УДК 513.6

©2012. **Н. М. Глазунов**

КВАЗИЛОКАЛЬНЫЕ ПОЛЯ КЛАССОВ ЭЛЛИПТИЧЕСКИХ КРИВЫХ И ФОРМАЛЬНЫЕ ГРУППЫ. I.

Исследуются норменные подгруппы одномерных формальных групп высоты редукции больше или равной три над кольцом целых локального или квазилокального поля.

Ключевые слова: *локальная теория полей классов, высота редукции формальной группы, группа Галуа, группы ветвления, норменный гомоморфизм, норменная подгруппа.*

1. Введение. В [1, 2] построены основы локальной теории полей классов эллиптических кривых. Автору настоящей работы О.Н. Введенским было предложено исследовать ситуацию с обобщением классического вычисления кондуктора локальной теории полей классов на одномерные формальные группы высоты редукции ≥ 3 (для одномерных формальных групп высоты редукции 2 эта задача решена в [1]). Поставленная задача была решена автором, а результаты кратко изложены в [3]. В настоящей работе содержится доказательство этих результатов.

Основные понятия и результаты, связанные с линейными алгебраическими группами и формальными группами изложены в [2, 4, 5]. Поэтому в работе представлен только необходимый для понимания исследуемой проблематики математический аппарат: теории локальных полей (п. 2), теории алгебраических групп и конечных групповых схем (п. 3), теории квазиалгебраических и проалгебраических групп (п. 4). Результаты автора, связанные с вычислением аналога кондуктора локальной теории полей классов для одномерных формальных групп высоты редукции больше, чем 2 изложены в п. 5 (случай одномерных формальных групп высоты редукции 2 исследован О.Н. Введенским в [6]).

2. Локальные поля. Поле K называется локальным [7], если оно полно в топологии, определяемой его показателем ν_K и если его поле вычетов конечно. Далее предполагается, что показатель ν_K нормализован, т.е. гомоморфизм $\nu_K^* \to \mathbb{Z}$ сюръективен. Такие поля имеют следующую структуру. Поле K характеристики ноль является конечным расширением p-адического поля $\mathbb{Q}_p$, которое есть пополнение поля рациональных чисел относительно p-адического показателя. Если $[K : \mathbb{Q}_p] = n$, то $n = ef$, где f – степень класса вычетов (т.е. $f = [k : \mathbb{F}_p]$) и $e = \nu_K(p)$. Поле K характеристики $p > 0$ изоморфно полю $k((T))$ формальных степенных рядов, где T – униформизирующий параметр.

Пусть L – конечное расширение локального поля K, l и k – их поля вычетов, $p = char\ k$, а $e_{L/K}$ – индекс ветвления L над K. Расширение L/K называется:

1) неразветвленным, если $e_{L/K} = 1$, а расширение l/k сепарабельно;

2) слабо разветвленным, если $p \nmid e_{L/K}$, а расширение l/k сепарабельно;

в) дико разветвленным, если $e_{L/K} = [L : K] = (char\ k)^s$ $(s \geq 1)$.

Обозначим через $Tr(L/K)$ и $Norm\ L/K$, соответственно, след и норму расшире-

ния L/K (будем использовать запись $Tr(L)$ и $Norm\, L$, если ясно, о каком расширении идет речь), а через K_{nr} – максимальное неразветвленное расширение поля K (в фиксированном алгебраическом замыкании Ω поля K) с полем вычетов k_S, которое является алгебраическим замыканием поля k.

Локальное поле с алгебраически замкнутым полем вычетов называют квазилокальным [1].

Лемма 1. *Если локальное поле K содержит примитивный корень ξ_p p-й степени из единицы, то $\nu_K(\xi_p - 1) = \frac{e}{p-1}$, где $e = \nu_K(p)$, а $p = char\ k$.*

Доказательство. Если ξ_p – примитивный корень p-й степени из единицы, то $\xi_p^p - 1 = 0$ и ξ_p есть корень неприводимого над K многочлена $x^{p-1} + \cdots + x + 1$. Тогда $\xi_p^p - 1$ – корень многочлена $(x+1)^{p-1} + \cdots + (x+1) + 1 = x^{p-1} + pP(x) + p$, где $P(x)$ – многочлен степени не выше $p-2$. Значение показателя p на корне такого многочлена равно $\frac{e}{p-1}$, т.е. $\nu_K(\xi_p - 1) = \frac{e}{p-1}$. $\square$

Следствие 1. *Если локальное поле K содержит примитивный корень p-й степени из единицы, то $e = \nu_K(p)$ делится на $p-1$.*

Пусть L/K – конечное расширение Галуа с группой Галуа $\mathcal{G}(L/K)$ (будем использовать запись $\mathcal{G}$, если это не вызывает недоразумений), а $\mathcal{O}_K$ – кольцо целых поля K. Определим группы ветвления $\mathcal{G}_i$ $(i = -1, 0, 1, \dots)$ равенством

$$\mathcal{G}_i = \{\sigma \in \mathcal{G} | \nu_L(\sigma a - a) \geq i + 1 \text{ для всех } a \in \mathcal{O}_L\}.$$

Нетрудно проверить, что: 1) группы $\mathcal{G}_i$ являются нормальными делителями группы $\mathcal{G}$; 2) $\mathcal{G}_{-1} = \mathcal{G}$; 3) существует такое число m, что $\mathcal{G}_{i+1} \subset \mathcal{G}_i$ для всех $i = -1, 0, 1, \dots, m-2$ и $\mathcal{G}_m = 1$.

