ВІСНИК ЛЬВІВ. УН-ТУ | *VISNYK LVIV UNIV.*
Серія мех.-мат. 2010. | *Ser. Mech. Math. 2010.*
Вип. 72. С. 195–200 | *Is. 72. P. 195–200*

УДК 513.6

ПРО НЕВИРОДЖЕНІСТЬ ДОБУТКУ ТЕЙТА ДЛЯ КРИВИХ НАД ПСЕВДОСКІНЧЕННИМИ ПОЛЯМИ

Володимир НЕСТЕРУК

Львівський національний університет імені Івана Франка,
79000 Львів, вул. Університетська, 1
e-mail: volodymyr-nesteruk@rambler.ru

Доведено невиродженість добутку Тейта для кривих над псевдоскінченними полями.

Ключові слова: добуток Тейта, проективна крива, якобіан кривої, псевдоскінченне поле.

1. Вступ. Дж. Тейт [9] та І. Р. Шафаревич [4] визначили добуток

$$\mathrm{H}^0(G, A) \times \mathrm{H}^1(G, \widehat{A}) \to \mathrm{Br}K,$$

де A – абелевий многовид над полем K; $\widehat{A}$ – двоїстий многовид; $\overline{K}$ – сепарабельне замикання поля K; $G = \mathrm{Gal}(\overline{K}/K)$ – абсолютна група Галуа поля K; $\mathrm{H}^0(G, A)$ і $\mathrm{H}^1(G, \widehat{A})$ – когомології Галуа; $\mathrm{Br}K$ – група Брауера поля K, і довели його невиродженість для випадку локального поля K.

Відтоді дослідженням властивостей добутку Тейта займалися багато відомих математиків, зокрема О. М. Введенський, Ф. Гесс, М. Папікіян. О. М. Введенський в [2] явно обчислив цей добуток в еліптичних кривих над локальними полями для простих циклічних розширень. Ф. Гесс у [7] навів елементарне доведення невиродженості добутку для випадку кривих, визначених над скінченним полем. Зокрема, М. Папікіян подав у [8] елементарне доведення невиродженості добутку для випадку кривих, визначених над повним дискретно нормованим полем зі скінченним полем лишків.

Мета нашої праці – дослідити невиродженості добутку Тейта для кривих над псевдоскінченними полями.

Псевдоскінченні поля ввів Дж. Акс у 1968 р. у праці [5]. Поле k називають *псевдоскінченним* [6], якщо k досконале, k має єдине розширення степеня n для кожного натурального числа n і кожний непорожній абсолютно незвідний многовид, визначений над полем k, має k-раціональну точку. Прикладами псевдоскінченних полів є неголовні ультрадобутки скінченних полів і нескінченні алгебричні розширення скінченних полів, які мають скінченний p-примарний степінь для кожного простого числа p.

Добуток Тейта є білінійним відображенням. Одне з означень цього добутку можна знайти у Ф. Гесса в [7], де наведено елементарне доведення невиродженості добутку Тейта між групою m-кручення якобіана $\mathrm{J}(C_K)$ кривої C та m-групою Морделла – Вейля $\mathrm{J}(C_K)/m\mathrm{J}(C_K)$ для випадку кривих, визначених над скінченним полем K, яке містить корені степеня m з 1, $(m, char(K)) = 1$.

Використовуючи метод, запропонований Ф. Гессом, ми доведемо невиродженість добутку Тейта для кривих над псевдоскінченними полями.

2. Криві над псевдоскінченними полями. Нехай C – абсолютно незвідна, неособлива проективна крива, визначена над псевдоскінченним полем k, K – алгебричне розширення поля k, $K(C)$ – поле функцій на кривій C. $\overline{k}$ (відповідно $\overline{K}$) означає сепарабельне замикання поля k (відповідно K). Далі m означає натуральне число таке, що $(m, char(k)) = 1$. Позначимо через $\mathrm{J}(C_K)$ якобіан кривої C, $\mathrm{J}(C_K)_m$ – підгрупу точок в $\mathrm{J}(C_K)$, порядок яких ділить m. Для класів дивізорів $x \in \mathrm{J}(C_K)_m$ та $y \in \mathrm{J}(C_K)/m\mathrm{J}(C_K)$ існують взаємно прості дивізори D і R такі, що $x = [D]$ і $y = [R] + m\mathrm{J}(C_K)$. Нехай $f \in K(C)$ функція з дивізором $(f) = mD$.

