УДК 513.6

В. І. Нестерук

ПРО НЕВИРОДЖЕНІСТЬ ДОБУТКУ ТЕЙТА ДЛЯ ЕЛІПТИЧНИХ КРИВИХ З НЕВИРОДЖЕНОЮ РЕДУКЦІЄЮ НАД ПСЕВДОЛОКАЛЬНИМ ПОЛЕМ

Доведено невиродженість добутку Тейта для еліптичних кривих з невиродженою редукцією над псевдолокальним полем.

В останні десять років з'ясувалося, що добуток Тейта та інші зв'язані з ним добутки можна застосовувати до проблем, пов'язаних з криптографією. Добуток Тейта ввів в 1957 році Дж. Тейт [10], його вивчали І. Р. Шафаревич [4] і одне з його означень можна знайти у Ф. Гесса [7].

Властивості добутку Тейта досліджували багато відомих математиків, зокрема І. Р. Шафаревич [4], О. М. Введенський [1], Ф. Гесс [7], М. Папікіян [8]. Ф. Гесс [7] навів елементарне доведення його невиродженості для кривих, визначених над скінченним полем, М. Папікіян [8] – для кривих, визначених над локальним полем, О. М. Введенський [1] обчислив добуток Тейта–Шафаревича і довів його невиродженість для еліптичих кривих над локальними полями для простих циклічних розширень. Доведено [3] невиродженість добутку Тейта для кривих над псевдоскінченним полем. Псевдоскінченні поля ввів Дж. Акс [5] у 1968 році. Поле k називають псевдоскінченним [6], якщо k досконале, має єдине розширення степеня n для кожного натурального числа n і кожний непорожній абсолютно незвідний многовид, визначений над полем k, має k-раціональну точку.

Мета цієї праці – довести методом М. Папікіяна [8] невиродженість добутку Тейта для еліптичних кривих, визначених над псевдолокальним полем K, тобто над повним дискретно нормованим полем з псевдоскінченним полем лишків k.

Нехай E – еліптична крива, визначена над псевдолокальним полем K, k – поле лишків K. $\overline{K}$ (відповідно $\overline{k}$) означає сепарабельне замикання поля K (відповідно $\overline{k}$). Далі m – натуральне число таке, що $(m, char(K)) = 1$, μ_m – група коренів степеня m з 1 в $\overline{K}$, $G = Gal\left(\overline{K}/K\right)$ – абсолютна група Галуа поля K, $g_K = Gal\left(K^{un}/K\right)$ – група Галуа максимального нерозгалуженого розширення поля K, $g_k = Gal\left(k^{ab}/k\right)$ – група Галуа абелевого розширення поля k. Позначимо через $E_m(K)$ групу m-кручення, $H^1\left(G, E\left(\overline{K}\right)\right)_m$ – підгрупу елементів в $H^1\left(G, E\left(\overline{K}\right)\right)$, порядок яких ділить m.

Для всіх $0 \le i \le 2$ групи $H^i\left(G, E_m\left(\overline{K}\right)\right)$ скінченні. Існує знакозмінний невироджений добуток $H^i\left(G, E_m\left(\overline{K}\right)\right) \times H^{2-i}\left(G, E_m\left(\overline{K}\right)\right) \to \mathbf{Z}/m\mathbf{Z}$, індукований $\cup$-добутком, добутком Вейля та відображенням інваріанта теорії полів класів загального локального поля [8].

Означення 1. Щойно визначений добуток індукує невироджений добуток

$$E(K)/mE(K) \times H^1\left(G, E\left(\overline{K}\right)\right)_m \to \mathbf{Z}/m\mathbf{Z},$$

який називають *добутком Тейта*.

Означення 2. Під *абелевим многовидом* розуміють алгебричний многовид, що наділений структурою абелевої групи і при цьому групова операція задана морфізмами над K: $A \times A \to A$ $((x, y) \to x + y)$ і $A \to A$ $(x \to -x)$.

ISSN 1810-3022. **Прикл. проблеми мех. і мат.** – 2010. – **Вип.** 8. – **С.** 37–40.

