СЕРИЯ
МАТЕМАТИЧЕСКАЯ
Том 39, № 6, 1975

УДК 513.015.7

М. И. БАШМАКОВ, А. Н. КИРИЛЛОВ

ФИЛЬТРАЦИЯ ЛЮТЦ ФОРМАЛЬНЫХ ГРУПП

§ 0. Обозначения

(0.1). Пусть p — простое число; K — конечное расширение поля p-адических чисел $\mathbf{Q}_p$; $\mathcal{O}=\mathcal{O}_K$ — кольцо целых элементов поля K, $\mathfrak{M}=\mathfrak{M}_K$ — максимальный идеал кольца $\mathcal{O}$, $k=\mathcal{O}/\mathfrak{M}$ — поле вычетов локального кольца $\mathcal{O}$. Идеал $\mathfrak{M}$ является главным; пусть π — его образующая. Дискретное нормирование $v=v_K$ поля K нормализуем так, чтобы $v_K(\pi)=1$.

Через $\overline{K}$ обозначается алгебраическое замыкание поля K; нормирование v продолжается естественным образом на $\overline{K}$. Это продолжение обозначается тем же символом v.

(0.2). Пусть $F(x, y)$ — одномерная формальная группа над $\mathcal{O}$. Известно, что тогда $F(x, y)$ является коммутативной. Для любого конечного расширения L/K через $F(L)$ обозначим абелеву группу, которая как множество есть $\mathfrak{M}_L$, а сложение определено при помощи формальной группы F:

$$\alpha \underset{F}{+} \beta = F(\alpha, \beta), \text{ где } \alpha, \beta \in \mathfrak{M}_L.$$

Через $F(\overline{K})$ обозначается $\bigcup\limits_{L/K} F(L)$, где $F(L)$ определено ранее, и L/K пробегает все конечные алгебраические расширения.

(0.3). На $\mathfrak{M}=\mathfrak{M}_K$ (соответственно на $\mathfrak{M}_L$, $\mathfrak{M}_{\overline{K}}$, ...) имеется фильтрация $\mathfrak{M} \supset \mathfrak{M}^2 \supset \ldots \supset \mathfrak{M}^s \supset \ldots$. Ясно, что $\mathfrak{M}^s=(\pi^s)$ и $\mathfrak{M}^s/\mathfrak{M}^{s+1} \simeq k$ (соответственно $\mathcal{O}_L/\mathfrak{M}_L$, $\overline{k}$, ...).

Заметим, что если $\alpha, \beta \in \mathfrak{M}_K^s$ (соотв. $\mathfrak{M}_L^s$, $\mathfrak{M}_{\overline{K}}^s$, ...), то $\alpha \underset{F}{+} \beta \in \mathfrak{M}_K^s$ (соотв. $\mathfrak{M}_L^s$, $\mathfrak{M}_{\overline{K}}^s$, ...) и, следовательно, абелева группа $F(K)$ (соотв. $F(L)$, $F(\overline{K})$, ...) снабжена фильтрацией: $F(K)=F_1(K) \supset F_2(K) \supset \ldots \supset F_s(K) \supset \ldots$ (соотв. для полей L, $\overline{K}$, ...). Так как $F(x, y) \equiv x+y \pmod{\deg 2}$, то $F_s(K)/F_{s+1}(K) \simeq k$.

Определение (0.3.1). Фильтрация $\{F_i(K)\}_{i \geqslant 1}$ группы $F(K)$ называется *фильтрацией Лютц* формальной группы F (над полем K).

(0.4). Формальный ряд $\varphi(x) \in \mathcal{O}[[x]]$, $\varphi(0)=0$, называется гомоморфизмом формальных групп, $F \xrightarrow{\varphi} G$, если $\varphi(F(x, y))=G(\varphi(x), \varphi(y))$. При

этом φ называется изогенией, если $\operatorname{Ker}\varphi$ конечно. Мы изучаем действие φ на фильтрации Лютц $\{F_i(K)\}$, $\{G_i(K)\}$ этих групп, а также факторфильтрацию на $\operatorname{Coker}\varphi$.

(0.5). К изучению поведения фильтраций формальных групп приводят различные задачи из теории эллиптических кривых. Простейшей из них является описание свойств элементарных абелевых p-расширений локального поля (случай $F=\mathbf{G}_m$). В работах ([2]), ([9]) изучалось деление точки эллиптической кривой над локальным полем на изогению. Работа ([8]) содержит описание норменного гомоморфизма на точках эллиптической кривой для Г-расширения локального поля. В настоящей работе развивается техника для изучения фильтраций формальных групп (фильтраций Лютц). В качестве иллюстрации приводятся новые доказательства указанных выше результатов. Основными результатами работы являются теорема (2.3.6) и предложение (3.1.6).

§ 1. Вспомогательные факты из теории формальных групп

(1.1). Высота эндоморфизма формальной группы. Пусть R — коммутативное кольцо с единицей, R^+ — аддитивная группа этого кольца.

ЛЕММА (1.1.1) ([3]). *Пусть* $\varphi\in\operatorname{End}_R(F)$, $\varphi\neq 0$. *Определим* $c(\varphi)=\varphi'(0)\in R$. *Тогда*:

1) *если* R^+ *не имеет* $\mathbf{Z}$*-кручения, то* $c(\varphi)\neq 0$;

2) *если* R^+ *имеет характеристику* p (p — *простое число*) *и если* $c(\varphi)=0$, *то существуют* $\psi(t)\in R[[t]]$ *и целое число* h, $h>0$, *такие, что*

а) $c(\psi)\neq 0$, $\psi(0)=0$,

б) $\varphi(t)=\psi(t^{p^h})$.