Нижняя и верхняя (Эрбрановская) нумерация групп ветвления может быть задана следующим образом. Пусть x $(x \geq -1)$ – вещественная переменная. Нижнюю нумерацию определим равенством $\mathcal{G}_x = \mathcal{G}_l$, где $l = \lceil x \rceil$. Обозначим через g_i порядок группы $\mathcal{G}_i$. Рассмотрим функцию

$$\varphi(x) = \begin{cases} x, & \text{если } -1 \leq x \leq 0 \\ \frac{1}{g_0}\left(g_1 + \cdots + g_m + (x-m)g_{m+1}\right), & \text{если } x \geq 0, \text{ где } m = \lfloor x \rfloor \end{cases}.$$

Функция $\varphi(x)$ непрерывна и строго возрастает. Следовательно, существует обратная функция $\psi(y)$ $(y \geq -1)$. Верхнюю нумерацию групп ветвления определим равенством $\mathcal{G}^{\varphi(x)} = \mathcal{G}_{\psi(y)}$, где $y = \varphi(x)$ и $x = \psi(y)$.

Обозначим через π_K – униформизирующий элемент поля K (т.е. $\nu_K(\pi_K) = 1$), а через $\mathfrak{m}_K = \pi_K \cdot \mathcal{O}_K$ – максимальный идеал кольца $\mathcal{O}_K$.

Пусть L/K – дико разветвленное расширение простой степени p. Определим дифференту $\mathcal{D}$ расширения L/K равенством

$$\mathcal{D} = (f'(\pi_L)), \tag{1}$$

где $f(x)$ – минимальный многочлен для π_L над K. Отметим, что

$$\mathfrak{D} \subset \mathfrak{A} \cdot \mathcal{D}^{-1} \Leftrightarrow Tr(\mathfrak{D}) \subset \mathfrak{A}, \tag{2}$$

где $\mathfrak{A}$ – дробный идеал в $\mathcal{O}_K$, а $\mathfrak{D}$ – дробный идеал в $\mathcal{O}_L$.

Пусть $m = \nu_L(\sigma\pi_L - \pi_L) - 1$, где σ – образующий элемент группы $\mathcal{G}(L/K)$. Тогда $f'(\pi_L) = \prod\limits_{\sigma \neq 1} (\pi_L - \sigma\pi_L)$ и $\nu_L(f'(\pi_L)) = (m+1)(p-1)$. Отсюда вытекает, что $\mathcal{D} = (\pi_L^{(m+1)(p-1)})$.

Лемма 2. *Для всех $n \geq 0$ истинно равенство*

$$Tr(\pi_L^n \cdot \mathcal{O}_L) = \pi_K^{y_0(n)} \cdot \mathcal{O}_K,$$

где $y_0(n) = \lfloor \frac{(m+1)(p-1)+n}{p} \rfloor$.

Доказательство. Положим $\mathfrak{D} = \pi_L^n \cdot \mathcal{O}_L$ и $\mathcal{D}^{-1} = \pi_L^{-(m+1)(p-1)} \cdot \mathcal{O}_L$ для идеалов из (2). Вычислим x в равенстве $\mathfrak{A} = \pi_L^x \cdot \mathcal{O}_L$ так, чтобы выполнялось равенство

$$\pi_L^n \cdot \mathcal{O}_L = \pi_L^x \cdot \mathcal{O}_L \cdot \pi_L^{-(m+1)(p-1)} \cdot \mathcal{O}_L. \tag{3}$$

Равенство (3) истинно при $x = (m+1)(p-1) + n$. Учитывая, что $Tr(\pi_L^n) \in \mathcal{O}_K$ и $\nu_L(\pi_K) = e$, получаем $Tr(\pi_L^n \cdot \mathcal{O}_L) = \pi_K^{\lfloor \frac{(m+1)(p-1)+n}{p} \rfloor} \cdot \mathcal{O}_K$. $\square$

Обозначим через $F(\mathfrak{m}_L) - Gal(L/K)$ модуль, задаваемый n-мерным групповым законом $F(X,Y)$ на произведении $\underbrace{\mathfrak{m}_L \times \cdots \times \mathfrak{m}_L}_{n \text{ раз}}$ максимальных идеалов кольца $\mathcal{O}_L$ любого конечного расширения Галуа L поля K. Определим гомоморфизм N модуля F_L в F_K формулой $N(a) = (a +_F \sigma_s a) +_F \cdots +_F \sigma_s a$, где $a +_F b$ – сложение точек в соответствии с групповой структурой модуля F_L, $a, b \in \mathfrak{m}_L$, $\mathcal{G} = Gal(L/K)$, $\sigma_s \in \mathcal{G}$ и $[\mathcal{G} : 1] = s$.

Пусть $p = char\ k$, $e = \nu_K(p)$ (отметим, что $e = \infty$, если характеристика поля K равна $p > 0$, и e – положительное число в противном случае), L/K – расширение Галуа простой степени q, а $f(x,y)$ – одномерный групповой закон над $\mathcal{O}_K$. Предположим, что $p > 0$.

Лемма 3. *Если $\Pi_s \in \pi_L^s \cdot \mathcal{O}_L$ и $s \geq 1$, то*

$$N(\Pi_s) \equiv Tr(\Pi_s) + \sum_{n=1}^{\infty} c_n (Norm\, \Pi_s)^n (mod\, Tr(\pi_L^{2s} \cdot \mathcal{O}_L)), \tag{4}$$

где $c_n \in \mathcal{O}_K$ – коэффициенты в p-й итерации группового закона.

