УДК 513.6

# Показники еліптичних кривих, визначених над локальним полем

*О. М. Введенський*

Ця замітка містить три пов'язаних між собою результати про еліптичні криві, які визначені над локальними полями: обчислення групи головних однорідних просторів для узагальнених якобієвих многовидів спеціального виду, тривіальність одновимірних когомологій Галуа групи класів іделей еліптичної кривої і інтерпретацію показника кривої роду один у термінах груп Брауера. Відповідні результати відомі для кривих довільного роду, визначених над локальним полем нульової характеристики [1, 2]. Далі подано, що вони мають місце і в характеристиці $p > 0$ для кривих роду один (обмеження на рід — свідоцтво про обмежену інформацію про дуальність Тейта у характеристиці $p > 0$ [3]). Обчислення у перших двох випадках повторюють нарис Тейта у нульовій характеристиці, а в третьому випадку запропоновано нове, більш коротке, ніж у [2], доведення, засноване на інтерпретації Ліхтенбаума [4] добутку Тейта.

1. Обчислення групи головних однорідних просторів для узагальнених якобієвих многовидів спеціального виду. Далі $k$ означає основне локальне поле (тобто повне дискретно нормоване поле — довільної характеристики — з скінченним полем лишків характеристики $p > 0$); $A$ — одновимірний абелів многовид над $k$ і $a_0 = e$ (нуль групи $A$) $a_1, \ldots, a_n$ — $(n+1)$ різних точок з групи $A(k)$; $F$ — замкнення у $A(k)$ підгрупи, породженої $a_1, \ldots, a_n$; нарешті, для додатного дивізора $\mathfrak{m}$ на $A$ нехай $J_{\mathfrak{m}}$ означає узагальнений якобіїв многовид кривої $A$ відносно модуля $\mathfrak{m}$ ($J_0 = J$ — якобіан $A$).

Теорема 1. *Якщо $\mathfrak{m}$ дивізор виду $r_0 l + r_1 a_1 + \ldots + r_n a_n$ (усі $r_1 > 0$), то група головних однорідних просторів над $J_{\mathfrak{m}}$ ізоморфна групі характерів (за Понтрягіним) групи $A(k)/F$.*

Доведення. По-перше, зазначимо, що всі відомості про многовиди $J_{\mathfrak{m}}$, які будуть далі використані, можна знайти у [5,6]. Нехай $\mathfrak{n}$ дивізор $l_1 + a_1 + \ldots + a_n$ і $l/k$ — скінченне розширення Галуа поля $k$ констант поля функцій $k(A) = K$ кривої $A$ над $k$, $\mathfrak{g} = \mathrm{Gal}(l/k)$. $\mathfrak{g}$ — модуль раціональних над $l$ точок ядра канонічного епіморфізму $J_{\mathfrak{m}}(l) \to J_{\mathfrak{n}}(l)$ ізоморфний $\prod_{i=0}^{n} U^1_{a_i}(L)/U^{r_i}_{a_i}(L)$ ($U^m_{a_i}(L)$ — $m$-та підгрупа фільтрації у групі одиниць поповнення поля функцій $L = l(A)$ за дивізором $a_i$) $\Rightarrow$ когомологічно тривіальний. Тому групу головних однорідних просторів досить підрахувати для $J_{\mathfrak{n}}$.

Розглянемо точну послідовність $\mathfrak{g}$-модулів

$$0 \to L_{\mathfrak{n}}(l) \to J_{\mathfrak{n}}(l) \to J(l) \to 0, \tag{1}$$

яка відповідає строго точній послідовності алгебраїчних груп над $k$ (див. [5]): $0 \to L_{\mathfrak{n}} \to J_{\mathfrak{n}} \to J \to 0$, $\mathfrak{g}$-модуль $J_{\mathfrak{n}}(l)$ (відповідно $J(l)$) ототожнюється з $\mathfrak{g}$-модулем класів нульового степеня раціональних над $l$ дивізорів на $A$ за модулем $\mathfrak{n}$ (відповідно $o$) еквівалентності, який, у свою чергу, ізоморфний фактор-модулю $C^0_{\mathfrak{n}}(L)$ (відповідно $C^0_{\mathfrak{o}}(L)$) $\mathfrak{g}$-модуля $C^0(L)$ класів нульового степеня іделей поля $L = l(A)$ за образом вкладення підмодуля $\mathfrak{g}$-модуля іделей поля $L$ у $C^0(L)$:

