УДК 513.6

В. І. Андрійчук, Л. М. Здомська

ПРО ГРУПУ ЗЕЛЬМЕРА ЕЛІПТИЧНОЇ КРИВОЇ

Нехай E – еліптична крива, визначена над полем алгебричних функцій від однієї змінної з квазіскінченним полем констант k. Нехай n – натуральне число, $(n, \mathrm{char} k) = 1$. Тоді група Зельмера $S^n(E/K)$ є скінченною.

Нехай E – еліптична крива, визначена над полем K і нехай n – натуральне число, взаємно просте з характеристикою поля K.

Доведемо скінченність групи Зельмера $S^n(E/K)$ для невиродженої еліптичної кривої E над полем алгебричних функцій з квазіскінченним [8] полем констант (тобто досконалим полем, яке для кожного $n \in \mathbb{N}$ має єдине з точністю до ізоморфізму розширення степеня n).

Доведення одержуємо за допомогою модифікації методів, використаних Мілном [7] для доведення скінченності групи Зельмера еліптичної кривої, визначеної над числовим полем.

Звідси, зокрема, отримуємо скінченність факторгрупи $E(K)/nE(K)$, тобто слабу теорему Морделла – Вейля для еліптичних кривих над полями алгебричних функцій з квазіскінченними полями констант.

Скінченність групи Зельмера у класичному випадку еліптичних кривих, визначених над числовими полями, є ключовим фактом для доведення теореми Морделла – Вейля, яка стверджує, що для кожної еліптичної кривої E над числовим полем K група $E(K)$ є скінченно породженою. Ця теорема була доведена Морделлом у 1922 р. у випадку $K = \mathbb{Q}$, а у випадку довільного числового поля – Вейлем у 1928 р. Таніяма у 1954 р. довів аналогічну теорему для абелевих многовидів над числовими полями.

Доведення теореми Морделла – Вейля отримуємо зі слабої теореми Морделла – Вейля за допомогою методу спуску.

Нагадаємо означення групи Зельмера (деталі можна знайти в [2]). Нехай $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ – група Галуа сепарабельного замикання поля K. Для еліптичної кривої E, визначеної над полем K, $E(K)$ означає групу її K-раціональних точок, а групи одновимірних когомологій Галуа $H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), E(K^{\mathrm{sep}}))$ та $H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), E(K^{\mathrm{sep}})_n)$ далі скорочено позначатимемо $H^1(K, E)$ та $H^1(K, E_n)$.

Нехай v – дискретне нормування поля K; K_v – поповнення поля K відносно цього нормування. Розглянемо групи $H^1(K_v, E)$ та $H^1(K_v, E_n)$. Існують природні гомоморфізми $H^1(K, E) \to H^1(K_v, E)$, $H^1(K, E_n) \to H^1(K_v, E_n)$ та $H^1(K, E_n) \to H^1(K_v, E)$.

Групою Зельмера $S^{(n)}(E/K)$ еліптичної кривої E над полем K називають множину таких елементів $\gamma \in H^1(K, E_n)$, що для кожного дискретного нормування v поля K образ $\gamma_v \in H^1(K_v, E_n)$ елемента γ є образом деякого елемента з $E(K_v)$.

Інакше кажучи, $S^{(n)}(E/K) = \mathrm{Ker}(H^1(K, E_n) \to \prod_v H^1(K_v, E))$.

Ще одна важлива група, зв'язана з кривою E, – це *група Тейта – Шафаревича*

$$Ш(E/K) = \mathrm{Ker}(H^1(K, E) \to \oplus_v H^1(K_v, E)).$$

Обидві групи $S^{(n)}(E/K)$ та $Ш(E/K)$ є групами кручення. Наступна точна послідовність зв'язує ці групи.

Теорема 1 [2]. *Існує точна послідовність*

$$0 \to E(K)/nE(K) \to S^{(n)}(E/K) \to Ш(E/K)_n \to 0.$$

Теорема 2. *Для кожної еліптичної кривої* E *над скінченним розширенням поля* $k(x)$ *раціональних функцій над квазіскінченним полем* k *і для кожного цілого додатного числа* $n, (n, \mathrm{char} k) = 1$, *група Зельмера* $S^{(n)}(E/L)$ *є скінченною.*

Для доведення цієї теореми потрібні декілька лем.