Доказательство. Отметим, что:

1) если $f(x,y)$ – одномерный групповой закон над кольцом $\mathcal{O}_K$, то p-я итерация $[p]_f[T]$ имеет вид

$$[p]_f[T] = p(T + \dots) + \sum_{i=1}^{\infty} c_i T^{p^i}, \tag{5}$$

где многоточие обозначает неизвестные степени больше 1;

2) если в разложение в ряд выражения $t_1 +_f t_2 +_f \cdots +_f t_n$ входит одночлен $t_1^{\alpha_1} \dots t_q^{\alpha_q}$, то входят и одночлены $t_1^{\alpha_{\delta(1)}} \dots t_q^{\alpha_{\delta(q)}}$, где δ – произвольная перестановка чисел $1, \dots, q$.

Пусть $\mathcal{G} = Gal(L/K)$. Если $\omega = r_1 + r_2\sigma + \cdots + r_q\sigma^q$ – элемент групповой алгебры $\mathbb{Z}[\mathcal{G}]$, то положив $\Pi_s^\omega = \Pi_s^{r_1}(\sigma\Pi_s)^{r_2} \dots (\sigma^{q-1}\Pi_s)^{r_q}$, получим

$$N(\Pi_s) = \Pi_s +_f \sigma\Pi_s +_f \cdots +_f \sigma^{q-1}\Pi_s = \sum_{(r_1,\dots,r_q)} d_{r_1,\dots,r_q}\Pi_s^\omega,$$

где $d_{r_1,\dots,r_q} \in \mathcal{O}_K$ и суммирование идет по соответствующим ω. В силу симметрии, в разложение $N(\Pi_s)$ вместе с $d_{r_1,\dots,r_q}\Pi_s^\omega$ входят и $d_{r_1,\dots,r_q}\Pi_s^{\sigma^i\omega}$ $(i = 1, \dots, q-1)$. А так как из

$$\sigma^i\omega = \omega, \tag{6}$$

где i – одно из чисел $1, \dots, q-1$ вытекает, что $\omega = n(1 + \sigma + \cdots + \sigma^{q-1})$, то

$$N(\Pi_s) = \sum_{n=1}^{\infty} d_n(Norm\,\Pi_s)^n + \sum_{\omega} d_{r_1,\dots,r_q}\,Tr(\Pi_s^\omega), \tag{7}$$

где суммирование идет по ω, не удовлетворяющим равенству (6).

Если $r_1 + \dots r_q > 1$, то $Tr(\Pi_s^\omega) \subset Tr(\pi_L^{2s} \cdot \mathcal{O}_K)$. Следовательно,

$$N(\Pi_s) \equiv Tr(\Pi_s) + \sum_{n=1}^{\infty} d_n(Norm\,\Pi_s)^n (mod\, Tr(\pi_L^{2s} \cdot \mathcal{O}_K)). \tag{8}$$

Покажем, что в качестве d_n можно взять c_n из (5). Действительно, как c_n, так и d_n определены с точностью до $mod\ p$. Для c_n это вытекает из (5). Так как

$$pg(Norm\,\Pi_s)^n = Tr(g(Norm\,\Pi_s)^n) \in Tr(\pi_L^{2s} \cdot \mathcal{O}_L) \quad (g \in \mathcal{O}_K),$$

а члены из $N(\Pi_s)$, входящие в $Tr(\pi_L^{2s} \cdot \mathcal{O}_L)$, дают сумму $p(b_2T^2 + b_3T^3 + \dots)$ $(b_2, b_3, \dots \in \mathcal{O}_K)$, то в (8) можно заменить d_n на c_n. □

Замечание 1. В [6] такая лемма доказана для случая одномерных групповых законов, соответствующих эллиптическим кривым.

3. Алгебраические группы и групповые схемы. Рассмотрим основные понятия, относящиеся к классу многообразий, порождаемых приведенными отделимыми гладкими схемами $(X, \mathcal{O}_X)$ конечного типа над алгебраически замкнутым полем [8]. Приведенность означает, что для открытых множеств $U \subset X$ кольца $\mathcal{O}_X(U)$ не имеют нильпотентных элементов, а отделимость схемы определяется через понятия произведения и замкнутости схем. Произведение схем определяется как произведение объектов в категории схем, а в терминах морфизмов схем над базисной схемой S (например, если S – алгебраически замкнутое поле) – как расслоеное произведение этих морфизмов. Морфизм схем $\varphi : Y \to X$ называют замкнутым вложением, если каждая точка $x \in X$ имеет такую аффинную окрестность U, что схема $\varphi^{-1}(U)$ аффинна и гомоморфизм $\psi_U : \mathcal{O}_X(U) \to \mathcal{O}_Y(\varphi^{-1}(U))$ эпиморфен. В категории схем над S определен морфизм $(1,1) : X \to X \times_S X$, который называют диагональю. Схему X называют замкнутой, если морфизм ее диагонали – замкнутое вложение, и схемой над кольцом R, если задан морфизм схем $X \to Spec\ R$. Схему X над кольцом R

называют схемой конечного типа над R, если она имеет такое конечное покрытие $X = \bigcup U_i$ ($U_i = SpecA_i$), что все A_i – алгебры конечного типа над R. Так как любое кольцо есть алгебра над кольцом $\mathbb{Z}$, то любая схема является схемой над $\mathbb{Z}$.

