УДК 512.7/78

В. І. Андрійчук, канд. фіз.-мат. наук (Львів. ун-т)

Про добуток Тейта — Шафаревича в еліптичних кривих над псевдолокальними полями з полями лишків характеристики 3

Нехай k—загальне локальне поле з псевдоскінченним полем лишків $\varkappa$, $\mathrm{char}\ \varkappa = 3$, A — еліптична крива, визначена над полем k. Доведено, що добуток Тейта — Шафаревича $H^1(k, A) \times A_k \to \mathbf{Q}/\mathbb{Z}$ групи $H^1(k, A)$ —головних однорідних просторів кривої A над полем k —і групи A_k її k-раціональних точок невироджений зліва.

Пусть k — общее локальное поле с псевдоконечным полем вычетов $\varkappa$, $\mathrm{char}\ \varkappa = 3$, A — эллиптическая кривая, определенная над полем k. Доказано, что произведение Тэйта — Шафаревича $H^1(k, A) \times A_k \to \mathbf{Q}/\mathbb{Z}$ группы $H^1(k, A)$ — главных однородных пространств кривой A над полем k — и группы A_k ее k-рациональных точек невырождено слева.

Нехай A — еліптична крива, визначена над локальним полем k. І. Р. Шафаревич [1] і Тейт [2] означили добуток

$$H^1(k, A) \times A_k \to \mathbf{Q}/\mathbb{Z} \tag{1}$$

групи $H^1(k, A_k)$ —головних однорідних просторів еліптичної кривої A над полем k- і групи A_k k-раціональних точок кривої A і довели двосторонню невиродженість цього добутку з точністю до p-компонент груп, що входять в (1), де p — характеристика поля лишків поля k.

О. М. Введенський [3] довів двосторонню невиродженість добутку (1) без обмеження на p-компоненти. Доведення грунтувалося на прямому обчисленні добутку Тейта—Шафаревича для простих циклічних розширень поля k. Крім того, О. М. Введенський поставив питання про пошук класу загальних локальних полів (тобто повних відносно дискретного нормування полів з квазіскінченними [4] полями лишків), для яких добуток Тейта—Шафаревича в еліптичних кривих є невиродженим зліва. У роботі [5] показано, що таким класом є клас псевдолокальних полів, тобто загальних локальних полів з псевдоскінченними за Аксом [6] полями лишків. А саме, у роботі [5] доведена невиродженість зліва добутку Тейта—Шафаревича в еліптичних кривих, визначених над псевдолокальним полем k, характеристика поля лишків якого відмінна від 2 і 3. Мета даної роботи — доведення невиродженості зліва добутку Тейта—Шафаревича у випадку, коли характеристика поля лишків псевдолокального поля k дорівнює 3. Випадок характеристики 2 буде розглянутий у наступній роботі.

Отже, далі k означає псевдолокальне поле з полем лишків $\varkappa$, $\mathrm{char}\ \varkappa = 3$. Справедлива така теорема.

Теорема. *Добуток Тейта—Шафаревича невироджений зліва для еліптичних кривих A над полем k.*

Основна відмінність розглянутого у теоремі випадку від ситуації, коли $\mathrm{char}\ \varkappa \neq 2, 3$, полягає у тому, що у цьому випадку не кожна крива типу (c) за Нероном над k стає ізоморфною кривій типу (a) або (b) за Нероном над слабо розгалуженим розширенням поля k. Якщо $\mathrm{char}\ \varkappa = 3$, то криві типів (c_1), (c_3), (c_6) і (c_8) за Нероном стають ізоморфними кривій типу (a) за Нероном над дико розгалуженими розширеннями основного поля k. Тому виникає необхідність доводити невиродженість зліва добутку Тейта—Шафаревича

$$H^1(\mathrm{Gal}(l/k), A_l) \times H^0(\mathrm{Gal}(l/k), A_l) \to \mathbf{Q}/\mathbb{Z} \tag{T_l}$$

для простих циклічних дико розгалужених розширень l/k.

Доведення теореми розбивається на два кроки. Перший крок (твердження 1) — доведення невиродженості зліва добутку Тейта—Шафаревича для кривих A типу (*a*) або (*b*) над k. Другий крок (твердження 2) — доведення невиродженості зліва для кривих типу (с) за Нероном.

Нехай $\mathfrak{O}_k$ — кільце цілих поля k, π — простий елемент кільця $\mathfrak{O}_k$, U_k — група одиниць кільця $\mathfrak{O}_k$. Якщо l/k — скінченне розширення Галуа поля k, то відповідні об'єкти поля l позначимо через $\mathfrak{O}_l$, Π, U_l. $\underline{\lambda}$ означає поле лишків поля l. Якщо $a \in \mathfrak{O}_k$, то $a \bmod \pi$ позначимо через $\bar{a}$. $\mathfrak{g} = \mathrm{Gal}\,(l/k)$ — група Галуа розширення l/k. Для $\mathfrak{g}$-модуля X через $H^n(\mathfrak{g}, X)$, $n \in \mathbb{Z}$, позначимо когомології Тейта групи $\mathfrak{g}$ з коефіцієнтами в X.

