Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет»

На правах рукописи

Иконникова Елена Валерьевна

Канонический базис Гензеля-Шафаревича для формальных модулей Любина-Тейта и Хонды

Специальность 01.01.06 –
«Математическая логика, алгебра и теория чисел»

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук, профессор
Востоков Сергей Владимирович

Санкт-Петербург
2022

Оглавление

Введение

Тема исследования, ее актуальность и разработанность

Исследования формальных групп связаны со многими активно развивающимися разделами математики.

Во-первых, они играют важнейшую роль в теории полей классов. Так, формальные группы Любина-Тейта являются ключевым элементом при описании абелевых расширений локального поля (локальная теорема Кронекера-Вебера) ([37]).

Во-вторых, построение формальных групп помогает в изучении эллиптических кривых ([41]).

В-третьих, формальные группы постоянно возникают в алгебраической топологии при изучении обобщенных теорий когомологий ([1]). Учитывая тесную связь обобщенных теорий когомологий со стабильной теорией гомотопий и изучением спектров, формальные группы чрезвычайно полезны и для этих областей. Применение их в алгебраической топологии началось с работ Новикова, Бухштабера и Квиллена ([22], [3], [38]).

В-четвертых, формальные группы можно рассматривать как "промежуточное звено" между группами Ли и алгебрами Ли.

Известны также примеры приложения формальных групп к столь неожиданной области, как раскраска гиперграфов.

Построение базисов формальных модулей является ключевым шагом к выведению явных формул для символа Гильберта. Данная задача имеет долгую историю. Еще в работе Э. Куммера [35] был доказан результат, который в современных терминах является явной формулой для символа Гильберта меж-

ду определёнными элементами кругового расширения поля p-адических чисел. Явные формулы несколько иного типа впервые появляются в работе Артина и Хассе [26]. В дальнейшем развивались оба направления — построение формул типа Артина-Хассе (где символ Гильберта выражается через след некоторого элемента) и типа Куммера (представляющих символ Гильберта в виде вычета определённого ряда).

Сначала опишем развитие формул типа Артина-Хассе. В круговом локальном поле $\mathbb{Q}_p(\zeta)$ явные формулы такого типа были получены К. Ивасавой ([34]), в произвольном локальном поле — Ш. Сеном ([39]). Также изучался символ Гильберта, определённый относительно формальной группы. А. Уайлс ([42]) получил формулу типа Артина-Хассе для формальных групп Любина-Тейта для поля деления изогении $[\pi^m]$, А. В. Колывагин ([20]) — для полей, содержащих поле деления изогении $[\pi^m]$. В мультипликативном случае и в случае формальных групп Любина-Тейта продвижения были также получены Р. Коулманом ([29]). Выдвинутая им гипотеза о виде формулы в общем случае формальных групп Любина-Тейта была доказана А. Де Шалитом [40]. Ф. Детрам [30] обобщил формулы Сена на случай формальных групп Любина-Тейта, а Д. Бенуа [27] — на случай p-делимых групп.

Изучение формул Куммеровского типа было продолжено в работе И. Р. Шафаревича [24]. С помощью теоремы Гензеля [33] Шафаревич построил мультипликативный базис группы главных единиц и, пользуясь разложением по этому базису, дал явное определение символа Гильберта в виде вычета некоторого ряда.

Более элементарные формулы в общем случае были получены в конце семидесятых годов независимо С. В. Востоковым ([12]) и Г. Брюкнером ([28]). В работе Востокова был преобразован и развит подход, использованный Шафаревичем. Метод, предложенный в этой работе, был впоследствии успешно применён в значительном количестве других важных случаев. Изложим подробнее основные шаги этого метода.

1. В соответствующем модуле (модуль формальной группы либо мультипликативная группа поля) строится система образующих, называемая обыч-

но системой образующих Гензеля или базисом Шафаревича (построение проводится по аналогии с методом, использованным Шафаревичем для построения базиса в работе [24]).

2. На кольце рядов строится формальное спаривание $\langle \cdot, \cdot \rangle$, заданное явной формулой как вычет некоторого ряда. Это спаривание определяется между формальными аналогами объектов, на которых задан символ Гильберта. Проверяется линейность и символьное свойство для формального спаривания. Затем с помощью разложения элементов поля K в ряды по простому элементу формальное спаривание переносится на K до спаривания $\{\cdot, \cdot\}$. Проверяется корректность этой конструкции, независимость результата от конкретного разложения в ряд и выбора простого элемента.

3. Полученное спаривание $\{\cdot, \cdot\}$ вычисляется на элементах системы образующих Гензеля, и на них проверяется её совпадение с символом Гильберта.

4. С использованием независимости явного спаривания совпадение построенного спаривания $\{\cdot, \cdot\}$ и символа Гильберта проверяется на всех элементах. Таким образом получается явная формула символа Гильберта.

Подобная схема была использована при построении формул типа Куммера для формальных групп Любина-Тейта ([4] - [7], [23]) относительных формальных групп Любина-Тейта ([8]), формальных групп Хонды ([9], [10]), для обобщенных формальных групп Любина-Тейта ([21]) и в ряде работ, посвященных многомерному локальному полю.

