$ была тривиальна. Для этого, как нетрудно видеть, достаточно, чтобы элемент u удовлетворял условию $\nu u(\nu^2(u+1)^2 + \nu^{2r+3}cu) \in U(k) \setminus U(k)^2$, т.е. $\nu u(u+1)^2 + \nu^{2r+2}cu \in U(k) \setminus U(k)^2$. Положим $u = -1$. Тогда, очевидно, нужное нам условие выполнено, и потому исходная алгебра неразветвлена. Рассмотрение алгебры $(\alpha, x + \nu \mid k(E)_x)$ показывает, что алгебра $(\alpha, x+\nu|k(E))$ нетривиальна. Таким образом, остается рассмотреть случай $c \in (k^*)^2$. В этом случае нужной нам алгеброй является алгебра $(\alpha, x \mid k(E))$. Действительно, ввиду следствия к лемме эта алгебра не изоморфна числовой. Кроме того,

$$\left(\frac{\alpha, x}{k(E)_x}\right) \cong \left(\frac{\alpha, x}{k\langle\sqrt{x}\rangle}\right) = \left(\frac{\pi, 1}{k\langle\sqrt{x}\rangle}\right),$$

и потому алгебра $(\alpha, x \mid k(E))$ неразветвлена. Ее нетривиальность следует из того, что

$$\left(\frac{\alpha, x}{k(E)_{x+\nu}}\right) \cong \left(\frac{\alpha, -\nu}{k\langle x + \nu\rangle}\right),$$

причем последняя алгебра нетривиальна. •

§9. Группа ${}_2\mathrm{Br}\,E$. Полуразложимый случай мультипликативной редукции

Следующая теорема описывает группу ${}_2\mathrm{Br}\,E$ в полуразложимом случае мультипликативной редукции.

Теорема 10. *Пусть E — эллиптическая кривая над недиадическим полем k с мультипликативной редукцией, причем имеет место полуразложимый случай. Тогда группа ${}_2\mathrm{Br}\,E$ представляется следующими элементами:*

В случае M.a)

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\quad \left[\left(\frac{\pi b,x+a}{k(E)}\right)\right],\quad \left[\left(\frac{\pi b,\alpha(x+a)}{k(E)}\right)\right].$$

В случае M.b)

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,x}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha x}{k(E)}\right)\right].$$

В случае M.c)

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,x+a}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,\pi(x+a)}{k(E)}\right)\right].$$

В случае M.d)

$$\left[\left(\frac{\pi,1}{k(E)}\right)\right],\quad \left[\left(\frac{\pi,\alpha}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,x+a-v\pi^m}{k(E)}\right)\right],\quad \left[\left(\frac{\alpha,\pi(x+a-v\pi^m)}{k(E)}\right)\right],$$

где $v\in U(k)$ и $v^2-ab\in U(k)\setminus U(k)^2$. Величины a, b, m означают то же самое, что и в соответствующем списке минимальных уравнений.

Доказательство. Как и в доказательстве предыдущей теоремы, нам достаточно указать в каждом из возможных случаев нетривиальную и неразветвленную алгебру кватернионов, не изоморфную числовой алгебре $(\pi,\alpha\mid k(E))$. Кривая E в нашем случае задается уравнением $y^2=x((x+a)^2+\pi^s bx)$, где $a,b\in U(k)$, $s>0$.

Пусть s нечетно. Рассмотрим алгебру $(\pi b,x+a|k(E))$. Эта алгебра не изоморфна числовой и неразветвлена ввиду

$$\left(\frac{\pi b,x+a}{k(E)_{x+a}}\right)\cong\left(\frac{\pi b,x+a}{k\langle x+a\rangle(\sqrt{\pi^s b})}\right)\cong\left(\frac{\pi,1}{k\langle x+a\rangle(\sqrt{\pi^s b})}\right).$$

Установим теперь нетривиальность алгебры $(\pi b,x+a\mid k(E))$. Пусть L — неразветвленное расширение k степени 3. Тогда ввиду следствия к лемме 1 в поле $\overline{L}$ существует элемент $\widetilde{w}\in(\overline{L}^*)^2$ такой, что $\overline{a}+\widetilde{w}\in\overline{L}^*\setminus(\overline{L}^*)^2$. Пусть w — прообраз $\widetilde{w}$ в L и $f(x)$ — его минимальный многочлен над k. Тогда

$$\left(\frac{\pi b,x+a}{k(E)_f}\right)\cong\left(\frac{\pi b,a+w}{k(w)\langle f\rangle\left(\sqrt{w((w+a)^2+\pi^m bw)}\right)}\right)$$
$$\cong\left(\frac{\pi b,a+w}{k(w)\langle f\rangle}\right)$$
$$\cong\left(\frac{\pi,\alpha+w}{k(w)\langle f\rangle}\right).$$

Последняя алгебра, очевидно, нетривиальна.

