

1 Используемые обозначения

Мы будем использовать следующие обозначения.

$q = p^f$, где $p \neq 2$ — простое число.

K — многомерное локальное поле такое, что существует цепочка полей

$$K = k^{(n)}, k^{(n-1)}, \dots, k^{(1)}, k^{(0)} = \mathbb{F}_q,$$

где $k^{(i)}$ при $1 \leq i \leq n$ является полным дискретно нормированным полем с полем вычетов $k^{(i-1)}$.

Набор t_n, \dots, t_1 — система локальных параметров поля K , то есть t_i является единицей в полях $K, k^{(n-1)}, \dots, k^{(i+1)}$ и при этом в поле $k^{(i)}$ является простым элементом. Таким образом, $t_n = \pi$ — простой элемент локального поля K .

$\bar{\mathbf{v}}_K = \bar{\mathbf{v}} = (\mathbf{v}_1, \dots, \mathbf{v}_n) : K^* \rightarrow \mathbb{Z}^n$ — нормирование ранга n в K . Здесь $\mathbf{v}_n(a) = \mathbf{v}_{k^{(n)}}(a)$, а для $1 \leq i < n$

$$v_i(a) = \mathbf{v}_{k^{(i)}} \left(\frac{a}{t_n^{\mathbf{v}_n(a)} \dots t_{i+1}^{\mathbf{v}_{i+1}(a)}} \right),$$

$$v_n(a) = \mathbf{v}_{k^{(n)}}(a).$$

$\mathfrak{O}_K = \{a \in K^* \mid \bar{\mathbf{v}}(a) \geq 0\}$ — кольцо нормирования, которое не зависит от выбора системы локальных параметров.

$\mathfrak{M}_K = \mathfrak{M} = \{a \in \mathfrak{O}_K \mid \bar{\mathbf{v}}(a) > 0\}$ — максимальный идеал кольца нормирования.

e_K — индекс ветвления поля K относительно нормирования $\mathbf{v} = \mathbf{v}_n$, то есть $\mathbf{v}(p) = e_K$.

\bar{e}_K — индекс ветвления поля K относительно нормирования $\bar{\mathbf{v}}$.

Введём обозначение: $\mathfrak{p}_K(r_1, \dots, r_n) = \{a \in K \mid (v_1(a), \dots, v_n(a)) \geq (r_1, \dots, r_n)\}$. Мы считаем, что группа \mathbb{Z}^n лексикографически упорядоченна: $(i_1, \dots, i_n) < (j_1, \dots, j_n)$, если для наибольшего индекса l , для которого $i_l \neq j_l$, выполняется $i_l < j_l$. Если $(r_1, \dots, r_n) > (0, \dots, 0)$, то $\mathfrak{p}_K(r_1, \dots, r_n)$ — идеал в \mathfrak{O}_K . Более того, любой идеал в \mathfrak{O}_K может быть представлен в виде $\mathfrak{p}_K(r_1, \dots, r_n)$.

Рассмотрим теперь набор мультииндексов $I \subset \mathbb{Z}^n$, будем называть набор I допустимым, если для любых i_n, \dots, i_{l+1} $1 \leq l \leq n$ найдётся целое число i такое, что из того, что $\bar{r} = (r_1, \dots, r_l, i_{l+1}, \dots, i_n) \in I$ следует $r_l \geq i$. Согласно работе [?], если мы зафиксируем B — произвольную систему представителей \mathbb{F}_q в K , то

$$\forall s \in K \quad s = \sum_{\bar{r} \in I} \alpha_{\bar{r}} t_n^{r_n} \dots t_1^{r_1},$$

где I — допустимый набор, а $\alpha_{\bar{r}} \in B$.

Рассмотрим многомерное локальное поле $K = k^{(n)}, k^{(n-1)}, \dots, k^{(1)}, k^{(0)} = \mathbb{F}_q$, в случае, когда $k^{(1)} = k$ — одномерное локальное поле характеристики ноль (конечное расширение \mathbb{Q}_p). В этом случае $K = k((t_2)) \dots ((t_n))$.

Пусть L — конечное расширение поля K без высшего ветвления, тогда $L = L^{(1)}((T_2)) \dots ((T_n))$, где L_1 — конечное расширение поля k . При этом $(\pi = t_1, t_2, \dots, t_n)$ и $(\Pi = T_1, T_2, \dots, T_n)$ — суть системы локальных параметров в полях K и L соответственно. И Пусть \mathfrak{R}_L — набор представителей Тейхмюллера в поле L .

Одномерная формальная группа $F(X, Y) \in \mathfrak{O}_K[[X, Y]]$ высоты h определяет фильтрацию Лютьца на модуле $F(\mathfrak{M}_L)$.

В одномерном случае в предложении 4 мы получили образующие модуля $F(\mathfrak{M}_L)$. В случае многомерных полей L/K этот результат получается аналогичным образом. Действительно, результаты работы [2] могут быть применены и к многомерным локальным полям L/K при условии малости абсолютного индекса ветвления поля K : $e_0 = e(K/\mathbb{Q}_p) < p$. Тогда очевидно, что рассуждения об образующих модуля $F(\mathfrak{M}_L)$ могут быть повторены для многомерного случая. Таким образом, мы получим, что, если поле L не содержит нетривиальных корней изогении $[p]_F$, а $e_0 < p$, то любой элемент $\alpha \in (\mathfrak{M}_L)$ единственным образом записывается в виде суммы $\alpha = \sum_{(F)}^* [p]_F^r \varepsilon_s(\theta_{s,r})$. Откуда, с учётом предложения 2, следует предложение 4 для многомерного случая.

С помощью предложения 5, взятого из работы [3] мы получили обобщённую функцию Артина-Хассе. В работе [3] рассматриваются обобщённые локальные поля, то есть этот результат применим и для случая многомерных локальных полей L/K . При этом поле $k^{(1)} = k$ не обязательно должно быть конечным расширением \mathbb{Q}_p , рассуждения верны для полных дискретно нормированных полей с совершенным полем вычетов полей. Тогда для многомерного случая будет верно и предложение 6 о свойствах обобщённой функции Артина-Хассе.