В случае классического локального поля с полем вычетов характеристики p, не содержащего корень из единицы степени p, элементы базиса Шафаревича выглядят следующим образом:

$$E(c_i X^i)|_{X=\pi},$$

где E — экспонента Артина-Хассе, π — униформизирующая локального поля, c_i принадлежат набору $\Re$ представителей в K базиса последнего поля вычетов

k над $\mathbb{F}_p$, $1 \leq i < \frac{pv(p)}{p-1}$. Любая главная единица поля единственным образом представима в виде произведения элементов базиса в целых p-адических степенях.

Если наибольшее m, такое, что поле содержит корень из единицы степени p^m, больше нуля, то в набор элементов базиса Шафаревича добавляется элемент

$$\omega(a) = E(as(X))|_{X=\pi},$$

где a — целый элемент подполя инерции, такой, что его след в $\mathbb{Q}_p$ не делится на p^m, а s — ряд с целыми коэффициентами из подполя инерции. При этом

$$s(X) = z(X)^{p^m} - 1,$$

где $z(X)$ — ряд с целыми коэффициентами из подполя инерции, причем

$$z(\pi) = \zeta_{p^m},$$

первообразному корню из единицы степени p^m. Любая главная единица поля представима в виде произведения элементов базиса в целых p-адических степенях, при этом базис является каноническим по модулю K^{p^m}, т. е. для двух элементов поля, отличающихся множителем из K^{p^m}, соответствующие показатели в представлении сравнимы по модулю p^m.

Цели и задачи исследования

Целью данного исследования является построение системы образующих для формальных модулей Любина-Тейта и Хонды.

Методы исследования

Работа носит теоретический характер. Использовались методы алгебраической теории чисел и теории формальных групп.

Научная новизна и степень достоверности

Все представленные результаты являются новыми, их достоверность подтверждается наличием математически строгих доказательств.

Публикации и апробация результатов

Основные результаты работы докладывались и обсуждались на:

- конференции "Local Arithmetic Geometry" (Санкт-Петербург, 2015),
- международной конференции по алгебре, анализу и геометрии (Казань, 26 июня - 2 июля 2016 года),
- XV международной конференции "Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения" (Тула, 28-31 мая 2018 года),
- семинарах в СПбГУ и ПОМИ.

Результаты опубликованы в 3 статьях ([18], [19], [13]). Статья [18] написана в соавторстве, диссертанту принадлежат леммы 2 и 3 из §1 и доказательство теоремы 5. Статья [13] написана в соавторстве, диссертанту принадлежит раздел 3.1. Все журналы, в которых были опубликаованы результаты, входят в список рекомендованных ВАК для соискателей ученой степени кандидата и доктора наук и в наукометрическую базу данных SCOPUS.

Положения, выносимые на защиту

Теорема 1. *Пусть n-мерное поле K не содержит корень из единицы степени p. Тогда любую его главную единицу можно представить в виде*

$$\prod_{\overrightarrow{r}\in\Omega} E(\theta_{\overrightarrow{r}}\overrightarrow{X}^{\overrightarrow{r}})^{a_{\overrightarrow{r}}}|_{\overrightarrow{X}=\overrightarrow{t}},$$

где

- Ω — *допустимое множество;*
- $\theta_{\overrightarrow{r}} \in \Re$, $\Re$ – *система представителей базиса последнего поля вычетов как векторного пространства над* $\mathbb{F}_p$*;*
- $a_{\overrightarrow{r}} \in \mathbb{Z}_p$*;*
- $\overrightarrow{t}$ — *локальные параметры;*
- $0 < \overrightarrow{r} < \frac{p\overrightarrow{v}(p)}{p-1}$*;*
- $p \not| \overrightarrow{r}$,

однозначно при $v_n(p) > 0$ *и с точностью до множителя из* K^{p^d} *для произвольного натурального* d *при* $v_n(p) = 0$*, причем такое представление канонично по модулю* K^{p^d}*.*

Теорема 2. *Пусть* K *– n-мерное поле, и наибольшее* m*, такое, что поле содержит корень из единицы степени* p^m*, больше нуля. Обозначим этот корень за* ζ*. Тогда любую главную единицу поля* K *можно представить в виде*

$$\prod_{\overrightarrow{r}\in\Omega} E(\theta_{\overrightarrow{r}}\overrightarrow{X}^{\overrightarrow{r}})^{a_{\overrightarrow{r}}} E(as(X))^b|_{\overrightarrow{X}=\overrightarrow{t}},$$

где

- Ω — *допустимое множество;*
- $\theta_{\overrightarrow{r}} \in \Re$*;*
- $a_{\overrightarrow{r}}, b \in \mathbb{Z}_p$*;*
- $\overrightarrow{t}$ — *локальные параметры;*
- $0 < \overrightarrow{r} < p\overrightarrow{v}(p)/(p-1)$*;*
- $p \not| \overrightarrow{r}$*;*
- a — *целый элемент подполя инерции, такой, что* $Tr_{T/\mathbb{Q}_p} a \equiv 1 \mod p^m$*;*

- $z(\overrightarrow{X}) \in R\{\{X_1\}\}\{\{X_2\}\}...\{\{X_{n-1}\}\}[[X_n]]$, *причем* $z(\overrightarrow{t}) = \zeta_{p^m}$, *первообразному корню из единицы степени* p^m;
- $s = z^{p^m} - 1$,

с точностью до множителя из K^{p^m}. *При этом базис является каноническим по модулю* K^{p^m}, *т.е. для двух элементов поля, отличающихся множителем из* K^{p^m}, *соответствующие показатели в представлении сравнимы по модулю* p^m.