$$\left(\prod_{P \notin \{a_0, \ldots, a_n\}} U_P(L)\right) \cdot \left(\prod_{i=0}^{n} U^1_{a_i}(L)\right) \to C^0(L),$$

де $P$ пробігає всі дивізори поля $L$ (відповідно за образом гомоморфізму $\prod_P U_P(L) \to C^0(L)$); позначення відповідають позначенням [7, § 5]. Ці ізоморфізми індукують, у свою чергу, ізоморфізм

$$i : L_{\mathfrak{n}}(l) \xrightarrow{\sim} \left(\prod_{i=1}^{n} U_{a_i}(L)/U^1_{a_i}(L) \xrightarrow{\sim} (l^*)^n\right). \tag{2}$$

(2) дає, між іншим, точність такого відрізка когомологічної послідовності, яка відповідає (1):

$$0 \longrightarrow H^1(\mathfrak{g}, J_{\mathfrak{n}}(l)) \longrightarrow H^1(\mathfrak{g}, J(l)) \xrightarrow{\delta} H^2(\mathfrak{g}, L_{\mathfrak{n}}(l)).$$

Для обчислення $\operatorname{Ker} \delta$, яке нас цікавить, досить перевірити комутативність діаграми

$$\begin{array}{ccc} H^1(\mathfrak{g}, J(l)) & \xrightarrow{\delta} & H^2(\mathfrak{g}, L_{\mathfrak{n}}(l)) \\ \Sigma^* \downarrow \wr & & i^* \downarrow \wr \\ H^1(\mathfrak{g}, A(l)) & \xrightarrow{\varphi} & (H^2(\mathfrak{g}, l^*))^n \end{array}$$

($\Sigma^*$ індукований додаванням $\Sigma$ на $A$, $i^*$ індукований $i$, визначення $\varphi$ є ($\alpha \in H^1(\mathfrak{g}, A(l))$)

$$\varphi(\alpha) = (-(\alpha, a_1), \ldots, -(\alpha, a_n)) \in (H^2(\mathfrak{g}, l^*))^n,$$

де $(\alpha, a_i)$ — результат множення за Тейтом класу $\alpha$ на $a_i \in A(k)$. [3] показує тоді, що $H^1(\mathfrak{g}, J_{\mathfrak{n}}(l))$ ізоморфна групі характерів групи $A(k)/(F + N_{\mathfrak{g}}(A(l)))$. Перехід до границі завершує доведення теореми 1.

Зауваження 1. При доведенні теореми 1 обчислено групу $H^1(\mathfrak{g}, C^0_{\mathfrak{m}}(L)) (\xrightarrow{\sim} H^1(\mathfrak{g}, J_{\mathfrak{m}}(l))$. Зрозуміло, що вона тривіальна, коли $\operatorname{supp} \mathfrak{m}$ містить систему представників нетривіальних класів $A(k)/N\mathfrak{g}(A(l))$.

**2. Тривіальність одновимірних когомологій Галуа групи класів іделей еліптичної кривої.** Позначення ті ж, що і в попередньому пункті. Нагадуємо, що $l/k$ скінченне розширення Галуа основного локального поля $k$, $\mathfrak{g} = \operatorname{Gal}(l/k)$, і $C(L)$ — група класів іделей поля $L = l(A)$, раціональних над $l$ функцій одновимірного абелевого многовиду, визначеного над $k$.

Теорема 2. $H^1(\mathfrak{g}, C(L)) = 0$.