Определение (1.1.2). Однозначно определенное в лемме (1.1.1) число $h=h(\varphi)$ называется высотой эндоморфизма φ.

Определение (1.1.3). Высота эндоморфизма $[p]_F$ называется высотой формальной группы F (над кольцом R, характеристики $p>0$).

Определение (1.1.4). Если R — локальное кольцо, $\mathfrak{M}$ — его максимальный идеал, $k=R/\mathfrak{M}$ — его поле вычетов и $F(x, y)$ — формальная группа над R, то высотой эндоморфизма $\varphi\in\operatorname{End}_R(F)$ (соотв. высотой F над R) называется высота $\bar{\varphi}\in\operatorname{End}_k(\bar{F})$ над полем k (соотв. высота $\bar{F}$ над k), где «черта» означает редукцию modulo $\mathfrak{M}$ (если $\bar{\varphi}\neq 0$). При $\bar{\varphi}=0$ положим $h(\varphi)=\infty$.

ЛЕММА (1.1.5) ([3]). *Пусть* $\varphi: F\longrightarrow G$ — *изогения формальных групп* (*над полем* K). *Тогда*:

1) *гомоморфизм* $\varphi: F(\bar{K})\longrightarrow F(\bar{K})$ *сюръективен*;

2) $\operatorname{Ker}\varphi(\bar{K})\overset{\text{def}}{=}\{\alpha\in F(\bar{K})\mid\varphi(\alpha)=0\}$ *является конечной абелевой группой порядка* $p^{h(\varphi)}$.

Следствие (1.1.6). *Пусть* F — *формальная группа* (*над полем* K), $h=h(\varphi)<\infty$. *Тогда* $[p]_F$ *является изогенией и*

$$\operatorname{Ker}([p]_F)(\bar{K})\simeq(\mathbf{Z}/p\,\mathbf{Z})^h.$$

(1.2). Многоугольник Ньютона формальной группы. Мы используем обозначения § 0.

Рассмотрим эндоморфизм $f \in \mathrm{End}_{\mathcal{O}}(F)$ формальной группы F. Пусть $f(x) = \sum_{i=1}^{\infty} a_i x^i$, где $a_i \in \mathcal{O}$. Условие $h = h(F) < \infty$ означает, что $v_K(a_i) \geqslant 1$, если $1 \leqslant i < q = p^h$ и $v(a_q) = 0$.

Нас, в дальнейшем, будет интересовать действие f на фильтрацию Лютц. Для этой цели используется многоугольник Ньютона эндоморфизма f. В области $M = \{(x, y) \in \mathbf{R}^2 \mid x \geqslant 0, \ y \geqslant 0\}$ отметим точки $(i, v_K(a_i))$, где $1 \leqslant i \leqslant q$. Из всех ломаных с вершинами в отмеченных точках и соединяющих точки $(1, v(a_1))$ и $(q, v(a_q))$ выберем наиболее близкую к границе области M. Эта ломаная является нижней границей выпуклой оболочки множества $\{(i, v(a_i)) \mid 1 \leqslant i \leqslant q\}$. Построенная ломаная называется многоугольником Ньютона эндоморфизма f. Его (собственные вершины) $(q_0, v(a_{q_0}))$, $(q_1, v(a_{q_1}))$, ..., $(q_m, v(a_{q_m}))$, где $1 = q_0 < q_1 < \ldots < q_m = q$, являются важными инвариантами формальной группы F. Заметим, что $v(a_{q_m}) = v(a_q) = 0$ и $v(a_1) = v(a_{q_0}) > v(a_{q_1}) > \ldots > v(a_{q_m}) = 0$. Отметим следующие, хорошо известные, свойства многоугольника Ньютона (мы следуем работе ([6])).

(1.2.1). Тангенс угла наклона прямой, соединяющей точки $(i, v(a_i))$ и $(j, v(a_j))$, где $j > i$, к X-ой оси координат равен

$$-\frac{v(a_j) - v(a_i)}{j - i}$$

и, следовательно, равен v-порядку элемента $z_0 \in \overline{K}$, для которого $v(a_i z_0^i) = v(a_j z_0^j)$.

(1.2.2). Обозначим $V = \mathrm{Ker}\, f(\overline{K})$, $\mathrm{Card}(V) = p^h$. Пусть

$$\alpha_i = \frac{v(a_{q_{i-1}}) - v(a_{q_i})}{q_i - q_{i-1}} \in \mathbf{Q},$$

где $1 \leqslant i \leqslant m$. Тогда

(1.2.2.1). $\mathrm{Card}\{x \in V \mid v(x) = \alpha_i\} = q_i - q_{i-1}$. Кроме того, v_K-порядок любого элемента из V равен α_i для некоторого i, $1 \leqslant i \leqslant m$. Ясно, что $\alpha_1 > \alpha_2 > \ldots > \alpha_m$.

(1.2.2.2). Положим $V^0 = 0$, $V^i = \{x \in V \mid v(x) \geqslant \alpha_i\}$ для $1 \leqslant i \leqslant m$. (Ясно, что $0 = V^0 \subset V^1 \subset \ldots \subset V^m = V$.) Тогда V^i являются подгруппами V и $\mathrm{Card}(V^i) = q_i$. Следовательно, $q_i = p^{h_i}$, где $0 < h_1 < \ldots < h_m = h$.

