ВІСНИК ЛЬВІВ. УН-ТУ
Серія мех.-мат.2001.Вип.59.С.33–40

VISNYK LVIV UNIV.
Ser.Mech-Math.2001.Vol.59.P.33–40

УДК 513.6

КРУЧЕННЯ І ГРУПИ БРАУЕРА ЕЛІПТИЧНИХ КРИВИХ НАД ПСЕВДОЛОКАЛЬНИМИ ПОЛЯМИ

Людмила СТАХІВ
Львівський національний університет імені Івана Франка
вул.Університетська, 1 79000 Львів, Україна

Нехай A – еліптична крива, визначена над повним дискретно нормованим полем з псевдоскінченним полем класів лишків, $(A(K))_n$ і $(BrA)_n$ – підгрупи групи K – раціональних точок кривої A і групи Брауера кривої A, яка складається з елементів, порядок яких ділить n. Показано, що $|(BrA)_n| \leqslant n|(A(K))_n|$. Використовуючи цю нерівність і метод В.І. Янчевського, Г.Л. Марголіна, описана група $(BrA)_n$.

Ключові слова: алгебраїчні многовиди, еліптичні криві, групи Брауера, псевдоскінченні поля.

Нехай K – псевдолокальне поле, тобто повне стосовно дискретного нормування v поле з псевдоскінченним за Аксом [1] полем класів лишків k, π – простий елемент поля K. O_K, P_K, U_K відповідно кільце цілих, ідеал нормування та група одиниць поля K. α – одиниця поля K, яка не є квадратом. K_s і k_s – сепарабельні замикання полів K і k , $G = Gal(K_s/K)$ – група Галуа поля K.

Нехай A – еліптична крива над полем K, $K(A)$ – поле функцій на кривій A, $A(K)$ – група K – раціональних точок кривої A, $A_0(K)$ – підгрупа точок групи $A(K)$, що редукуються в неособливі, $A_0(k)$ – образ групи $A_0(K)$ при відображенні редукції, $A_1(K)$ – ядро редукції. $BrK(A)$ – група Брауера поля $K(A)$, BrA – група Брауера кривої A [2]. Відомо, що група BrA є підгрупою групи $BrK(A)$ і вивчення групи $BrK(A)$ зводиться до вивчення групи BrA, бо факторгрупа $BrK(A)/BrA$ є відомою згідно з результатами [3], (див. також [4]). $BrK(A)$ є періодичною абельовою групою, тому вивчення групи BrA зводиться до вивчення підгруп $(BrA)_n$, що складаються з елементів, порядок яких є дільником n. Надалі вважаємо, що $(n, chark) = 1$. μ_n – група коренів n - го степеня з 1, що містяться в полі k_s. Для розширення Галуа L/K з групою Галуа G через $H^i(L/K, M)$ або $H^i(G, M)(i \in \mathbb{Z})$ позначаємо когомології Галуа G – модуля M, $H^i(K, M) =^{df} H^i(Gal(K_s/K), M)$.

В.І. Янчевський і Г.Л. Марголін [4] дослідили групу Брауера еліптичних і гіпереліптичних кривих над локальним полем і описали підгрупу $(BrA)_2$ цієї групи.

Мета цієї праці – показати, що аналогічні результати правильні і для еліптичних кривих, визначених над псевдолокальним полем. Зауважимо, що у зв'язку з тим, що немає інформації про невиродженість добутку Тейта - Шафаревича в абельових многовидах розмірності більшої ніж одиниця, визначених над псевдолокальним полем, ми не можемо поки що одержати аналоги згаданих результатів В.І. Янчевського і Г.Л. Марголіна для гіпереліптичних кривих.

Ми позначимо символом $|G|$ порядок скінченної групи G. Сформулюємо спочатку теорему, яка дає, зокрема, оцінку зверху для порядку групи $(BrA)_n$. Зазначимо, що перші два твердження цієї теореми правильні для відповідних алгебраїчних многовидів, визначених над загальними локальними полями [8], і клас загальних локальних полів містить класичні локальні та псевдолокальні поля.

Теорема 1.

1. Нехай A – абельовий многовид, визначений над загальним локальним полем K; n - натуральне число, взаємно просте з характеристикою поля лишків k поля K. Тоді група $A(K)/nA(K)$ скінченна.