Нехай A — еліптична крива над полем k;

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathfrak{O}_k \tag{2}$$

— рівняння Вейєрштрасса кривої A, A_k — група k-раціональних точок кривої A, $A'_\varkappa$ — редукція групи A_k по $\bmod \pi$, Γ_k — ядро редукції — підгрупа Лютц групи A_k, $\Gamma_k \supset \Gamma_k^2 \supset \ldots$ — стандартна фільтрація групи Γ_k. Якщо $t \in \pi\mathfrak{O}_k$, то через $\varepsilon(t)$ позначимо $(1 + a_2t^2 + a_4t^4 + a_6)^{1/2} = 1 + \frac{a_2}{2}t^2 + \ldots$. Три крапки тут і далі означають члени вищого порядку.

Нагадаємо потрібні нам властивості добутку Тейта—Шафаревича в еліптичних кривих над загальним локальним полем, сформульовані Тейтом [2] у вигляді діаграм, для яких О. М. Введенським у роботі [3] прийняті позначення (r_1), (r_2) і (r_3).

Має місце комутативна діаграма з точними рядками

$$\begin{array}{ccccccc} 0 \to H^1(\mathfrak{g}, A_l) & \to & H^1(k, A) & \to & H^1(l, A) & & \\ \big\downarrow \theta_{l/k} & & \big\downarrow \theta_k & & \big\downarrow \theta_l & , & (r_2) \\ 0 \to H^0(\mathfrak{g}, A_l)^* & \to & A_k^* & \to & A_l^* & & \end{array}$$

нижній рядок якої є двоїстим за Понтрягіном до точної послідовності $A_l \xrightarrow{N_{l/k}} A_k \to H^0(\mathfrak{g}, A_l) \to 0$, де $N_{l/k}$ — норменний гомоморфізм, $\theta_{l/k}$, θ_k, θ_l — гомоморфізми, індуковані добутком Тейта—Шафаревича.

Розглянемо башту скінченних розширень Галуа з відповідними групами Галуа $\underbrace{k \overset{\mathfrak{g}}{—} l \overset{\mathfrak{h}}{—} l_1}_{\mathfrak{g}_1}$, де $\mathfrak{g}$ — циклічна. Має місце комутативна діаграма з точними рядками

$$\begin{array}{ccccccc} 0 \to H^1(\mathfrak{g}, A_l) & \to & H^1(\mathfrak{g}_1, A_{l_1}) & \to & H^1(\mathfrak{h}, A_{l_1})^{\mathfrak{g}} & \to & H^0(\mathfrak{g}, A_l) \\ \big\downarrow \theta_{l/k} & & \big\downarrow \theta_{l_1/k} & & \big\downarrow \theta_l & & \big\downarrow (-1)\,\omega_{l/k} \qquad (r_3) \\ 0 \to H^0(\mathfrak{g}, A_l)^* & \to & H^0(\mathfrak{g}_1, A_{l_1})^* & \to & (H^0(\mathfrak{h}, A_{l_1})^*)^{\mathfrak{g}} & \to & H^1(\mathfrak{g}, A_l)^*, \end{array}$$

нижній рядок якої є двоїстим за Понтрягіном до точної послідовності дискретних абелевих груп

$$H^1(\mathfrak{g}, A_l) \to H_0(\mathfrak{g}_1, H^0(\mathfrak{h}, A_{l_1})) \to H^0(\mathfrak{g}_1, A_{l_1}) \to H^0(\mathfrak{g}, A_l) \to 0.$$

У діаграмі (r_3) $\theta_{l/k}$, $\theta_{l_1/k}$, θ_l — гомоморфізми, індуковані добутком Тейта—Шафаревича, $(-1)\,\omega_{l/k}$ — помножене на -1 обмеження гомоморфізму $\omega_k : A_k \to H^1(k, A)^*$, двоїстого за Понтрягіном до θ_k.

Наслідуючи О. М. Введенського [3], перевірку невиродженості добутку Тейта—Шафаревича

$$H^1(\mathfrak{g}, A_l) \times H^0(\mathfrak{g}, A_l) \to \mathbf{Q}/\mathbb{Z}$$

для простого циклічного розширення l/k будемо проводити таким спосоом: нехай коцикл f — представник деякого класу $H^1(\mathfrak{g}, A_l)$ і $a_k \in A_k$ — представник деякого класу $H^0(\mathfrak{g}, A_l)$. Нехай $\mathfrak{g} = \{1, \sigma, \ldots, \sigma^{n-1}\}$, φ — функція з поля $k(A)$ функцій на кривій A над k з дивізором $f(\sigma) \dot{+} \sigma f(\sigma) + \ldots$ $\ldots + \sigma^{n-1} f(\sigma) - n\infty$ (∞ — нуль групи A), а $u \in A_k$ таке, що $a \dot{+} u$ (додавання на A) і $u \neq f(\sigma)$, ∞. Розглядувані класи не ортогональні за Тейтом—Шафаревичем тоді і тільки тоді, коли $\dfrac{\varphi(a \dot{+} u)}{\varphi(u)}$ не лежить в $N_{\mathfrak{g}} l^*$.

Твердження 1. *Добуток Тейта—Шафаревича* (1) *невироджений зліва для еліптичних кривих типів* (*a*) *і* (*b*) *за Нероном, визначених над псевдолокальним полем* k *з полем лишків характеристики* 3.

Доведення твердження 1 опирається на леми 1 і 2.