(1.2.2.3). Положим $t_i = \alpha_{m-i+1}$ (таким образом, $t_1 < t_2 < \ldots < t_m$) для $1 \leqslant i \leqslant m$, $t_0 = 1$, $t_{m+1} = \infty$. Тогда если $x \in \overline{K}$, $t_k \leqslant v(x) < t_{k+1}$, то

$$\min\{v(a_1 x), v(a_2 x^2), \ldots, v(a_q x^q)\} = v(a_{q_{m-k}} x^{q_{m-k}}) =$$

$$= q_{m-k} v(x) + v(a_{q_{m-k}}) \text{ для } 1 \leqslant k \leqslant m.$$

Определение (1.2.3). *Функция Эрбрана для многоугольника Ньютона.*

Пусть $q_0, q_1, \ldots, q_m$ и $t_0, t_1, \ldots, t_m, t_{m+1}$ — инварианты многоугольника Ньютона. Положим для $x \in \mathbf{R}^+$,

$$\varphi(x) = qt_1 + (t_2 - t_1)q_{m-1} + (t_3 - t_2)q_{m-2} + \ldots + (x - t_k)q_{m-k},$$

если $t_k \leqslant x < t_{k+1}$, $0 \leqslant k \leqslant m$. Тогда (рекуррентные соотношения!) получаем, что если $t_k \leqslant v(x) < t_{k+1}$, $0 \leqslant k \leqslant m$, то $v(a_{q_{m-k}} x^{q_{m-k}}) = \varphi(v(x))$.

Ясно, что φ строго возрастает. Через ψ будет обозначаться обратная к φ функция.

Следствие (1.2.4). *Если* $x \in \overline{K}$, $v(x) = i (\geqslant 0)$, *то* $\min\{v(a_1 x), \ldots, v(a_q x^q)\} = \varphi(i)$.

Предложение (1.2.5). 1) *Если* $x \in \mathfrak{M}_K^i$, *то* $f(x) \in \mathfrak{M}_K^{\varphi(i)}$.

2) *Если* $x \in \mathfrak{M}_K^i \setminus \mathfrak{M}_K^{i+1}$, $i \notin \{t_1, \ldots, t_m\}$, *то* $f(x) \in \mathfrak{M}_K^{\varphi(i)} \setminus \mathfrak{M}_K^{\varphi(i)+1}$.

Доказательство. 1) Имеем:

$$v(f(x)) \geqslant \min\{v(a_1 x), \ldots, v(a_q x^q)\} = \varphi(v(x)).$$

2) Если $x \in \mathfrak{M}_k^i \setminus \mathfrak{M}_K^{i+1}$, $i \notin \{t_1, \ldots, t_m\}$, то

$$v(f(x)) = v(a_1 x + \ldots + a_q x^q) = \min\{v(a_1 x), \ldots, v(a_q x^q)\} = \varphi(i).$$

Так как φ строго возрастает, то если $v(f(x)) > \varphi(i)$, то $x \in \mathfrak{M}_K^{i+1}$.

Замечания.

(1.2.6). Результаты пункта (1.2.2) показывают, что многоугольник Ньютона зависит лишь от класса изоморфных (над $\mathcal{O}$) формальных групповых законов.

(1.2.7). Многоугольник Ньютона можно определять и с помощью разложения Вейерштрасса формального ряда (над $\mathcal{O}$) [см. ([2])].

(1.2.8). Из пункта (1.2.6) легко следует, что $\varphi_{f \circ g} = \varphi_f \circ \varphi_g$.

(1.2.9). О связи многоугольника Ньютона формальной группы и характеристического многочлена эндоморфизма Фробениуса в алгебре $\mathrm{End}_k(\overline{F})$ см. ([4]).

(1.3). Примеры.

(1.3.1). (Высота 1.) В этом случае $f(x) = a_1 x + a_2 x^2 + \ldots + a_p x^p + \ldots$, где $v(a_i) \geqslant 1$ при $1 \leqslant i \leqslant p-1$, $v(a_p) = 0$. Следовательно, $m = 1$, $t_1 = \dfrac{v(a_1)}{p-1}$.

Если $h = h(F)$, то $a_1^h \sim p$ и $v(a_1) = \dfrac{e}{h}$.

Функция Эрбрана

$$\varphi(i) = \begin{cases} pi, & \text{если } 0 \leqslant i \leqslant t_1, \\ pt_1 + (i - t_1), & \text{если } i \geqslant t_1, \end{cases}$$

$$\psi(i) = \begin{cases} \dfrac{i}{p}, & \text{если } 0 \leqslant i \leqslant pt_1, \\ t_1 + (i - pt_1), & \text{если } i \geqslant pt_1. \end{cases}$$

(1.3.2). (Высота 2.) В этом случае $f(x)=a_1x+a_2x^2+\ldots+a_px^p+\ldots$ $\ldots+a_{p^2}x^{p^2}+\ldots$, где $v(a_i)\geqslant 1$ при $1\leqslant i\leqslant p^2-1$, $v(a_{p^2})=0$. Пусть $e_1=v(a_1)$, $r=v(a_p)$. Положим

$$t_2'=\frac{e_1-r}{p-1},\quad t_1'=\frac{r}{p^2-p},\quad e_2=\frac{e_1}{p^2-1}.$$

Возможны два случая:

1) $t_1'<t_2'$. Тогда $t_1'<e_2<t_2'$. Следовательно, $m=2$, $h_1=1$, $t_1=t_1'$, $t_2=t_2'$. Функция Эрбрана

$$\varphi(i)=\begin{cases}p^2i, & \text{если } 0\leqslant i\leqslant t_1,\\ p^2t_1+p(i-t_1), & \text{если } t_1\leqslant i\leqslant t_2,\\ p^2t_1+p(t_2-t_1)+(i-t_2), & \text{если } i\geqslant t_2.\end{cases}$$

2) $t_1'\geqslant t_2'$. Тогда $t_1'\geqslant e_2\geqslant t_2'$. Следовательно, $m=1$, $t_1=e_2$. Функция Эрбрана

$$\varphi(i)=\begin{cases}p^2i, & \text{если } 0\leqslant i\leqslant t_1,\\ p^2t_1+p(i-t_1), & \text{если } i\geqslant t_1.\end{cases}$$

§ 2. Свойства фильтрации Лютц

(2.0). Пусть $F(x,y)\in\mathcal{O}[[x,y]]$ — формальная группа над кольцом целых элементов $\mathcal{O}$ локального поля K, $\operatorname{char}k=p>0$, где k — поле вычетов. Рассмотрим конечное расширение Галуа L/K с группой $G=\operatorname{Gal}(L/K)$. В группе G имеется фильтрация (группами ветвления): G_0 — группа инерции, $G_i=\{\sigma\in G_0\mid \Pi^\sigma-\Pi\in\Pi^{i+1}\mathcal{O}_L\}$, где $i\geqslant 1$, Π — простой элемент поля L. Опишем действие группы G на фильтрацию Лютц $\{F_i(L)\}$.