Для групи A (відповідно $\mathcal{A}$), що визначена над полем K (відповідно k), позначимо через $A(K)$ (відповідно $\mathcal{A}(k)$) її групу K-раціональних точок (відповідно k-раціональних точок групи $\mathcal{A}$), $A^1(K)$ – ядро відображення редукції $A(K) \to \mathcal{A}(k)$, $A_m(K)$ (відповідно $\mathcal{A}_m(k)$) – підгрупу елементів в $A(K)$ (відповідно в $\mathcal{A}(k)$), що мають порядок m.

Лема. *Нехай K – повне дискретно нормоване поле з псевдоскінченним полем лишків k, A – абелевий многовид, визначений над полем K, що має добру редукцію $\mathcal{A}$ над k, $\mathbf{l} = chark$ і $(m, \mathbf{l}) = 1$. Тоді*

$$| A(K)/mA(K) | = | A(K)_m | .$$

Доведення. Розглянемо точну послідовність

$$0 \to A^1(K) \to A(K) \to \mathcal{A}(k) \to 0.$$

Застосуємо лему про змію до комутативної діаграми

$$\begin{array}{ccccccc} 0 & \to & A^1(K) & \to & A(K) & \to & \mathcal{A}(k) \to 0 \\ & & \downarrow m & & \downarrow m & & \downarrow m \\ 0 & \to & A^1(K) & \to & A(K) & \to & \mathcal{A}(k) \to 0, \end{array}$$

з якої випливає, що

$$0 \to A(K)/mA(K) \to \mathcal{A}(k)/m\mathcal{A}(k) \to 0 \text{ і } A(K)/mA(K) \cong \mathcal{A}(k)/m\mathcal{A}(k).$$

З послідовності

$$0 \to \mathcal{A}_m(\bar{k}) \to \mathcal{A}(\bar{k}) \xrightarrow{m} \mathcal{A}(\bar{k}) \to 0$$

отримаємо:

$$A(K)/mA(K) \cong \mathcal{A}(k)/m\mathcal{A}(k) \cong H^1(g_k, \mathcal{A}_m(\bar{k})). \qquad (1)$$

Так само з попередньої комутативної діаграми дістанемо:

$$\mathcal{A}_m(k) \cong A_m(K).$$

Використовуючи той факт, що $H^i(g_K, A_m(\bar{K})) \cong H^i(g_k, \mathcal{A}_m(\bar{k}))$, одержуємо при $i = 1$

$$H^1(g_K, A_m(\bar{K})) \cong H^1(g_k, \mathcal{A}_m(\bar{k}))$$

і перепишемо (1) так:

$$A(K)/mA(K) \cong \mathcal{A}(k)/m\mathcal{A}(k) \cong H^1(g_k, \mathcal{A}_m(\bar{k})) \cong H^1(g_K, A_m(\bar{K})).$$

З одного боку,

$$H^1(g_K, A_m(\bar{K})) \cong A(K)/mA(K),$$

з іншого –

$$H^1(g_K, A_m(\bar{K})) \cong H^1(\mathbf{Z}, A_m(\bar{K})) \cong H^0(\mathbf{Z}, A_m(\bar{K})) \cong A_m(K),$$

де $\mathbf{Z}$ — вільна топологічна група з однією твірною. Отже,

$$A(K)/mA(K) \cong A(K)_m \text{ і } | A(K)/mA(K) | = | A(K)_m | .$$

Означення 3. Білінійний добуток $t : A \times B \to C$ абелевих груп A, B, C *невироджений*, якщо відповідні гомоморфізми $A \to Hom(B, C)$ і $B \to Hom(A, C)$ ін'єктивні.

Використовуючи метод, запропонований М. Папікіяном, доведемо невиродженість добутку Тейта для еліптичних кривих над псевдолокальним полем.