Лема 1. *Нехай* K *– поле, повне відносно дискретного нормування* v. *Нехай* E *– еліптична крива над* K *з доброю редукцією і* $n \in \mathbb{N}$ *не ділиться на характеристику поля лишків* k *поля* K. *Тоді гомоморфізм редукції* $\phi : E(K) \to \to E(k)$ *є сюр'єктивним і* $nE(K) = \phi^{-1}(nE(k))$.

Д о в е д е н н я. Відображення редукції є сюр'єктивним згідно з теоремою 3 з [9, с. 189]. За цією ж теоремою ядро гомоморфізму редукції $E_1(K)$ однозначно подільне на натуральні числа n, взаємно прості з характеристикою поля k. Тому, якщо $A' = nB'$ в $E(k)$ і $A \in \phi^{-1}(A')$, $B \in \phi^{-1}(B')$, то $A - nB \in \in E_1(K) = nC$ для деякої точки $C \in E_1(K)$. Звідси одержуємо $A = n(B + C)$, тобто $nE(K) \supset \phi^{-1}(nE(k))$. Обернене включення очевидне. $\diamondsuit$

Нехай L/K – скінченне розширення дискретно нормованого поля K; $\mathcal{O}_K$, $\mathcal{O}_L$ – кільця нормувань полів K і L відповідно; $\mathcal{M}_K$ і $\mathcal{M}_L$ – максимальні ідеали кілець $\mathcal{O}_K$ і $\mathcal{O}_L$, причому $\mathcal{O}_K = \mathcal{O}_L \cap K$ і $\mathcal{M}_K = \mathcal{M}_L \cap \mathcal{O}_K$. Нагадаємо, що в цьому випадку поле L називається *нерозгалуженим* розширенням поля K, якщо $[L : K] = [\mathcal{O}_L/\mathcal{M}_L : \mathcal{O}_K/\mathcal{M}_K]$ і розширення $\mathcal{O}_L/\mathcal{M}_L/\mathcal{O}_K/\mathcal{M}_K$ є сепарабельним.

Наступний класичний результат можна знайти, зокрема, в [1].

Лема 2. *Нехай* K *– поле, повне відносно дискретного нормування* v, k *– поле лишків поля* K. *Тоді для кожного скінченного розширення* l *поля* k *існує нерозгалужене розширення* L *поля* K *з полем лишків* l, *у якому ціле замикання кільця нормування поля* K *є кільцем нормування поля* L.

Нехай A – дедекіндове кільце з полем дробів K; $\mathfrak{p}$ – простий ідеал кільця A і $v_\mathfrak{p}$ – відповідне дискретне нормування.

Твердження 1. *Нехай* E *– еліптична крива з дискримінантом* Δ *над полем* K, T *– скінченна множина простих ідеалів, яким належить елемент* $2n\Delta$. *Тоді для кожного* $\gamma \in S^{(n)}(E/K)$ *і кожного* $\mathfrak{p} \notin T$ *існує скінченне нерозгалужене розширення* $L_{v_\mathfrak{p}}$ *поповнення* $K_{v_\mathfrak{p}}$ *поля* K *відносно нормування* $v_\mathfrak{p}$, *для якого* γ *відображається у нуль в* $H^1(L_{v_\mathfrak{p}}, E_n)$.

Д о в е д е н н я. З означення групи Зельмера випливає, що існує точка $X \in \in E(K_{v_\mathfrak{p}})$, яка відображається в $\gamma_\mathfrak{p} \in H^1(K_{v_\mathfrak{p}}, E_n)$. Оскільки $\mathfrak{p}$ не ділить $2n\Delta$, E має добру редукцію відносно $v_\mathfrak{p}$. З лем 1 і 2 випливає існування нерозгалуженого розширення $L_{v_\mathfrak{p}}$ поля $K_{v_\mathfrak{p}}$, для якого $X \in nE(L_{v_\mathfrak{p}})$. Як і у випадку числового основного поля [7], з комутативної діаграми

$$\begin{array}{ccccc}
E(K) & \xrightarrow{n} & E(K) & \longrightarrow & H^1(K, E_n) \\
\downarrow & & \downarrow & & \downarrow \\
E(K_{v_\mathfrak{p}}) & \xrightarrow{n} & E(K_{v_\mathfrak{p}}) & \longrightarrow & H^1(K_{v_\mathfrak{p}}, E_n) \\
\downarrow & & \downarrow & & \downarrow \\
E(L_{v_\mathfrak{p}}) & \xrightarrow{n} & E(L_{v_\mathfrak{p}}) & \longrightarrow & H^1(L_{v_\mathfrak{p}}, E_n)
\end{array}$$