ЛЕММА (2.0.1). 1) *Если* $P\in F_a(L)$, $\sigma\in G_i$ $(i\geqslant 1)$, *то*

$$P^\sigma\underset{F}{-}P\in F_{a+i}(L).$$

2) *Если* $(a,p)=1$, $P\in F_a(L)\setminus F_{a+1}(L)$, $\sigma\in G_i\setminus G_{i+1}$, *то*

$$P^\sigma\underset{F}{-}P\in F_{a+i}(L)\setminus F_{a+i+1}(L).$$

Доказательство. Имеем:

$$P^\sigma\underset{F}{-}P=F(z^\sigma,[-1]_F(z))=z^\sigma-z+\sum_{\substack{i+j\geqslant 2\\ i\geqslant 1,j\geqslant 0}}a_{ij}(z^{i\sigma}-z^i)([-1]_F(z))^j,$$

где $a_{ij}\in\mathcal{O}_K$ (это коэффициенты формальной группы $F(x,y)$), $z\in\mathfrak{M}_L$ — параметр, соответствующий точке $P\in F(L)$. Ясно, что $[-1]_F(z)\equiv -z \pmod{\deg 2}$. Следовательно,

$$v_L(P^\sigma\underset{F}{-}P)=v_L(z^\sigma-z).$$

Но $z^\sigma-z=\Pi^{a+i}\xi$, где $\xi\in\mathcal{O}_L$, и при выполнении условий п. 2) $\xi\in\mathcal{O}_L^*$.

(2.1). Действие эндоморфизма f на фильтрацию Лютц. (Обозначения (1.2.2).)

Предложение (2.1.1). 1) *Если* $P \in F_i(K) \setminus F_{i+1}(K)$, $i \notin \{t_1, \ldots, t_m\}$, *то*

$$f(P) \in F_{\varphi(i)}(K) \setminus F_{\varphi(i)+1}(K)$$

(это переформулировка предложения (1.2.6)).

2) *Если* $i \notin \{t_1, \ldots, t_m\}$, *то* f *индуцирует изоморфизм*

$$F_i(K)/F_{i+1}(K) \simeq F_{\varphi(i)}(K)/F_{\varphi(i)+1}(K).$$

3) *Имеет место точная последовательность*

$$0 \to V^{m-r}/V^{m-r-1} \to F_{t_r}(K)/F_{t_r+1}(K) \xrightarrow{\overline{f}} F_{\varphi(t_r)}(K)/F_{\varphi(t_r)+1}(K) \to D_r \to 0,$$

где D_r — *конечная абелева группа,* $\operatorname{Card}(D_r) = \operatorname{Card}(V^{m-r}/V^{m-r-1}) = p^{m-r-h_{m-r-1}}$.

Следствие (2.1.2). 1) *Если* $P \in F_a(K) \setminus F_{a+1}(K)$, $\varphi(t_k) < a < \varphi(t_{k+1})$, $0 \leqslant k \leqslant m$, *и* $a \equiv 0 \pmod{q_{m-k}}$, *то существует точка* $R \in F(K)$ *такая, что*

$$P \underset{F}{-} f(R) \in F_{a+1}(K).$$

2) *Если* $a > \varphi(t_m)$, *то* $F_a(K) \subset \operatorname{Im} f(K)$.

(2.3). Деление точек на изогению f. В этом пункте предположим дополнительно, что ядро изогении f определено над полем K. Тогда инварианты $t_1, \ldots, t_m$ являются целыми числами.

Определение (2.3.0) (поле K_P). Для каждой точки $P \in F(K)$ существует точка $Q \in F(\overline{K})$ такая, что $f(Q) = P$. Рассмотрим поле K_P — минимальное поле определения точки Q. Это поле не зависит от выбора точки Q. Опишем свойства полей K_P.

(2.3.1). Расширение K_P/K является расширением Галуа, группа Галуа которого $G(P) = \operatorname{Gal}(K_P/K)$ является абелевой p-группой.

(2.3.2). Гомоморфизм $G(P) \to V$, определенный как $\sigma \to Q^\sigma \underset{F}{-} Q$, не зависит от выбора точки Q и является инъективным.

(2.3.3). Если $P \in F_a(K) \setminus F_{a+1}(K)$, $(a, p) = 1$, $\varphi(t_k) < a < \varphi(t_{k+1})$, $0 \leqslant k \leqslant m$, то гомоморфизм пункта (2.3.2) определяет изоморфизм

$$G(P) \to V^{m-k}.$$

Доказательство. Так как по условию V определено над полем K, то все эти утверждения следуют из теории Куммера.

Следствие (2.3.4). 1) *Если* $P \in F_a(K) \setminus F_{a+1}(K)$, $(a, p) = 1$, $\varphi(t_k) < a < \varphi(t_{k+1})$, $0 \leqslant k \leqslant m$, *то расширение* K_P/K *вполне разветвлено и имеет степень* q_{m-k}.