Рассмтрим теперь построение системы образующих для формальных модулей Любина-Тейта. Опишем рассматриваемую ситуацию. У нас имеется локальное поле K_0 нулевой характеристики, k_0 — поле вычетов K_0, $|k_0| = q = p^f > 0$, K — полное дискретно нормированное поле, содержащее K_0, с полем вычетов k. Пусть также $F(X, Y)$ — формальная группа Любина-Тейта над O_0 (кольцом целых K_0), $F(M)$ – формальный O_0-модуль, натянутый на максимальный идеал поля K.

Основные результаты (в обозначениях, вводимых далее) выглядят так:

Теорема 3. *Пусть* k *совершенно. Тогда множества*

$$E(\Theta\pi^s), s \in S_e, s \neq e_m,$$

$$E(H\pi^{e_m}) \text{ и } E(\Xi\pi^{e_1}),$$

являются системой образующих модуля $F(M)$ *над* O_0. *Т.е., любой элемент* $\alpha \in F(M)$ *представим в виде*

$$\alpha = [a_*]\eta_*\pi^{e_m} +_F \sum\nolimits_F [a_i]\varepsilon_i,$$

где ε_i *пробегает все упомянутые множества, кроме элемента* $\eta_* \in Ker\psi$, $a_i, a_* \in O_0$. *При этом* a_i, a_* *определены однозначно по модулю* π_0^n.

Теорема 4. *Пусть* k *несовершенно. Тогда множество*

$$E(A^{q^\mu}[T_{q^\mu}]\pi^{q^\mu s}) \cup E(\Gamma\pi^{qe_1})$$

является системой образующих модуля $F(M)$ *над* O_T*. Т.е., любой элемент* $\alpha \in F(M)$ *представим в виде*

$$\beta = \sum_{s,\mu,(k),(r)} [a_{\alpha,\beta}] E(\alpha^{q^\mu} t_{(r)}^{(k)} \pi^{q^\mu s}) +_F \sum\nolimits_F [b_{\gamma,\beta}] E(\gamma \pi^{e_1}).$$

При этом $a_{\alpha,\beta}, b_{\gamma,\beta}$ *определены однозначно по модулю* π_0^n*.*

Далее мы переходим к построению системы образующих для формальных модулей Хонды. Пусть k – локальное поле характеристики 0, $\bar{k} = \mathbb{F}_q$, $q = p^f$, $p \neq 2$, k'/k – конечное неразветвленное расширение с униформизующей π, K – n-мерное локальное поле, L – конечное расширение K, имеющее вид

$$L = L_1((T_2)) \dots ((T_n)),$$

L_1 – конечное расширение K_1 и $L_i = L_1((T_2)) \dots ((T_i)))$, $\mathfrak{M}$ – максимальный идеал в L. Пусть $F(X,Y) \in \mathcal{O}_K[[X,Y]]$ – формальная группа.

Теорема 5. *Элементы*

$$\widetilde{\omega}_i(b), b \in \mathcal{O}_K, \quad 1 \leq i \leq h,$$

$$\widetilde{\mathcal{E}}_N^0(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}),$$

$$\widetilde{\mathcal{E}}_N^{\rho,a}(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}),$$

где $\theta \in \mathcal{R}$, $a \in \mathcal{O}_K^*$, $1 \leq \rho < fh$, $p \nmid \overrightarrow{i}$, $0 < i_n \leq e_* = p^h e_n/(p^h - 1)$, $\mathcal{E}_N^0$, $\mathcal{E}_N^{\rho,a}$ *– определенные далее изоморфизмы, связанные с многочленами Эньяра, являются множеством образующих для* $F(\mathfrak{M})$*.*

Структура диссертации

Текст диссертации изложен на 77 страницах. Он включает в себя введение, четыре главы и заключение. Список литературы состоит из 42 наименований.

В первой главе приведены необходимые предварительные сведения о формальных группах. Вторая глава посвящена построению базиса Шафаревича

для многомерного поля с совершенным последним полем вычетов. Третья глава посвящена построению системы образующих для формальных модулей Любина-Тейта. В четвертой главе рассматривается случай формальных модулей Хонды.

Глава 1

Предварительные сведения

В этой главе мы изложим основные определения и теоремы теории формальных групп. Изложение материала основывается на [31].

1.1 Формальные группы: определение и простейшие свойства

В этом разделе A – коммутативное кольцо с единицей.

Определение 1. Формальный степенной ряд от двух переменных $F(X,Y) \in A[[X,Y]]$ задает коммутативную формальную группу над кольцом A, если выполняются условия

$$F(X,0) = F(0,X) = X, \tag{1.1}$$

$$F(F(X,Y),Z) = F(X,F(Y,Z)), \tag{1.2}$$

$$F(X,Y) = F(Y,X). \tag{1.3}$$

Простейшими примерами являются аддитивная формальная группа

$$F_+(X,Y) = X + Y \tag{1.4}$$

и мультипликативная формальная группа

$$F_{\times}(X,Y) = X + Y + XY = (1+X)(1+Y) - 1. \tag{1.5}$$

Из определения следует, что формальная группа имеет вид

$$F(X,Y) = X + Y + \sum_{i+j \geqslant 2} a_{ij} X^i Y^j, \quad a_{ij} \in A. \tag{1.6}$$

Определение 2. Формальный степенной ряд $f(X) \in XA[[X]]$ называется гомоморфизмом из формальной группы F в формальную группу G, если

$$f(F(X,Y)) = G(f(X), f(Y)). \tag{1.7}$$

f называется изоморфизмом, если существует обратный к нему относительно композиции ряд $g = f^{-1}$, т.е., $(f \circ g)(X) = (g \circ f)(X) = X$.