Исследование алгебраических уравнений и алгебраических групп в конечных полях может быть охарактеризовано следующим образом [9]. Пусть X – схема конечного типа над $\mathbb{Z}$. Точку x схемы X называют замкнутой, если соответствующий ей идеал j_x максимален. Пусть $\widetilde{X}$ – множество замкнутых точек схемы X, $N(x)$ – число элементов поля вычетов $k(x)$ в точке $x \in \widetilde{X}$, а X_0 – алгебраическое многообразие над полем $\mathbb{F}_q$ ($q = p^n$). А. Гротендик определил для любого числа $l \neq p = char\ k$ группы l-адических когомологий $H^i(X, Q_l)$ и l-адических когомологий с компактным носителем [9], которые совпадают, если X – собственное многообразие. Пусть F – морфизм Фробениуса, отображающий точку $(x_1, \ldots, x_n)$ в точку $(x_1^q, \ldots, x_n^q)$, а F^* – геометрический Фробениус, определяемый по F при поднятии F до морфизма схем. Точки многообразий являются неподвижными точками отображения F^*.

Конечной групповой схемой [10,11] называют групповую схему, локально свободную ранга m над R. Такая групповая схема G определяется пучком локально свободных алгебр A ранга m над R. Структура групповой схемы задается гомоморфизмами $\mu : A \to \otimes_R A$, $\varepsilon : A \to R$ и автоморфизмом $i : A \to A$, задающими, соответственно, групповой закон, единицу и взятие обратного элемента, которые удовлетворяют известным аксиомам [4,9]. Если в алгебраической группе (или в групповой схеме) G фиксирована групповая структура S, то пишут G_S.

4. Квазиалгебраические и проалгебраические группы. Далее все группы, если не оговорено противное, предполагаются коммутативными. В настоящем разделе через K обозначено совершенное поле (алгебраически замкнутое поле), через p – его характеристическая экспонента. Все многообразия считаем определенными над K.

Известно, что в категории алгебраических групп над K существуют морфизмы, не являющиеся морфизмами в смысле алгебраических групп (т.е. категория алгебраических групп аддитивная, но не абелева).

Пример 1. Пусть $K = k$ – алгебраически замкнутое поле характеристики $p > 0$. Топологические пространства алгебраических групп X и Y (они обозначаются теми же буквами) задаются условием $X = Y = k$. Пусть групповая операция каждой из групп задана отображением $\mu(x, y) = x + y$ ($x, y \in k$). Рассмотрим гомоморфизм $\varphi : X \to Y$ алгебраических групп X и Y, определяемый формулой $\varphi(x) = x^p$. Как точечное отображение он взаимно-однозначен и как отображение абстрактных групп является изоморфизмом. Но как регулярное отображение многообразий изоморфизмом не является, так как соответствующий ему гомоморфизм колец $\varphi^* : k[Y] \to k[X]$, $\varphi^*(T) = T^p$, $k[X] = k[Y] = k[T]$ не является изоморфизмом.

Понятие квазиалгебраической группы [12] объединяет в один класс алгебраические группы, между которыми существуют биекции, которые могут и не быть изоморфизмами алгебраических групп.

Пусть G_S – алгебраическая группа и $\mathcal{O}$ – пучок функций на G_S. Если $q = p^n$ ($n \in \mathbb{Z}$), то обозначим через $\mathcal{O}^q$ пучок, сечения которого открытыми множествами

$U \in G$ – q-е степени сечений пучка $\mathcal{O}$ над U. Положим $\mathcal{O}^{p^{-\infty}} = \bigcup\limits_{n\in\mathbb{Z}} \mathcal{O}^{p^n}$. Если $q \geq 1$, то соответствующее пучку $\mathcal{O}^q$ многообразие G^q – алгебраическая группа.

Пусть G – группа. Если S – структура алгебраической группы на G, совместимая со структурой группы, то через G_S обозначают соответствующую алгебраическую группу, а через T_S и $\mathcal{O}_S$ – соответственно, топологию и пучок колец. В предположении, что под «морфизмом» понимается регулярное отображение алгебраических групп, истинно следующее утверждение ([12], стр. 6).

Предложение 1. Пусть S_1 и S_2 – структуры алгебраической глуппы на G, совместимые со структурой группы. Следующие условия эквивалентны:

(i) существует такая структура S_3, что тождественные отображения $S_3 \to S_1$ и $S_3 \to S_2$ – морфизмы;

(ii) существует такая структура S_4, что тождественные отображения $S_1 \to S_4$ и $S_2 \to S_4$ – морфизмы;

(iii) для произвольной положительной степени q числа p тождественное отображение $G_{S_1} \to G_{S_2}$ – морфизм алгебраических групп.

(iv) $T_{S_1} = N_{S_2}$ и $\mathcal{O}_{S_1}^{p^{-\infty}} = \mathcal{O}_{S_2}^{p^{-\infty}}$.

Пусть G – абстрактная группа, а S_1 и S_2 – структуры алгебраической группы на G, совместимые со структурой группы G. Говорят, что S_1 и S_2 эквивалентны, если они удовлетворяют условиям предложения 1. Квазиалгебраической группой, соответствующей группе G, называют класс эквивалентных структур алгебраической группы на G, совместимых со структурой группы G. Если G – квазиалгебраическая группа, то структуру алгебраической группы на G, выбранную из класса эквивалентных структур алгебраической группы на G, называют совместимой с квазиалгебраической структурой на G.