Доведення. Досить довести, що $H^1(\mathfrak{g}, C^0(L)) = 0$.

Розглянемо точну послідовність $\mathfrak{g}$-модулів

$$0 \to E \to C^0(L) \to C^0_{\mathfrak{o}}(L) \to 0, \tag{3}$$

$E = \dfrac{L^* \prod\limits_P U_P(L)}{L^*}$, $P$ пробігає всі дивізори поля $L$; гомоморфізми у послідовності (3) — природні. Нехай $Q$ — дивізор поля $L$, який відповідає точці $Q \in A(k)$. Ізоморфізм $\mathfrak{g}$-модулів $\left(\prod\limits_{P \neq Q} U_P(L)\right) U_Q^1(L) \xrightarrow{\sim} E$, індукований вкладенням підгрупи $\left(\prod\limits_{P \neq Q} U_P(L)\right) U_Q^1(L)$ групи іделів поля $L$ у підгрупу $\prod\limits_P U_P(L)$ цієї групи, показує, що $H^1(\mathfrak{g}, E) \approx 0$ і що виділення у $\left(\prod\limits_{P \neq Q} U_P(L)\right) U_Q^1(L)$ множників, які відповідають дивізорам поля $L$, які породжуються точками $A(k)$, визначає ізоморфізм

$$p: H^2(\mathfrak{g}, E) \xrightarrow{\sim} \Big[\prod_{x \in A(k), x \neq Q} H^2(\mathfrak{g}, U_x(L)/U_x^1(L))\Big] \oplus Y,$$

де $Y$ — деяка абелева група (відзначимо, $U_x^1(L)$ когомологічно тривіальні для всіх $x \in A(k)$. Тепер зрозуміло, що (3) відповідає точна послідовність

$$0 \longrightarrow H^1(\mathfrak{g}, C^0(L)) \longrightarrow H^1(\mathfrak{g}, C_0^0(L)) \xrightarrow{\delta} H^2(\mathfrak{g}, E). \tag{4}$$

Завершує доведення теореми 2 перевірка тривіальності ядра $\delta$ у (4).

Нехай $f_1, \ldots, f_s$ — коцикли, які є системою представників нетривіальних класів $\alpha_1, \ldots, \alpha_s$ групи $H^1(\mathfrak{g}, A(l))$ і $b_1, \ldots, b_s$ — система представників нетривіальних класів $A(k)/N\mathfrak{g}(A(l))$ (див. [3] відносно інформації про групи $H^n(\mathfrak{g}, A(l))$). Виберемо тепер точку $Q \in A(k)$ так, щоб $Q$, $Q_1 = Q - b_1, \ldots, Q_s = Q - b_s$ (дії на $A$) були відмінними від точок $\{\pm \sigma f_i(\tau), e\}$ $\sigma$; $\tau$ — довільні з $\mathfrak{g}$, що завжди можна зробити, бо $A(k)$ нескінченна. Нехай

$$\pi_Q: \Big[\prod_{x \in A(k), x \neq Q} H^2(\mathfrak{g}, U_x(L)/U_x^1(L))\Big] \oplus Y \to (H^2(\mathfrak{g}, l^*))^s$$

є композицією проектування добутку на компоненти, які відповідають точкам $Q_1, \ldots, Q_s$, при якому $Y$ відображається в нуль, і ізоморфізму типу (2)

$$\prod_{i=1}^{s} H^2(\mathfrak{g}, U_{Q_i}(L)/U_{Q_i}^1(L)) \xrightarrow{\sim} (H^2(\mathfrak{g}, l^*))^s.$$

Неважко перевірити комутативність діаграми

$$\begin{array}{ccccc}
H^1(\mathfrak{g}, J(l)) & \xrightarrow[\sim]{\omega} & H^1(\mathfrak{g}, C_0^0(L)) & \xrightarrow{\delta} & H^2(\mathfrak{g}, E) \\
\Sigma^{*-1} \uparrow \wr & & & & \downarrow \pi_Q o p \\
H^1(\mathfrak{g}, A(l)) & & \xrightarrow{\quad\quad\lambda\quad\quad} & & (H^2(\mathfrak{g}, l^*))^s
\end{array}$$