Означення 1. *Білінійне відображення*

$$t_m \colon \mathrm{J}(C_K)_m \times \mathrm{J}(C_K)/m\mathrm{J}(C_K) \longrightarrow K^*/K^{*m},$$

для якого $t_m(x, y) = f(R)$ *називають добутком Тейта.*

Для доведення невиродженості добутку Тейта для кривих, визначених над псевдоскінченними полями, нам будуть потрібні декілька лем про псевдоскінченні поля та абелеві многовиди над ними, одна загальна лема про білінійні добутки скінченних абелевих груп та аналог теореми щільності Чеботарьова.

Лема 1. *Нехай* k *– псевдоскінченне поле. Припустимо, що група* μ_m *коренів степеня* m *з 1 міститься в* k*. Тоді* $k^*/k^{*m} \cong \mathbb{Z}/m\mathbb{Z}$.

Доведення. З точної послідовності

$$0 \to \mu_m(\overline{k}) \to \overline{k}^* \stackrel{m}{\to} \overline{k}^* \to 0$$

отримуємо точну послідовність груп когомологій

$$0 \to \mu_m(k) \to k^* \stackrel{m}{\to} k^* \to \mathrm{H}^1(k, \mu_m(\overline{k})) \to \mathrm{H}^1(k, \overline{k}^*).$$

За теоремою Гільберта 90 $\mathrm{H}^1(k, \overline{k}^*) = 0$, тому маємо точну послідовність

$$0 \to \mu_m(k) \to k^* \stackrel{m}{\to} k^* \to \mathrm{H}^1(k, \mu_m(\overline{k})) \to 0.$$

Враховуючи, що абсолютна група Галуа поля k ізоморфна $\widehat{\mathbb{Z}}$, $\widehat{\mathbb{Z}}$ – вільна топологічна група з однією твірною і $\mu_m(\overline{k}) = \mathbb{Z}/m\mathbb{Z}$, одержуємо, що

$$k^*/k^{*m} \cong \mathrm{H}^1(k, \mu_m(\overline{k})) \cong \mathrm{Hom}(\widehat{\mathbb{Z}}, \mu_m(\overline{k})) \cong \mathrm{Hom}(\widehat{\mathbb{Z}}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

□

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

Лема 2. *Нехай A – абелевий многовид, визначений над псевдоскінченним полем k. Тоді* $\mathrm{H}^1(k, A(\overline{k})) = 0$.

Елементи групи $\mathrm{H}^1(k, A(\overline{k}))$ інтерпретують як головні однорідні простори для многовиду A. Оскільки псевдоскінченне поле k є псевдоалгебрично замкненим, то кожний многовид визначений над k має k-раціональну точку і звідси випливає, що група головних однорідних просторів тривіальна.

Лема 3. *Нехай A – абелевий многовид над псевдоскінченним полем k. Тоді групи $A(k)/mA(k)$ та $A(k)_m$ скінченні і мають однаковий порядок.*

Доведення. З точної послідовності

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

отримуємо точну послідовність груп когомологій

$$0 \to A(k) \xrightarrow{m} A(k) \to \mathrm{H}^1(k, A(\overline{k})_m) \to \mathrm{H}^1(k, A(\overline{k})).$$

Враховуючи, що $\mathrm{H}^1(k, A(\overline{k})) = 0$ за попередньою лемою 2 і $\mathrm{H}^1(k, A(\overline{k})_m) \cong$ $\cong \mathrm{H}^1(\widehat{\mathbb{Z}}, A(\overline{k})_m) \cong A(k)_m$, одержуємо $A(k)/mA(k) \cong A(k)_m$. □