Истинно следующее утверждение ([12], стр. 8).

Предложение 2. Пусть G и G' – квазиалгебраические группы и $f : G \to G'$ гомоморфизм групп в теоретико-множественном смысле. Следующие условия эквивалентны:

a) на G и G' существуют такие структуры S и S' алгебраических групп, совместимые с квазиалгебраическими структурами, что $f : G \to G'$ – регулярное отображение алгебраических групп;

b) отображение f непрерывно, и если φ – сечение пучка $\mathcal{O}_{G'}^{p^{-\infty}}$ над открытым множеством U', то $\varphi \circ f$ – сечение пучка $\mathcal{O}_{G}^{p^{-\infty}}$ над открытым множеством $f^{-1}(U')$;

c) график отображения f есть замкнутая подгруппа в $G \times G'$.

Если G и G' – квазиалгебраические группы, то морфизмом из G в G' называют гомоморфизм $f : G \to G'$, удовлетворяющий условиям предложения 2. Объекты – квазиалгебраические группы, а также морфизмы между ними, удовлетворяют известным теоретико-категорийным свойствам [10]. Тем самым определена категория квазиалгебраических групп $\mathcal{QG}_K$, которая является абелевой по построению.

Замечание 2. Определение квазиалгебраической группы может быть следующим образом дано и в терминах групповых схем. Расширяем категорию алгебраи-

ческих групп до категории групповых схем над K. Так как мы рассматриваем только коммутативные группы, то ограничимся категорией коммутативных групповых схем $\mathcal{CG}_K$ над K. Пусть $H, G \in \mathcal{CG}_K$ и $\varphi : H \to G$ чисто несепарабельная изогения из H в G. Назовем H и G эквивалентными, если существует групповая схема $F \in \mathcal{CG}_K$ и чисто несепарабельные изогении $\psi : F \to H$ и $\tau : F \to G$. Квазиалгебраической группой является класс эквивалентных групповых схем.

Пример 2. По всякой алгебраической группе G можно каноническим образом определить квазиалгебраическую группу $G^{p^{-\infty}}$, структурным пучком которой является пучок $\mathcal{O}_G^{p^{-\infty}}$.

Проалгебраической группой называют группу G и такое непустое семейство $\mathcal{C}$ ее подгрупп, что для каждого $H \in \mathcal{C}$ множество G/H имеет структуру квазиалгебраической группы, причем выполнены следующие четыре аксиомы:

П1. Если $H, H' \in \mathcal{C}$, то $H \cap H' \in \mathcal{C}$.

П2. Пусть $H \in \mathcal{C}$. Подгруппа H', содержащая H и лежащая в $\mathcal{C}$ есть прообраз замкнутой подгруппы из G/H.

П3. Если $H, H' \in \mathcal{C}$ и $H \subset H'$, то $G/H \to G/H'$ – морфизм квазиалгебраических групп.

П4. Естественное отображение $G \to \varprojlim G/H$ – биекция G на проективный предел групп G/H $(H \in \mathcal{C})$.

Пример 3.

1. Любую квазиалгебраическую группу G можно каноническим образом наделить структурой проалгебраической группы: в качестве $\mathcal{C}$ достаточно выбрать множество замкнутых подгрупп группы G. Для каждого $H \in \mathcal{C}$ фактор-группа G/H имеет структуру квазиалгебраической группы, причем аксиомы П1-П4 выполнены.

2. Пусть G – компактная вполне несвязная топологическая группа, а $\mathcal{C}$ – множество открытых полугрупп в G. Если $H \in \mathcal{C}$, то фактор-группа G/H – конечная, и следовательно, является квазиалгебраической группой размерности ноль [10]. Аксиомы П1-П4 выполнены. Такую проалгебраическую группу называют проалгебраической группой размерности ноль.

Пусть G_1 и G_2 – проалгебраические группы с полными определяющими множествами $\mathcal{C}_1$ и $\mathcal{C}_2$. Морфизмом из G_1 в G_2 называют такой гомоморфизм $f : G_1 \to G_2$, что для каждого $H_2 \in \mathcal{C}_2$ имеет место $f^{-1}(H_2) \in \mathcal{C}_1$ и отображение из $G_1/f^{-1}(H_2)$ в G_2/H_2, определяемое по f, является морфизмом квазиалгебраических групп. Полученная таким способом категория $\mathtt{P}G_K$ проалгебраических групп над K является абелевой категорией [12]. Она эквивалентна прокатегории $Pro(QG_k)$.

Пусть G – квазиалгебраическая группа. Обозначим через G^0 связную компоненту единичного элемента группы G. Далее G^0 называется просто связной компонентой группы G. Пусть G – проалгебраическая группа с полным определяющим множеством $\mathcal{C}$. Для $H \in \mathcal{C}$ связная компонента $(G/H)^0$ фактор-группы G/H является замкнутой подгруппой в G/H, и если $H' \subset H$, то образ G/H' в G/H – это $(G/H)^0$. Поэтому можно положить $G/G_0 = \varprojlim (G/H)/(G/H)^0$. Фактор-группа G/G_0 обозначается через $\pi_0(G)$ и называется 0-й гомотопической группой проалгебраической

группы G.