2. Нехай A – повна, неособлива, абсолютно незвідна алгебраїчна крива, визначена над загальним локальним полем K. Тоді група $(BrA)_n$ скінченна.

3. Нехай A – еліптична крива, визначена над псевдолокальним полем K. Тоді група $(BrA)_n$ скінченна і правильна нерівність: $|(BrA)_n| \leqslant n|(A(K))_n|$.

Для доведення цієї теореми нам буде потрібно декілька лем.

Лема 1. *Нехай M – скінченний G-модуль над загальним локальним полем K. Тоді $H^1(K, M)$ – скінченна група.*

Доведення. Припустимо спочатку, що $\mu_n \subset K$. Розглянемо точну послідовність G-модулів $1 \to \mu_n \to K_s^* \to K_s^* \to 1$, з якої одержуємо точну послідовність когомологій Галуа

$$1 \to \mu_n \to K^* \to K^* \to H^1(K, \mu_n) \to H^1(K, K_s^*).$$

$H^1(K, K_s^*) = 0$ за теоремою Гільберта - 90. А тому $H(K, \mu_n) \cong K^*/K^{*n}$.

Покажемо, що група K^*/K^{*n} скінченна. Оскільки K – повне стосовно дискретного нормування поля, то $K^* = \mathbb{Z} \oplus U$, де U – група одиниць поля K. Звідси легко одержати, що послідовність груп $1 \to U/U^n \to K^*/K^{*n} \to \mathbb{Z}/n\mathbb{Z} \to 0$ точна. Тому група K^*/K^{*n} скінченна, якщо група U/U^n скінченна. Перевіримо, що група U/U^n скінченна. Розглянемо підгрупу $U_1 = 1 + \pi O_K$. Відомо, що $U/U_1 \cong k^*$. Тому можна розглянути таку комутативну діаграму з точними рядками, в якій вертикальні стрілки є гомоморфізмами множення на n:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_1 & \longrightarrow & U & \longrightarrow & k^* & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \\ 1 & \longrightarrow & U_1 & \longrightarrow & U & \longrightarrow & k^* & \longrightarrow & 1 \end{array}.$$

З цієї діаграми та з подільності елементів групи U_1 на n випливає, що $U/U^n \cong k^*/k^{*n}$. Покажемо, що k^*/k^{*n} скінченна група. Для цього розглянемо точну когомологічну послідовність $1 \to \mu_n \to k^* \to k^* \to H^1(k, \mu_n) \to 0$, яка відповідає точній послідовності $1 \to \mu_n \to k_s^* \to k_s^* \to 1$. Тут $H^1(k, \mu_n) \cong \mu_n$, бо $\mu_n \subset K$. Звідси $k^*/k^{*n} \cong \mu_n$ і остаточно отримуємо, що $|K^*/K^{*n}| = n^2$ і група $H^1(K, \mu_n)$ – скінченна.

Припустимо, що $\mu_n \not\subset K$. Розглянемо скінченне розширення Галуа L/K таке, що $\mu_n \subset L$. Скористаємось відрізком спектральної послідовності Хохшільда-Серра [5, с.21]

$$1 \to H^1(L/K, \mu_n) \to H^1(K, \mu_n) \to H^1(L, \mu_n)^{Gal(L/K)}.$$

Оскільки групи $H^1(L/K, \mu_n)$ і $H^1(L, \mu_n)^{Gal(L/K)}$ скінченні, то і група $H^1(K, \mu_n)$ скінченна.

Нехай L/K – скінченне розширення Галуа, над яким модуль M стає тривіальним. Можна вважати, що $M = \oplus\mu_{n_i}$, причому $\mu_{n_i} \subset L$. Оскільки когомології комутують з прямими сумами, то $H^1(L, M) \cong \oplus H^1(L, \mu_{n_i})$. Це означає, що група $H^1(L, M)$ скінченна. Тому, знову застосувавши спектральну послідовність Хохшільда-Серра

$$1 \longrightarrow H^1(L/K, M) \longrightarrow H^1(K, M) \longrightarrow H^1(L, M)^{Gal(L/K)}$$

і використовуючи скінченність груп $H^1(L, M)$ та $H^1(L/K, M)$, одержуємо скінченність групи $H^1(K, M)$. □

Лема 2. *Група $A_1(K)$ однозначно подільна на всі натуральні числа, що взаємно прості з характеристикою поля лишків поля K.*

Доведення. Доведення цієї леми можна знайти, наприклад, у [6].