Лема 1. *Нехай A — еліптична крива над полем k.*

а). *Якщо A — крива типу* (*a*) *за Нероном і l/k — скінченне нерозгалужене розширення Галуа, то групи $H^i(\mathfrak{g}, A_l)$, $i \in \mathbb{Z}$, тривіальні.*

б). *Якщо A — крива типу* (*a*) *за Нероном і l/k — чисто слабо розгалужене розширення простого степеня q, то добуток (T_l) невироджений зліва.*

в). *Якщо A— крива типу* (*a*) *за Нероном з інваріантом Гассе редукції рівним нулю і l/k — дико розгалужене розширення степеня* 3, *то добуток (T_l) невироджений зліва.*

г). *Якщо A—крива типу* (*b*) *за Нероном, то добуток Тейта—Шафаревича $H^1(k, A) \times A_k \to \mathbb{Q}/\mathbb{Z}$ невироджений зліва.*

Доведення. Випадки а) і б) — це відповідно леми 1 і 2 роботи [5], які справедливі без обмежень на характеристику поля лишків.

Твердження випадку в) справедливе, навіть коли поле k є довільним загальним локальним полем. Це доводиться за допомогою очевидної незначної модифікації міркувань лем 4 і 5 роботи [3], які справедливі і у випадку, коли характеристика поля лишків поля k дорівнює 3.

Крива типу (*b*) за Нероном над k — це крива з рівнянням

$$y^2 = x^3 + \varepsilon x^2 + a_4 x + \delta\pi^n, \quad \varepsilon, \delta \in U_k, \quad a_4 = \delta_1 \pi^s, \quad s > \frac{n}{2}, \quad \delta_1 \in U_k.$$

Якщо $\sqrt{\varepsilon} \in k$, остання крива є кривою з мультиплікативною редукцією (типу (II) в термінології роботи [3]). Всі міркування, за допомогою яких у роботі [3] доведено невиродженість зліва добутку Тейта—Шафаревича для кривих з мультиплікативною редукцією визначених над довільним загальним локальним полем k у припущенні, що char $\varkappa > 3$ справедливі після очевидної модифікації у випадку, коли char $\varkappa = 3$. Якщо $\sqrt{\varepsilon} \notin k$, то крива типу (*b*) ізоморфна кривій з мультиплікативною редукцією над полем $l = k(\sqrt{\varepsilon})$. Незначна модифікація міркувань леми 4 з [4] завершує доведення п. г) леми 1.

Незважаючи на те, що доведення леми 2 теж є модифікацією на випадок char $\varkappa = 3$ ситуації леми 3 роботи [5], наведемо його повністю. Справа в тому, що у цьому випадку явне обчислення добутку Тейта—Шафаревича особливо просте і дає хорошу ілюстрацію прийому, за допомогою якого з невиродженості добутку Тейта—Шафаревича в еліптичних кривих над локальними полями одержується невиродженість цього добутку в еліптичних кривих над псевдолокальними полями.

Лема 2. *Якщо A — крива типу* (*a*) *за Нероном з інваріантом Гассе редукції, відмінним від нуля, і l/k — дико розгалужене розширення Галуа степеня* 3, *то добуток Тейта — Шафаревича*

$$H^1(\mathfrak{g}, A_l) \times H^0(\mathfrak{g}, A_l) \to \mathbb{Q}/\mathbb{Z} \qquad (T_l)$$

невироджений зліва.

Доведення. Оскільки інваріант Гассе редукції кривої A не дорівнює нулю, то у рівнянні (2) кривої A $\bar{a}_2 \neq 0$.

Припустимо, що нетривіальна точка $(e, 0)$ другого порядку кривої A належить до A_k. Якщо нетривіальний клас групи $H^1(\mathfrak{g}, A_l)$ представлений коциклом $f(\sigma) = \gamma \in \Gamma_l$ (тут і далі σ означає твірний елемент групи

$\mathfrak{g} = \mathrm{Gal}(l/k)$), то γ визначає нетривіальний клас у $\Gamma_l^m/\Gamma_l^{m+1}$, інакше кажучи, γ визначається параметром $\mu\Pi^m$, $\mu \in U_l$, m — номер останньої нетривіальної групи галуження розширення l/k. Виберемо γ так, щоб $\gamma \notin \Gamma_k$, додавши до γ (якщо $\gamma \in \Gamma_k$) елемент з $(\sigma - 1)\Gamma_l$, який не лежить у Γ_k.

Розглянемо функцію на кривій A з дивізором $\gamma + \sigma\gamma + \sigma^2\gamma - 3\infty$. Вона має вигляд $y - \alpha_1 x - \alpha_0$, де α_0 і α_1 — розв'язки системи рівнянь

$$T^{-2}\alpha_1 + \alpha_0 = T^{-3}\varepsilon(T), \qquad (\sigma T)^{-2}\alpha_1 + \alpha_0(\sigma T)^{-3}\varepsilon(\sigma T). \tag{3}$$

Система (3) є системою Крамера ($\gamma \notin \Gamma_k$) і тому має єдиний розв'язок ($N_{l/k}$ — норменний гомоморфізм розширення l/k) $\alpha_0 = -N_{l/k}(T)^{-1}(1 + \ldots)$, $\alpha_1 \in \pi\mathfrak{O}_k$.