Теорема 1 основывается на предложениях 4 и 6, эти предложения верны для случая многомерного локального поля, а значит верным будет и утверждение Теоремы 1.

Пусть L/K — нормальное расширение поля K , а $\mathfrak{O}_L, \mathfrak{M}_L$ — кольцо целых поля L и его максимальный идеал. Через π обозначим простой элемент поля L , а $e = e(L/\mathbb{Q}_p)$ абсолютный индекс ветвления поля L относительно нормирования \mathfrak{v}_L , полученного продолжением нормирования $\mathfrak{v} = \mathfrak{v}_n$ с поля K на поле L .
 G — группа Галуа расширения L/K .

2 Формальный групповой закон

Будем рассматривать $F(X, Y) \in \mathfrak{O}_K[[X, Y]]$ — формальный групповой закон высоты для одномерной формальной группы конечной высоты h , заданный над кольцом целых многомерного локального поля K .

Пусть L/K — нормальное расширение поля K , а $\mathfrak{O}_L, \mathfrak{M}_L$ — кольцо целых поля L и его максимальный идеал. Через π обозначим простой элемент поля L , а $e = e(L/\mathbb{Q}_p)$ абсолютный индекс ветвления поля L относительно нормирования \mathfrak{v}_L , полученного продолжением нормирования $\mathfrak{v} = \mathfrak{v}_n$ с поля K на поле L .
 G — группа Галуа расширения L/K .

$[p]_F(X) \in pX + \mathfrak{O}_K[[X]]X^2$ — эндоморфизм умножения на p формальной группы F .

Рассмотрим максимальный идеал кольца целых поля L и его степени $\mathfrak{M}_L \supset \mathfrak{M}_L^2 \supset \dots$, с помощью группового закона $F(X, Y)$ на этих идеалах можно задать структуру формальных \mathbb{Z}_p -модулей:

$$\begin{aligned} \forall \alpha, \beta \in \mathfrak{M}_L^i : \alpha +_F \beta &= F(\alpha, \beta), \\ \forall a \in \mathbb{Z}_p, \forall \alpha \in \mathfrak{M}_L^i : a\alpha &= [a]_F(\alpha). \end{aligned}$$

3 Обозначения

В данной работе нам потребуются следующие обозначения.

K — локальное поле (конечное расширение поля \mathbb{Q}_p).

$e_0 = e(K/\mathbb{Q}_p) < p$ — абсолютный индекс ветвления поля K .

π — простой элемент поля K .

\mathfrak{O}_K — кольцо целых поля K .

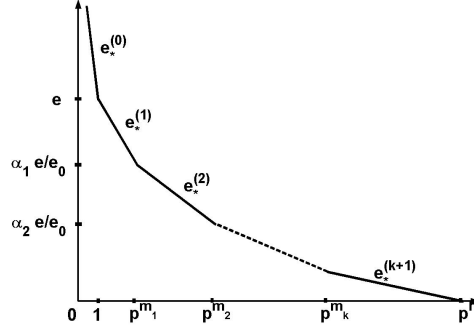
$F(X, Y)$ — одномерная формальная группа высоты h , заданная над \mathfrak{O}_K .

$[p]_F(X) \in pX + \mathfrak{O}_K[[X]]X^2$ — эндоморфизм умножения на p формальной группы F . В соответствии с работой [2] $[p]_F(X) = \sum_{i=1}^{\infty} a_i X^i$ можно записать в виде

$$[p]_F(X) = pc_0(X)X + \pi^{\alpha_1} c_1(X)X^{p^{m_1}} + \dots + \pi^{\alpha_k} c_k(X)X^{p^{m_k}} + c_h(X)X^{p^h},$$

где $c_i(X) \in \mathfrak{O}_K[[X]]^*$, $c_0(X) \equiv 1 \pmod{X}$, $\alpha_0 := e_0 > \alpha_1 > \alpha_2 > \dots > \alpha_k > \alpha_{k+1} := 0$, $0 = m_0 < m_1 < m_2 < \dots < m_k < m_{k+1} := h$.

Для изогении $[p]_F(X)$ можно построить многоугольник Ньютона. В области $M = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0, y \geq 0\}$ отметим точки $(i, \mathfrak{v}(a_i))$, где $1 \leq i \leq p^h$. Из всех ломаных с вершинами в отмеченных точках и соединяющих точки $(1, \mathfrak{v}(a_1))$ и $(p^h, \mathfrak{v}(a_{p^h}))$ выберем наиболее близкую к границе области M . Эта ломаная является нижней границей выпуклой оболочки множества $\{i, \mathfrak{v}(a_i) \mid 1 \leq i \leq p^h\}$. Построенная ломаная называется многоугольником Ньютона изогении $[p]_F(X)$. В нашем случае многоугольник Ньютона будет выглядеть примерно так:



Обозначим через $e_*^{(i)}$ тангенс угла наклона прямой, соединяющей точки $(p^{m_i}, \mathfrak{v}(a_{p^{m_i}}))$ и $(p^{m_{i-1}}, \mathfrak{v}(a_{p^{m_{i-1}}}))$:

$$e_*^{(i)} := \frac{e}{e_0} \frac{\alpha_{i-1} - \alpha_i}{p^{m_i} - p^{m_{i-1}}}.$$

Числа p^{m_i} и $e_*^{(i)}$ являются важными инвариантами формальной группы F (см. [4]).

В работе [2] доказано, что, если $e_0 < p$, то $e_*^{(1)} > e_*^{(2)} > \dots > e_*^{(k+1)}$. Более того, верно следующее утверждение (см. лемму 2 в [2]).

Предложение 1. Пусть z — ненулевой корень изогении $[p]_F(X)$ в поле L . Тогда

$$\mathfrak{v}(z) = e_*^{(i)}$$

при некотором $i : 1 \leq i \leq k+1$, если $h \geq 2$. Если же $h = 1$, то

$$\mathfrak{v}(z) = \frac{e}{p-1}.$$

Аналогичные обозначения будут для других полей:

T_K — подполе инерции поля K (максимальное неразветвлённое подполе в расширении K/\mathbb{Q}_p), простым элементом в T_K будет p .