Означення 3. *Білінійний добуток $t\colon A \times B \to Z$ абелевих груп A, B і Z невироджений, якщо відповідні гомоморфізми $A \to \mathrm{Hom}\,(B, Z)$ і $B \to \mathrm{Hom}\,(A, Z)$ ін'єктивні.*

Лема 4. *Нехай A, B – скінченні абелеві групи з показником m і $|A| = |B|$. Білінійний добуток $t\colon A \times B \to \mathbb{Z}/m\mathbb{Z}$ невироджений тоді і тільки тоді, коли відповідний гомоморфізм $A \to \mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z})$ ін'єктивний.*

Доведення можна знайти у [7]. Для зручності читача нагадуємо доведення леми.

Доведення. Добуток t невироджений за означенням, якщо відповідні гомоморфізми $A \to \mathrm{Hom}\,(B, \mathbb{Z}/m\mathbb{Z})$ і $B \to \mathrm{Hom}\,(A, \mathbb{Z}/m\mathbb{Z})$ ін'єктивні.

Якщо $A \xrightarrow{t} \mathrm{Hom}\,(B, \mathbb{Z}/m\mathbb{Z})$ ін'єктивне, то воно також сюр'єктивне, оскільки $|A| = |B| = |\mathrm{Hom}\,(B, \mathbb{Z}/m\mathbb{Z})|$. Нехай $b \in B$ і $c \in \mathbb{Z}/m\mathbb{Z}$ елементи однакового порядку d, а $h \in \mathrm{Hom}\,(B, \mathbb{Z}/m\mathbb{Z})$ такий, що $h(b) = c$. Із сюр'єктивності t випливає існування елемента $a \in A$, що $h = t(a, \,\cdot\,)$ і $t(a, b) = c$. Це означає, що $t(\,\cdot\,, b)$ має як мінімум порядок d і, отже, гомоморфізм $B \to \mathrm{Hom}\,(A, \mathbb{Z}/m\mathbb{Z})$ ін'єктивний. □

Введемо такі позначення. Нехай $L/K(C)$ – скінченне розширення Галуа поля $K(C)$ з групою Галуа $\mathfrak{g}$, $\tau \in \mathfrak{g}$ і n – натуральне число.

Означення 4. *Групою розвинення точки P поля L у полі L називають підгрупу $\mathfrak{g}_P$ групи $\mathfrak{g}$, яка складається з тих елементів σ групи $\mathfrak{g}$, для яких $\sigma P = P$.*

Розглянемо множину $M(L)$ всіх точок поля L та її підмножини $D_n(L, \tau) =$ $= \{P \in M(L) |\ \mathfrak{g}_P$ ізоморфні циклічній групі, породженій елементом τ, $deg(P) = n\}$ Для кожного τ знайдеться n таке, що множина $D_n(L, \tau)$ буде нескінченною [1].

Теорема 1. *(Аналог теореми щільності Чеботарьова [1]). Нехай $L/K(C)$ – скінченне розширення Галуа поля $K(C)$, $\mathfrak{g} = \mathrm{Gal}(L/K(C))$ і $\tau \in \mathfrak{g}$. Існує нескінченна множина різних точок поля L, що мають своєю групою розвинення циклічну підгрупу, породжену елементом τ.*

3. Добуток Тейта для кривих над псевдоскінченними полями. В цьому параграфі доведено невиродженість добутку Тейта для кривих над псевдоскінченними полями.

Теорема 2. *Добуток Тейта t_m – невироджений у випадку кривих, визначених над псевдоскінченним полем K, що містить корені степеня m з одиниці.*

Доведення. Доведення теореми ґрунтується на лемах з попереднього параграфа і використовує метод, запропонований Ф. Гессом [7] для кривих над скінченним полем. Нехай $x = [D]$ – довільний клас дивізора D в $\mathrm{J}(C_K)_m$ порядку s і $f \in K(C)$ функція з дивізором $(f) = sD$, де $s|m$. Поліном $T^s - f$ незвідний в $K(C)[T]$, визначає розширення Куммера поля $K(C)$, група Галуа $\mathfrak{g}$ якого є циклічною.