випливає, що γ відображається у нуль в $H^1(L_{v_\mathfrak{p}}, E_n)$. $\diamondsuit$

Наступна лема зводить властивість скінченності групи Зельмера еліптичної кривої E над полем K до властивості скінченності групи Зельмера еліптичної кривої E, розглянутої над скінченним розширенням поля K.

Лема 3. *Для кожного скінченного розширення Галуа L поля K образ $S^{(n)}(E/K)$ при природному гомоморфізмі з $H^1(K,E_n)$ в $H^1(L,E_n)$ міститься в $S^{(n)}(E/L)$ і ядро цього гомоморфізму є скінченним.*

Д о в е д е н н я. Те, що образ групи $S^{(n)}(E/K)$ міститься в $S^{(n)}(E/L)$, безпосередньо випливає з означень. Тому досить довести, що ядро гомоморфізму $H^1(K,E_n) \to H^1(L,E_n)$ є скінченним. Але це ядро є скінченною групою $H^1(\mathrm{Gal}(L/K),E_n(L))$, оскільки $\mathrm{Gal}(L/K)$ і $E_n(L)$ – скінченні групи. $\diamondsuit$

Нехай A – дедекіндове кільце з полем дробів K і нехай L – скінченне розширення Галуа поля K, яке містить $E_n(K^{\mathrm{sep}})$ і групу $\mu_n(K^{\mathrm{sep}})$ коренів n-го степеня з 1 в K^{sep}. Позначимо через B ціле замикання A в L, а через $U(B)$ і $C(B)$ – відповідно групу одиниць і групу класів ідеалів кільця B.

Надалі для групи $C(B)$ через $C_n(B)$ позначатимемо підгрупу $\{a \in C_n(B) : na = 0\}$.

Лема 4. *Якщо групи $U(B)/U^n(B)$ і $C_n(B)$ є скінченними, то й група $S^{(n)}(E/K)$ є скінченною.*

Д о в е д е н н я. Згідно з лемою 3 можна вважати, що у полі K містяться всі корені n-го степеня з 1 та точки n-го порядку кривої E. Нехай L/K – скінченне розширення Галуа таке, що для кожного $\mathfrak{p} \notin T$ елементи групи Зельмера $S^{(n)}(E/K)$ відображаються у нуль у групі $H^1(L_{v_\mathfrak{p}},E_n)$. Розширення L/K існує за твердженням 1. Тоді з діаграми

$$\begin{array}{ccc} H^1(K,E_n) & \cong & (K^*/K^{*n})^2 \\ \downarrow & & \downarrow \\ H^1(L_{v_\mathfrak{p}},E_n) & \cong & (L^*_{v_\mathfrak{p}}/L^{*n}_{v_\mathfrak{p}})^2 \end{array}$$

отримуємо, що група Зельмера $S^{(n)}(E/K)$ міститься в ядрі гомоморфізму $(K^*/K^{*n})^2 \to \oplus_{v_\mathfrak{p}}(L^*_{v_\mathfrak{p}}/L^{*n}_{v_\mathfrak{p}})^2$, отже, в ядрі гомоморфізму

$$(L^*/L^{*n})^2 \to \oplus_{v_\mathfrak{p}}(L^*_{v_\mathfrak{p}}/L^{*n}_{v_\mathfrak{p}})^2 \overset{a \mapsto \oplus_{v_\mathfrak{p}}(\mathrm{ord}_\mathfrak{p} \bmod n)}{\longrightarrow} (\mathbb{Z}/n\mathbb{Z})^2.$$

Нехай U_T – група T-одиниць поля L. Розглянемо точну послідовність [7]

$$0 \to U_T \to L^* \overset{a \mapsto (\mathrm{ord}_\mathfrak{p}(a))}{\longrightarrow} \oplus_{\mathfrak{p} \notin T}\mathbb{Z} \to C_T \to 0. \tag{1}$$