(де $\Sigma^{*-1}(\alpha_i)$ є клас $H^1(\mathfrak{g}, J(l))$, представником якого є коцикл, значення якого на $\sigma \in \mathfrak{g}$ є клас лінійної еквівалентності дивізора $(f_i(\sigma) - e)$, $\omega$ індукований ізоморфізмом $J(l) \xrightarrow{\sim} C_0^0(L)$ і $\lambda(\alpha_i) = ((\alpha_i, b_1), \ldots, (\alpha_i, b_s)) \in (H^2(\mathfrak{g}, l^*))^*$ $(i = 1, \ldots, s)$ $((\alpha_i, b_j)$ — добуток Тейта класу $\alpha_i \in H^1(\mathfrak{g}, A(l))$ з $b_j \in A(k))$; тривіальність ядра $\delta$ випливає з тривіальності ядра $\lambda$, яка має місце завдяки невиродженості добутку Тейта (3). Доведення теореми закінчене.

З а у в а ж е н н я 2. Нагадаємо, що $C^0(L) = \varprojlim C_{\mathfrak{m}}^0(L)$ (проективна границя груп $C_{\mathfrak{m}}^0(L)$, коли $\mathfrak{m}$ пробігає всі додатні дивізори поля $L$). Після цього зв'язок між теоремами 1 і 2 стає очевидним.

3. Інтерпретація показника еліптичної кривої у термінах груп Брауера. Нехай $V$ — крива роду один над $k$, яку можна подати [8] як головний однорідний простір над деяким одновимірним абелевим многовидом $A$, визначеним над $k$. Нехай $k(V)$ — поле функцій на кривій $V$ над $k$.

Теорема 3. *Ядро гомоморфізму* $\mathrm{Br}\, k \to \mathrm{Br}(k(V))$, *індукованого вкладенням* $k^* \to k(V)^*$, *є циклічна група, порядку, що дорівнює показникові* $V$.

Доведення. Нехай $\mathrm{Div}(V)$ (відповідно $\mathrm{Pic}(V)$) група дивізорів (відповідно група класів дивізорів за модулем лінійної еквівалентності) на $V$ раціональних над сепарабельним замкненням $k_s$ поля $k$; $\mathrm{Div}_0(V)$ (відповідно $\mathrm{Pic}_0(V)$) — підгрупа $\mathrm{Div}(V)$ (відповідно $\mathrm{Pic}(V)$), яка складається з дивізорів (відповідно класів дивізорів) нульового степеня.

Комутативній діаграмі з точними рядками (гомоморфізми — природні)

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Pic}_0(V) & \to & \mathrm{Pic}(V) & \to & Z & \to & 0 \\ & & \uparrow & & \uparrow & & \uparrow{\scriptstyle 1} & & \\ 0 & \to & \mathrm{Div}_0(V) & \to & \mathrm{Div}(V) & \to & Z & \to & 0 \end{array}$$

відповідає комутативна діаграма когомологій Галуа ($G = \mathrm{Gal}(k_s/k)$, когомології рахуються за неперервними ланцюгами) також з точними рядками

$$\begin{array}{ccccccc} \mathrm{Pic}(V)^G & \to & Z & \to & H^1(G, \mathrm{Pic}_0(V)) & & \\ \uparrow & & \uparrow{\scriptstyle 1} & & f\uparrow & & \\ \mathrm{Div}(V)^G & \to & Z & \to & H^1(G, \mathrm{Div}_0(V)) & \to & H^1(G, \mathrm{Div}(V)). \end{array} \tag{5}$$

За лемою Шапіро, $H^1(G, \mathrm{Div}(V)) = 0$. Тому із рівності показника $[Z : \mathrm{Im}(\mathrm{Div}(V)^G)]$ і порядку $[Z : \mathrm{Im}(\mathrm{Pic}(V)^G)]$ кривої $V$ випливає, що $f$ — мономорфізм (рівність порядку і показника — див. [4,9]).