Операция факторизации $\pi_0(G) = G/G_0$ определяет функтор $\pi_0 : \mathtt{P}G_K \to \mathtt{P}G_K^0$ из категории $\mathtt{P}G_K$ в категорию $\mathtt{P}G_K^0$ проалгебраических групп размерности ноль. Левые производные функторы функтора π_0 будем называть i-ми гомотопическими группами проалгебраической группы G и обозначать $\pi_i(G)$ (наличие в категории $\mathtt{P}G_K$ достаточного числа проективных объектов делает такое определение корректным). Фундаментальной группой группы G называют первую гомотопическую группу $\pi_1(G)$.

Группу $G \in \mathtt{P}G_K$ называют: 1) связной, если $G = G^0$; 2) односвязной, если $\pi_0(G) = 0$. В [12] доказаны следующие утверждения.

Предложение 3. Если G – проалгебраическая группа размерности ноль, то $\pi_i(G) = 0$ для всех $i \geq 1$.

Предложение 4. Пусть $G \in \mathtt{P}G_K$. Существуют такие связная и односвязная проалгебраическая группа $\overline{G}$ и морфизм $u : \overline{G} \to G$, что ядро и коядро u – проалгебраические группы размерности ноль. Пара $(\overline{G}, u)$ единственна с точностью до изоморфизма.

Пара $(\overline{G}, u)$ называется универсальной накрывающей группы G.

Замечание 3. Взятие универсальной накрывающей определяет ковариантный функтор «универсальное накрытие» из категории $\mathtt{P}G_K$ в категорию связных односвязных проалгебраических групп.

Рассмотрим вычисление фундаментальной группы в простейших случаях.

Пусть $G \in \mathtt{P}G_K$. Для каждого $n \in \mathbb{Z}$ отображение $x \to nx$ $(x \in G)$ является эндоморфизмом G, который будем обозначать $n : G \to G$. Истинно следующее утверждение.

Лемма 4. *Пусть G – связная проалгебраическая группа, а $n \in \mathbb{Z}$ взаимно просто с $p = char\ K$. Тогда морфизм $n : G \to G$ сюръективен.*

Пусть ${}_nG$ – ядро отображения $n : G \to G$, т.е. ${}_nG$ – подгруппа G, образованная такими $x \in G$, что $nx = 0$. Истинно следующее утверждение ([12], стр. 45).

Предложение 5. Пусть G – связная проалгебраическая группа, а l – простое число. Предположим, что морфизм $l : G \to G$ сюръективен. Тогда l-я компонента $\pi_1(G)_l$ группы $\pi_1(G)$ проективна и фактор-группа $\pi_1(G)_l/l\pi_1(G)_l$ изоморфна группе ${}_lG$.

Следствие 2. *В условиях предложения 5 предположим, что ${}_lG$ изоморфна $\mathbb{Z}/l\mathbb{Z}^{\mathcal{J}}$, где $\mathcal{J}$ – произвольное множество индексов. Тогда $\pi_1(G)_l$ изоморфна $(\mathbb{Z}_l)^{\mathcal{J}}$.*

Следствие 3. *Пусть $G \in \mathtt{P}G_K$ и l – простое, отличное от характеристики поля K. Тогда $\pi_1(G)_l = 0$ при $i \geq 2$ и $\pi_1(G)$ изоморфна произведению групп $\mathbb{Z}_l$.*

5. Теорема об ограниченности снизу норменных подгрупп. В настоящем разделе рассматриваются одномерные формальные группы любой натуральной высоты больше или равной 3, определенные над кольцом целых локального или квазилокального поля.

Пусть L/K – конечное расширение Галуа локального или квазилокального поля K с группой Галуа $\mathcal{G}$, $f(x, y)$ – одномерный групповой закон над кольцом целых $\mathcal{O}_K$

поля K. На максимальном идеале $\mathfrak{m}_L$ кольца целых $\mathcal{O}_L$ любого конечного расширения Галуа L поля K формальная группа f определяет $f(\mathfrak{m}_L)$–$\mathcal{G}$-модуль, который будем обозначать f_L.

Если K – квазилокальное поле и L/K – конечное расширение Галуа, то на группе f_L можно навести структуру проалгебраической группы. Обозначим такую группу через $\widetilde{f_L}$, а ее фундаментальную группу – через $\pi_1(\widetilde{f_L})$.

Определение. Пусть K – локальное (соответственно, квазилокальное) поле. Подгруппа $P \subset f_K$ (соответственно, $P' \subset \pi_1(\widetilde{f_K})$) называется норменной, если существует такое конечное расширение Галуа L/K, что $P = N_{L/K}(f_L)$ (соответственно, $P' = N_{L/K}(\pi_1(\widetilde{f_L}))$).

Теорема. *Для любого расширения Галуа L/K с такой группой Галуа $\mathcal{G}$, что $\mathcal{G}^n = \{1\}$ и любой одномерной формальной группы f высоты редукции больше или равной 3, определенной над кольцом целых $\mathcal{O}_K$ локального (соответственно, квазилокального) поля K имеет место включение*

$$N_{L/K}(f_L) \supset f_K^n \quad (\textit{соответственно, } N_{L/K}(\pi_1(\widetilde{f_L})) \supset \pi_1(\widetilde{f_K}^n)). \tag{9}$$

Доказательство. Для всех действительных $s \geq -1$ положим $f_L^s = f^{\lceil s \rceil}$. Пусть $\varphi_{L/K}$ и $\psi_{L/K}$ – соответствующие расширению L/K функции, задающие, соответственно, верхнюю и нижнюю нумерации групп ветвления. Рассмотрим циклическое расширение L/K простой степени. Имеет место следующая лемма.