За аналогом теореми щільності Чеботарьова (теорема 1) для $d|s$ існує точка P степеня l, тобто $K(P)/K$ – скінченне розширення, $[K(P):K] = l$, така що $T^s - f(P)$ розкладається на незвідні множники степеня s/d в $K(P)[\sqrt[s]{f}]$. Запишемо розвинення полінома $T^s - f(P)$ так:

$$T^s - f(P) = g_1 \cdot g_2 \cdot g_3 \cdot \ldots \cdot g_d. \tag{1}$$

Для $d = 1$ і $d = s$ існують точки P і Q однакового порядку, які не належать носію дивізора D. Перепишемо (1), прийнявши $d = 1$, $T^s - f(P) = g_1$. Далі при $d = s$ маємо, що $T^s - f(Q) = g_1 \cdot g_2 \cdot g_3 \cdot \ldots \cdot g_s$. Прийнявши, $E := P - Q$ і $y := [E] + m\mathrm{J}(C_K)$, одержуємо, що $t_m(x, y) \notin K^{*m}$.

Позначимо через μ_s групу коренів степеня s з 1 в K. Розглянемо точну послідовність

$$1 \to \mu_s(\overline{K}) \to \overline{K}^* \xrightarrow{s} \overline{K}^* \to 1,$$

з якої отримуємо точну послідовність груп когомологій

$$K^* \xrightarrow{s} K^* \to \mathrm{H}^1(K, \mu_s(\overline{K})) \to \mathrm{H}^1(K, \overline{K}^*).$$

За теоремою Гільберта 90 $\mathrm{H}^1(K, \overline{K}^*) = 0$ і $K^*/K^{*s} \cong \mathrm{H}^1(K, \mu_s(\overline{K}))$. Так само з точної послідовності

$$1 \to \mu_s(\overline{K(P)}) \to \overline{K(P)}^* \xrightarrow{s} \overline{K(P)}^* \to 1,$$

випливає, що $K(P)^*/K(P)^{*s} \cong \mathrm{H}^1(K(P), \mu_s(\overline{K(P)}))$. За попередніми міркуваннями отримуємо, що $K(P)^*/K(P)^{*s} \cong K^*/K^{*s}$.

Покажемо, що норменний гомоморфізм $NK(P)/K$ сюр'єктивний. Для цього використовуємо той факт, що $\widehat{\mathrm{H}}^0(\mathfrak{g}, K(P)^*) \cong \mathrm{H}^2(\mathfrak{g}, K(P)^*)$, де $\widehat{\mathrm{H}}^0(\mathfrak{g}, K(P)^*)$ – когомології Тейта. З одного боку, $\widehat{\mathrm{H}}^0(\mathfrak{g}, K(P)^*) = K(P)^{*\mathfrak{g}}/N_{K(P)/K}(K(P)) = K^*/N_{K(P)/K}(K(P))$, з іншого – $\mathrm{H}^2(\mathfrak{g}, K(P)^*) = 0$, оскільки когомологічна розмірність псевдоскінченного (навіть квазіскінченного) поля дорівнює 1 [10]. Звідси випливає, що $N_{K(P)/K}(K(P)^*) = K^*$. Отже, норма $N_{K(P)/K}$ – сюр'єктивна та індукує епіморфізм $K(P)^*/K(P)^{*s} \to K^*/K^{*s}$.