Множество $\mathrm{End}_A(F)$ эндоморфизмов формальной группы F (гомоморфизмов из F в F) обладает структурой кольца относительно сложения

$$f(X) +_F g(X) = F(f(X), g(X)) \tag{1.8}$$

и композиции.

Лемма 1. *Существует единственный гомоморфизм* $\mathbb{Z} \to \mathrm{End}_A(F)$*:*

$$n \mapsto [n]_F. \tag{1.9}$$

Доказательство. Положим

$$[0]_F = 0, \quad [1]_F(X) = X, \quad [n+1]_F(X) = F([n]_F(X), X) \text{ при } n \geqslant 0. \tag{1.10}$$

Теперь покажем, что существует формальный степенной ряд $[-1]_F(X) \in XA[[X]]$ такой, что $F(X, [-1]_F(X) = 0$. Положим $\varphi_1(X) = -X$. Предположим,

что

$$F(X, \varphi_i(X)) \equiv 0 \mod \deg(i+1) \text{ при } 1 \leqslant i \leqslant m \tag{1.11}$$

и, кроме того,

$$F(X, \varphi_m(X)) \equiv c_{m+1} X^{m+1} \mod \deg(m+2). \tag{1.12}$$

Тогда, положив

$$\varphi_{m+1}(X) = \varphi_m(X) - c_{m+1} X^{m+1}, \tag{1.13}$$

получим

$$F(X, \varphi_{m+1}(X)) = X + \varphi_m(X) - c_{m+1} X^{m+1} + \sum_{i+j \geqslant 2} a_{ij} X^i \varphi^i(\varphi_{m+1}(X))^j \equiv$$
$$\equiv F(X, \varphi_m(X) - c_{m+1} X^{m+1} \equiv 0 \mod \deg(m+2) \tag{1.14}$$

Предел $\lim \varphi_m(X)$ обладает требуемым свойством. Взяв его за $[-1]_F(X)$, положим

$$[n]_F(X) = F([n+1]_F(X), [-1]_F(X) \tag{1.15}$$

для $n \leqslant -2$. Легко видеть, что полученное отображение является гомоморфизмом. □

Пусть теперь K – поле характеристики 0.

Предложение 1. *Любая формальная группа над K изоморфна аддитивной формальной группе F_+, т.е., существует формальный степенной ряд $\lambda(X) \in XK[[X]]$, $\lambda(X) \equiv X \mod \deg 2$, такой что*

$$F(X, Y) = \lambda^{-1}(\lambda(X) + \lambda(Y)). \tag{1.16}$$

Доказательство. Обозначим за $F_2'(X, Y)$ частную производную $\frac{\partial F}{\partial Y}(X, Y)$. До-

кажем, что

$$F_2'(F(X,Y),0) = F_2'(X,Y)F_2'(Y,0). \tag{1.17}$$

Сначала заметим, что

$$F_2'(X,F(Y,Z))F_2'(Y,Z) = \frac{\partial}{\partial Z}F(X,F(Y,Z)) = \frac{\partial}{\partial Z}F(F(X,Y),Z). \tag{1.18}$$

Подставим $Z=0$. Теперь возьмем такой ряд $\lambda(X) = X + \sum\limits_{n\geqslant 2} c_n X^n$, что

$$\lambda'(X) = 1 + \sum_{n\geqslant 2} nc_n X^{n-1} = \frac{1}{F_2'(X,0)} = \frac{1}{1 + X + \sum\limits_{i\geqslant 1} a_{i1}X^i}. \tag{1.19}$$

Тогда

$$\frac{\partial}{\partial Y}\lambda(F(X,Y)) = \frac{F_2'(X,Y)}{F_2'(F(X,Y),0)} = \frac{1}{F_2'(Y,0)} = \frac{\partial}{\partial Y}\lambda(Y) \tag{1.20}$$

и, следовательно,

$$\frac{\partial}{\partial Y}\left(\lambda(F(X,Y) - \lambda(Y)\right) = 0. \tag{1.21}$$

Таким образом, $\lambda(F(X,Y)) = \lambda(Y) + g(X)$ для некоторого ряда $g(X) \in K[[X]]$. Положив $Y=0$, получим, что $\lambda(X) = \lambda(F(X,0)) = g(X)$. В итоге,

$$F(X,Y) = \lambda^{-1}(\lambda(X) + \lambda(Y)). \tag{1.22}$$

Определение 3. Ряд $\lambda(X)$ из предложения 1 называется логарифмом формальной группы F и часто обозначается как $\log_F(X)$, а обратный к нему относительно композиции – как $\exp_F(X)$.