Рассмотрим случай четного s. Если $-a \notin (k^*)^2$, то алгебра $(\pi, x \mid k(E))$ удовлетворяет нашим требованиям. Действительно, ввиду следствия к лемме 9 она не изоморфна числовой алгебре. Кроме того,

$$\left(\frac{\pi, x}{k(E)_x}\right) \cong \left(\frac{\pi, x}{k\langle x\rangle\left(\sqrt{x((x+a)^2+\pi^s bx)}\right)}\right) \cong \left(\frac{\pi, x}{k\langle\sqrt{x}\rangle}\right) \cong \left(\frac{\pi, 1}{k\langle\sqrt{x}\rangle}\right).$$

Покажем, что алгебра $(\pi, x \mid k(E))$ нетривиальна. Для этого отыщем элемент $\widetilde{v} \in (\overline{k}^*)^2$ такой, что $\widetilde{v}^2 + (-\overline{ab}) \in \overline{k}^* \setminus (\overline{k}^*)^2$. Неприводимость многочлена $(x+a)^2 + \pi^s bx$ над k влечет $ab \notin (k^*)^2$. В случае $\overline{k} = \mathbf{F}_3$ из последнего условия вытекает, что $(-\overline{ab}) \in (\overline{k}^*)^2$, а тогда ввиду следствия к лемме 1 существование $\widetilde{v}$ доказано. Если $|\overline{k}| \geq 5$, то условие $\widetilde{v} + (-\overline{ab}) \in \overline{k}^* \setminus (\overline{k}^*)^2$ ввиду того же следствия выполнено для подходящего $\widetilde{v}$.

Обозначим через v прообраз $\widetilde{v}$ в k. Тогда

$$\left(\frac{\pi, x}{k(E)_{x+a-\pi^m v}}\right) \cong \left(\frac{\pi, -a}{k\langle x+a-\pi^m v\rangle\left(\sqrt{(-a)(\pi^{2m}v^2 + (-a+\pi^m v)\pi^{2m}b)}\right)}\right)$$
$$= \left(\frac{\pi, -a}{k\langle x+a-\pi^m v\rangle\left(\sqrt{-a(v^2-ab)}\right)}\right) = \left(\frac{\pi, -a}{l\langle x+a-\pi^m v\rangle}\right),$$

а последняя алгебра нетривиальна.

Наконец, рассмотрим случай четного s, когда $(-a) \in (k^*)^2$. Если $-1 \in (k^*)^2$, то $a \in (k^*)^2$, $b \notin (k^*)^2$ и нам подходит алгебра $(\alpha, x+a|k(E))$. Как и раньше, для доказательства ее неразветвленности достаточно установить неразветвленность алгебры $(\alpha, x+a \mid k(E)_{x+a})$.

Заметим, что $k(E)_{x+a} \cong k\langle x+a\rangle\left(\sqrt{(-a)\pi^s b(-a)}\right) = k\langle x+a\rangle(\sqrt{b})$. Тогда

$$\left(\frac{\alpha, x+a}{k(E)_{x+a}}\right) \cong \left(\frac{\alpha, x+a}{k\langle x+a\rangle(\sqrt{b})}\right) \cong \left(\frac{\pi, 1}{k\langle x+a\rangle(\sqrt{b})}\right).$$

Таким образом, алгебра $(\alpha, x+a \mid k(E))$ неразветвлена. Покажем ее нетривиальность. Пусть $K = k(\sqrt[3]{\pi})$ и $f(x)$ — минимальный многочлен элемента $(-a + \sqrt[3]{\pi})$ над k. Тогда, если $\Pi = \sqrt[3]{\pi}$, то

$$\left(\frac{\alpha, x+a}{k(E)_f}\right) \cong \left(\frac{\alpha, \Pi}{k\langle f\rangle(\Pi)\left(\sqrt{(-a+\Pi)(\Pi^2+\Pi^{3s}b(-a+\Pi))}\right)}\right) \cong \left(\frac{\alpha, \Pi}{k\langle f\rangle(\Pi)}\right),$$

и последняя алгебра, очевидно, нетривиальна. Следовательно, нетривиальна и алгебра $(\alpha, x+a \mid k(E))$. Кроме того, она не изоморфна числовой алгебре. Пусть s четно и $-1, a(k^*)^2$. Рассмотрим алгебру $(\alpha, x+u \mid k(E))$, где $u = a - v\pi^m$ и $v \in U(k)$