Теорема. *Нехай E – еліптична крива з доброю редукцією, що визначена над псевдолокальним полем K. Тоді добуток Тейта*

$$E(K)/mE(K)\times H^1\left(G,E\left(\bar{K}\right)\right)_m \to \mathbf{Z}/m\mathbf{Z}$$

невироджений для кривих, визначених над псевдолокальним полем K.

Доведення. Розглянемо точну послідовність груп

$$0 \to I \to G \to g_K \to 0,$$

де I – підгрупа інерції G [2].
З точної послідовності інфляції-обмеження [9]

$$0 \to H^1\left(g_K, E_m^I\left(\bar{K}\right)\right) \to H^1\left(G, E_m\left(\bar{K}\right)\right) \to H^1\left(I, E_m\left(\bar{K}\right)\right)^{g_K} \to H^2\left(g_K, E_m^I\left(\bar{K}\right)\right).$$

Враховуючи, що $H^2\left(g_K, E_m^I\left(\bar{K}\right)\right) = 0$ (когомологічна розмірність групи g_K дорівнює 1) і $E_m(K)$ інваріантні за дії I, оскільки E має добру редукцію, одержуємо точну послідовність:

$$0 \to H^1\left(g_K, E_m^I\left(\bar{K}\right)\right) \to H^1\left(G, E_m\left(\bar{K}\right)\right) \to H^1\left(I, E_m\left(\bar{K}\right)\right)^{g_K} \to 0. \qquad (2)$$

Порівнюючи точну послідовність

$$0 \to E(K)/mE(K) \to H^1\left(G, E_m\left(\bar{K}\right)\right) \to H^1\left(G, E\left(\bar{K}\right)\right)_m \to 0$$

з (2), отримуємо:

$$H^1\left(I, E_m\left(\bar{K}\right)\right)^{g_K} \cong H^1\left(G, E\left(\bar{K}\right)\right)_m. \qquad (3)$$

Нехай Δ — образ I у слабо розгалуженій частині групи G, тобто

$$0 \to P \to I \to \Delta \to 0,$$

де P — група дикого галуження, $\Delta \cong \prod_{s\neq \mathbf{l}} \mathbf{Z}_s(1)$.
Використовуючи точну послідовність інфляції-обмеження

$$0 \to H^1\left(\Delta, E_m\left(\bar{K}\right)\right) \to H^1\left(I, E_m\left(\bar{K}\right)\right) \to H^1\left(P, E_m\left(\bar{K}\right)\right)^{\Delta} \to 0$$

і враховуючи, що $H^1\left(P, E_m\left(\bar{K}\right)\right) = Hom\left(P, E_m\left(\bar{K}\right)\right) = 0$, одержуємо, що

$$\begin{aligned} &H^1\left(I, E_m\left(\bar{K}\right)\right)^{g_K} = H^1\left(\Delta, E_m\left(\bar{K}\right)\right)^{g_K} = Hom\left(\Delta, E_m\left(\bar{K}\right)\right)^{g_K} \\ &= Hom\left(\prod_{s\neq \mathbf{l}} \mathbf{Z}_s(1), E_m\left(\bar{K}\right)\right)^{g_K} = \prod_{s=m} Hom\left(\mathbf{Z}_s(1), E_m\left(\bar{K}\right)\right)^{g_K} \\ &= Hom\left(\mathbf{Z}_m(1), E_m\left(\bar{K}\right)\right)^{g_K} = Hom\left(\mu_m, E_m\left(\bar{K}\right)\right)^{g_K}. \end{aligned} \qquad (4)$$

З одного боку, згідно з доведенням леми

$$H^1\left(g_K, E_m\left(\bar{K}\right)\right) \cong E_m(K),$$

а з іншого –

$$H^1\left(g_K, E_m\left(\bar{K}\right)\right) \cong E(K)/mE(K).$$

Звідси випливає, що $E(K)/mE(K) \cong E_m(K)$.

Враховуючи (3) і (4), отримуємо, що $E(K)\Big/mE(K) \cong H^1\left(G, E\left(\bar{K}\right)\right)_m$.

За попередньою лемою, якщо m таке, що $(m, chark) = 1$, одержуємо, що $|E(K)/mE(K)| = |E(K)_m|$.