Лема 3. *Нехай A – довільна еліптична крива, визначена над псевдолокальним полем K або крива з виродженою редукцією, визначена над загальним локальним полем K. Тоді*

$$|A(K)/nA(K)| = |(A(K))_n|. \tag{1}$$

Доведення. Якщо редукція кривої невироджена, то рівність $|A(K)/nA(K)| = |(A(K))_n|$ доведена у [7] і в [14]. У випадку виродженої редукції треба розглянути окремо випадки кривих з мультиплікативною та адитивною редукціями.

Якщо A – крива з мультиплікативною редукцією, то рівність (1) доведена у [15]. Нехай A – крива з адитивною редукцією. Множення на n в точній послідовності редукції визначає таку діаграму:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(K) & \longrightarrow & A_0(K) & \longrightarrow & k^+ & \longrightarrow & 0 \\ & & \downarrow n & & \downarrow n & & \downarrow n & & \\ 0 & \longrightarrow & A_1(K) & \longrightarrow & A_0(K) & \longrightarrow & k^+ & \longrightarrow & 0 \end{array},$$

в якій лівий крайній вертикальний гомоморфізм є ізоморфізмом на підставі леми 2, а правий крайній вертикальний гомоморфізм є ізоморфізмом тому, що $(n, chark) = 1$. Отже, середній гомоморфізм також є ізоморфізмом і ми отримуємо, що

$$|A_0(K)/nA_0(K)| = |(A_0(K))_n| = 0.$$

Відомо [9], що група $A_0(K)$ вкладається в точну послідовність

$$0 \longrightarrow A_0(K) \longrightarrow A(K) \longrightarrow H \longrightarrow 0, \tag{2}$$

де група H може мати порядок 1, 2, 3 або 4 [9], група порядку 4 може бути як циклічною, так і нециклічною.

Нехай 2 ділить n і $|H| = 2$, що відповідає типам (c2) і (c7) за Нероном [9]. У цьому випадку, застосувавши лему про змію до діаграми, що одержується з точної послідовності (2) за допомогою множення на 2, одержуємо, що

$$|(A(K))_n| = |A(K)/nA(K)| = |(A(K))_2| = |A(K)/2A(K)| = |\mathbb{Z}/2\mathbb{Z}| = 2.$$

Нехай 2 ділить n і H- циклічна група четвертого порядку, що відповідає типам (c4) і$(c5_{2k})$ за Нероном. Тоді аналогічно одержуємо, що

$$|(A(K))_n| = |A(K)/nA(K)| = |(A(K))_2| = |A(K)/2A(K)| = |\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}| = 4.$$

Якщо 2 ділить n і H – циклічна група четвертого порядку, що відповідає типу $(c5_{2k+1})$ за Нероном, то одержимо, що $|(A(K))_n| = |A(K)/nA(K)| = 2$.

Нарешті, якщо 2 ділить n і A – крива типу (c3) або (c6)(тобто H – група третього порядку), то $|(A(K))_n| = |A(K)/nA(K)| = 0$.

Якщо 3 ділить n, а крива A має тип (c1), (c2), (c4), (c5), (c7) або (c8) за Нероном, то $|(A(K))_n| = |A(K)/nA(K)| = 0$.

Залишився випадок, коли 3 ділить n, а крива A має тип (c3) або (c6) за Нероном. Тоді, застосовуючи гомоморфізм множення на n до точної послідовності (2), одержуємо $|(A(K))_n| = |A(K)/nA(K)| = |(A(K))_n| = 3$.