Неважко показати, що добуток за Тейтом — Шафаревичом класу з представником $f(\sigma) = \gamma$ і довільного класу з $H^0(\mathfrak{g}, A_l)$, представником якого є точка з Γ_k, дорівнює 0. Знайдемо цілу точку $(\xi, \eta) \in A_k \setminus \Gamma_k$ таку, щоб добуток за Тейтом — Шафаревичом класу $f(\sigma)$ і класу з $H^0(\mathfrak{g}, A_l)$, представником якого є різниця $(\xi, \eta) \dot{-} (e, 0)$ ($\dot{+}$ — додавання, а $\dot{-}$ — віднімання точок у розумінні закону додавання на кривій A), був відмінний від нуля, тобто щоб елемент

$$\frac{(y - \alpha_1 x - \alpha_0)((\xi, \eta) \dot{-} (e, 0) \dot{+} (e, 0))}{(y - \alpha_1 x - \alpha_0)((e, 0))} = 1 - \alpha_0^{-1}\eta + \ldots =$$

$$= 1 + N_{l/k}(T)\eta + \ldots \tag{4}$$

не належав до $N_{l/k}(U_l)$.

Для цього зауважимо, що $T = \mu\Pi^m$ задовольняє співвідношення $\mathrm{Tr}_{l/k}(\mu\Pi^m) + a_2 N_{l/k}(\mu\Pi^m) \equiv 0 \pmod{\pi^{m+1}}$ (тут $\mathrm{Tr}_{l/k}$ і $N_{l/k}$ — слід і норма розширення l/k), отже, $N_{l/k}(\mu\Pi^m) \equiv -a_2^{-1}\mathrm{Tr}_{l/k}(\mu\Pi^m) \pmod{\pi^{m+1}}$. Таким чином, праву частину (4) можна записати у вигляді

$$1 - a_2^{-1}\mathrm{Tr}(\mu\Pi^m) + \ldots . \tag{5}$$

З іншого боку, для $d \in \mathfrak{O}_k$ маємо

$$N_{l/k}(1 + d\mu\Pi^m) = 1 + d\,\mathrm{Tr}_{l/k}(\mu\Pi^m) + d^3 N_{l/k}(\mu\Pi^m) + \ldots$$

$$\ldots = 1 + (d - a_2^{-1}d^3)\,\mathrm{Tr}(\mu\Pi^m) + \ldots . \tag{6}$$

Порівнюючи (5) і (6), одержуємо: для того, щоб добуток за Тейтом — Шафаревичом класів з представниками $f(\sigma) = \gamma$ і $a_k \in A_k \setminus \Gamma_k$ був відмінний від нуля, повинна існувати точка $(\xi, \eta) \in A_k \setminus \Gamma_k$ така, що $\overline{\eta} \neq \overline{d}^3 - \overline{a}_2 d_2$ для всех $\overline{d} \in \varkappa$ ($\overline{a} = a \bmod \pi$). Таким чином, твердження про невиродженість зліва добутку Тейта — Шафаревича в даній ситуації формулюється в термінах елементарних висловлень про поле лишків і, оскільки за невиродженістю добутку Тейта — Шафаревича в еліптичних кривих над локальними полями це висловлення справедливе для скінченних полів, за результатами роботи [6] воно справедливе і для псевдоскінченних полів. Звідси і випливає невиродженість добутку (T_l) у даній ситуації.

У випадку, коли представник нетривіального класу групи $H^1(\mathfrak{g}, A_l)$ має своїм представником коцикл $f(\sigma) = a_l \in A_l \setminus \Gamma_l$, коефіцієнти α_0 і α_1 функції φ належать до $\mathfrak{O}_k$, тому що вони задовольняють рівність

$$y^2 - (\alpha_1 x + \alpha_0)^2 = \prod_{i=0}^{2}(x - \sigma^i(\text{абсц. } a_l)).$$

Виберемо точку $(\xi, \eta) \in A_k \setminus \Gamma_k$ так, щоб $(\overline{\xi}, \overline{\eta}) \neq \overline{a}_l$ (або $-\overline{a}_l$) і щоб елемент $\overline{\xi}$ не був розв'язком рівняння

$$4(x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6)\,\overline{\alpha}_1^2 = (2\overline{a}_2 x + \overline{a}_4)^2.$$

Нехай $(\xi+\Delta\xi,\ \eta+\Delta\eta)=(\xi,\eta)\dot{+}\gamma_k$ — сума точок (ξ,η) і $\gamma_k\in\Gamma_k$, де γ_k визначений значенням t параметра з $v_k(t)=m$ (v_k — нормування поля k). Добуток класів з $H^1(\mathfrak{g}, A_l)$ і $H^0(\mathfrak{g}, A_l)$ з представниками $f(\sigma)$ і γ_k є класом $H^0(\mathfrak{g}, l^*)$ з представником

$$\frac{\eta+\Delta\eta-\alpha_1(\xi+\Delta\xi)-\alpha_0}{\eta-\alpha_1\xi-\alpha_0}=1+(\eta-\alpha_1\xi-\alpha_0)^{-1}(2a_2\xi+a_4+2\alpha_1\eta)t+\ldots, \tag{7}$$

Клас з представником (7) відмінний від нуля для тих значень параметру t, для яких вираз (7) не є нормою. Такі значення t існують згідно з [4].

Якщо нетривіальна точка $(e, 0)$ другого порядку кривої A не належить до A_k, то потрібно розглянути скінченне нерозгалужене розширення $\tilde{k}$ поля k таке, що $A_{\tilde{k}}$ містить нетривіальну точку другого порядку. Доведення у цьому випадку завершується застосуванням діаграми (r_3) так, як це вказано в [3]. Лема 2 доведена.

Доведення твердження 1 випливає з лем 1 і 2 та факту розв'язності груп Галуа загальних локальних полів за допомогою редукційно діаграми (r_3).

Твердження 2. *Добуток Тейта—Шафаревича невироджений зліва для еліптичних кривих типу (c) за Нероном, визначених над псевдолокальним полем k з полем лишків характеристики 3.*

Для доведення твердження 2 нам потрібні такі леми.