\mathfrak{O}_{T_K} — его кольцо целых.

L — нормальное расширение поля K .

$\mathfrak{O}_L, \mathfrak{M}_L$ — кольцо целых поля L и его максимальный идеал.

Π — простой элемент поля L .

$e = e(L/\mathbb{Q}_p)$ — абсолютный индекс ветвления поля L . Мы считаем, что L/K не имеет высшего ветвления, то есть $(e, p) = 1$.

$\mathfrak{v} = \mathfrak{v}_L$ — нормирование в поле L .

T_L, \mathfrak{O}_{T_L} — подполе инерции поля L и его кольцо целых.

\mathfrak{R}_L — представители Тейхмюллера в поле L .

$G = \text{Gal}(L/K)$ — группа Галуа расширения L/K .

Пусть L/K — нормальное расширение без высшего ветвления с группой Галуа $G = \text{Gal}(L/K)$. Тогда так же, как в работе [1], сделаем $\mathfrak{O}_{T_K}[G]$ -модуль из $\mathfrak{O}_{T_L}[X]$. В поле L всегда можно выбрать такой простой элемент Π , что элемент

$$\varepsilon_\sigma = \frac{\Pi^\sigma}{\Pi} \in \mathfrak{R}_L$$

является корнем из единицы степени взаимно простой с p для любого автоморфизма $\sigma \in G$.

Теперь в кольце многочленов $\mathfrak{O}_{T_L}[X]$ можно задать действие операторов из группы G , положив

$$X^\sigma = \varepsilon_\sigma X, \sigma \in G.$$

Тем самым кольцо $\mathfrak{O}_{T_L}[X]$ становится модулем над групповым кольцом $\mathfrak{O}_{T_K}[G]$.

Рассмотрим $\mathfrak{O}_{T_K}[G]$ -подмодуль A_I из $\mathfrak{O}_{T_L}[X]$ с \mathfrak{O}_{T_K} -образующими X^i , где I — некоторая полная система вычетов по модулю $\frac{e}{e_0}$. Тогда, в соответствии с леммой 3 работы [1] имеем следующее предложение.

Предложение 2. Пусть L/K — нормальное расширение без высшего ветвления. Тогда $\mathfrak{O}_{T_K}[G]$ -модуль A_I является свободным $\mathfrak{O}_{T_K}[G]$ -модулем ранга 1.

4 Образующие модуля $F(\mathfrak{M}_L)$

Рассмотрим формальный \mathbb{Z}_p -модуль $F(\mathfrak{M}_L)$, который как множество совпадает с максимальным идеалом \mathfrak{M}_L кольца целых поля L . Структуру \mathbb{Z}_p -модуля на $F(\mathfrak{M}_L)$ зададим с помощью формального группового закона F :

$$\forall \alpha, \beta \in F(\mathfrak{M}_L) \quad \alpha +_F \beta := F(\alpha, \beta),$$

$$\forall \alpha \in F(\mathfrak{M}_L), a \in \mathbb{Z}_p \quad a\alpha := [a]_F(\alpha).$$

Тогда, если $e_0 = e(K/\mathbb{Q}_p) < p$, то, согласно работе [2], получим следующие сравнения для элемента $\alpha \in F(\mathfrak{M}_L)$.

$$[p]_F(\alpha) \equiv \begin{cases} c_h(0)\alpha^{p^h} \mod \Pi^{p^h \mathfrak{v}(\alpha)+1}, & 1 \leq \mathfrak{v}(\alpha) < e_*^{(k+1)} \\ \pi^{\alpha_i} c_i(0)\alpha^{p^{m_i}} \mod \Pi^{\alpha_i \frac{e}{e_0} + p^{m_i} \mathfrak{v}(\alpha)+1}, & e_*^{(i+1)} < \mathfrak{v}(\alpha) < e_*^{(i)} \\ & 1 \leq i \leq k \\ pc_0(0)\alpha \mod \Pi^{e+\mathfrak{v}(\alpha)+1}, & e_*^{(1)} < \mathfrak{v}(\alpha) \\ \pi^{\alpha_{i-1}} c_{i-1}(0)\alpha^{p^{m_{i-1}}} + \pi^{\alpha_i} c_i(0)\alpha^{p^{m_i}} \mod \Pi^{\alpha_i \frac{e}{e_0} + e_*^{(i)} p^{m_i} + 1}, & \mathfrak{v}(\alpha) = e_*^{(i)} \\ & 1 \leq i \leq k+1 \end{cases}$$

С помощью этих сравнений можно получить образующие для формального модуля $F(\mathfrak{M}_L)$. Пусть θ из \mathfrak{R}_L , тогда с помощью $\varepsilon_s(\theta)$ сопоставим θ некий элемент из $F(\mathfrak{M}_L)$ такой, что $\varepsilon_s(\theta) \equiv \theta \Pi^s \mod \Pi^{s+1}$.

Предложение 3. Любой элемент $\alpha \in F(\mathfrak{M}_L)$ представим в виде суммы

$$\alpha = \sum_{(F)}^* [p]_F^r \varepsilon_s(\theta_{s,r}),$$

где символ $\sum_{(F)}^*$ обозначает суммирование по всем неотрицательным r и по индексам s из некоторого специального индексного множества I . При этом, если поле L не содержит нетривиальных корней изогении $[p]_F$, то такое представление однозначно.

В частности, в множестве I не будут встречаться индексы, большие $e_*^{(1)} + e$. Запишем I в виде $I = \{1 \leq s \leq e_*^{(1)} + e \mid \star\}$, где \star — некое условие, которое мы получим ниже.

Доказательство. Для начала индукцией проверим, что любой элемент α из $F(\mathfrak{M}_L)$ можно представить в виде суммы следующего вида: $\alpha = \sum_{s=1(F)}^{\infty} \varepsilon_s(\theta_s)$, где $\theta_s \in \mathfrak{R}_L$, $\varepsilon_s(\theta_s) \in F(\mathfrak{M}_L)$ такие, что $\varepsilon_s(\theta_s) \equiv \theta \Pi^s \pmod{\Pi^{s+1}}$.