Нехай 2 не ділить n і 3 не ділить n, тоді $(n, |H|) = 1$, тому множення на n є ізоморфізмом групи H. Розглянемо таку діаграму гомоморфізму множення на n:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_0(K) & \longrightarrow & A(K) & \longrightarrow & H & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \\ 0 & \longrightarrow & A_0(K) & \longrightarrow & A(K) & \longrightarrow & H & \longrightarrow & 0 \end{array} \qquad (3)$$

Як зазначено вище, множення на n в групі $A_0(K)$ є ізоморфізмом. Тому середній вертикальний гомоморфізм в (3) є ізоморфізмом групи $A(K)$. Отже,

$$|(A(K))_n| = |A(K)/nA(K)| = 0,$$

і це завершує доведення леми у випадку адитивної редукції.

Доведення теореми 1. 1. Відомо [11], що $(A(K_s))_n \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ і, отже, за лемою 1 група $H^1(K, (A(K_s))_n)$ скінченна. Розглянемо точну послідовність

$$0 \to (A(K))_n \to A(K_s) \to A(K_s) \to 0$$

множення на n в $A(K_s)$ і відповідну їй точну когомологічну послідовність

$$\begin{array}{c} A(K) \xrightarrow{n} A(K_s) \longrightarrow H^1(K, (A(K_s))_n) \longrightarrow \\ H^1(K, A(K_s)) \xrightarrow{n} H^1(K, A(K_s)) \longrightarrow \cdots \end{array} \qquad (4)$$

З останньої послідовності випливає, що група $A(K)/nA(K)$ ізоморфна підгрупі групи $H^1(K, (A(K_s))_n)$, і отже, є скінченною групою.

2. Нехай A – довільна повна абсолютно незвідна алгебраїчна крива, визначена над загальним локальним полем K, $\bar{A}$ – крива A, розглянута над полем K_s. Відомо [12], що G-модуль $Pic^0\bar{A}$ ізоморфний якобіану кривої $\bar{A}$. Аналогічно тому, як ми одержали послідовність (4), маємо точну послідовність

$$H^1(K, (Pic^0\bar{A})_n) \longrightarrow H^1(K, Pic^0\bar{A}) \xrightarrow{n} H^1(K, Pic^0\bar{A}),$$

яка показує, що група $H^1(G, Pic^0\bar{A})_n$ є гомоморфним образом скінченної (згідно з лемою 1) групи $H^1(K, (Pic^0\bar{A})_n)$, отже, є скінченною групою. Розглянемо ще точну послідовність G-модулів $0 \to Pic^0\bar{A} \to Pic\bar{A} \to \mathbb{Z} \to 0$. У відповідній послідовності когомологій Галуа $H^0(G, \mathbb{Z}) = \mathbb{Z}$, $H^1(G, \mathbb{Z}) = 0$. Тому група $H^1(G, Pic^0\bar{A})$ вкладається в точну послідовність

$$\mathbb{Z} \longrightarrow H^1(G, Pic^0\bar{A}) \longrightarrow H^1(G, Pic\bar{A}) \longrightarrow 0,$$

з якої одержуємо, що $H^1(G, Pic\bar{A})_n$ скінченна група. З точної послідовності

$$\begin{array}{c} 0 \longrightarrow Pic\bar{A} \longrightarrow H^0(K, Pic\bar{A}(K_s)) \longrightarrow BrK \longrightarrow \\ \longrightarrow BrA \longrightarrow H^1(K, Pic\bar{A}(K)) \longrightarrow H^3(K, K_s^*) \end{array} \qquad (5)$$

[12] отримуємо з урахуванням того, що $H^3(K, K_s^*) = 0$ (когомологічна розмірність поля K дорівнює 2) [5], таку точну послідовність

$$0 \longrightarrow \hat{Br}K \longrightarrow BrA \longrightarrow H^1(G, Pic\bar{A}),$$

де $\hat{Br}A$ – деяка факторгрупа групи BrK. Для загального локального поля K група $BrK \cong \mathbb{Q}/\mathbb{Z}$ [8] є повною, тому кожна її факторгрупа є теж повною. Звідси випливає, що $(\hat{Br}A)_n$ скінченна. З точної послідовності

$$0 \longrightarrow (\hat{Br}K)_n \longrightarrow (BrA)_n \longrightarrow (H^1(G, Pic\bar{A}))_n$$

одержуємо, що група $(BrA)_n$ скінченна.

3. Нерівність $|(BrA)_n| \leqslant n\,|A(K)/nA(K)|$ доведено в праці [14].