□

Определение 4. ([14]) Пусть K_0 – локальное поле, K – его конечное расширение, $\mathcal{O} = \mathcal{O}_K$ и $\mathcal{O}_0 = \mathcal{O}_{K_0}$ – соответствующие кольца целых. Формальную

группу $F(X,Y)$ над $\mathcal{O}$ с логарифмом $\lambda(X) \in K[[x]]$ назовем формальной $\mathcal{O}_0$-модульной группой, если определен кольцевой гомоморфизм

$$\begin{gathered}[\cdot] : \mathcal{O}_0 \to \mathrm{End}_{\mathcal{O}}(F), \\ a \mapsto [a]_F(X) = \lambda^{-1}(a\lambda(X)).\end{gathered} \tag{1.23}$$

1.2 Формальные группы Любина-Тейта

1.2.1 Определение формальных групп Любина-Тейта

Пусть K – локальное числовое поле, с полем вычетов k мощности q и простым элементом π. Обозначим через $\mathcal{F}_\pi$ множество формальных степенных рядов $f(X) \in \mathcal{O}_K[[X]]$, таких что выполняются два условия:

$$f(X) \equiv \pi X \mod \deg 2, \tag{1.24}$$

$$f(X) \equiv X^q \mod \pi. \tag{1.25}$$

($\mathcal{O}_K$ – кольцо целых поля K.)

Теорема 6. *Пусть $f(X) \in \mathcal{F}_\pi$. Тогда существует единственная формальная группа $F = F_f$ над $\mathcal{O}_K$, такая что*

$$F_f(f(X), f(Y)) = f(F_f(X), F_f(Y)). \tag{1.26}$$

При этом для любого $\alpha \in \mathcal{O}_K$ существует единственный эндоморфизм $[\alpha]_F \in \mathrm{End}_{\mathcal{O}_K}(F)$, такой что

$$[\alpha]_F(X) \equiv \alpha X \mod \deg 2. \tag{1.27}$$

Более того, отображение $\mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$:

$$\alpha \mapsto [\alpha]_F \tag{1.28}$$

является гомоморфизмом колец. При этом $f = [\pi]_F$. Если $g \in \mathcal{F}_\pi$ и $G = F_g$ –

соответствующая формальная группа, то F_f и F_g изоморфны над $\mathcal{O}_K$.

Определение 5. Построенная выше формальная группа F_f называется формальной группой Любина-Тейта.

Предложение 2 ([4])**.** *В классе изоморфных формальных групп Любина-Тейта, соответствующих множеству $\mathcal{F}_\pi$, найдется такая формальная группа F с логарифмом λ, что для любого $n \geqslant 1$ коэффициенты ряда*

$$\lambda_a^{-1} \circ \lambda \circ [\pi^n], \tag{1.29}$$

где

$$\lambda_a(X) = X + \frac{X^q}{\pi} + \frac{X^{q^2}}{\pi^2} + \dots \tag{1.30}$$

– логарифм Артина-Хассе, при степенях, меньших q^n, делятся на π, а при степени q^n коэффициент равен 1.

1.2.2 Формальные модули Любина-Тейта

Пусть F_f, $f(X) \in \mathcal{F}_\pi$ – формальная группа Любина-Тейта над $\mathcal{O}_K$, где K – локальное числовое поле. Пусть L – пополнение алгебраического расширения над K. На максимальном идеале $\mathcal{M}_L$ можно ввести структуру $\mathcal{O}_K$-модуля $F(\mathcal{M}_L)$, задав сложение и умножение следующим образом:

$$\alpha +_F \beta = F(\alpha, \beta), \tag{1.31}$$

$$a \cdot \alpha = [a]_F(\alpha), \tag{1.32}$$

для $a \in \mathcal{O}_K$, $\alpha, \beta \in \mathcal{M}_L$. Пусть

$$\kappa_n = \left\{\alpha \in \mathcal{M}_{K^{sep}} : [\pi^n]_F(\alpha) = 0\right\}. \tag{1.33}$$

Определим поле $L_n = K(\kappa_n)$. Тогда L_n/K – вполне разветвленное абелево расширение степени $q^n(q-1)$ и $\mathrm{Gal}(L_n/K)$ изоморфна $U_K/U_{n,K}$. Положим $K_\pi =$

$\bigcup\limits_{i\geqslant 1} L_n$ и обозначим через Ψ_K отображение взаимности.

Важность формальных групп Любина-Тейта для теории полей классов обусловлена следующей теоремой:

Теорема 7. *L_n является полем классов для $\langle\pi\rangle \times U_{n,K}$, а K_π – полем классов для $\langle\pi\rangle$.*

Группа Галуа $\mathrm{Gal}(K^{ab}/K)$ *изоморфна прямому произведению* $\mathrm{Gal}(K^{ur}/K)\times \mathrm{Gal}(K_\pi/K)$ *и*

$$\Psi_K(\pi^a u)(\xi) = [u^{-1}]_F(\xi) \tag{1.34}$$

для $\xi \in \bigcup\limits_{i\geqslant 1} \kappa_n$, $a \in \mathbb{Z}$, $u \in U_K$.

1.2.3 Примарные элементы

Используя обозначения предыдущего раздела, предположим, что поле L содержит ядро изогении $[\pi^n]$. Обозначим через $\frac{1}{[\pi^n]}\omega$ решение уравнения

$$[\pi^n](X) = \omega. \tag{1.35}$$

Определение 6. Элемент $\omega \in F(\mathcal{M}_L)$ называется π^n-примарным, если расширение $L\left(\frac{1}{[\pi^n]}\omega\right)/L$ неразветвлено.

Из условия $\mathrm{Ker}[\pi^n] \subseteq L$ следует, что расширение $L\left(\frac{1}{[\pi^n]}\omega\right)/L$ абелево.

1.3 Формальные группы Хонды

В этом разделе K будет локальным полем с конечным полем вычетов $\mathbb{F}_q$ характеристики $p \neq 2$ ($q = p^f$). Пусть π – униформизующая K. Через L будет обозначено конечное неразветвленное расширение поля K.