Лемма 5. *Пусть $n \geq 1$ и циклическое расширение Галуа M/K простой степени локального (соответственно, квазилокального) поля таково, что $\mathcal{G}^n = \{1\}$. Тогда для всех действительных $s \geq \psi_{M/K}(n)$ имеет место включение*

$$N_{\mathcal{G}}(f_M^s) = f_K^{\varphi_{M/K}(s)} \quad (\textit{соответственно, } N_{\mathcal{G}}(\pi_1(\widetilde{f_M}^s)) = \pi_1(\widetilde{f_K}^{\varphi_{M/K}(s)})). \tag{10}$$

Доказательство. Пусть M/K неразветвлено (в этом случае, очевидно, K не является квазилокальным полем). Тогда $\varphi_{M/K}(x) = x$ для всех действительных $x \geq -1$ и следует использовать фильтрацию Лютц (отметим, что здесь $\Pi_M = \Pi_R$), что и доказывает лемму.

Пусть M/K – чисто слабо разветвленное расширение. Для нижней фильтрации $\mathcal{G}$ получаем: $\mathcal{G} = \mathcal{G}_0$ и $\mathcal{G}_1 = \mathcal{G}_2 = \cdots = \{1\}$.

Если $[\mathcal{G}_0 : 1] = [M : K] = q$, то $\varphi_{M/K}(x) = q^{-1}x$ и $\psi_{M/K}(x) = qx$ для всех действительных $x \geq 0$. Нужно показать, что

$$N_{\mathcal{G}}(f_M^s) = f_K^{\frac{s}{q}} \tag{11}$$

при $s \geq \psi_{M/K}(n) = qn$.

Норменный гомоморфизм $N_{M/K} : f_M \to f_K$ индуцирует для всех действительных $r \geq 1$ изоморфизмы

$$f_M^{\psi_{M/K}(r)} / f_M^{\psi_{M/K}(r)+1} \simeq f_K^r / f_K^{r+1}. \tag{12}$$

Доказательство (12) аналогично рассуждениям, приведенным в [6].

Из (12) вытекает, что

$$N_{\mathcal{G}}\left(f_M^{\psi_{M/K}(\frac{\tau}{q})-(q-1)}\right)=\left(f_M^{\psi_{M/K}(\frac{\tau}{q})}\right)=f_K^{\frac{\tau}{q}}=f_K^{\frac{s}{q}},$$

где $\tau=\lceil s\rceil$. А так как $\psi_{M/K}(\frac{\tau}{q})-(q-1)\le\psi_{M/K}(\frac{\tau}{q})$, то

$$N_{\mathcal{G}}(f_M^{\tau})=N_{\mathcal{G}}(f_M^{s})=f_K^{\frac{\tau}{q}}=f_K^{\frac{s}{q}},$$

т.е. равенство (11) истинно.

Пусть M/K – чисто дикое разветвленное расширение Галуа простой степени, а m – номер последней нетривиальной группы ветвления расширения M/K. Тогда

$$\psi_{M/K}(x)=\begin{cases}x, & \text{если } 0\le x<m\\ m+p(x-m), & \text{если } x\ge m\end{cases}\qquad(x\in\mathbb{R}).$$

Так как $\mathcal{G}_{\psi_{M/K}(n)}=\mathcal{G}^n=\{1\}$, то $\psi_{M/K}(n)\ge m+1$. Покажем что для всех действительных $s\ge\psi_{M/K}(n)$ имеет место равенство

$$N_{\mathcal{G}}(f_M^{s})=f_K^{\frac{1}{p}(s-m)+m}. \tag{13}$$

Из результатов, полученных в работе [6], вытекает, что норменный гомоморфизм $N_{L/K}:f_M\to f_K$ индуцирует для всех целых $r>m$ изоморфизм (12). Следовательно, для всех $s\ge\psi_{M/K}(n)$

$$f_K^{\frac{1}{p}(s-m)+m}=N_{\mathcal{G}}\left(f_L^{\psi_{L/K}(\frac{1}{p}(s-m)+m)}\right)=N_{\mathcal{G}}\left(f_L^{\psi_{L/K}(\frac{1}{p}(s-m)+m)-(p-1)}\right).$$

Из

$$\psi_{L/K}\left(\frac{1}{p}(s-m)+m\right)\ge\tau\ge\psi_{L/K}\left(\frac{1}{p}(s-m)+m\right)-(p-1),$$

вытекает, что

$$N_{\mathcal{G}}(f_L^{\tau})=N_{\mathcal{G}}(f_L^{s})=f_K^{\frac{1}{p}(s-m)+m}=f_K^{\varphi_{L/K}(s)},$$

т.е. равенство (13) истинно.

В условиях леммы 5 для простого циклического расширения M/K легко проверить связность ядра эпиморфизма $N_{\mathcal{G}}:\widetilde{f_M}^{\,s}\to\widetilde{f_K}^{\varphi_{M/K}(s)}$ проалгебраических групп. Отсюда получаем эпиморфизм

$$N_{\mathcal{G}}\left(\pi_1(\widetilde{f_M}^{\,s})\right)=\pi_1\left(\widetilde{f_K}^{\varphi_{M/K}(s)}\right). \tag{14}$$

Эпиморфность (14) завершает доказательство леммы. □

Теперь достаточно доказать теорему для локального поля (в случае квазилокального поля та же схема доказательства, но возникают дополнительные громоздкие выкладки). Доказательство проведем индукцией по числу простых множителей в степени произвольного конечного расширения Галуа L/K, воспользовавшись разрешимостью групп Галуа локальных полей.