Лема 3. *Якщо A — еліптична крива типу (c_2), (c_4), (c_5) або (c_7) над полем k, то добуток Тейта—Шафаревича невироджений зліва для кривої A.*

Доведення є нескладною модифікацією міркувань тверджень 2 і 3 (див. §§ 2, 3) роботи [5].

Лема 4. *Якщо добуток Тейта—Шафаревича невироджений зліва для еліптичних кривих типу (c_3) над k, то він невироджений зліва і для еліптичних кривих типів (c_1), (c_6) і (c_3) над k.*

Доведення. Кожна крива типу (c_1), (c_6) або (c_8) ізоморфна кривій типу (c_3) над слабо розгалуженим розширенням Галуа l поля k, причому $[l:k]=2^s$, $s\leqslant 5$. Легко переконатися в тому, що $H^i(\mathrm{Gal}(l/k), A_l)=0$. Тому справедливість леми 4 випливає з діаграми (r_2).

Лема 5. *Якщо добуток Тейта — Шафаревича невироджений зліва для еліптичних кривих типу (c_3), рівняння Вейєрштрасса $y^2=x^3+a_2x^2+ a_4x+a_6$, $a_i\in\mathfrak{O}_k$, яких задовольняють умови*

$$a_6,\ \Delta\in k^2,\quad v_k(\Delta)>12,\quad v_k(a_2)\geqslant 6,\quad 4\mid v_k(\Delta) \tag{8}$$

(тут $\Delta=-(4a_4^3+27a_6^2+4a_2^3a_6-18a_2a_4a_6-a_2^2a_4^2)$ — дискримінант кривої A, v_k — нормування поля k), то він невироджений і для всіх кривих типу (c_3) за Нероном над k.

Доведення. Нехай A — довільна еліптична крива типу (c_3) над k;

$$A: y^2=x^3+a_2x^2+a_4x+\delta\pi^2,\quad v_k(a_2)\geqslant 1,\quad v_k(a_4)\geqslant 2,\quad \delta\in U_k.$$

Нехай $\Delta=\delta_1\pi^n$, $\delta_1\in U_k$, $n\in\mathbb{N}$, ζ — первісний корінь 16-го степеня з одиниці. Розглянемо башту полів

$$k — \tilde{k}=k(\zeta, \sqrt{\delta_1}, \sqrt{\delta}) — l=\tilde{k}(\sqrt[16]{\pi}).$$

Над полем l крива A ізоморфна кривій C типу (c_3) з рівнянням

$$v^2=u^3+a_2'u^2+a_4'u+a_6',\quad a_{2i}'(\sqrt{\pi})^{10i}=a_{2i},\quad i=1, 2, 3,$$

причому коефіцієнти кривої C над полем l та її дискримінант задовольняють умови (8). Тому за нашим припущенням добуток Тейта—Шафаревича невироджений зліва для кривої C над полем l. Далі

$$H^i(\mathrm{Gal}(l/\tilde{k}), A_l)\cong H^i(\mathrm{Gal}(l/\tilde{k}), C_l),\quad H^i(\mathrm{Gal}(l/\tilde{k}), C_l)\cong H^i(\mathrm{Gal}(l/\tilde{k}), C_l^0),$$

оскільки $\pi_0(C_l) \cong \mathbb{Z}/3\mathbb{Z}$ (тут C_l^0 — підгрупа точок групи C_l, що редукуються в неособливі, $\pi_0(C_l) = C_l/C_l^0$). $H^i(\mathrm{Gal}(l/\tilde{k}), C_l^0) = 0$ тому, що всі фактори фільтрації $C_l^0 \supset \Gamma_l \supset \Gamma_l^2 \supset \ldots$ ізоморфні λ-адитивній групі поля лишків поля l. Отже, $H^i(\mathrm{Gal}(l/\tilde{k}), A_l) = 0$, і діаграма (r_2), записана для розширення $l/\tilde{k}$, показує, що добуток Тейта — Шафаревича невироджений зліва для кривої A над полем $\tilde{k}$. Аналогічні міркування показують, що цей добуток невироджений зліва для кривої A і над полем k.

Лема 6. *Нехай еліптична крива A типу (c_3) над k задовольняє умови леми 5 і l — поле розкладу многочлена $x^3 + a_2x^2 + a_4x + a_6$. Над полем l крива A ізоморфна кривій B з невиродженою редукцією: $A \overset{\alpha}{\simeq} B$. Якщо B_l і $\Gamma(B_l)$ — відповідно група l-раціональних точок кривої B та ядро редукції групи B_l, то позначимо через B_l^α та $\Gamma(B_l^\alpha)$ $\mathfrak{g}$-модулі з наведеною за допомогою ізоморфізму α дією групи $\mathfrak{g} = \mathrm{Gal}(l/k)$. Тоді $H^i(\mathfrak{g}, A_l) \cong$ $\cong H^i(\mathfrak{g}, \Gamma(B_l^\alpha))$.*

Доведення. Многочлен $x^3 + a_2x^2 + a_4x + a_6$ незвідний над k і поле розкладу l цього многочлена є простим циклічним розширенням Галуа поля k, $[l:k] = 3$. Якщо $\tilde{\Pi}$ — корінь многочлена $x^3 + a_2x^2 + a_4x + a_6$, то $v_l(\tilde{\Pi}) = 2$. Зафіксуємо прості елементи π і Π полів k і l так, наприклад, щоб $\pi^2 = a_6$ і $\Pi = \pi^{-1}\tilde{\Pi}^2$.