База индукции очевидна, так как любой элемент из $F(\mathfrak{M}_L)$ имеет вид $\alpha = \theta_1 \Pi + \dots \Rightarrow \alpha \equiv \theta_1 \Pi \pmod{\Pi^2}$.

$$\begin{aligned} \text{Пусть теперь } \alpha &\equiv \sum_{s=1(F)}^t \varepsilon_s(\theta_s) \pmod{\Pi^{t+1}} \Rightarrow \alpha = \sum_{s=1(F)}^t \varepsilon_s(\theta_s) + \\ + \theta_{t+1} \Pi^{t+1} + \dots &\equiv \sum_{s=1(F)}^t \varepsilon_s(\theta_s) + \theta_{s+1} \Pi^{t+1} \pmod{\Pi^{t+2}} \equiv \sum_{s=1(F)}^t \varepsilon_s(\theta_s) +_F \\ +_F \theta_{s+1} \Pi^{t+1} &\pmod{\Pi^{t+2}}. \end{aligned}$$

Таким образом, мы получили, что для каждого $t > 0$ $\alpha \equiv \sum_{s=1(F)}^t \varepsilon_s(\theta_s) \pmod{\Pi^{t+1}}$, а значит $\alpha = \sum_{s=1(F)}^{\infty} \varepsilon_s(\theta_s)$.

Далее, пользуясь сравнениями, уберём лишние индексы в этой сумме. Будем считать, что $\beta \equiv \theta \Pi^{\mathbf{v}(\beta)} \pmod{\Pi^{\mathbf{v}(\beta)+1}} \in F(\mathfrak{M}_L)$, $c_i(0) = c_i + \dots$, $\pi = \xi \Pi^{\frac{e}{e_0}} + \dots$, $p = \zeta \Pi^e + \dots$, где $\theta, c_i, \xi, \zeta \in \mathfrak{R}_L$.

1. Если $s = \mathbf{v}(\beta) > e_*^{(1)}$, то $[p]_F(\beta) = p c_0(0) \beta + \dots \equiv \zeta c_0 \theta \Pi^{s+e} \pmod{\Pi^{s+e+1}}$, следовательно, если в качестве θ взять $\theta = \theta_{s+e} (\zeta c_0)^{-1} \in \mathfrak{R}_L$, то $\beta \equiv \theta \Pi^s \pmod{\Pi^{s+1}} \equiv \varepsilon_s(\theta) \pmod{\Pi^{s+1}}$, а для слагаемого с индексом $s + e$ получим следующее сравнение:

$$\varepsilon_{s+e}(\theta_{s+e}) \equiv [p]_F(\beta) \pmod{\Pi^{s+e+1}} \equiv [p]_F(\varepsilon_s(\theta)) \pmod{\Pi^{s+e+1}}.$$

Это сравнение означает, что в сумме $\alpha = \sum_{s=1(F)}^{\infty} \varepsilon_s(\theta_s)$ любое слагаемое $\varepsilon_j(\theta_j)$ индекса $j > e_*^{(1)} + e$ можно заменить на слагаемое вида $[p]_F(\varepsilon_{j-e}(\theta_{j-e,1}))$, то есть в индексном множестве I нет индексов, больших $e_*^{(1)} + e$.

2. Если $1 \leq s = \mathbf{v}(\beta) < e_*^{(k+1)}$, то $[p]_F(\beta) \equiv c_h \theta p^h \Pi^{p^h s} \pmod{\Pi^{p^h s+1}}$. Представители Тейхмюллера \mathfrak{R}_L p -делимы, значит $\theta = (c_h^{-1} \theta_{p^h s})^{\frac{1}{p^h}}$ будет лежать в \mathfrak{R}_L . При таком θ получим, что

$$[p]_F(\varepsilon_s(\theta)) \equiv [p]_F(\beta) \pmod{\Pi^{p^h s+1}} \equiv \theta_{p^h s} \Pi^{p^h s} \pmod{\Pi^{p^h s+1}}.$$

А это означает, что в сумме $\alpha = \sum_{s=1(F)}^{\infty} \varepsilon_s(\theta_s)$ будут отсутствовать слагаемые вида $\varepsilon_{p^h s}(\theta_{p^h s})$, где $1 \leq s < e_*^{(k+1)}$.

3. Если $e_*^{(i+1)} < s = \mathbf{v}(\beta) < e_*^{(i)}$ для некоторого $1 \leq i \leq k$, то

$$\begin{aligned} [p]_F(\varepsilon_s(\theta)) &\equiv [p]_F(\beta) \pmod{\Pi^{\alpha_i \frac{e}{e_0} + p^{m_i} s + 1}} \equiv \\ &\equiv \xi^{\alpha_i} c_i \theta p^{m_i} \Pi^{\alpha_i \frac{e}{e_0} + p^{m_i} s} \pmod{\Pi^{\alpha_i \frac{e}{e_0} + p^{m_i} s + 1}}. \end{aligned}$$

$\xi^{\alpha_i} c_i \theta p^{m_i s} \in \mathfrak{R}_L$, поэтому мы можем рассмотреть $\theta = (\xi^{-\alpha_i} c_i^{-1} \theta_{\alpha_i \frac{e}{e_0} + p^{m_i} s})^{\frac{1}{p^{m_i}}} \in \mathfrak{R}_L$. Тогда получим, что для любого индекса $j = \alpha_i \frac{e}{e_0} + p^{m_i} s$ при некотором $1 \leq i \leq k$ и $e_*^{(i+1)} < s < e_*^{(i)}$ будет выполняться сравнение

$$[p]_F(\varepsilon_s(\theta)) \equiv \varepsilon_j(\theta_j) \pmod{\Pi^{j+1}},$$

а значит из индексного множества I можно убрать все такие индексы j .