Нехай $\mathfrak{D}$ — підгрупа дивізорів функцій у $\mathrm{Div}_0(V)$. Тоді точній послідовності $0 \to \mathfrak{D} \to \mathrm{Div}_0(V) \to \mathrm{Pic}_0(V) \to 0$ відповідає завдяки мономорфності $f$ у (5) точна послідовність $\mathrm{Pic}_0(V)^G \xrightarrow{d} H^1(G, \mathfrak{D}) \to 0$. Ізоморфізм $\mathfrak{D} \xrightarrow{\simeq} k_s(V)^*/k_s^*$ ($k_s(V)$ — поле функцій $V$ над $k_s$) індукує ізоморфізм $H^1(G, \mathfrak{D}) \xrightarrow[\simeq]{g} H^1(G, k_s(V)^*/k_s^*)$. Нарешті, точній послідовності $1 \to k_s^* \to k_s(V)^* \to k_s(V)^*/k_s^* \to 1$ відповідає точна послідовність

$$H^1(G, k_s(V)^*/k_s^*) \xrightarrow{\delta} H^2(G, k_s^*) \xrightarrow{h} H^2(G, k_s(V)^*). \tag{6}$$

Композиція

$$\mathrm{Pic}_0(V)^G \xrightarrow{d} H^1(G, \mathfrak{D}) \xrightarrow[\simeq]{g} H^1(G, k_s(V)^*/k_s^*) \xrightarrow{\delta} H^2(G, k_s^*)$$

є гомоморфізмом

$$\psi : \mathrm{Pic}_0(V)^G \to H^2(G, k_s^*) = \mathrm{Br}\, k \tag{7}$$

Ліхтенбаума [4,9]. Попередні міркування показують, що у (6) і (7)

$$\mathrm{Im}\, \psi = \mathrm{Im}\, \delta = \mathrm{Ker}\, h.$$

Залишається тепер нагадати, що $\psi(\mathrm{Pic}_0(V)^G)$ є, за Ліхтенбаумом [4], результат множення Тейта класу головних однорідних просторів з представником $V$ на всю групу $A(k) \to$ за невиродженістю добутку Тейта — це циклічна підгрупа $\mathrm{Br}\, k$, порядок якої такий же, як порядок $V$ [3,9]. Нарешті, оскільки $H^2(G, k_s(V)^*)$ вкладається у $\mathrm{Br}(k(V))$, то

$$\mathrm{Kep}(Brk \to \mathrm{Br}(k(V)) = \mathrm{Ker}\, h,$$

що і доводить теорему 3.

Зауваження 3. Наведене доведення теореми є, по суті, простим наслідком результатів Ліхтенбаума [4]. Інше доведення, яке використовує теорему 2, у Рокетта [2].

## ЛІТЕРАТУРА


1. J. Tate, Sem. Bourbaki, № 156, 1957.
2. P. Roquette, Nagoya Math. Journ., 27, 452, 1966.
3. О. М. Введенський, Локальні поля класів еліптичних кривих, ДАН УРСР, серія А, № 10, 1968.
4. S. Lichtenbaum, Period — Index Problem for elliptic curves, Препринт, 1968.
5. Т. Серр, Алгебраические группы и поля классов, М. 1968.
6. M. Rosenlicht, Ann. Math., 59, 505, 1954.
7. J. P. Serre, BSMF, 89, 104, 1961.
8. J. W. S. Cassels, Journ. London Math. Sos. 41, 193, 1966.
9. О. М. Введенський, Підгрупи норм в еліптичних кривих, визначених над локальним полем, УМЖ, т. 22, № 4, 1970.


Надійшла 27.VII 1969 р.
Львівський державний університет