Нехай m — номер останньої нетривіальної групи галуження розширення l/k, σ — твірна групи $\mathfrak{g}$. Тоді

$$\sigma\Pi = \Pi + \mu\Pi^{m+1}, \quad \sigma\tilde{\Pi} = \tilde{\Pi} + 2\mu\Pi^{m+2} + \ldots, \quad \sigma^2\tilde{\Pi} = \tilde{\Pi} + 4\mu\Pi^{m+2} + \ldots, \quad \mu \in U_l,$$

і легко підрахувати, що $v_k(\Delta) = 2(m+2)$.

Над полем l рівняння кривої A можна записати у вигляді

$$y^2 = (x - \tilde{\Pi})(x - \tilde{\Pi} - 2\mu\Pi^{m+2} + \ldots)(x - \tilde{\Pi} - 4\mu\Pi^{m+2} + \ldots),$$

де $m+2$ парне, тому що $4 \mid v_k(\Delta)$. Розглянемо ізоморфізм α над полем l кривої A і кривої B з рівнянням

$$v^2 = u(u - 2\mu + \ldots)(u - 4\mu + \ldots)$$

такий, що

$$\alpha(x, y) = \left(\frac{x - \tilde{\Pi}}{\Pi^{m+2}}, \ \frac{y}{\Pi^{\frac{3(m+2)}{2}}} \right) = (u, v).$$

Крива B є кривою з невиродженою редукцією над полем l. Запишемо для кривої B точну послідовність редукції

$$0 \to \Gamma(B_l^\alpha) \to B_l^\alpha \to B_\varkappa'^\alpha \to 0. \qquad (9)$$

У цій послідовності $\Gamma(B_l^\alpha)$, B_l^α, $B_\varkappa'^\alpha$ — $\mathfrak{g}$-модулі з наведеною за допомогою ізоморфізму α дією групи $\mathfrak{g}$: для $\sigma \in \mathfrak{g}$

$$\sigma_\alpha(u, v) = \left(\left(\sigma(u) + \frac{\sigma\tilde{\Pi} - \tilde{\Pi}}{\sigma\Pi^{m+2}} \right) \left(\frac{\sigma\Pi}{\Pi} \right)^{m+2}, \quad \sigma(v) \left(\frac{\sigma\Pi}{\Pi} \right)^{\frac{3(m+2)}{2}} \right).$$

Дослідимо групи $H^i(\mathfrak{g}, B_l^\alpha) \cong H^i(\mathfrak{g}, A_l)$. Для цього обчислимо групи $H^i(\mathfrak{g}, B_\varkappa'^\alpha)$. Якщо $(u, v) \in B_\varkappa'$, то $\sigma_\alpha(\bar{u}, \bar{v}) = (\bar{u} + 2\bar{\mu}, \bar{v})$ і неважко показати, що $H^i(\mathfrak{g}, B_\varkappa'^\alpha) = 0$. Звідси і з точної послідовності когомологій, відповідної точній послідовності (9), випливає $H^i(\mathfrak{g}, A_l) \cong H^i(\mathfrak{g}, \Gamma(B_l^\alpha))$. Лема доведена.

Нехай $\Gamma(B_l) \supset \Gamma^2(B_l) \supset \ldots$ — стандартна фільтрація Лютц групи $\Gamma(B_l)$. Позначивши $\alpha^{-1}(\Gamma^i(B_l))$ через $\Gamma^i(A_l)$, маємо $H^i(\mathfrak{g}, A_l) \cong$ $\cong H^i(\mathfrak{g}, \Gamma(A_l))$.

Лема 7. *Якщо у позначеннях леми 6 група $H^1(\mathfrak{g}, A_l)$ має нетривіальний елемент, представлений коциклом $f(\sigma) = \gamma \in A_l$, для якого $\gamma \notin \Gamma^{\frac{m+2}{2}+1}(A_l)$, то існує точка $\gamma_k \in \Gamma_k$ така, що добуток за Тейтом — Шафаревичом класів з представниками γ і γ_k відмінний від нуля.*

Доведення. Якщо $\gamma \notin \Gamma^{\frac{m+2}{2}+1}(A_l)$, то $\gamma = (d, e)$ — ціла точка кривої A. Нехай $y - \alpha_1 x - \alpha_0$ — функція на A з дивізором $\gamma + \sigma\gamma + \sigma^2\gamma - 3\infty$. α_0 і α_1 задовольняють систему рівнянь

$$\begin{cases} a_2 + \operatorname{Tr} d = \alpha_1^2, \\ a_4 + \operatorname{Tr}(d\sigma d) = 2\alpha_0\alpha_1, \\ a_6 + N(d) = \alpha_0^2 \end{cases}$$