4. В случае, если $s = \mathfrak{v}(\beta) = e_*^{(i)}$ для некоторого $1 \leq i \leq k+1$, рассмотрим $j = \alpha_i \frac{e}{e_0} + p^{m_i} s$, тогда

$$\begin{aligned} [p]_F(\varepsilon_s(\theta)) &\equiv [p]_F(\beta) \pmod{\Pi^{j+1}} \equiv \\ &\equiv (\xi^{\alpha_{i-1}} c_{i-1} \theta^{p^{m_{i-1}}} + \xi^{\alpha_i} c_i \theta^{p^{m_i}}) \Pi^j \pmod{\Pi^{j+1}}. \end{aligned}$$

Будем считать, что сравнения

$$\theta_j \equiv \xi^{\alpha_{i-1}} c_{i-1} \theta^{p^{m_{i-1}}} + \xi^{\alpha_i} c_i \theta^{p^{m_i}} \pmod{\Pi}$$

имеют решения θ в \mathfrak{R}_L для любого θ_j из \mathfrak{R}_L , тогда индексы вида $e_*^{(i)}$, где $1 \leq i \leq k+1$, можно выкинуть из множества I .

Таким образом, условие \star состоит из четырёх пунктов:

1. $s \leq e + e_*^{(1)} = \alpha_0 \frac{e}{e_0} + p^{m_0} e_*^{(1)}$,
2. $s \neq p^h j = \alpha_{k+1} \frac{e}{e_0} + p^{m_{k+1}} j$ ни для какого $1 \leq j < e_*^{(k+1)}$,
3. $s \neq \alpha_i \frac{e}{e_0} + p^{m_i} j$ ни для каких $1 \leq i \leq k$ и $e_*^{(i+1)} < j < e_*^{(i)}$,
4. $s \neq \alpha_i \frac{e}{e_0} + p^{m_i} e_*^{(i)}$ ни для какого $1 \leq i \leq k+1$.

В итоге любой элемент α из $F(\mathfrak{M}_L)$ можно представить в виде суммы $\alpha = \sum_{(F)}^* [p]_F^r \varepsilon_s(\theta_{s,r})$, где символ $\sum_{(F)}^*$ означает, что суммирование ведётся по всем неотрицательным r , а s берутся из индексного множества $I = \{1 \leq s \leq e + e_*^{(1)} \mid \star\}$.

Ясно, что, если L не содержит нетривиальных корней изогении $[p]_F$, то такое представление будет однозначным. \square

Разобьём индексное множество I на непересекающиеся подмножества так, чтобы в каждом из них было по $\frac{e}{e_0}$ различных представителей вычетов по модулю $\frac{e}{e_0}$. Рассмотрим числа $i_j := \alpha_j \frac{e}{e_0} + p^{m_j} e_*^{(j+1)}$, $0 \leq j \leq k+1$ (здесь и в дальнейшем будем считать, что $e_*^{(k+2)} = 0$), тогда I представляется в виде объединения непересекающихся множеств $I_j := \{i_j \leq s < i_{j+1} \mid \star\}$: $I = \bigcup_{j=1}^{k+1} I_j$. Заметим, что для каждого j все индексы $s = \alpha_j \frac{e}{e_0} + p^{m_j} l$, где $e_*^{(j+1)} < l < e_*^{(j)}$, лежат в интервале I_j . Действительно:

$$\begin{aligned} s &= \alpha_j \frac{e}{e_0} + p^{m_j} l > \alpha_j \frac{e}{e_0} + p^{m_j} e_*^{(j+1)} = i_j, \\ s &= \alpha_j \frac{e}{e_0} + p^{m_j} l < \alpha_j \frac{e}{e_0} + p^{m_j} e_*^{(j)} = \alpha_j \frac{e}{e_0} + p^{m_j} \frac{e}{e_0} \frac{\alpha_{j-1} - \alpha_j}{p^{m_j} - p^{m_{j-1}}} = \\ &= \frac{e}{e_0} \frac{p^{m_j} \alpha_j - p^{m_{j-1}} \alpha_j + p^{m_j} \alpha_{j-1} - p^{m_j} \alpha_j}{p^{m_j} - p^{m_{j-1}}} = \frac{e}{e_0} \frac{p^{m_j} \alpha_{j-1} - p^{m_{j-1}} \alpha_j}{p^{m_j} - p^{m_{j-1}}} = \\ &= \frac{e}{e_0} \frac{p^{m_j} \alpha_{j-1} - p^{m_{j-1}} \alpha_{j-1} + p^{m_{j-1}} \alpha_{j-1} - p^{m_{j-1}} \alpha_j}{p^{m_j} - p^{m_{j-1}}} = \\ &= \alpha_{j-1} \frac{e}{e_0} + p^{m_{j-1}} \frac{e}{e_0} \frac{\alpha_{j-1} - \alpha_j}{p^{m_j} - p^{m_{j-1}}} = \alpha_{j-1} \frac{e}{e_0} + p^{m_{j-1}} e_*^{(j)} = i_{j-1}. \end{aligned}$$

Таким образом, условие \star в каждом из множеств I_j будет равномерно «выкалывать» индексы с шагом p^{m_j} . Из каждого I_j будет «выколото» ровно $e_*^{(j)} - e_*^{(j+1)}$ индексов, а значит из всех $e + e_*^{(1)}$ индексов в множестве I будет «выколото» ровно $(e_*^{(k+1)} - e_*^{(k+2)}) + (e_*^{(k)} -$

$-e_*^{(k+1)}) + \dots + (e_*^{(1)} - e_*^{(2)}) = e_*^{(1)}$ индексов, а значит в I останется e индексов. Разобьём их на e_0 групп по $\frac{e}{e_0}$ в каждой. Ясно, что если для любого j $\frac{e}{e_0}$ делит $(p^{m_j} - 1)$: $t_j \frac{e}{e_0} = p^{m_j} - 1$, то каждое из множеств I_j разбивается в объединение $t_j(e_*^{(j)} - e_*^{(j+1)})$ множеств по $\frac{e}{e_0}$ представителей вычетов по модулю $\frac{e}{e_0}$. Следовательно можно будет наше множество I представить в виде объединения $I = \bigcup_{i=1}^{e_0} I_{\frac{e}{e_0}}^i$, где множества $I_{\frac{e}{e_0}}^i$ имеют такой вид, как требуется в предложении 1.