Незважаючи на те, що доведена теорема дає лише оцінку зверху для порядку групи n-кручення групи Брауера кривої A, вона, як і у випадку еліптичних кривих над локальними полями, може бути використана для повного описання групи $(BrA)_2$ за допомогою кватерніонних алгебр.

Вважаємо, що характеристика поля K відмінна від 2. Тоді Вейєрштрассове рівняння кривої A має вигляд

$$y^2 = x^3 + ax^2 + bx + c. \tag{6}$$

де $a, b, c \in O_K$. Многочлен $g(x) = x^3 + ax^2 + bx + c$ може мати три, один або не мати жодного кореня. Залежно від того, скільки коренів має многочлен $g(x)$ говорять, відповідно, про розкладний, напіврозкладний і нерозкладний випадки. Вважаємо, що рівняння (6) є мінімальним, тобто $v(\Delta)$, де Δ – дискримінант многочлена $g(x)$ приймає найменше можливе значення. У розкладному випадку мінімальне рівняння Вейєрштрасса кривої A можна звести до вигляду $y^2 = x(x - e_1)(x - e_2), e_1, e_2 \in O_K$. У напіврозкладному випадку це рівняння зводиться до вигляду $y^2 = x(x^2 + ax + b)$, $a, b \in O_K$ і многочлен $x^2 + ax + b$ незвідний над K. У нерозкладному випадку маємо рівняння $y^2 = x^3 + ax^2 + bx + c$, де $a, b, c \in O_K$ і многочлен $x^3 + ax^2 + bx + c$ незвідний над K.

Нагадаємо, що алгеброю $(\frac{a,b}{K})$ узагальнених кватерніонів називають алгебру, породжену елементами 1, x, y, z, де $x^2 = a$, $y^2 = b$, $z^2 = -ab$, 1 - одиничний елемент, і елементи x, y, z попарно антикомутують, $[\frac{a,b}{K}]$ – елемент групи BrK з представником $(\frac{a,b}{K})$.

Теорема 2. *Нехай A – еліптична крива з невиродженою редукцією над повним стосовно дискретного нормування полем K з псевдоскінченним полем лишків k. Тоді група $(BrA)_2$ складається з елементів*

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

у розкладному випадку. У напіврозкладному випадку група $(BrA)_2$ складається з елементів

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

У нерозкладному випадку група $(BrA)_2$ складається з елементів

$$\left[\frac{\alpha, 1}{K(A)}\right], \left[\frac{\alpha, \pi}{K(A)}\right].$$

Теорема 2, в більш послабленому формулюванні, та начерк її доведення вже були опубліковані в [14], але вимога обмеження обсягу праці [14] не дала змоги навести там в явному вигляді зображення елементів групи $(BrA)_2$ кватерніонними алгебрами. Для доведення цієї теореми потрібна така лема.

Лема 5. *([4]) Нехай* $\left[\frac{f,g}{K(A)}\right]$ *і крива* A *визначена рівнянням* $y^2 = x(x^2+ax+b)$. *Тоді, якщо* f *– унітарний многочлен з* $K[x]$, *то* $\left[\frac{f,g}{K(A)}\right]_\infty$ *тривіальна алгебра над* $K(A)_\infty$.

Доведення. Доведення цієї леми, наведене в праці [4] для локальних полів, дослівно переноситься на випадок псевдолокальних полів.

Доведення теореми 2. Враховуючи лему 5 і дослівно повторюючи міркування В.І. Янчевського і Г.Л. Марголіна [4, теорема 8], одержуємо нерозгалуженість, нетривіальність і попарну неізоморфність алгебр зі списків з формулювання теореми 2. Тепер з теореми 1 випливає, що група $(BrA)_2$ має не більше ніж 8 елементів у розкладному випадку, має не більше ніж 4 елементи у напіврозкладному випадку і має не більше ніж 2 елементи у нерозкладному випадку. Тому наведені в формулюванні теореми списки є повними.