Нехай маємо відображення $f : A \to B$ і $\alpha : B \to ¤/¢$. Тоді відображення f визначає відображення $f : B^D \to A^D$, яке діє за правилом: якщо $\alpha \in B^D$, то $\alpha f \in A^D$ і $0^D = 0$. Застосовуючи це до точної послідовності

$$0 \to E(K)/mE(K) \to \quad H^1\left(G, E_m\left(\bar{K}\right)\right) \to \quad H^1\left(G, E\left(\bar{K}\right)\right)_m \to 0,$$

одержуємо:

$$0 \to \left(H^1\left(G, E\left(\bar{K}\right)\right)_m\right)^D \to \left(H^1\left(G, E_m\left(\bar{K}\right)\right)\right)^D \to \left(E(K)/mE(K)\right)^D \to 0.$$

Розглянемо комутативну діаграму

$$\begin{array}{ccccccc} 0 \to & E(K)/mE(K) & \to & H^1\left(G, E_m\left(\bar{K}\right)\right) & \to & H^1\left(G, E\left(\bar{K}\right)\right)_m & \to 0 \\ & \downarrow f & & \downarrow w & & \downarrow h & \\ 0 \to & \left(H^1\left(G, E\left(\bar{K}\right)\right)_m\right)^D & \to & \left(H^1\left(G, E_m\left(\bar{K}\right)\right)\right)^D & \to & \left(E(K)/mE(K)\right)^D & \to 0, \end{array}$$

де f визначене добутком Тейта, w – добутком Вейля, w – бі'єктивне, тому f і h ін'єктивні. Отже, добуток

$$E(K)/mE(K) \times H^1\left(G, E\left(\bar{K}\right)\right)_m \to \mathbf{Z}/m\mathbf{Z}$$

невироджений.

1. *Введенский О. Н.* О локальных «полях классов» эллиптических кривых // Изв. АН СССР. – 1973. – 37, № 1. – С. 20–88.
2. *Касселс Дж., Фрёлих А.* Алгебраическая теория чисел. – М.: Мир, 1969. – 484 с.
3. *Нестерук В. І.* Про невиродженість добутку Тейта для кривих над псевдо скінченними полями // Вісник Львів. ун-ту. Сер. мех.о-мат. (в друці).
4. *Шафаревич И. Р.* Группа главных однородных алгебраических многообразий // ДАН СССР. – 1959. – 124, № 1. – С. 42–43.
5. *Ax J.* The elementary theory of finite fields // Ann. Math. – 1968. – 88, № 2. – P. 239–271.
6. *Fried M., Jarden M.* Field arithmetic. Springer–Verlag. – New York, Berlin: Heidelberg, 2005. – 818 p.
7. *Hess F.* A Note on the Tate Pairing of Curves over Finite Fields. – Computer Science Department, Woodland Road, University of Bristol, preprint.
8. *Papikian M.* On Tate Local Duality, preprint.
9. *Serre J. P.* Corps locaux. – Paris: Hermann, 1962. – 242 p.
10. *Tate J.* WC – group over p–adic fields // Sem. Bourbaki. – 1956. – 156.

О НЕВЫРОЖДЕНОСТИ СПАРИВАНИЯ ТЭЙТА ДЛЯ ЭЛЛИПТИЧЕСКИХ КРИВЫХ С НЕВЫРОЖДЕННОЙ РЕДУКЦИЕЙ НАД ПСЕВДОЛОКАЛЬНЫМ ПОЛЕМ

Приведено доказательство невырожденности спаривания Тэйта для эллиптических кривых с невырожденной редукцией над псевдолокальным полем.

ON NONDEGENERACY OF TATE PAIRING FOR ELLIPTIC CURVES WITH GOOD REDUCTION OVER PSEUDOLOCAL FIELD

A proof of nondegeneracy of the Tate pairing on elliptic curves with good reduction over pseudolocal field is given.

Львів. нац. ун-т імені Івана Франка, Львів

Одержано 01.09.10