Введем также следующие обозначения:

- φ – непрерывное продолжение автоморфизма Фробениуса поля K на пополнение K^{ur} его максимального неразветвленноно расширения;

- $\Delta(\sum \alpha_i X^i) = \sum(\varphi(\alpha_i)X^{qi})$ при $\alpha_i \in K^{ur}$.

1.3.1 Формальные группы Хонды и их тип

Рассмотрим множество операторов вида

$$\sum_{i \geqslant 0} a_i \Delta^i, \quad a_i \in \mathcal{O}_L. \tag{1.36}$$

Если ввести в нем умножение по правилу

$$\Delta a = a^{\varphi}\Delta \text{ при } \quad a \in \mathcal{O}_L, \tag{1.37}$$

это множество превратится в некоммутативное кольцо.

Определение 7. Формальная группа $F \in \mathcal{O}_L[[X, Y]]$ с логарифмом $log_F(X) \in L[[X]]$ называется формальной группой Хонды, если

$$u \circ log_F \equiv 0 \mod \pi \tag{1.38}$$

для некоторого оператора

$$u = \pi + a_1\Delta + \ldots \in \mathcal{O}_L[[\Delta]]. \tag{1.39}$$

Такой оператор u называется типом формальной группы F.

Заметим, что над неразветвленным расширением $\mathbb{Q}_p$ каждая одномерная формальная группа является группой Хонды.

Определение 8. Типы u и v формальной группы F называются эквивалентными, если $u = \varepsilon \circ v$ для некоторого $\varepsilon \in \mathcal{O}_L[[\Delta]]$, $\varepsilon(0) = 1$.

Пусть F – формальная группа типа u. Тогда $v = \pi + b_1\Delta + \ldots \in \mathcal{O}_L[[\Delta]]$ является типом F тогда и только тогда, когда u и v эквивалентны.

Пользуясь подготовительной леммой Вейерштрасса, можно доказать, что для каждой формальной группы Хонды существует единственный канонический тип

$$u = \pi - a_1\Delta - \ldots - a_h\Delta^h, a_1, \ldots, a_{h-1} \in \mathcal{M}_L, a_h \in \mathcal{O}_L^*. \tag{1.40}$$

Он однозначно (с точностью до изоморфизма) задает группу F. h называется высотой F.

Пусть F, G – две формальных группы Хонды, типов u и v соответственно. Тогда

$$\mathrm{Hom}_{\mathcal{O}_L}(F, G) = \{a \in \mathcal{O}_L : au = va\}, \tag{1.41}$$

$$\mathrm{End}_{\mathcal{O}_L}(F) = \mathcal{O}_K. \tag{1.42}$$

Наряду с (1.40), порой полезно использовать эквивалентный ему тип

$$\widetilde{u} = \pi - a_h\Delta^h - a_{h+1}\Delta^{h+1} - \ldots \tag{1.43}$$

Его можно получить из u применением оператора, обратного к

$$C = a - \frac{a_1}{\pi}\Delta - \ldots - \frac{a_{h-1}}{\pi}\Delta^{h-1}, \tag{1.44}$$

то есть,

$$\widetilde{u} = \left(\pi^{-1}\left(u + a_h\Delta^h\right)\right)^{-1} = \pi - \left(\pi^{-1}\left(u + a_h\Delta^h\right)\right)^{-1} a_h\Delta^h. \tag{1.45}$$

1.3.2 Классификационные теоремы

Сформулируем две классификационные теоремы для формальных групп Хонды, доказанные в [15]

Теорема 8. *Пусть F – формальная группа Хонды типа*

$$\widetilde{u} = \pi - a_h\Delta^h - a_{h+1}\Delta^{h+1} - \ldots, \quad a_i \in \mathcal{O}_L, \tag{1.46}$$

и a_h обратим. Пусть

$$u = \pi - a_1\Delta - \ldots - a_h\Delta^h, a_1, \ldots, a_{h-1} \in \mathcal{M}_L \tag{1.47}$$

– канонический тип F и $\lambda = log_F$ – ее логарифм. Положим $\lambda_1 = B_1\lambda^{\varphi^h}$, где

$$B_1 = 1 + \frac{a_{h+1}}{a_h}\Delta + \frac{a_{h+2}}{a_h}\Delta^2 + \ldots \tag{1.48}$$

(таким образом, $\widetilde{u} = \pi - a_hB_1\delta^h$).

Тогда

1. *λ_1 является типом некоторой формальной группы Хонды F_1 типа $\widetilde{u}_1 = a_h^{-1}\widetilde{u}a_h$, и каноническим типом F_1 является $u_1 = a_h^{-1}ua_h$;*
2. *$f = \left[\frac{\pi}{a_h}\right]$ является $\mathcal{O}_L$ - гомоморфизмом из F в F_1 и $f(X) \equiv X^{q^h} \mod \pi$.*

Теорема 9. *Пусть $f \in \mathcal{O}_L[[X]]$ – степенной ряд, удовлетворяющий условиям*

$$f(X) \equiv X^{q^h} \mod \pi, \tag{1.49}$$

$$f(X) \equiv \frac{\pi}{a_h} \mod \deg 2, \tag{1.50}$$

где a_h – обратимый элемент $\mathcal{O}_L$. Пусть также

$$u = \pi - a_1\Delta - \ldots - a_h\Delta^h, a_1, \ldots, a_{h-1} \in \mathcal{M}_L \tag{1.51}$$

и

$$C = a - \frac{a_1}{\pi}\Delta - \ldots - \frac{a_{h-1}}{\pi}\Delta^{h-1}. \tag{1.52}$$

Положим

$$\widetilde{u} = C^{-1}u = \pi - a_h\Delta^h - a_{h+1}\Delta^{h+1} - \dots. \tag{1.53}$$

Тогда существует и единственна формальная группа Хонды F типа $\widetilde{u}$ и канонического типа u, такая что $f = \left[\frac{\pi}{a_h}\right]$ является $\mathcal{O}_L$ - гомоморфизмом из F в F_1 (где F_1 строится способом, указанным в предыдущей теореме.)

