УДК 513.6

О порядке и показателе главного однородного пространства для эллиптической кривой над общим локальным полем

В. И. Андрийчук

Под общим локальным полем, следуя Артину — Тейту [1], будем понимать полное дискретно нормированное поле с квазиконечным полем вычетов.

С. Ленг и Дж. Тейт [2] привели пример главного однородного пространства над общим локальным полем характеристики 0, для которого порядок не равен показателю [3]. Цель этой заметки — привести аналогичный пример для случая, когда квазиконечное поле вычетов имеет положительную характеристику.

Известно, что И. Р. Шафаревич [3] и С. Лихтенбаум [4] показали, что для локальных полей, т. е. для полных дискретно нормированных полей с конечным полем вычетов, порядок главного однородного пространства над эллиптической кривой, определенной над локальным полем, равен его показателю (для p-компоненты в характеристике p основного поля это было доказано в [5]).

Для построения примера рассмотрим, следуя О. Н. Введенскому [6], некоторое специальное общее локальное поле и некоторую эллиптическую кривую над ним. Пусть K — поле формальных степенных рядов от одного неизвестного, коэффициенты которых являются элементами некоторого алгебраически замкнутого поля характеристики $p > 3$. Для поля K, как это следует из результатов, приведенных Ж.-П. Серром [7], существует расширение Галуа, группа Галуа которого изоморфна произведению всех групп Z_q, когда q пробегает все простые числа. Поэтому существует [7] подполе $\varkappa$ (содержащее K) алгебраического замыкания $\overline{K}$ поля K, являющееся квазиконечным. Возьмем за наше общее локальное поле полное дискретно нормированное поле k с этим квазиконечным полем вычетов $\varkappa$.

Пусть $\mathfrak{A}$ — эллиптическая кривая над K, уравнение которой в вейерштрассовой форме имеет своими коэффициентами элементы поля коэффициентов наших формальных степенных рядов, т. е. $\mathfrak{A}$ определена над этим последним полем. Будем считать, что инвариант Хассе кривой $\mathfrak{A}$ отличен от нуля. Рассмотрим теперь эллиптическую кривую A над k, редукцией которой есть $\mathfrak{A}$.

Пусть q — простое число, отличное от характеристики p поля вычетов $\varkappa$.

Т е о р е м а. *Существует главное однородное пространство V над A с порядком q и показателем q^2.*

Д о к а з а т е л ь с т в о. Заметим, что группа A_q всех точек порядка q на A содержится в A_k и что $A_k/qA_k = 0$.

Действительно, первый факт отмечен в работе О. Н. Введенского [6], а второй следует из того, что умножение на q в ядре редукции — подгруп-

пе Лютц — является изоморфизмом, а для группы рациональных над $\varkappa$ точек редукции $A'_\varkappa$ имеем $A'_\varkappa/qA'_\varkappa = 0$ ввиду [6].

Действительно, соответствующая куммеровской точной последовательности умножения на q в $\mathfrak{A}$

$$0 \to \mathfrak{A}_q \to \mathfrak{A} \xrightarrow{q} \mathfrak{A} \to 0$$

($\mathfrak{A}_q$ — подгруппа точек порядка q на $\mathfrak{A}$) точная последовательность когомологии Галуа

$$\mathfrak{A}_\varkappa \xrightarrow{q} \mathfrak{A}_\varkappa \to \mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A}_q) \to \mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A}) \xrightarrow{q} \mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A})$$

показывает, что умножение на q в $\mathfrak{A}_\varkappa$ является эпиморфизмом, ибо $\mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A}_q) \cong (Z/qZ)^2$ в силу предыдущих замечаний, а $\mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A})$ имеет подгруппой $(Z/qZ)^2$, ибо редукция $\mathfrak{A}'$ есть прямое слагаемое $\mathfrak{A}$ в категории $\mathrm{Gal}\ (\bar{\varkappa}/\varkappa)$-модулей.

Пусть l/k — расширение Галуа с группой Галуа $(Z/qZ)^2$ (относительно этой возможности см. [7]). Ясно, что все предыдущие рассуждения имеют место и для поля l, поэтому $A_l/qA_l = 0$. Рассмотрим индуцированную точной куммеровской последовательностью умножения на q в A коммутативную диаграмму є точными строчками

$$\begin{array}{ccccc} 0 \to & \mathcal{H}^1(k, A_q) & \to & \mathcal{H}^1(k, A)_q & \to 0 \\ & \mathrm{res}\ \downarrow & & \mathrm{res}\ \downarrow & \\ 0 \to & \mathcal{H}^1(l, A_q) & \to & \mathcal{H}^1(l, A)_q & \to 0. \end{array}$$

Очевидно, что ядро R гомоморфизма в правом столбце состоит из группы всех главных однородных пространств над A порядка q, которые расщепляются в l, что в свою очередь означает, что показатель их есть делитель q^2. Ясно, что

$$R \cong \mathrm{Hom}\ (\mathrm{Gal}\ (l/k),\ A_q) \cong (Z/qZ)^4.$$

Поле l имеет $q+1$ подполе степени q над k. Для каждого из этих подполей l_1 группа R_1 главных однородных пространств над A порядка q, которые расщепляются в l_1, изоморфна $(Z/qZ)^2$. Значит, общее число главных однородных пространств V над A порядка q и показателя q не превышает $(q+1)q^2 - q$. Так как $q^4 > q^3 + q^2 - q$, то найдется главное однородное пространство V над A порядка q и показателя, который делит q^2 и не совпадает с q. Теорема доказана.