Далі потрібно показати, що $\mathrm{J}(C_K)_m \cong \mathrm{J}(C_K)/m\mathrm{J}(C_K)$ і $K^*/K^{*m} \cong \mathbb{Z}/m\mathbb{Z}$. Те, що $K^*/K^{*m} \cong \mathbb{Z}/m\mathbb{Z}$ випливає з леми 1. Ізоморфізм груп $\mathrm{J}(C_K)_m$ та $\mathrm{J}(C_K)/m\mathrm{J}(C_K)$ випливає з леми 3, оскільки $\mathrm{J}(C_K)$ має структуру абелевого многовиду над псевдоскінченним полем.

Ми вже знаємо, що гомоморфізм $\mathrm{J}(C_K)_m \xrightarrow{\tau} \mathrm{Hom}(\mathrm{J}(C_K)/m\mathrm{J}(C_K), \mathbb{Z}/m\mathbb{Z}))$, індукований добутком Тейта ін'єктивний, оскільки $|\mathrm{J}(C_K)_m| = |\mathrm{J}(C_K)/m\mathrm{J}(C_K)| =$

$= |\mathrm{Hom}\,(\mathrm{J}(C_K)/m\mathrm{J}(C_K), \mathbb{Z}/m\mathbb{Z})|$, то гомоморфізм τ сюр'єктивний. Враховуючи лему 4 про білінійні добутки скінченних абелевих груп, одержуємо невиродженість добутку Тейта. □

---

1. *Андрійчук В.І.* Аналог теореми щільності Чеботарьова для псевдоглобальних полів / *Андрійчук В.І.* // Вісн. Київ. ун-ту. Сер. фіз.-мат. науки. – 2000. – №4. – С. 11-16.
2. *Введенский О.Н.* О локальных "полях классов" эллиптических кривых / *Введенский О.Н.* // Изв. АН СССР. – 1973. – Т. 37. – С. 20-88.
3. *Касселс Дж.* Алгебраическая теория чисел / *Касселс Дж., Фрёлих А.* – М., 1969.
4. *Шафаревич И.Р.* Группа главных однородных алгебраических многообразий / *Шафаревич И.Р.* // Докл. АН СССР. – 1959. – Т. 124, №1. – С. 42-43.
5. *Ax J.* The elementary theory of finite fields / *Ax J.* // Ann. Math. – 1968. – Vol. 88, №2. – P. 239-271.
6. *Fried M.* Field arithmetic / *Fried M., Jarden M.* – New York, Berlin, Heidelberg: Springer-Verlag, 2005.
7. *Hess F.* A Note on the Tate Pairing of Curves over Finite Fields / *Hess F.* // Computer Science Department, Woodland Road, University of Bristol, preprint.
8. *Papikian M.* On Tate Local Duality / *Papikian M.* // preprint.
9. *Tate J.* WC-group over p-adic fields / *Tate J.* // Sem. Bourbaki. – 1956. – №156.
10. *Серр Ж.-П.* Когомологии Галуа / *Серр Ж.-П.* – М., 1968.

ON NONDEGENERACY OF TATE PRODUCT FOR CURVES OVER PSEUDOFINITE FIELDS

Volodymyr NESTERUK

Ivan Franko National University of L'viv,
79000 L'viv, Universytets'ka Str., 1
e-mail: volodymyr-nesteruk@rambler.ru

A proof of nondegeneracy of the Tate product on curves over pseudofinite fields is given.

Key words: Tate pairing, projective curve, Jacobian of curve, pseudofinite field.

О НЕВЫРОЖДЕННОСТИ ПРОИЗВЕДЕНИЯ ТЭЙТА ДЛЯ КРИВЫХ НАД ПСЕВДОКОНЕЧНЫМИ ПОЛЯМИ

Владимир НЕСТЕРУК

Львовский национальный университет имени Ивана Франко,
79000 Львов, ул. Университетская, 1
e-mail: volodymyr-nesteruk@rambler.ru

Доказано невырожденность произведения Тэйта для кривых над псевдоконечными полями.

Ключевые слова: произведение Тэйта, проективная кривая, якобиан кривой, псевдоконечное поле.

Стаття надійшла до редколегії 09.02.2010

Прийнята до друку 22.12.2010