УДК 513.6

В.І.Андрійчук

ДЕЯКІ ПИТАННЯ, ЗВ"ЯЗАНІ З ДОБУТКОМ ТЕЙТА-ШАФАРЕВИЧА В ЕЛІПТИЧНИХ КРИВИХ НАД ПСЕВДОЛОКАЛЬНИМИ ПОЛЯМИ

Нехай A – еліптична крива, визначена над псевдолокальним полем k, тобто над повним відносно дискретного нормування полем k з псевдоскінченним, за Аксом [5], полем лишків $\varkappa$. Вважатимемо, що $char\,\varkappa \neq 2,3$.

Взаємодія фільтрацій. У праці [2] визначені зростаюча фільтрація $(H^1(k,A))_n^n, n\in\mathbb{Z}, n\geq -1$ групи головних однорідних просторів $H^1(k,A)$ еліптичної кривої A над загальним локальним полем k і спадна фільтрація $A_k^n, n\in\mathbb{Z}, n\geq -1$ групи A_k – k – раціональних точок кривої A і доведена теорема про їх взаємодію при добутку Тейта-Шафаревича у випадку локального поля k, а для кривих з мультиплікативною редукцією й у випадку довільного загального локального поля k.

Доведемо аналог теореми про взаємодію фільтрацій для еліптичних кривих, визначених над псевдолокальним полем k.

Нехай $[(H^1(k,A))^*]^n$ – група характерів дискретної групи $H^1(k,A)$, тривіальних на підгрупі $(H^1(k,A))_n^n$, $\omega_k : A_k \longrightarrow (H^1(k,A))^*$ – гомоморфізм, індукований добутком Тейта-Шафаревича. Існує така теорема.

Теорема І. $\omega_k(A_k^n)\subset[(H^1(k,A))^*]^n$ для всіх $n\in\mathbb{Z}, n\geq -1$.

Доведення. Нехай l/k – скінченне розширення Галуа поля k, A_l – група l – раціональних точок кривої A, $\mathcal{Y}$ – група Галуа розширення l/k. Для $n\in\mathbb{Z}, n\geq -1$ нехай $\mathcal{Y}^n$ – n підгрупа верхньої фільтрації [1] групи $\mathcal{Y}$.

Згідно з працею [2] досить показати, що для довільного скінченного розширення Галуа l/k, для якого $\mathcal{Y}^n=\{1_{\mathcal{Y}}\}$, має місце $N_{\ell/k} A_\ell \supset A_k^n$ ($N_{\ell/k}$ - норменний гомоморфізм $\mathcal{Y}$ - модуля A_ℓ, $n \in \mathbb{Z}$, $n \geq -1$).

Нехай A - крива з невиродженою редукцією. При $n=-1$ доводити не потрібно. Якщо $n=0$, то розширення ℓ/k нерозгалужене. Отже (див. лему I [1]), тейтівські когомології $H^i(\mathcal{Y}, A_\ell)$ тривіальні. Зокрема, $H^0(\mathcal{Y}, A_\ell)=0$. Це означає, що $N_{\ell/k} A_\ell = A_k = A_k^0$, а для $n \geq 1$ твердження $N_{\ell/k} A_\ell \supset A_k^n$ доведено О.М.Введенським [2] в ситуації довільного загального локального поля k.

Доведення теореми I для кривих типу (b), за Нероном [8], редукується до доведення для кривих з мультиплікативною редукцією [2], але при доведенні рівності $N_{\ell/k} A_\ell^0 = A_k^0$ замість підрахунку кількості елементів в $\operatorname{Ker} N_{\ell/k}$ потрібно в нашому випадку використати те, що $H^1(\mathcal{Y}, \lambda^*) = 0$ з огляду на теорему Гільберта-90 (λ^* - мультиплікативна група поля лишків поля ℓ).

Залишається зауважити, що кожна еліптична крива, визначена над полем k, k - ізоморфна кривій типу (a), (b) або (c) за Нероном, а в праці [2] показано, як редукувати доведення у випадку кривої типу (c) до випадку кривої типу (a) або типу (b).

Порядок і показник. Теорема 2. Нехай V - головний однорідний простір для еліптичної кривої A над псевдолокальним полем k. Тоді порядок V дорівнює його показнику.

Доведення. Використовуючи міркування С.Ліхтенбаума [7] і О.М.Введенського [5], розглянемо комутативну діаграму з точними стрічками та стовпчиками

$$
\begin{tikzcd}
 & Br\,k \arrow[r, "1"] & Br\,k & \\
0 \arrow[r] & {[Pic_0(V)]^G} \arrow[r] \arrow[u, "\psi_1"] & {[Pic(V)]^G} \arrow[r] \arrow[u, "\psi_2"] & \mathbb{Z} \\
0 \arrow[r] & {[Div_0(V)]^G} \arrow[r] \arrow[u] & {[Div(V)]^G} \arrow[r] \arrow[u] & \mathbb{Z} \arrow[u]
\end{tikzcd}
$$

Тут $G = Gal\,(k_s/k)$ – група Галуа сепарабельного замикання k_s поля k, $Div\,(V)$ – група k_s – раціональних дивізорів на V, $Pic(V)$ – факторгрупа $Div(V)$ за модулем лінійної еквівалентності. $Div(V)$ і $Pic_0(V)$ – відповідні групи дивізорів нульового степеня. X^G – підмодуль G – інваріантних елементів G – модуля X. Гомоморфізми ψ_1 і ψ_2 визначені у праці [7]. Інші позначення та гомоморфізми стандартні.