(Tr і N — слід і норма розширення l/k), тому $\alpha_0, \alpha_1 \in \mathfrak{O}_k$. Виберемо точку $(\xi, \eta) \in A_k^0 \setminus \Gamma_k$ так, щоб $v_k(3\xi^2 + 2a_2\xi + a_4 - 2\alpha_1\eta) = s < m$ і $(\bar{\xi}, \bar{\eta}) \neq (\bar{d}, \bar{e})$. Такий вибір точки (ξ, η) завжди можливий. Справді, якщо $s = \min\{v_k(3), v_k(a_2), v_k(a_4), v_k(\alpha_1)\}$, то $s < m$, тому що в іншому випадку $\min\{v_k(3), v_k(a_2), v_k(a_4)\} \geqslant m$ і $2(m+2) = v_k(\Delta) \geqslant 3m \Rightarrow m \leqslant 4$, що неможливо, оскільки $2(m+2) > 12$. Виберемо $(\bar{\xi}, \bar{\eta}) \in A'_\varkappa$ так, щоб $(\bar{\xi}, \bar{\eta})$ не задовольняла рівняння

$$((3 \bmod \pi^s)\,\bar{\xi}^2 + (2a_2 \bmod \pi^s)\,\bar{\xi} + a_4 \bmod \pi^s)^2 - 4(\alpha_1 \bmod \pi^s)^2\,\bar{\eta}^2 = 0 \quad (10)$$

і щоб $\bar{\xi} \neq \bar{e}$. Піднімемо $(\bar{\xi}, \bar{\eta})$ до точки $(\xi, \eta) \in A_k^0 \setminus \Gamma_k$, яка задовольняє всі потрібні умови.

Розглянемо добуток за Тейтом—Шафаревичом класу $H^1(\mathfrak{g}, A_l)$ з представником $f(\sigma) = \gamma$ і класу $H^0(\mathfrak{g}, A_l)$, представником якого є точка $\gamma_k = (t^{-2}, \varepsilon(t)\,t^{-3})$. Позначивши через $(\xi + \Delta\xi, \eta + \Delta\eta)$ суму тільки що вибраної точки (ξ, η) і точки γ_k, одержимо, що цей добуток є класом групи $H^0(\mathfrak{g}, l^*)$ з представником

$$\frac{(y - \alpha_1 x - \alpha_0)\,((\xi + \Delta\xi, \eta + \Delta\eta)}{\eta - \alpha_1\xi - \alpha_0} = 1 + (\eta - \alpha_1\xi - \alpha_0)^{-1} \times$$
$$\times (3\xi^2 + 2a_2\xi + a_4 - 2\alpha_1\eta)\,t + \ldots . \quad (11)$$

Підібравши тепер значення параметру t так, щоб $v_k(t) = m - s$ і щоб останній вираз (11) не був нормою, що завжди можливо [4], одержуємо, що добуток розглянутих класів відмінний від нуля.

Залишилося дослідити випадок, коли представники класів групи $H^1(\mathfrak{g}, A_l)$ мають вигляд $f(\sigma) = \gamma \in \Gamma^{\frac{m+2}{2}+1}(A_l)$. Це дослідження ми проводимо в останніх двох лемах. Далі позначаємо $\Gamma^{\frac{m+2}{2}+n}(A_l)$ через Γ_l^n.

Якщо коцикл $f(\sigma) = \gamma \in \Gamma_l^n$ представляє клас групи $H^1(\mathfrak{g}, A_l)$, то $\gamma = (T^{-2}, \varepsilon(T)\,T^{-3})$, $T = \rho\Pi^n$, $\rho \in U_l$. Нехай $y - \alpha_1 x - \alpha_0$ — функція на A з дивізором $\gamma + \sigma\gamma + \sigma^2\gamma - 3\infty$. Легко бачити, що α_0 і α_1 задовольняють систему рівнянь

$$\begin{cases} (a_6 - \alpha_0^2)\,N(T)^2 + 1 = 0, \\ (a_4 - 2\alpha_0\alpha_1)\,N(T)^2 = \operatorname{Tr}(T^2) \\ (a_2 - \alpha_1^2)\,N(T)^2 = \operatorname{Tr}(T^2\sigma T^2) \end{cases}$$

(N і Tr — норма і слід в l/k), і, таким чином, $\alpha_0 N(T) \in U_k$, $\alpha_1 \in \pi\mathfrak{O}_k$.

Лема 8. *Якщо коцикл $f(\sigma) = \gamma \in \Gamma_l^n$ і $n < m - \min\{v_k(3), v_k(a_2), v_k(a_4), v_k(\alpha_1)\}$, то існує точка $\gamma_k \in \Gamma_k$ така, що добуток за Тейтом — Шафаревичом класу коциклу $f(\sigma)$ і класу точки γ_k відмінний від нуля.*

Доведення. Візьмемо точку $(\xi, \eta) \in A_k^0 \setminus \Gamma_k$ так, щоб $(\bar{\xi}, \bar{\eta})$ не задовольняла (10). Добутком за Тейтом — Шафаревичом класів з представниками $f(\sigma)$ і $\gamma_k = (t^{-2}, \varepsilon(t)\,t^{-3}) \in \Gamma_k$ є клас групи $H^0(\mathfrak{g}, l^*)$ з представником

$$\frac{(y-\alpha_1 x-\alpha_0)((\xi,\eta)\dot{+}\gamma_k)}{\eta-\alpha_1\xi-\alpha_0}=1+(\alpha_0 N(T)+\alpha_1\xi N(T)-\eta N(T))^{-1}\times$$

$$\times(3\xi^2+2a_2\xi+a_4-2\alpha_1\eta)\,tN(T)+\ldots,$$

який не є нормою для відповідного значення параметра t з $v_k(t)=m-n-\min\{v_k(3), v_k(a_2), v_k(a_4), v_k(\alpha_1)\}$. Тому добуток розглянутих класів відмінний від нуля.