такое, что $\overline{v}^2 - \overline{a}\overline{b} \in \overline{k}^* \setminus (\overline{k}^*)^2$. (Заметим, что такой элемент существует ввиду следствия к лемме 1). Тогда

$$\left(\frac{\alpha, x+u}{k(E)_{x+u}}\right) \cong \left(\frac{\alpha, x+u}{k\langle x+u\rangle\left(\sqrt{(-a)(v^2\pi^{2m} + \pi^{2m}b(-a+v\pi^m))}\right)}\right)$$
$$\cong \left(\frac{\alpha, x+u}{k\langle x+u\rangle(\sqrt{v^2-ab})}\right)$$
$$\cong \left(\frac{\pi, 1}{k\langle x+u\rangle(\sqrt{v^2-ab})}\right).$$

Поскольку в силу леммы 9 $(\alpha, x+u \mid k(E)_\infty)$ тривиальна, то неразветвленность алгебры $(\alpha, x+u \mid k(E))$ установлена. Покажем ее нетривиальность. Снова пусть $\Pi = \sqrt[3]{\pi}$, $K = k(\Pi)$ и $f(x)$ — минимальный многочлен элемента $-u + \Pi$ над k. Тогда

$$\left(\frac{\alpha, x+u}{k(E)_f}\right) \cong \left(\frac{\alpha, x+u}{k\langle f\rangle(\Pi)\left(\sqrt{(-u+\Pi)((\Pi+v\pi^m)^2 + \pi^{2m}b(-a+v\pi^m+\Pi))}\right)}\right)$$
$$= \left(\frac{\alpha, \Pi}{k(\Pi)\langle f\rangle\sqrt{\Pi^2 + \Pi^r\delta}}\right),$$

где $r > 2$ и $\delta \in U(k)$. Тогда последняя алгебра имеет вид $(\alpha, \Pi \mid k(\Pi)\langle f\rangle)$ и, следовательно, нетривиальна, что влечет нетривиальность алгебры $(\alpha, x+u \mid k(E))$. Так как последняя алгебра не изоморфна числовой, то доказательство теоремы завершено. •

Список литературы

1. Demeyer F. R., Knus M. A., *The Brauer group of a real curve*, Proc. Amer. Math. Soc. **57** (1976), no. 2, 233–270.
2. Gross B. H., Harris J., *Real algebraic curuves*, Ann. Scient. Norm. Sup. **14** (1981), 157–182.
3. Witt E., *Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Functionkörper*, J. Reine Angew. Math. **171** (1934), 4–11.
4. Scharlau W., *Über bie Brauer-Gruppe eines algebraischen Funktionenkörpers in einer Variabein*, J. für die reine und angew. Math. **239–240** (1969), 1–6.
5. Lichtenbaum S., *Duality Theorems for Curuves over P-adic Fields*, Invent. Math. **7** (1969), 120–136.
6. Colliot-Thelene J.-P. (with the collaboration of J.-J. Sansuc), *The rationality problem for fields of invariants under linear algebraic groups (with special regard to the Brauer group)*, Unpublished Lecture Notes from the 9th ELAM, Santiago de Chile, 1988.
7. Tate J., *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions in One Variable IV, Lect. Not. Math., vol. 476 (1975), 33–52.
8. Серр Ж.-П., *Когомологии Галуа*, Мир, М., 1968.
9. Tate J., *WC-groups over p-adic fields*, Seminaire Bourbaki, Décembre 1957, n. 1556.
10. Башмаков М. И., *Когомологии абелевых многообразий над числовым полем*, Успехи мат. наук **27** (1972), вып. 6 (168), 25–66.
11. Schoof R., *Nonsingular plane curves over finite fields*, J. Combin. Theory, ser. A **46** (1987), no. 2, 183–211.
12. Voloh J. F., *A note on elliptic curves over finite fields*, Bull. Soc. Math. France **116** (1988), 455–458.

13. Waterhouse W.C., *Abelian varieties over finite fields*, Ann. Sci. E.N.S., ser. 4 **2** (1969), 521–560.
14. Silverman J., *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1985.
15. Husemöller D., *Elliptic Curves. Graduate Texts in Math., bf111*, Springer-Verlag, 1986.

Поступило 24 июня 1994

Институт математики АНБ
220073, Беларусь, Минск
ул.Сурганова, 11

Институт технической кибернетики АНБ,
220000 Беларусь, Минск,
ул. Сурганова, 6