З попередніх міркувань випливає, що група $S^{(n)}(E/K)$ міститься в ядрі N гомоморфізму

$$L/L^{*n} \longrightarrow \oplus_{\mathfrak{p}\notin T}\mathbb{Z}/n\mathbb{Z}, \quad a \mapsto \mathrm{ord}_\mathfrak{p}(a) \bmod n.$$

З іншого боку, група N вкладається в точну послідовність

$$0 \to U_T/U_T^n \to N \to (C_T)_n. \tag{2}$$

Справді, нехай C_T – група з точної послідовності (1) і нехай $a \in N$. Тоді $n|\mathrm{ord}_\mathfrak{p}(a)$ для всіх $\mathfrak{p} \notin T$. Поставивши у відповідність елементу $a \in N$ клас елемента $\left(\frac{\mathrm{ord}_\mathfrak{p}(a)}{n}\right)$ в C_T, одержуємо коректно визначене відображення $N \to$ $\to (C_T)_n$ з ядром U_T/U_T^n.

З точної послідовності (2) випливає твердження леми 4. $\diamondsuit$

Для доведення теореми 2 залишається довести скінченність груп U_T/U_T^n і $(C_T)_n$ для цілого замикання кільця $k[x]$ многочленів над квазіскінченним полем k у скінченному розширенні L поля $k(x)$. З результатів [3, розд. 2, §7] випливає, що група U_T/k^* є скінченно породженою. Тоді скінченність групи U_T/U_T^n випливає з такої леми.

Лема 5. *Нехай k – квазіскінченне поле. Тоді група k^*/k^{*n} є скінченною для всіх $n \in \mathbb{N}$.*

Д о в е д е н н я. $|k^*/k^{*n}| = |H^1(G, \mu_n)| = |H^0(G, \mu_n)| = |\mu_n(k)|$ згідно з лемою 3 [5, с. 322]. ◊

Доведемо тепер скінченність групи $(C_T)_n$.

Розглянемо для цього наступну комутативну діаграму з точними рядками [6, с. 297]:

$$\begin{array}{ccccccccc} (1) & \longrightarrow & k^* & \longrightarrow & k(X)^* & \longrightarrow & \mathrm{Div}^0(X) & \xrightarrow{\mathrm{cl}} & \mathrm{Pic}^0(X) & \longrightarrow & (0) \\ & & \downarrow & & \| & & \downarrow \mathrm{res} & & \downarrow \varphi & & \\ (1) & \longrightarrow & U(B) & \longrightarrow & k(X)^* & \longrightarrow & \mathrm{Div}(B) & \longrightarrow & C(B) & \longrightarrow & (1), \end{array} \tag{3}$$

де X – неособлива повна крива, відповідна полю L; $\mathrm{Div}^0(X)$ – підгрупа вільної абелевої групи над множиною нормувань, що складається з елементів степеня 0; $\mathrm{Div}(B)$ – вільна абелева група над множиною нормувань, кільця яких містять B; $\mathrm{Pic}^0(X)$ – якобіан кривої X; cl – фактор-відображення, res – відображення обмеження.

Відомо, що коядро гомоморфізму φ є скінченним (див. [6, VIII, Prop. 9.2]). З діаграми (3) отримуємо наступну комутативну діаграму з точними рядками:

$$\begin{array}{ccccccccc} (1) & \longrightarrow & \mathrm{Pic}^0(X)/\mathrm{Ker}(\varphi) & \longrightarrow & C(B) & \longrightarrow & \mathrm{Coker}(\varphi) & \longrightarrow & (0) \\ & & \downarrow \theta_1 & & \downarrow \theta_2 & & \downarrow \theta_3 & & \\ (1) & \longrightarrow & \mathrm{Pic}^0(X)/\mathrm{Ker}(\varphi) & \longrightarrow & C(B) & \longrightarrow & \mathrm{Coker}(\varphi) & \longrightarrow & (0), \end{array} \tag{4}$$

де вертикальні стрілки є множеннями на n.