Лема 9. *Якщо у позначеннях леми 6 клас групи* $H^1(\mathfrak{g}, A_l)$ *має своїм представником коцикл* $f(\sigma)=\gamma=(T^{-2}, \varepsilon(T)T^{-3})$, *причому* $v_l(T)\geqslant m-\min\{v_k(3), v_k(a_2), v_k(a_4), v_k(\alpha_1)\}$, *то цей клас тривіальний.*

Доведення. Обчислимо спочатку $(\sigma_\alpha-1)\Gamma(B_l^\alpha)$. Якщо $\gamma'\in\Gamma^s(B_l)$, γ' визначене параметром $T'=d\Pi^s$, то параметром $\sigma_\alpha\gamma'\dot{-}\gamma'\in ds\mu\Pi^{m+s}+\ldots$. Звідси випливає, що елементи з $(\sigma-1)\Gamma(A_l)$ цілком заповнюють фактори $\Gamma_l^n/\Gamma_l^{n+1}$ для $n\geqslant m/2$, $n\not\equiv m \pmod 3$.

Вияснимо тепер, використовуючи методи роботи [7], які елементи $\gamma\in\Gamma_l$ можуть лежати в ядрі норменного гомоморфізму $N:\Gamma_l\to\Gamma_k$. Для цього за допомогою безпосереднього обчислення переконуємося, що третя ітерація формальної групи, відповідної кривій A, має вигляд

$$9(t+\ldots)+4a_2t^3+(a_4^2-4a_2a_6)t^9+\ldots \tag{12}$$

(три крапки означають члени з вищими степенями t), причому коефіцієнти при степенях t в пропущених в (12) членах в дужках мають норму в k не меншу ніж одиниця, а коефіцієнти при степенях t в інших пропущених членах мають норму в k не меншу ніж $\min\{v_k(3), v_k(a_2), v_k(a_4^2-4a_2a_6)\}+1$.

Використовуючи (12) і міркування роботи [7], маємо

$$N(T)\equiv \mathrm{Tr}\,T+4a_2\,\mathrm{Norm}(T)+(a_4^2-4a_2a_6)\,\mathrm{Norm}(T)^2 \pmod{\mathrm{Tr}\,\Pi^{2n}} \tag{13}$$

(N — норменний гомоморфізм $\mathfrak{g}$-модуля Γ_l; Tr, Norm — слід і норма в l/k). Оскільки $n\geqslant m-\min\{v_k(a_2), v_k(a_4), v_k(3)\}$, то з (13) одержуємо

$$N(T)\equiv \mathrm{Tr}\,T \pmod{\pi^{n+1}}. \tag{14}$$

Нагадаємо, що П-ізоморфізмом $\Gamma_l^n/\Gamma_l^{n+1}\to\lambda$ називається ізоморфізм, який одержується співставленням класу точки з Γ_l^n, що відповідає значенню параметра $d\,\Pi^n$, $d\in\mathfrak{O}_l$, елемента $d \bmod \Pi$ з λ.

Нехай $u=v_l(T)$. Якщо $n\geqslant m/2$, то враховуючи інформацію про $(\sigma-1)\Gamma(A_l)$, одержану на початку доведення леми, бачимо, що досить дослідити випадок, коли $n\equiv m \pmod 3$. У цьому випадку бачимо, враховуючи (14), що при переході до П-ізоморфізмів норменний гомоморфізм $\mathfrak{g}$-модуля Γ_l визначає ізоморфізм $N_n:\lambda\to\lambda$ такий, що $N_n(z)=\alpha z$, $\alpha\neq 0$. Очевидно, $\mathrm{Ker}\,N_n=0$, тому клас коциклу $f(\sigma)$ — тривіальний.

Якщо $n<m/2$, то з наших припущень випливає, що $\min\{v_k(3), v_k(a_2), v_k(a_4)\}>m/2$, $\Rightarrow$, $m\leqslant 4$, що суперечить умовам (8). Лема доведена.

Доведення твердження 2. Леми 6—9 показують, що якщо A — еліптична крива типу (c_3), яка задовольняє умови леми 5, то добуток Тейта—Шафаревича (l/k — розширення з леми 6)

$$H^1(\mathfrak{g}, A_l)\times H^0(\mathfrak{g}, A_l)\to\mathbf{Q}/\mathbb{Z}$$

невироджений зліва, а з діаграми (r_2) випливає справедливість і твердження 2 для таких кривих. Справедливість твердження 2 для довільної кривої типу (c) за Нероном витікає з лем 3—5.

1. *Шафаревич И. Р.* Группа главных однородных алгебраических многообразий // Докл. АН СССР.— 1959.— **124**.— С. 42—43.
2. *Tate J.* *WC*-group over *p*-adic fields // Sem. Bourbaki.— 1967.— N 157.
3. *Введенский О. Н.* О локальных «полях классов» эллиптических кривых // Изв. АН СССР. Сер. мат.— 1973.— **37**, № 1.— С. 20—88.

4. *Serre J.-P.* Corps locaux.— Paris.: Hermann, 1962.
5. *Андрийчук В. И.* Об эллиптических кривых над псевдолокальными полями // Мат. сб.— 1979.— **110**, № 9.— С. 88—101.
6. *Ax J.* The elementary theory of finite fields // Ann. Math.— 1968.— **88**, N 2.— P. 239—271.
7. *Введенский О. Н.* Двойственность в эллиптических кривых над локальным полем. I, II // Изв. АН СССР. Сер. мат.— 1964.— **28**.— С. 1091—1112; 1966.— **30**.— С. 891—922.

Одержано 06.03.92