Розглянемо розкладний випадок кривої A з виродженою редукцією. У цьому випадку відомо [4], що мінімальне рівняння Вейєрштрасса кривої A має один з таких виглядів:

1) $y^2 = x(x+\alpha)(x-\pi^m a), m > 0$, якщо редукція мультиплікативна, але дотичні в особливій точці редукції невизначені над полем k;

2) $y^2 = x(x+1)(x-\pi^m a), m > 0$, якщо редукція мультиплікативна й обидві дотичні в особливій точці редукції визначені над полем k;

3) $y^2 = x(x-\pi a)(x-\pi b), a \neq b$, якщо редукція адитивна;

4) $y^2 = x(x-\pi a)(x-\pi^m b), m > 1$, якщо редукція адитивна.

Тут a і $b \in U_K$, а α – одиниця поля K, яка не є квадратом.

Теорема 3. *Нехай* A *– еліптична крива, задана над* K *одним з попередніх рівнянь. Тоді у випадку 1 група* $(BrA)_2$ *складається з елементів*

$$\left[\frac{\pi,1}{K(A)}\right], \left[\frac{\pi,\alpha}{K(A)}\right], \left[\frac{\pi,x}{K(A)}\right], \left[\frac{\pi,\alpha x}{K(A)}\right],$$

$$\left[\frac{\alpha,x+\alpha}{K(A)}\right], \left[\frac{\alpha,\alpha(x+\alpha)}{K(A)}\right], \left[\frac{\pi,x-\pi^m\alpha}{K(A)}\right], \left[\frac{\pi,\alpha(x-\pi^m\alpha)}{K(A)}\right].$$

У випадку 2 група $(BrA)_2$ *складається з елементів*

$$\left[\frac{\pi,1}{K(A)}\right], \left[\frac{\pi,\alpha}{K(A)}\right], \left[\frac{\pi,x}{K(A)}\right], \left[\frac{\pi,\alpha x}{K(A)}\right],$$

$$\left[\frac{\alpha,x}{K(A)}\right], \left[\frac{\alpha,\pi x}{K(A)}\right], \left[\frac{\pi\alpha,x}{K(A)}\right], \left[\frac{\pi\alpha,\alpha x}{K(A)}\right].$$

У випадках 3 і 4 група $(BrA)_2$ *складається з елементів*

$$\left[\frac{\alpha,1}{K(A)}\right], \left[\frac{\alpha,\pi}{K(A)}\right], \left[\frac{\alpha,x}{K(A)}\right], \left[\frac{\alpha,x-\pi\alpha}{K(A)}\right],$$

$$\left[\frac{\alpha, \pi(x-\pi\alpha)}{K(A)}\right], \left[\frac{\alpha, \pi x}{K(A)}\right], \left[\frac{\alpha, x-\pi^m b}{K(A)}\right], \left[\frac{\alpha, \pi(x-\pi^m b)}{K(A)}\right],$$

де $m = 1$ *у випадку 3 і* $m > 1$ *у випадку 4.*

Для доведення цієї теореми використовуємо метод В.І. Янчевського і Г.Л. Марголіна, застосований ними для еліптичних кривих над локальними полями. Для цього нам треба мати аналог леми 1 з [4]. Сформулюємо його у вигляді леми.

Лема 6. *Нехай* k *– псевдоскінченне поле характеристики відмінної від 2. Тоді в групі* k^* *виконується кожне з таких тверджень:*

1) існує $u \neq 0$ *таке, що* $u \in (k^*)^2$ *і* $(u+1) \in (k^*)^2$;

2) існує $u \neq 0$ *таке, що* $u \in (k^*)^2$ *і* $(u+1) \notin (k^*)^2$;

3) існує $u \neq 0$ *таке, що* $u \notin (k^*)^2$ *і* $(u+1) \in (k^*)^2$;

4) існує $u \neq 0$ *таке, що* $u \notin (k^*)^2$ *і* $(u+1) \notin (k^*)^2$.