Данные теоремы позволяют нам определить на множестве форммальных групп Хонды над кольцом $\mathcal{O}_L$ обратимый оператор $\mathcal{A} : F \to F_1$ и построить цепочку формальных групп

$$F \to F_1 \to \dots \to F_n, \tag{1.54}$$

где $F_m = \mathcal{A}^m F$.

Обозначим через $\lambda_m = \log_{F_m}$ логарифм формальной группы F_m и через u_m ее канонический тип. Положим

$$\pi_1 = \pi/a_h, \quad \pi_m = \pi_1^{\varphi^{h(m-1)}} = \pi/a_h^{\varphi^{h(m-1)}}, \tag{1.55}$$

$$\pi_1^{(m)} = \prod_{i=1}^{m} \pi_i = \pi^m/a_h^{1+\varphi^h+\dots+\varphi^{h(m-1)}}. \tag{1.56}$$

Тогда $u_m \circ \pi_1^{(m)} = \pi_1^{(m)} u$.

Введя обозначение $f^{(m)} = f_{m-1} \circ f_{m-2} \circ \dots \circ f_1 \circ f$, из теоремы 8 можно вывести, что

$$f_{m-1}(X) \equiv \pi_m X \mod \deg 2, \tag{1.57}$$

$$f^{(m)}(X) \equiv \pi_1^{(m)} X \mod \deg 2. \tag{1.58}$$

Глава 2

Канонический базис для многомерного локального поля

Определение 9. Поле K называется n-мерным локальным полем над полем k, если задана последовательность полных дискретно нормированных полей $K_n = K$, K_{n-1}, $\ldots$, $K_0 = k$, где каждое последующее поле является полем вычетов предыдущего.

При данной терминологии классическое локальное поле является одномерным локальным полем над некоторым конечным полем.

Результатом этой главы является построение базиса Шафаревича для многомерного поля с совершенным последним полем вычетов.

2.1 Обозначения

Будем придерживаться следующих обозначений:

- K - n-мерное локальное поле над совершенным полем k, char $K = 0$, char $k = p$;

- $\overrightarrow{t} = (t_1, t_2, .., t_n)$ – набор локальных параметров в K;
- R - система представителей Тейхмюллера поля вычетов k;
- $\Re$ - система представителей базиса k как векторного пространства над $\mathbb{F}_p$, $\Re \subset R$;
- $\overrightarrow{v}()$ - n-мерное нормирование поля K;
- $\overrightarrow{e} := \overrightarrow{v}(p)$;
- $\overrightarrow{e}_1 := \frac{\overrightarrow{e}}{p-1}$ (не обязательно целочисленный вектор);
- для индекса $\overrightarrow{r} \in \mathbb{Z}^n$ $\overrightarrow{r} = (r_1, r_2, ..., r_n)$;
- на индексах введен лексикографический порядок:

$$\overrightarrow{q} > \overrightarrow{r} \Longleftrightarrow \exists 1 \leq l \leq n : q_n = r_n, q_{n-1} = r_{n-1}, ..., q_{l+1} = r_{l+1}, q_l > r_l$$

  (в частности, будем называть индекс положительным, если его первый с конца ненулевой элемент положителен);
- $\overrightarrow{t}^{\overrightarrow{i}} := t_1^{i_1} t_2^{i_3} ... t_n^{i_n}$;
- $\overrightarrow{t}^{\overrightarrow{i_1}} \equiv \overrightarrow{t}^{\overrightarrow{i}_2} \mod \overrightarrow{t}^{\overrightarrow{r}}+ \Longleftrightarrow \exists \overrightarrow{r}_1 > \overrightarrow{r} : \overrightarrow{t}^{\overrightarrow{i_1}} \equiv \overrightarrow{t}^{\overrightarrow{i_2}} \mod \overrightarrow{t}^{\overrightarrow{r}_1}$;
- $p \equiv \theta_0 \overrightarrow{t}^{\overrightarrow{e}} \mod \overrightarrow{t}^{\overrightarrow{e}}+$;
- $\overline{a}$ — вычет, соответствующий элементу $a \in K$;
- $rep : k \to R$ – отображение, сопоставляющее вычету его представитель Тейхмюллера.

2.2 Сходимость рядов с p-адическими коэффициентами

Теперь рассмотрим вопрос сходимости в многомерном локальном поле степенных рядов с p-адическими коэффициентами при подстановке в них элементов максимального идеала, а также сходимость сумм результатов таких подстановок.