Выделим в L/K циклическое подрасширение L_1/K простой степени. Получим тогда башню полей с соответствующими группами Галуа $\mathcal{G}$ и h:

$$K - L_1 - L, \quad \mathcal{G} = \mathcal{G}(L/K), \quad h = \mathcal{G}(L/L_1), \quad \mathcal{G}/h = \mathcal{G}(L_1/K).$$

По индукции можно считать, что утверждение леммы 5 доказано для этажа L/L_1 башни. Так как $\mathcal{G}^n = \{1\}$, то по теореме Эрбрана $(\mathcal{G}/h)^n = \{1\}$. Следовательно, для всех действительных $s \geq \psi_{L_1/K}(n)$

$$N_{\mathcal{G}/h}(f_{L_1}^s) = f_K^{\varphi_{L_1/K}(s)}. \tag{15}$$

Используя верхнюю и нижнюю нумерации групп ветвления, получим

$$h^{\varphi_{L/K}(n)} = h_{\psi_{L/L_1}(\psi_{L_1/K}(n))} = h_{\psi_{L/K}(n)} \subset \mathcal{G}^n = \{1\}.$$

Так как $n \geq 1$, то $\psi_{L_1/K}(n) \geq 1$, причем $\psi_{L_1/K}(n)$ – целое. Следовательно, по предположению индукции для всех действительных $s \geq \psi_{L/L_1}(\psi_{L_1/K}(n))$ истинно равенство (роль n в условиях леммы 5 играет $\psi_{L_1/K}(n)$)

$$N_h(f_L^s) = f_{L_1}^{\varphi_{L/L_1}(n)}. \tag{16}$$

Из (16) вытекает, что для любого действительного числа $\Sigma \geq \psi_{L_1/K}(n)$ истинно равенство $N_h(f_L^\Sigma) = f_{L_1}^{\varphi_{L/L_1}(\Sigma)}$. А так как φ – строго возрастающая функция, то

$$\varphi_{L/L_1}(\Sigma) = \varphi_{L/L_1}(\psi_{L/K}(n)) = \psi_{L_1/K}(n).$$

Применяя (15), получим

$$N_{\mathcal{G}/h}\left(f_L^{\varphi_{L/L_1}(\Sigma)}\right) = f_K^{\varphi_{L_1/K}(\varphi_{L/L_1}(\Sigma))} = f^{\varphi_{L/K}(\Sigma)} = N_{\mathcal{G}}(f_L^\Sigma).$$

Следовательно,

$$N_{\mathcal{G}}(f) = N_{\mathcal{G}}(f^1) \supset N_{\mathcal{G}}(f_L^{\psi_{L/K}(n)}) = f^{\varphi_{L/K}(\psi_{L/K}(n))} = f_K^n,$$

что и требовалось доказать. □

1. *Введенский О.Н.* О локальных «полях классов» эллиптических кривых // Изв. АН СССР. Сер. матем. – 1973. – № 1. – С. 20-88.
2. *Введенский О.Н.* Об «универсальных нормах» формальных групп, определенных над кольцом целых чисел локального поля // Изв. АН СССР. Сер. матем. – 1973. – № 4. – С. 737-751.

3. *Глазунов Н.М.* Про «нормені підгрупи» одновимірних формальних груп визначених над кільцем цілих локального поля // Доповіді АН УРСР. Серія А. – 1973. – № 11. – С. 965-968.
4. *Борель А.* Линейные алгебраические группы. – М.: Мир, 1972. – 269 с.
5. *Demazur M.* Lectures on p-divisible groups. – Berlin: Springer-Verlag, 1972. – 280 p.
6. *Введенский О.Н.* Двойственность в эллиптических кривых над локальным полем. I. // Изв. АН СССР. Сер. матем. – 1964. – № 5. – С. 1091-1112.
7. Агебраическая теория чисел. – М.: Мир, 1969. – 483 с.
8. *Шафаревич И.Р.* Основы алгебраической геометрии. – Т. 2. – М.: Наука, 1988. – 304 с.
9. *Deligne P.* La conjecture de Weil // Publ. Math. IHES. – 1974. – P. 273-307.
10. *Милн Дж.* Этальные когомологии. – М.: Мир, 1983. – 392 с.
11. *Гельфанд С.И., Манин Ю.И.* Методы гомологической алгебры. – М.: Наука, 1988. – 416 с.
12. *Serre J.-P.* Groups proalgebriques // Publ. Math. IHES. – 1960. – № 7. – 65 p.

N. M. Glazunov

Quasi-local class fields of elliptic curves and formal groups. I.

Norm subgroups of one-dimensional formal groups of height reduction greater or equal three defined over integer ring of local or quasi-local field are investigated.

Keywords: *local class field theory, the height of reduction of formal group, Gallous group, ramification groups, norm homomorphsm, norm subgroup.*

М. М. Глазунов

Квазілокальні поля класів еліптичних кривих та формальні групи. I.

Досліджено нормені підгрупи одновимірних формальних груп висоти редукції більше або рівній трьом над кільцем цілих локального або квазілокального поля.

Ключові слова: *локальна теорія полів класів, висота редукції формальної групи, група Галуа, групи розгалуження, нормений гомоморфізм, нормена підгрупа.*

Национальный авиационный ун-т, Киев
glanm@yahoo.com

Получено 31.05.12