2) *Если* $P \in F_{\varphi(t_m)} \setminus \operatorname{Im} f(K)$, *то расширение* K_P/K *неразветвлено.*

ТЕОРЕМА (2.3.6). *Рассмотрим* $P \in F_a(K) \setminus F_{a+1}(K)$, $(a, p) = 1$. *Тогда скачки в верхней фильтрации высшими группами ветвления для группы* $G(P)$ *происходят в следующих значениях*:

$$\{\varphi(t_1) - a, \varphi(t_2) - a, \ldots, \varphi(t_m) - a\}.$$

Замечание (2.3.6.1). В условиях теоремы мы считаем, что $G^x=0$ при $x<0$.

Доказательство теоремы (2.3.6). Докажем сначала следующую лемму.

ЛЕММА (2.3.5). *Пусть точка* $P\in F_a(K)\setminus F_{a+1}(K)$, $(a, p)=1$, $\varphi(t_k)<a<\varphi(t_{k+1})$, $0\leqslant k<m$. *Определим функцию* $\theta(a)=q_{m-k}\psi(a)$. *Пусть* $Q\in F(\overline{K})$ — *такая точка, что* $f(Q)=P$. *Тогда*

$$Q\in F_{\theta(a)}(K_P)\setminus F_{\theta(a)+1}(K_P).$$

Доказательство леммы (2.3.5). Если $Q\in F_i(K_P)\setminus F_{i+1}(K_P)$, то из условия $f(Q)=P$ следует, что $q_{m-k}a=\varphi_{K_P}(i)=q_{m-k}\varphi\left(\frac{i}{q_{m-k}}\right)$, т. е. $i=q_{m-k}\psi(a)=\theta(a)$, q. e. d.

Пусть теперь $G=G(P)$. Рассмотрим $\sigma\in G_i\setminus G_{i+1}$ (см. (2.0)). Так как $(\theta(a), p)=1$ (см. (2.3.5)), то по лемме (2.0.1) получаем:

$$Q^\sigma \underset{F}{-} Q\in F_{\theta(a)+i}(K_P)\setminus F_{\theta(a)+i+1}(K_P).$$

С другой стороны, $Q^\sigma \underset{F}{-} Q\in V$; следовательно,

$$Q^\sigma \underset{F}{-} Q\in F_{a_{m-k}t_r}(K_P)$$

для некоторого r, где $k+1\leqslant r\leqslant m$ (см. (2.3.4.1) и (1.2.2.2)). Отсюда следует, что скачки в нижней фильтрации высшими группами ветвления для группы G происходят в следующих значениях:

$$\{q_{m-k}t_{k+1}-\theta(a),\ q_{m-k}t_{k+2}-\theta(a),\ \ldots,\ q_{m-k}t_m-\theta(a)\}$$

(см. (2.3.3)). Переходя к верхней фильтрации, получаем, что

$$\varphi_{K_P/K}(q_{m-k}t_{k+u}-\theta(a))=\varphi(t_{k+u})-a,\quad 1\leqslant u\leqslant m-k,$$

q. e. d.

(2.4). Примеры.

(2.4.1). (Высота 1.) В этом случае (см. (1.3.1)) $m=1$, $t_1=\frac{v(a_1)}{p-1}=\frac{e_0}{h}$, где $e_0=\frac{e}{p-1}$ и $h=h(F)$; $\varphi(t_1)=pt_1$. Пусть $1\leqslant a<pt_1$, $(a, p)=1$. Рассмотрим точку $P\in F_a(K)\setminus F_{a+1}(K)$, поле K_P и группу $G=G(P)$ (см. (2.3.0)). Тогда $G=G_0=G_1=\ldots=G_{c(a)}\neq G_{c(a)+1}=\ldots=\{1\}$, где $c(a)=pt_1-a$ (для циклических расширений степени p верхняя и нижняя фильтрации в группе G совпадают). Предположим, что корни p-ой степени из единицы лежат в поле K. Тогда $K_P=K(\sqrt[p]{\alpha})$, где $\alpha\in K^*\setminus K^{*p}$. Пусть $\omega_K(\alpha)$ — «главная часть mod$^*p$» элемента α. Тогда известно, что $\omega_K(\alpha)+c(a)=pe_0$ [см. ([5])]. Следовательно, $\omega_K(\alpha)=pe_0-c(a)=pht_1-(pt_1-a)=a+pt_1(h-1)$.

Замечание (2.4.1.1). Этот результат (в другом контексте) был получен в ([2]).

(2.4.1.2). (Случай мультипликативной группы $\mathbf{G}_m$). Рассмотрим группу $F(x, y)=x+y+xy$. Ясно, что $F(K)\simeq U_1$ и $F_a(K)\simeq U_a=\{\alpha\in O \mid \alpha\equiv$

$\equiv 1 \pmod{\pi^a}\}$. Фильтрация $\{U_a\}_{a\geqslant 1}$ в группе K^* индуцирует фильтрацию в группе $K^*/K^{*p}=C_0\supset C_1\supset \ldots \supset C_{pe_0}\supset C_{pe_0+1}=\{1\}$ (отметим, что $C_{pi}=C_{pi+1}$ для $1\leqslant i<e_0$). Тогда $\omega_K(\alpha)$ для элемента $\alpha\in K^*\setminus K^{*p}$ (см. (2.4.1)) — это максимальное целое число s такое, что образ α в K^*/K^{*p} лежит в C_s (отметим, что $(\omega_K(\alpha), p)=1$, кроме случая $\omega_K(\alpha)=pe_0$). Положим $\omega_K(\alpha)=\infty$, если $\alpha\in K^{*p}$. Пусть $c_K(\alpha)=pe_0-\omega_K(\alpha)$, если $1\leqslant \leqslant\omega_K(\alpha)<pe_0$.