З діаграми (4) за лемою про змію отримуємо наступну точну послідовність:

$$(0) \to (\mathrm{Pic}^0(X)/\mathrm{Ker}(\varphi))_n \to C_n(B) \to \mathrm{Ker}(\theta_3).$$

Звідси випливає, що для доведення скінченності групи $C_n(B)$ досить довести скінченність групи $(\mathrm{Pic}^0(X)/\mathrm{Ker}(\varphi))_n$. Розглянемо ще одну комутативну діаграму з точними рядками:

$$\begin{array}{ccccccccc} (1) & \longrightarrow & \mathrm{Ker}(\varphi) & \longrightarrow & \mathrm{Pic}^0(X) & \longrightarrow & \mathrm{Pic}^0(X)/\mathrm{Ker}(\varphi) & \longrightarrow & (0) \\ & & \downarrow \sigma_1 & & \downarrow \sigma_2 & & \downarrow \sigma_3 & & \\ (1) & \longrightarrow & \mathrm{Ker}(\varphi) & \longrightarrow & \mathrm{Pic}^0(X) & \longrightarrow & \mathrm{Pic}^0(X)/\mathrm{Ker}(\varphi) & \longrightarrow & (0), \end{array}$$

де знову вертикальні стрілки є множеннями на n.

За лемою про змію звідси одержуємо точну послідовність

$$(\mathrm{Pic}^0(X))_n \longrightarrow (\mathrm{Pic}^0(X)/\mathrm{Ker}(\varphi))_n \longrightarrow \mathrm{Coker}(\sigma_1).$$

Кількість елементів групи $(\mathrm{Pic}^0(X))_n$ є скінченною і залежить від роду кривої [4], а скінченність групи $\mathrm{Coker}(\sigma_1)$ випливає зі скінченної породженості групи $\mathrm{Ker}(\varphi)$. Тому й група $(\mathrm{Pic}^0(X)/\mathrm{Ker}(\varphi))_n$ є скінченною, що завершує доведення скінченності групи $C_n = C_n(B)$. Тепер, знову застосовуючи лему про змію до точної послідовності

$$\oplus_{\mathfrak{p} \in T} \mathbb{Z} \to C(B) \to C_T(B) \to 0$$

(див. [3, §7]), одержуємо скінченність групи $(C_T)_n$, а тому й скінченність групи Зельмера $\mathcal{S}^{(n)}(E/k(X))$. ◊

1. *Алгебраическая* теория чисел / Под ред. Дж. Касселса, А. Фрелиха. – М: Мир, 1969. – 483 с.
2. *Касселс Дж.* Диофантовы уравнения со специальным рассмотрением эллиптических кривых // Математика (Период. сб. пер. иностр. статей). – 1968. – 12:1; 12:2. – С. 113–158; 3–48.
3. *Ленг С.* Основы диофантовой геометрии. – М.: Мир, 1986. – 446 с.
4. *Мамфорд Д.* Абелевы многообразия. – М.: Мир, 1971. – 299 с.
5. *Платонов В. П., Рапинчук А. С.* Алгебраические группы и теория чисел. – М.: Мир, 1991. – 654 с.
6. *Lorenzini D.* An invitation to arithmetic geometry. – Providence: Amer. Math. Soc., 1996. – 397 p.
7. *Milne J. S.* Elliptic curves. Course Notes. – 1996. – http:/www.jmilne.org/math/. – 158 p.
8. *Serre J.-P.* Corps locaux. – Paris: Hermann, 1962. – 247 p.
9. *Tate J.* The arithmetic of elliptic curves // Invent.Math. – 1974. – **23**. – P. 179–206.

О ГРУППЕ ЗЕЛЬМЕРА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Пусть E *– эллиптическая кривая, определенная над полем алгебраических функций от одной переменной с квазиконечным полем констант* k *. Пусть* n *– натуральное число,* $(n, \mathrm{char} k) = 1$ *. Тогда группа Зельмера* $S^n(E/K)$ *конечна.*

ON THE SELMER GROUP OF ELLIPTIC CURVE

Let E *be an elliptic curve defined over an algebraic function field in one variable over quasifinite constant field* k *. Let* n *be a positive integer,* $(n, \mathrm{char} k) = 1$ *. Then the Selmer group* $S^n(E/K)$ *is finite.*

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

Одержано
09.09.03