Порядок (відп. показник) V дорівнює [7] індексу образу $[Pic(V)]^G$ (відп. $[Div(V)]^G$) в $\mathbb{Z}$. Нехай порядок V дорівнює n. Тоді існує $D \in [\,Pic\,(V)]^G$ з $deg\,D = n$. Рівність порядку і показника V випливає з двох фактів [7]

$$\psi_1([Pic_0(V)]^G) = \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}\,, \tag{I}$$

$$\psi_2(D) \subset \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}\,. \tag{2}$$

Доведемо (I). Нагадаємо [7], що $Im\,\psi_1$ – результат добутку Тейта-Шафаревича класу V з усією групою A_k, k – раціональних точок кривої A. Нехай $\psi_1([Pic_0(V)]^G) = \frac{1}{m}\mathbb{Z}/\mathbb{Z}$, де m/n . Якщо $W = mV$ в $H^1(k,A)$, то $\psi_q([Pic_s(V)]^G)=0$. З невиродженості зліва добутку Тейта-Шафаревича [1] випливає, що $W=0$ в $H^1(k,A)$. Отже, $m=n$.

Доведення (2) Ліхтенбаума [7] не використовує специфіки локальних полів і придатне для довільних загальних локальних полів.

Нетривіальність двовимірних когомологій Галуа і ядра справа в добутку Тейта-Шафаревича. Нехай $\varkappa$ – псевдоскінченне поле, що містить як поле абсолютних чисел алгебраїчне замикання $\overline{\mathbb{Z}/p\mathbb{Z}}$ простого поля $\mathbb{Z}/p\mathbb{Z}$ (відносно цієї можливості див. [2]). Нехай $k = \varkappa((t))$ – поле формальних степеневих рядів від t з коефіцієнтами з поля $\varkappa$.

Нехай $\mathfrak{A}$ – еліптична крива, Вейєрштрасове рівняння якої має своїми коефіцієнтами елементи з $\mathbb{Z}/p\mathbb{Z}$. Розглянемо криву A над k , Вейєрштрасове рівняння якої збігається з рівнянням для $\mathfrak{A}$. Тоді A – крива з невиродженою редукцією. $H^2(k,A)$ – група двовимірних когомологій Галуа для A над k .

Теорема 3. $H^2(k,A) \neq 0$.

Доведення. Нехай q – просте число, $q \neq p$, $n \in \mathbb{Z}$, $n \geq 1$, A' – редукція кривої A (тобто крива $\mathfrak{A}$, розглянута над $\varkappa$). Група $A'_{\varkappa}$ – $\varkappa$ – раціональних точок кривої A' містить всі точки порядку q^n на A' . Справді, $\mathfrak{A}_{q^n} \subset \mathfrak{A}_{\mathbb{Z}/p\mathbb{Z}} \subset A'_{\varkappa}$. Оскільки $A'_{\varkappa} \subset A_k$, то ${}_{q^n}(A_k) \simeq (\mathbb{Z}/q^n\mathbb{Z})$ з тривіальною дією операторів з $Gal(k_s/k)$. Отже, для q – компоненти $H^2(k,A)$ маємо, використовуючи результати праці [7]

$$H^2(k,A)(q) = \varinjlim H^2(k, A_{q^n}) = \varinjlim H^2(k,(\mathbb{Z}/q^n\mathbb{Z})^2) \simeq (\mathbb{Q}_q/\mathbb{Z}_q)^2.$$

($\mathbb{Q}_q$ (відп. $\mathbb{Z}_q$) – група q – адичних (відп. цілих q – адичних) чисел).

Теорема 4. Ядро справа в добутку Тейта-Шафаревича в еліптичних кривих над псевдолокальними полями може бути нескінченним.

Доведення. Нехай A – крива, використана при доведенні теореми 3. Припустимо додатково, що інваріант Хассе редукції кривої A дорівнює нулю. Ядро справа містить підгрупу універсальних норм $D_k = \bigcap N_{\ell/k} A_\ell$ (перетин береться по всіх скінченних розширеннях Галуа ℓ/k). Нескладне обчислення показує, що група D_k містить у свою чергу групу $\mathfrak{A}_{\overline{\mathbb{Z}/p\mathbb{Z}}}$, що й завершує доведення.

Автор висловлює подяку О.М.Введенському за постановку задач і допомогу при їх розв"язанні.

Список літератури: І. Андрийчук В.И. Об эллиптических кривых над псевдолокальными полями. – Мат. сб., 1979, т. 110, № 1, с. 88-101. 2. Введенский О.Н. О локальных "полях классов" эллиптических кривых. Изв. АН СССР. Сер. мат., 1973, 37, с. 20-88. 3. Введенський О.М. Підгрупи норм у еліптичних кривих, визначених над локальним полем. – Укр. мат. журн., 1970, т. 20, № 4. Серр Ж.-П. Когомологии Галуа. – М.: Мир, 1968. – 235 с. 5. Ax J. The elementary theory of finite fields. – Ann. Math., 1968, 80, N2, p.245-255. 6. Artin E, Tate J. Class field theory. Harvard, 1961. - 175p. 7. Lichtenbaum S. The period-index problem for elliptic curves. - Amer. J. Math, 1968, 90, N4, p.981-992. 8. Neron A. Modeles minimaux des varietes abeliennes sur les corps locaux et globaux. Publ. Math IHES, 1964, N21, p.341-356.

Стаття надійшла до редколегії 05.03.84