ЛЕММА (2.4.1.2′). *Пусть L/K — конечное p-расширение Галуа, $\psi_{L/K}$ — функция Эрбрана расширения L/K. Пусть $\alpha\in K^*\setminus K^{*p}$ — такой элемент, что $c_K(\alpha)$ отлично от скачков функции $\psi_{L/K}$. Тогда*

$$c_L(\alpha)=\psi_{L/K}(c_K(\alpha)).$$

Доказательство. Для циклического расширения простой степени эта лемма доказана, например, в ([9]). Общий случай следует из мультипликативности функции Эрбрана.

(2.4.2). (Высота 2.)

Случай 1). $m=2$, $h_1=1$, $t_1=\frac{r}{p^2-p}$, $t_2=\frac{e_1-r}{p-1}$, $t_1<t_2$. Рассмотрим точку $P\in F_a(K)\setminus F_{a+1}(K)$, $(a, p)=1$. Поле K_P и группа $G=G(P)$ — как в (2.3.0). Из теоремы (2.3.6) следует, что

$$G=G^0=G^1=\ldots=G^{\varphi(t_1)-a}\neq G^{\varphi(t_1)-a+1}=\ldots=G^{\varphi(t_2)-a}\neq G^{\varphi(t_2)-a+1}=\{1\}.$$

Из определений находим:

$$\varphi(t_1)-a=p^2t_1-a,\quad \varphi(t_2)-a=p[t_2+(p-1)t_1]-a.$$

Предположим, что корни p-ой степени из единицы лежат в поле K и что $K_P=K(\sqrt[p]{\alpha}, \sqrt[p]{\beta})$, где $\alpha,\beta\in K^*$ (это условие выполняется, если, например, F соответствует эллиптической кривой). Из теоремы Эрбрана (см. ([1]), стр. 66, теорема 9.2) следует, что, например,

$$c_K(\alpha)=p^2t_1-a,\quad c_K(\beta)=\varphi(t_2)-a.$$

Следовательно,

$$\omega_K(\alpha)=pe_0-p^2t_1+a,\quad \omega_K(\beta)=pe_0-p[t_2+(p-1)t_1]+a.$$

I. Если теперь $f=[p]_F$, $h(F)=2$, то $e_1=e$ и $e_0=t_2+pt_1$. Таким образом,

$$\omega_K(\alpha)=pt_2+p^2t_1-p^2t_1+a=a+pt_2,$$
$$\omega_K(\beta)=pt_2+p^2t_1-pt_2-p^2t_1+pt_1+a=a+pt_1.$$

II. Если $f=g^2$, $h(g)=1$, $h=h(F)\geqslant 2$, то $e_1=\frac{2e}{h}$, $r=\frac{e_1}{2}$. Следовательно, $t_1=\frac{e_1}{2p(p-1)}$, $t_2=\frac{e_1}{2(p-1)}$. Таким образом, $t_2=pt_1$ и из теоремы (2.3.6) получаем:

$$\omega_K(\alpha)=pe_0-(p^2t_1-a)=a+pt_2(h-1),$$
$$\omega_K(\beta)=pe_0-[pt_2+p(p-1)t_1]+a=a+t_2+pt_2(h-2).$$

Случай II был разобран впервые в работе ([3]).

Случай 2). $m=1$, $t_1=\frac{e_1}{p^2-1}$. Пусть $1\leqslant a<p^2t_1$, $(a, p)=1$. Тогда из теоремы (2.3.6) следует, что

$$\boldsymbol{G}=G^0=G^1=\ \ldots\ =G^{p^2t_1-a}\neq G^{p^2t_1-a+1}=\ \ldots\ =\{1\}.$$

Если, как в случае 1), $K_P=K(\sqrt[p]{\alpha}, \sqrt[p]{\beta})$, $\alpha, \beta\in K^*$, то

$$c_K(\alpha)=c_K(\beta)=p^2t_1-a.$$

Следовательно,

$$\omega_K(\alpha)=\omega_K(\beta)=pe_0-p^2t_1+a.$$

Пусть теперь $f=[p]_F$, $h(F)=2$. Тогда $e_1=e$, $e_0=(p+1)t_1$. Следовательно, $\omega_K(\alpha)=\omega_K(\beta)=a+pt_1$.

Замечание (2.4.2).

1. Случай 2) реализуется, например, для эллиптических кривых, определенных над $\mathbf{Q}_p$, редукция которых по модулю p невырождена и суперсингулярна.

2. Случай 1) II реализуется для кривых с комплексным умножением, для которых p ветвится в поле комплексного умножения и не делит кондуктора.

3. Случай 2) реализуется для кривых с комплексным умножением, для которых p распадается в поле комплексного умножения и не делит кондуктора.

§ 3. Оператор нормы

(3.1). Пусть F — формальная группа над $\mathcal{O}_K$. Рассмотрим конечное расширение Галуа L/K с группой Галуа G. Определим гомоморфизм нормы $N_F: F(L)\to F(K)$: для $x\in F(L)$ положим

$$N_F(x\ \ \sum_{\sigma\in G}^{(F)} x^\sigma\quad (\in F(K)),$$

где $\Sigma^{(F)}$ обозначает сумму относительно формальной группы F. Предположим теперь, что $(L:K)=p$, $h=h(F)$.

ЛЕММА (3.1.1) ([10]). *Имеет место следующее разложение*:

$$N_F(x)=\mathrm{Tr}_{L/K}(x)+\sum_{i=1}^{h} a_{p^i}N_{L/K}(x^{p^{i-1}})+\ \ldots,$$

где многоточие означает члены более высокого v-порядка, чем выписанные.