Используя результаты этого параграфа, получим, что $\mathfrak{O}_{T_K}[G]$ -модуль A_I , построенный на $\mathfrak{O}_{T_K}[X]$ образующих X^s , где s из нашего индексного множества $I = \{1 \leq s \leq e + e_*^{(1)} \mid \star\}$ будет представляться в виде прямой суммы модулей $A_{I_{\frac{e}{e_0}}^i}$: $A_I = \bigoplus_{i=1}^{e_0} A_{I_{\frac{e}{e_0}}^i}$. В предложении 2 говорится, что каждый модуль $A_{I_{\frac{e}{e_0}}^i}$ является свободным $\mathfrak{O}_{T_K}[G]$ -модулем ранга 1, а значит будет верным следующее предложение.

Предложение 4. Пусть $I = \{1 \leq s \leq e + e_*^{(1)} \mid \star\}$. Рассмотрим $\mathfrak{O}_{T_K}[G]$ -модуль A_I , с \mathfrak{O}_{T_K} -образующими X^s , где $s \in I$. Тогда A_I является свободным $\mathfrak{O}_{T_K}[G]$ -модулем ранга e_0 .

5 Функция Артина-Хассе

Теперь займёмся построением аналога функции Артина-Хассе

$$E(X) = \exp \left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \dots \right)$$

для нашего случая. Для этого мы воспользуемся результатами работы [3].

$F(X, Y)$ — p -типическая одномерная формальная группа, определённая над \mathfrak{O}_K . Тогда её логарифм имеет вид:

$$\lambda_F(X) = X + c_1 X^p + c_2 X^{p^2} + \dots = \Lambda_F(\Delta)(X),$$

где Δ действует на переменную X как возведение в степень p , а на коэффициенты, как автоморфизм Фробениуса в расширении K/\mathbb{Q}_p . В работе [3] доказано, следующее.

Предложение 5.

1. Существуют ряд $v_F(\Delta) = p + \pi \sum_{i \geq 1} b_i \Delta^i$ и ряд $u_F(\Delta) = p + \sum u_j \Delta^j$, где $b_i \in \mathfrak{O}_K$, а u_j лежат в \mathfrak{O}_{T_K} , такие, что $\Lambda_F(\Delta) = \frac{v_F(\Delta)}{u_F(\Delta)}$. При этом, если $h = htF < \infty$ — высота формальной группы F , то $p \mid u_1, u_2, \dots, u_{h-1}$; $u_h \in \mathfrak{O}_{T_K}^*$.
2. В классе изоморфных над \mathfrak{O}_K формальных групп существует единственная формальная группа F_{ah} с логарифмом

$$\lambda_{ah}(X) = \Lambda_{ah}(\Delta)(X) = \frac{v(\Delta)}{u(\Delta)}(X), \text{ где}$$

$$v(\Delta) = p + \pi b_1 \Delta + \dots + \pi b_h \Delta^h,$$

$$u(\Delta) = p + p u_1 \Delta + \dots + p u_{h-1} \Delta^{h-1} + u_h \Delta^h.$$

При этом $\text{tr}_{K/T_K} b_i = 0$.

Ряд $E_F(X) = (\lambda_F^{-1} \circ \lambda_{ah})(X)$ будет задавать строгий изоморфизм формальных групп над \mathfrak{O}_K $E_F : F_{ah} \rightarrow F$. Рассмотрим функцию $E_F(\varphi) := (\Lambda_F^{-1} \circ \Lambda_{ah})(\Delta)(\varphi)$. Она будет действовать из $\mathfrak{O}_L[[X]]$ в $F(\mathfrak{O}_L[[X]])$ и будет обладать следующими свойствами.

Предложение 6.

$$E_F(\varphi) = (\Lambda_F^{-1} \circ \Lambda_{ah})(\Delta)(\varphi) : \mathfrak{O}_L[[X]] \rightarrow F(\mathfrak{O}_L[[X]]), \text{ тогда}$$

$$1. \forall \varphi, \psi \in \mathfrak{O}_L[[X]] \quad E_F(\varphi + \psi) = E_F(\varphi) +_F E_F(\psi).$$

$$2. E_F(pX^m) = [p]_F E_F(X^m).$$

$$3. \forall \sigma \in \text{Gal}(L/K) \quad E_F(X^\sigma) = (E_F(X))^\sigma.$$

$$4. \forall a \in \mathfrak{O}_L \quad E_F(aX^m) \equiv aX^m \pmod{X^{m+1}}.$$

Доказательство. E_F задаёт изоморфизм формальных групп F и F_{ah} , то есть $E_F(F_{ah}(X, Y)) = F(E_F(X), E_F(Y))$. $\Lambda_{ah}(\Delta)$ — линейный оператор, поэтому $\Lambda_{ah}(\Delta)(\varphi + \psi) = \Lambda_{ah}(\Delta)(\varphi) + \Lambda_{ah}(\Delta)(\psi)$. Отсюда очевидно следует, что

$$\begin{aligned} E_F(\Delta)(\varphi + \psi) &= \Lambda_F^{-1}(\Lambda_{ah}(\Delta)(\varphi + \psi)) = \\ &= \Lambda_F^{-1}(\Lambda_{ah}(\Delta)(\varphi) + \Lambda_{ah}(\Delta)(\psi)) = \\ &= \Lambda_F^{-1}(\Lambda_F \circ \Lambda_F^{-1} \circ \Lambda_{ah}(\Delta)(\varphi) + \Lambda_F \circ \Lambda_F^{-1} \circ \Lambda_{ah}(\Delta)(\psi)) = \\ &= \Lambda_F^{-1}(\Lambda_F(E_F(\varphi)) + \Lambda_F(E_F(\psi))) = E_F(\varphi) +_F E_F(\psi). \end{aligned}$$

Свойство 1 доказано.

Из свойства 1 по определению эндоморфизма $[p]_F$ сразу же вытекает свойство 2.