Доведення. Якби k було скінченним полем, то формулювання цієї леми цілком збігалося б з формулюванням вищезгаданої леми 1 праці [4]. Доведення цього результату у [4] суттєво використовує скінченність поля. Якщо цей результат вже доведений для скінченних полів, то для того щоб переконатися у його правильності і для псевдоскінченних полів, достатньо сформулювати його мовою логіки першого порядку [1]. Це легко зробити. Потрібне формулювання має такий вигляд:

$$\exists u(\neg u = 0 \wedge \exists x \exists y(u = x^2 \wedge u + 1 = y^2)) \wedge$$

$$\exists u(\neg u = 0 \wedge \exists x \forall y(u = x^2 \wedge \neg u + 1 = y^2)) \wedge$$

$$\exists u(\neg u = 0 \wedge \forall x \exists y(\neg u = x^2 \wedge u + 1 = y^2)) \wedge$$

$$\exists u(\neg u = 0 \wedge \forall x \forall y \neg(u = x^2 \vee u + 1 = y^2)).$$

Доведення теореми 3. Доведення ґрунтується на модифікації доведення аналогічного результату В.І. Янчевського і Г.Л. Марголіна [4]. Доведення нерозгалуженості, нетривіальності і попарної неізоморфності алгебр зі списків доводиться тими самими методами, що і в [4], враховуючи леми 5 та 6, і той факт, що кожна абсолютно незвідна, неособлива крива, визначена над K, має K-раціональну точку. Ці алгебри є повною системою представників групи $(BrA)_2$, оскільки за теоремою 1 група $(BrA)_2$ має не більше ніж 8 елементів.

Автор висловлює щиру вдячність В.І. Андрійчуку за формулювання задачі, постійну увагу до праці, поради й обговорення.

1. *Ax J.* The elementary theory of finite field // Ann. Math. – 1968. – Vol 88. – №2. – P.239-271.

2. *Милн Дж.* Абелевы многообразия. – М., 1983.

3. *Scharlau W.* Uber die Brauer-Gruppe eines algebraischen Funktionen korpers in einer Voriablen// J. fur die reine und angew. Math. – 1969. – Bd. 239-240. – P.1-6.

4. *Янчевский В.И., Марголин Г.Л.* Кручение и группы Брауэра локальных эллиптических и гиперэллиптических кривых// Ч.1, Ч.2, препринты 6(509),7(510), Инст. Матем. АН Беларуси. – Минск, 1994.
5. *Серр Ж.-П.* Когомологии Галуа. – М., 1968.
6. *Tate J.* The arithmetic of elliptic curves// Invent. Math. – 1974. – Vol. 23. – P.179-206.
7. *Платонов В.И., Рапинчук А.С.* Алгебраические группы и теория чисел. – М., 1991.
8. *Serre J.P.* Corps locaux. – Paris; Hermann, 1962.
9. *Neron A.* Modeles Minimaux Des Varietes Abeliennes sur Les Corps Locaux et Globaux// IHES. – 1964. – №21.
10. *Fried M., Jarden M.* Field arithmetic. – Springer, 1986.
11. *Мамфорд Д.* Абелевы многообразия. – М., 1971.
12. *Lichtenbaum S.* Duality Theorems for Curves over P-adic Fields // Invent. Math. – 1969. – Vol. 7. – P.120-136.
13. *Андрийчук В.И.* Об эллиптических кривых над псевдолокальными полями // Мат. сб. – 1979. – Т. 110. – №9. – С.88-101.
14. *Стахів Л.Л.* Кручення і групи Брауера еліптичних кривих з невиродженою редукцією над псевдолокальним полем // Вісник державного університету "Львівська політехніка". Прикладна математика. – 1998. – №337. – С.59-62.
15. *Андрійчук В.И., Стахів Л.Л.* Про групу Брауера еліптичних кривих // Вісник Київського університету імені Тараса Шевченка. Сер. фіз.-мат. наук. – 1999. – Вип. 2. – С.10-13.

TORSION OF THE BRAUER GROUP OF AN ELLIPTIC CURVE OVER PSEUDOLOCAL FIELD

L. Stakhiv

Ivan Franko National University of Lviv, 1 Universitetska Str. 79000 Lviv, Ukraine

Let A be elliptic curve defined over a complete with respect to discrete valuation field K with a psevdofihite residue field, $(A(K))_n$ and $(BrA)_n$ are the subgroups of the group of K-rational points and of the Brauer group of A, consisting of elements of exponent dividing n. It is shown that $|(BrA)_n| \leqslant n|(A(K))_n|$. Using this inequality and following V.Yanchevskii and G.Margolin we describe $(BrA)_2$.

Key words: Brauer groups, elliptic curves, pseudolocal fields.

Стаття надійшла до редколегії 20.02.2000

Прийнята до друку 03.07.2001