Рассмотрим многочлен

$$g(z)=\sum_{i=1}^{h} a_{p^i}z^{p^{i-1}}.$$

Пусть

$$s_0 = 1 < s_1 < \ldots < s_n = p^{h-1}, \quad u_0 = 0 < u_1 < \ldots < u_n < u_{n+1} = \infty$$

— инварианты многоугольника Ньютона для $g(z)$. Через φ_N обозначим функцию Эрбрана для $g(z)$, т. е. $\varphi_N = \varphi_g$.

Замечание (3.1.2). Если $t_1, \ldots, t_m$ — инварианты многоугольника Ньютона для F (см. (1.2)), то $u_i \geqslant t_i$, $0 \leqslant i \leqslant n$.

ЛЕММА (3.1.3). *Для любого $a \in \mathbf{Q}$, $a \geqslant 0$, существует единственное k такое, что $p\varphi_N(u_k) - u_k + p \leqslant a < p\varphi_N(u_{k+1}) - u_{k+1} + p$.*

Доказательство очевидно.

Определение (3.1.4). Пусть D — v_L-порядок дифференты расширения L/K. Через k_0 обозначим целое число такое, что

$$p\varphi_N(u_{k_0}) - u_{k_0} + p \leqslant D < p\varphi_N(u_{k_0+1}) - u_{k_0+1} + p$$

(см. (3.13)) (эквивалентное определение: $\dfrac{p\varphi_N(u_{k_0}) - u_{k_0}}{p-1} < \dfrac{D}{p-1} \leqslant \dfrac{p\varphi_N(u_{k_0+1}) - u_{k_0+1}}{p-1}$).

Предложение (3.1.5). *Если $x \in F_i(L)$, то $N_F(x) \in F_{\mu(i)}(K)$, где*

$$\mu(i) = \begin{cases} \varphi_N(i), & \text{если } i \leqslant \left[\dfrac{D - p\varphi_N(u_{k_0}) + ps_{n-k_0}u_{k_0}}{ps_{n-k_0} - 1}\right] - \delta_{n,k_0}, \\ \left[\dfrac{D+i}{p}\right], & \text{если } i \geqslant \left[\dfrac{D - p\varphi_N(u_{k_0}) + ps_{n-k_0}u_{k_0}}{ps_{n-k_0} - 1}\right] - \delta_{n,k_0}, \end{cases}$$

$$\delta_{n,k_0} = \begin{cases} 0, & \text{если } n \neq k_0, \\ 1, & \text{если } n = k_0. \end{cases}$$

Доказательство. Ясно, что если $v_K(z) = i$, то

$$\min\{v(a_p z),\ v(a_{p^2} z^p),\ \ldots,\ v(a_{p^h} z^{p^{h-1}})\} = \varphi_N(i).$$

Следовательно, $v(N_F(x)) \geqslant \min\left\{\left[\dfrac{D+i}{p}\right],\ \varphi_N(i)\right\}$.

Шаг I. $\left[\dfrac{D+i}{p}\right] \leqslant s_{n-k}i + v(a_{ps_{n-k}}) \Leftrightarrow i > \dfrac{D - pv(a_{ps_{n-k}}) - p}{ps_{n-k} - 1}$.

Действительно, $\dfrac{D+i}{p} - 1 < \left[\dfrac{D+i}{p}\right] \leqslant \dfrac{D+i}{p}$. Таким образом,

$$\left[\frac{D+i}{p}\right] \leqslant s_{n-k}i + v(a_{ps_{n-k}}) \Leftrightarrow \frac{D+i}{p} - 1 < s_{n-k}i + v(a_{ps_{n-k}}).$$

Шаг II. $u_k \leqslant \dfrac{D - pv(a_{ps_{n-k}}) - p}{ps_{n-k} - 1} < u_{k+1} \Leftrightarrow$

$$p\varphi_N(u_k) - u_k + p \leqslant D < p\varphi_N(u_{k+1}) - u_{k+1} + p.$$

Это вытекает из следующих формул:

$$\varphi_N(u_k) = u_k s_{n-k} + v(a_{ps_{n-k}}), \quad \varphi_N(u_{k+1}) = u_{k+1} s_{n-k} + v(a_{ps_{n-k}}).$$

Шаг III.

$$\min\left\{\left[\frac{D+i}{p}\right], \varphi_N(i)\right\} = \begin{cases} \varphi_N(i), & \text{если } i \leqslant \dfrac{D - pv(a_{ps_{n-k_0}}) - p}{ps_{n-k_0} - 1}, \\ \left[\dfrac{D+i}{p}\right], & \text{если } i > \dfrac{D - pv(a_{ps_{n-k_0}}) - p}{ps_{n-k_0} - 1}. \end{cases}$$

Действительно, пусть $u_k \leqslant i < u_{k+1}$. Тогда

$$\min\left\{\left[\frac{D+i}{p}\right], \varphi_N(i)\right\} = \left[\frac{D+i}{p}\right] \Leftrightarrow i > \frac{D - pv(a_{ps_{n-k}}) - p}{ps_{n-k} - 1}$$

(см. Шаг I). Значит, $\dfrac{D - pv(a_{ps_{n-k}}) - p}{ps_{n-k} - 1} < u_{k+1}$. Следовательно, $k \geqslant k_0$ и

$$i > \frac{D - pv(a_{ps_{n-k_0}}) - p}{ps_{n-k_0} - 1}.$$

Мы должны теперь показать, что если

$$i > \frac{D - pv(a_{ps_{n-k_0}}) - p}{ps_{n-k_0} - 1}$$

и $u_k \leqslant i < u_{k+1}$, то

$$i > \frac{D - pv(a_{ps_{n-k}}) - p}{ps_{n-k} - 1}.$$

Заметим сначала, что $k \geqslant k_0$. Для $k = k_0$ утверждение очевидно. Пусть $k > k_0$ и предположим, что

$$i < \frac{D - pv(a_{ps_{n-k}}) - p}{ps_{n-k} - 1}.$$

Тогда

$$u_k < \frac{D - pv(a_{ps_{n-k}}) - p}{ps_{n-k} - 1}$$

и, следовательно, $k \leqslant k_0$ — противоречие. Предложение доказано.