Для доказательства свойства 3 рассмотрим σ из группы Галуа G , тогда $X^\sigma = \varepsilon_\sigma X$, где $\varepsilon_\sigma \in \mathfrak{K}_L$. Следовательно, $\Delta(X^\sigma) = \Delta(\varepsilon_\sigma X) = \varepsilon_\sigma^p \Delta(X)$. С другой стороны, $(\Delta(X))^\sigma = (X^\sigma)^\sigma = \varepsilon_\sigma^p X^\sigma$. Отсюда следует, что $\Delta(X^\sigma) = (\Delta(X))^\sigma$ и

$$E_F(X^\sigma) = (\Lambda_F^{-1} \circ \Lambda_{ah})(\Delta)(X^\sigma) = (\Lambda_F^{-1} \circ \Lambda_{ah})(\Delta)(X)^\sigma = (E_F(X))^\sigma.$$

Так как $(\lambda_F^{-1} \circ \lambda_{ah})(X)$ задаёт строгий изоморфизм формальных групп F и F_{ah} , то $(\Lambda_F^{-1} \circ \Lambda_{ah})(\Delta) \equiv 1 \pmod{(\Delta)}$, а значит выполнено свойство 4: $E_F(aX^m) \equiv aX^m \pmod{X^{m+1}}$. \square

6 Итоговый результат

Рассмотрим $\mathfrak{O}_{T_K}[G]$ -модуль A_I , который по предложению 4 является свободным $\mathfrak{O}_{T_K}[G]$ -модулем ранга e_0 . Пусть $\beta_1, \beta_2, \dots, \beta_{e_0}$ образуют нормальный базис модуля A_I , то есть элементы

$\{\beta_l^\sigma \mid 1 \leq l \leq e_0, \sigma \in G\}$ образуют базис модуля A_I над \mathfrak{O}_{T_K} . Тогда, если $b_1, b_2, \dots, b_n \in \mathfrak{O}_{T_K}$ образуют базис кольца \mathfrak{O}_{T_K} над \mathbb{Z}_p , то множество $\{b_j \beta_l \mid 1 \leq l \leq e_0, 1 \leq j \leq n\}$ является нормальным базисом модуля A_I как $\mathbb{Z}_p[G]$ -модуля, а это означает, что A_I является свободным $\mathbb{Z}_p[G]$ -модулем ранга ne_0 , где $n = (\mathfrak{O}_{T_K} : \mathbb{Z}_p)$.

В предложении 3 говорилось, что любой α из $F(\mathfrak{M}_L)$ представим в виде $\alpha = \sum_{(F)}^* [p]_F^r \varepsilon_s(\theta_{s,r})$, где $\varepsilon_s(\theta_{s,r}) \equiv \theta_{s,r} \Pi^s \pmod{\Pi^{s+1}}$. Из свойств функции E_F ясно, что $\varepsilon_s(\theta_{s,r}) \equiv E_F(\theta_{s,r} X^s)|_{X=\Pi} \pmod{\Pi^{s+1}}$, а значит

$$\forall \alpha \in F(\mathfrak{M}_L) \quad \alpha = E_F\left(\sum_{s \in I} \sum_{r \geq 0} p^r \theta_{s,r} X^s\right)|_{X=\Pi} = E_F(\varphi)|_{X=\Pi},$$

где φ из A_I . Так как $E_F(\varphi + \psi) = E_F(\varphi) +_F E_F(\psi)$, то получаем, что функция E_F задаёт гомоморфизм \mathbb{Z}_p -модулей A_I и $F(\mathfrak{M}_L)$. Если поле L не содержит нетривиальных корней изогении $[p]_F$, то E_F , по предложению 3, будет \mathbb{Z}_p -изоморфизмом. Более того, по свойству 3, $E_F(X^\sigma) = (E_F(X))^\sigma$ для любого σ из группы Галуа G , а значит E_F задаёт изоморфизм A_I и $F(\mathfrak{M}_L)$ как $\mathbb{Z}_p[G]$ -модулей.

Рассмотрим образующие $\mathbb{Z}_p[G]$ -модуля A_I :

$$\{b_j\beta_l \mid 1 \leq l \leq e_0, 1 \leq j \leq n\}.$$

Отображение E_F будет переводить их в образующие $\mathbb{Z}_p[G]$ -модуля $F(\mathfrak{M}_L)$, а это значит, что $F(\mathfrak{M}_L)$ является свободным $\mathbb{Z}_p[G]$ -модулем ранга ne_0 .

Аналогичные рассуждения можно провести и для остальных модулей $F(\mathfrak{M}_L^i)$ фильтрации Лютц.

В итоге, мы получили следующий результат.

Теорема 1. Пусть K — конечное расширение поля \mathbb{Q}_p , с индексом ветвления $e_0 = e(K/\mathbb{Q}_p) < p$, и пусть L/K — нормальное расширение без высшего ветвления с группой Галуа $G = \text{Gal}(L/K)$. Рассмотрим формальную группу $F(X, Y)$ конечной высоты h , заданную над кольцом целых \mathfrak{O}_K поля K . Пусть $[p]_F(X) = pc_0(X)X + \pi^{\alpha_1}c_1(X)X^{p^{m_1}} + \dots + \pi^{\alpha_k}c_k(X)X^{p^{m_k}} + c_h(X)X^{p^h}$ — эндоморфизм умножения на p формальной группы F . Тогда, если выполняются следующие условия:

1. L не содержит нетривиальных корней изогении $[p]_F$,
2. Для любого i из $\{1, 2, \dots, k+1\}$ сравнение $\theta_* \equiv \xi^{\alpha_{i-1}}c_{i-1}\theta^{p^{m_{i-1}}} + \xi^{\alpha_i}c_i\theta^{p^{m_i}} \pmod{\Pi}$ имеет решение $\theta \in \mathfrak{R}_L$ для любого $\theta_* \in \mathfrak{R}_L$, где $\pi = \xi\Pi^{\frac{e}{e_0}} + \dots$,

то $F(\mathfrak{M}_L)$ является свободным $\mathbb{Z}_p[G]$ -модулем ранга ne_0 , где $n = (\mathfrak{O}_{T_K} : \mathbb{Z}_p)$. Аналогичный результат верен и для $F(\mathfrak{M}_L^i)$.