Автор выражает искренную благодарность О. Н. Введенскому за руководство этой работой.

ЛИТЕРАТУРА

1. E. Artin, J. Tate, Class Field Theory, Harvard, 1961.
2. S. Lang, J. Tate, Principal Homogenous Spaces over Abelian Varieties, Amer. J. of Math., vol. 80, n. 3, 1958.
3. И. Р. Шафаревич, Показатели эллиптических кривых, ДАН СССР, т. 114, № 4, 1957.
4. S. Lichtenbaum, The Period — index Problem for Elliptic Curves, Amer. J. of Math., vol. 90, № 4, 1968.
5. О. Н. Введенский, Подгруппы норм в эллиптических кривых, определенных над локальным полем, УМЖ, т. 22, № 4, 1970.
6. О. Н. Введенский, О локальных «полях классов» эллиптических кривых, Изв. АН СССР, сер. матем., т. 37, № 1, 1973.
7. J.-P. Serre, Corps locaux, Paris, Hermann, 1962.

Поступила 5.III 1973 г.
Львовский государственный университет

пе Лютц — является изоморфизмом, а для группы рациональных над $\varkappa$ точек редукции $A'_\varkappa$ имеем $A'_\varkappa/qA'_\varkappa = 0$ ввиду [6].

Действительно, соответствующая куммеровской точной последовательности умножения на q в $\mathfrak{A}$

$$0 \to \mathfrak{A}_q \to \mathfrak{A} \xrightarrow{q} \mathfrak{A} \to 0$$

($\mathfrak{A}_q$ — подгруппа точек порядка q на $\mathfrak{A}$) точная последовательность когомологии Галуа

$$\mathfrak{A}_\varkappa \xrightarrow{q} \mathfrak{A}_\varkappa \to \mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A}_q) \to \mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A}) \xrightarrow{q} \mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A})$$

показывает, что умножение на q в $\mathfrak{A}_\varkappa$ является эпиморфизмом, ибо $\mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A}_q) \cong (Z/qZ)^2$ в силу предыдущих замечаний, а $\mathcal{H}^1(\mathrm{Gal}\ (\bar{\varkappa}/\varkappa),\ \mathfrak{A})$ имеет подгруппой $(Z/qZ)^2$, ибо редукция $\mathfrak{A}'$ есть прямое слагаемое $\mathfrak{A}$ в категории $\mathrm{Gal}\ (\bar{\varkappa}/\varkappa)$-модулей.

Пусть l/k — расширение Галуа с группой Галуа $(Z/qZ)^2$ (относительно этой возможности см. [7]). Ясно, что все предыдущие рассуждения имеют место и для поля l, поэтому $A_l/qA_l = 0$. Рассмотрим индуцированную точной куммеровской последовательностью умножения на q в A коммутативную диаграмму є точными строчками

$$\begin{array}{ccccc} 0 \to & \mathcal{H}^1(k, A_q) & \to & \mathcal{H}^1(k, A)_q & \to 0 \\ & \mathrm{res}\ \downarrow & & \mathrm{res}\ \downarrow & \\ 0 \to & \mathcal{H}^1(l, A_q) & \to & \mathcal{H}^1(l, A)_q & \to 0. \end{array}$$

Очевидно, что ядро R гомоморфизма в правом столбце состоит из группы всех главных однородных пространств над A порядка q, которые расщепляются в l, что в свою очередь означает, что показатель их есть делитель q^2. Ясно, что

$$R \cong \mathrm{Hom}\ (\mathrm{Gal}\ (l/k),\ A_q) \cong (Z/qZ)^4.$$

Поле l имеет $q+1$ подполе степени q над k. Для каждого из этих подполей l_1 группа R_1 главных однородных пространств над A порядка q, которые расщепляются в l_1, изоморфна $(Z/qZ)^2$. Значит, общее число главных однородных пространств V над A порядка q и показателя q не превышает $(q+1)q^2 - q$. Так как $q^4 > q^3 + q^2 - q$, то найдется главное однородное пространство V над A порядка q и показателя, который делит q^2 и не совпадает с q. Теорема доказана.

Автор выражает искренную благодарность О. Н. Введенскому за руководство этой работой.

ЛИТЕРАТУРА

1. E. Artin, J. Tate, Class Field Theory, Harvard, 1961.
2. S. Lang, J. Tate, Principal Homogenous Spaces over Abelian Varieties, Amer. J. of Math., vol. 80, n. 3, 1958.
3. И. Р. Шафаревич, Показатели эллиптических кривых, ДАН СССР, т. 114, № 4, 1957.
4. S. Lichtenbaum, The Period — index Problem for Elliptic Curves, Amer. J. of Math., vol. 90, № 4, 1968.
5. О. Н. Введенский, Подгруппы норм в эллиптических кривых, определенных над локальным полем, УМЖ, т. 22, № 4, 1970.
6. О. Н. Введенский, О локальных «полях классов» эллиптических кривых, Изв. АН СССР, сер. матем., т. 37, № 1, 1973.
7. J.-P. Serre, Corps locaux, Paris, Hermann, 1962.

Поступила 5.III 1973 г.
Львовский государственный университет