Следствие (3.1.6). *Если* $z \in F_a(K)$,

$$a > \varphi_N\left(\left[\frac{D - pv(a_{ps_{n-k_0}})}{ps_{n-k_0} - 1}\right] - \delta_{n,k_0}\right),$$

то $z \in N_F(F(L))$.

Предложение (3.1.7). *Пусть* F *— формальная группа над* O_K, K_∞ / K *—* Γ*-расширение, соответствующее простому числу* p. *Тогда если* $h(F) \geqslant 2$, *то группа универсальных норм в* $F(K)$ *из поля* K_∞ *равна нулю.*

Доказательство. Пусть $K=K_0—K_1—\ldots—K_m—\ldots$ — «этажи» Г-расширения; $(K_m:K_{m-1})=p$, $K_\infty=\bigcup\limits_{m\geqslant 0} K_m$. Тогда расширение K_m/K_{m-1} вполне разветвлено для $m\geqslant m_0$ для некоторого m_0. Ясно, что можно считать $m_0=1$. Заметим, что если $\varphi_{N,m}$ — функция Эрбрана, построенная для полей K_m/K_{m-1}, $m\geqslant 1$, то

$$\varphi_{N,m}(i)=p^{m-1}\varphi_N\left(\frac{i}{p^{m-1}}\right),\ \text{где}\ \varphi_N=\varphi_{N,1}.$$

Далее, если $u_k\leqslant i<u_{k+1}$, то

$$\varphi_N(i)=s_{n-k}i+v(a_{ps_{n-k}})\geqslant pi$$

при условии, что $k<n$, и $\varphi_N(i)=i+v(a_p)$, если $k=n$.

Таким образом, если

$$\varphi_N^{(r)}(i)=\underbrace{\varphi_N(\varphi_N(\ldots(\varphi_N}_{r\ \text{раз}}(i))\ldots)),$$

то для фиксированного i (при условии, что $h(F)\geqslant 2$) имеем:

$$\varphi_N^{(r)}(i)\xrightarrow[r\to+\infty]{}+\infty.$$

Следовательно:

Шаг I. Для вычисления функции $\mu_m(i)$ можно считать, что

$$\mu_m(i)=\left[\frac{D(K_m/K_{m-1})+i}{p}\right],\ \text{где}\ m\geqslant r_0.$$

В силу результатов Тэйта ([7]), для $m\geqslant m_0$

$$D_m=D(K_m/K_{m-1})=(p^{m+1}e_0-c)(p-1),$$

где c — константа, не зависящая от m. Ясно, что можно считать $m_0=1$.

Шаг II. Существует s_0 такое, что для любого $m\geqslant s_0$ выполняется условие: если $i\geqslant i_0^{(m)}$, то $\left[\frac{D_m+i}{p}\right]\geqslant i_0^{(m-1)}$, где

$$i_0^{(m)}=\left[\frac{D_m-p^{m+1}v(a_{-i_0}}{ps_{n-k_0}-1}\right].$$

Доказательство очевидно.

Ясно, что можно считать $s_0=1$.

Пусть теперь $\mu_m^{(r)}=\mu_{m-r+1}(\mu_{m-r+2}(\ldots\mu_m(i)))$. Тогда

$$\mu_m^{(r)}(i)\geqslant r(p-1)p^{m+1-r}e_0-\frac{c_1}{p-1}+\frac{i}{p^r},$$

где $c_1=\text{const}$. Следовательно, $\mu_m^{(m)}(i)\geqslant m(p-1)pe_0-\text{const}$, где const не зависит от m, i. Итак, если $\alpha\in F(K)$ является универсальной нормой из поля K_∞, то в предыдущей формуле можно взять m такое, что $\mu_m^{(m)}>v(\alpha)$. Следовательно, $\alpha=0$, q. e. d.

Поступило
15.VII.1974

Литература

[1] Алгебраическая теория чисел, М., «Мир», 1969.

[2] **Беркович В. Г.**, О делении на изогению точек эллиптической кривой, Матем. сб., 93 (135) (1974), 465—486.

[3] **Frölich A.**, Formal goups, Lecture notes in math., 74 (1968), Berlin.

[4] **Cox L.**, Formal A-modules, Bull. Amer. Math. Soc.. 79 (1973), 690—694.

[5] **Serre J.—P.**, Corps Locaux, Paris, 1962.

[6] **Serre J.—P.**, Propriétès Galoisiennes des Pointes d'ordre, Fini des Courbes Elliptigues, Invent. Math., 15 (1972), № 4, 259—331.

[7] **Tate J.**, p-Divisible Groups, Proc. of a Conference on Local Fields held at Driebergen, Springer (158—183) (Русский перевод «Математика», 13 : 2 (1969), 3—25).

[8] **Hazevinkel M.**, On Norm for One Dimensional Formal Groups, II, Beport 7210 on the Econometric Institute, Rotterdam, 1972.

[9] **Башмаков М. И., Аль-Надер Н. Ж.**, Поведение кривой $x^3+y^3=$ в круговом Г-расширении, Матем. сб., 90 (132) (1973), 117—130.

[10] **Введенский О. Н.**, Двойственность эллиптических кривых над локальным полем. II. Изв. АН СССР. Сер. матем., 30 (1966), № 4, 891—922.