7 Обозначения

В данной работе будем рассматривать многомерное локальное поле $K = k^{(n)}, k^{(n-1)}, \dots, k^{(1)}, k^{(0)} = \mathbb{F}_q$, в случае, когда $k^{(1)} = k$ — одномерное локальное поле характеристики ноль (конечное расширение \mathbb{Q}_p). В этом случае $K = k((t_2)) \dots ((t_n))$, где набор t_n, \dots, t_1 — система локальных параметров поля K . Таким образом, t_i является единицей в полях $K, k^{(n-1)}, \dots, k^{(i+1)}$ и при этом в поле $k^{(i)}$ является простым элементом. Для всех $0 \leq i < n$ поле $k^{(i)}$ является полем вычетов для полного дискретно нормированного поля $k^{(i+1)}$. Через $\pi = t_n$ будем обозначать простой элемент поля $k^{(n)}$, а $\mathbf{v}_{k^{(i)}}$ — нормирование в поле $k^{(i)}$. $\overline{\mathbf{v}}_K = \overline{\mathbf{v}} = (\mathbf{v}_1, \dots, \mathbf{v}_n) : K^* \rightarrow \mathbb{Z}^n$ — нормирование ранга n в K . Здесь $\mathbf{v}_n(a) = \mathbf{v}_{k^{(n)}}(a)$, а для $1 \leq i < n$

$$v_i(a) = \mathbf{v}_{k^{(i)}} \left(\frac{a}{t_n^{\mathbf{v}_n(a)} \dots t_{i+1}^{\mathbf{v}_{i+1}(a)}} \right),$$

$\mathfrak{O}_K = \{a \in K^* \mid \overline{\mathbf{v}}(a) \geq 0\}$ — кольцо нормирования, которое не зависит от выбора системы локальных параметров.

$\mathfrak{M}_K = \mathfrak{M} = \{a \in \mathfrak{O}_K \mid \overline{\mathbf{v}}(a) > 0\}$ — максимальный идеал кольца нормирования. \mathbb{Z}^n считается лексикографически упорядоченным.

e_K — индекс ветвления поля K относительно нормирования $\mathbf{v} = \mathbf{v}_n$, то есть $\mathbf{v}(p) = e_K$.

\overline{e}_K — индекс ветвления поля K относительно нормирования $\overline{\mathbf{v}}$.

Пусть L/K — нормальное расширение без высшего ветвления с группой Галуа $G = \text{Gal}(L/K)$, тогда $L = L^{(1)}((T_2)) \dots ((T_n))$, где $L^{(1)}$ — конечное расширение поля k . При этом обозначим через $(\Pi = T_1, T_2, \dots, T_n)$ — систему локальных параметров в поле L . $\mathfrak{O}_L, \mathfrak{M}_L$ — кольцо целых поля L и его максимальный идеал, а $\overline{e} = (e_1, e_2, \dots, e_n)$ абсолютный индекс ветвления поля L относительно нормирования $\overline{\mathbf{v}}_L = (\mathbf{v}_1^L, \dots, \mathbf{v}_n^L)$, полученного продолжением нормирования $\overline{\mathbf{v}}$ с поля K на поле L . \mathfrak{R}_L — мультипликативная система представителей Тейхмюллера поля $L^{(0)}$, где L_0 — подполе инерции в расширении L_1/\mathbb{Q}_p .

Также, нам могут понадобиться \mathfrak{O}_k и \mathfrak{O}_{L_1} — кольца целых одномерных локальных полей k и $L^{(1)}$ соответственно, и их максимальные идеалы: \mathfrak{M}_k и \mathfrak{M}_{L_1} .

Возьмём $F(X, Y) \in \mathfrak{O}_K[X, Y]$ — формальный групповой закон, определяющий одномерную формальную группу конечной высоты h .

Рассмотрим максимальный идеал кольца целых поля L и его степени $\mathfrak{M}_L \supset \mathfrak{M}_L^2 \supset \dots$, с помощью группового закона $F(X, Y)$ на этих идеалах можно задать структуру формальных \mathbb{Z}_p -модулей. $F(\mathfrak{M}_L^i)$ совпадает с \mathfrak{M}_L^i как множество. Определим на нём операцию сложения через $F(X, Y)$: $\forall \alpha, \beta \in \mathfrak{M}_L^i : \alpha +_F \beta = F(\alpha, \beta)$. Кольцо \mathbb{Z}_p вкладывается в кольцо эндоморфизмов формальной группы F ([6, §2]), поэтому для любого скаляра $a \in \mathbb{Z}_p$ и любого $\alpha \in \mathfrak{M}_L^i$ естественным образом определяется умножения на скаляр: $a\alpha = [a]_F(\alpha)$. Более того, эндоморфизмы F вкладываются в \mathfrak{O}_K , так как группа определена над \mathfrak{O}_K . $[p]_F(X) \in pX + \mathfrak{O}_K[[X]]X^2$ — эндоморфизм умножения на p формальной группы F .

Список литературы

- [1] С. В. Востоков, «Фильтрация Лютц как модуль Галуа в расширении без высшего ветвления», *Аналитическая теория чисел и теория функций*. 8, Зап. научн. сем. ЛОМИ, **160**, ЛОМИ, Ленинград, 1987, 182-192.
- [2] С. В. Востоков, А. Н. Зиновьев, «Арифметика модуля корней изогении формальной группы в малом ветвлении», *Вопросы теории представлений алгебр и групп*. 14, Зап. научн. сем. ПОМИ, **338**, ПОМИ, СПб., 2006, 125-136.
- [3] М. В. Бондарко, С. В. Востоков, «Явная классификация формальных групп над локальными полями», *Теория чисел, алгебра и алгебраическая геометрия*, Сборник статей. К 80-летию со дня рождения академика Игоря Ростиславовича Шафаревича, Тр. МИАН, **241**, Наука, М., 2003, 43-67.
- [4] М. И. Башмаков, А. Н. Кириллов, «Фильтрация Лютц формальных групп», *Изв. АН СССР. Сер. матем.*, **39**:6 (1975), 1227-1239.
- [5] С. В. Востоков, «Норменное спаривание в формальных модулях», *Изв. АН СССР. Сер. матем.*, **43**:4 (1979), 765-794.
- [6] С. В. Востоков, «Символы на формальных группах», *???*, **43**:4 (1981), 985-1014.