Определение 10. Набор индексов Ω будем называть допустимым, если для любых $i_n, ..., i_{n-k+1} \in \mathbb{Z}$ найдется $i_{n-k} \in \mathbb{Z}$ такое, что для каждого $\overrightarrow{r} \in \Omega$ с $r_n = i_n, \ldots, r_{n-k+1} = i_{n-k+1}$, выполняется неравенство $r_{n-k} \geq i_{n-k}$

Определение 11. Множество наборов индексов $\{\Omega_i, i \in I\}$ будем называть допустимым, если:

1. любой индекс встречается не более чем в конечном числе наборов множества;
2. $\bigcup_{i \in I} \Omega_i$ — допустимый набор индексов.

Следующие две теоремы доказаны в статье [17].

Теорема 10. *Пусть $\{\Omega_i, i \in I\}$ — допустимое множество наборов индексов. Тогда для любых $b_{i,\overrightarrow{r}} \in R$ сумма*

$$\sum_{i \in I} \sum_{\overrightarrow{r} \in \Omega_i} b_{i,\overrightarrow{r}} \overrightarrow{t}^{\overrightarrow{r}} \tag{2.1}$$

сходится.

Теорема 11. *Пусть $\{\Omega_i, i \in I\}$ — допустимое множество наборов положительных индексов. Тогда для любых $b_{i,\overrightarrow{r}} \in R$ произведение*

$$\prod_{i \in I} (1 + \sum_{\overrightarrow{r} \in \Omega_i} b_{i,\overrightarrow{r}} \overrightarrow{t}^{\overrightarrow{r}}) \tag{2.2}$$

сходится.

Замечание. Если множество $\{\Omega_i, i \in I\}$ не является допустимым, нетрудно видеть, что сумма и произведение из теорем 10 и 11 могут расходиться.

Теперь докажем подготовительную лемму:

Лемма 2. *Пусть Ω — допустимый набор положительных индексов. Тогда $\Omega^* = \{\overrightarrow{r}_1 + \overrightarrow{r}_2 + ... + \overrightarrow{r}_m | r_i \in \Omega, m \in \mathbb{N}\}$ – допустимый набор индексов, при этом любой его элемент может быть представлен в виде суммы индексов из Ω не более чем конечным числом способов.*

Доказательство. Сначала докажем допустимость, используя индукцию. Докажем, что, выбрав последние k элементов значения суммы индексов, мы ограничиваем некоторой константой количество слагаемых с хотя бы одним ненулевым элементом среди последних k элементов, а также количество возможных наборов их последних k элементов. Заметим, что это утверждение для k, равного длине индекса, равносильно второму утверждению теоремы. И докажем, что тогда есть оценка снизу на $(n-k)$-ый элемент суммы.

При $k = 0$ ограничение последнего индекса снизу такое же, как в Ω. При $k = 1$ и значении последнего элемента суммы s у слагаемых последний элемент не может быть больше s и меньше 0, следовательно, количество допустимых наборов конечно. Из этого и допустимости Ω сразу следует ограничение снизу на предпоследний элемент суммы. С другой стороны, слагаемых с ненулевым последним элементом также не может быть больше s.

Теперь докажем переход от $k-1$ к k. Пусть зафиксированы последние k значений суммы. Тогда ограничено некоторой константой количество слагаемых с хотя бы одним ненулевым элементом среди последних $k-1$ элементов, а также (по индукционному предположению) количество возможных наборов их последних $k-1$ элементов. Отсюда и из допустимости Ω сразу следует ограничение снизу на k-ый с конца элемент их суммы, а также каждого слагаемого. У каждого слагаемого есть еще и ограничение сверху, так как сумма для них ограничена сверху. Для индексов с нулевыми последними $(k-1)$-ми элементами и ненулевыми k-ми отсюда также следует ограничение на количество, а также значения k-х элементов. Из ограничений следует, что число допустимых

наборов последних k элементов слагаемых конечно, поэтому $(k+1)$-ый с конца элемент их суммы ограничен снизу из допустимости Ω. $\square$

Следствие 1. *Пусть Ω_1, Ω_2 — два допустимых набора положительных индексов. Тогда $\Omega_+ = \{\overrightarrow{r}_1 + \overrightarrow{r}_2 | r_i \in \Omega_i\}$ — допустимый набор индексов, при этом любой его элемент может быть представлен в виде суммы индексов из Ω_1 и Ω_2 только конечным числом способов.*

Доказательство. Набор $\Omega_\bigcup = \Omega_1 \bigcup \Omega_2$ допустим. При этом для него $\Omega^*_\bigcup$ по лемме 2 является допустимым набором и содержит Ω_+, значит, Ω_+ также допустим. Представления в виде сумм индексов также содержат все представления вида $\overrightarrow{r}_1 + \overrightarrow{r}_2$, $r_i \in \Omega_i$, и их конечное число. $\square$

Лемма 3. *Для любого ряда $f(X) \in \mathbb{Z}_p[[X]]$ и любого мультииндекса $\overrightarrow{r} > \overrightarrow{0}$ корректна подстановка*

$$f(X)\big|_{X=\overrightarrow{t}^{\overrightarrow{r}}}. \tag{2.3}$$

Доказательство. Запишем ряд f в виде

$$f(X) = \sum_{i \geq 0} c_i X^i. \tag{2.4}$$

Разложим p по степеням локальных параметров:

$$p = \sum_{\overrightarrow{q} \in \Gamma} \theta_{\overrightarrow{q}} \overrightarrow{t}^{\overrightarrow{q}}, \tag{2.5}$$

где Γ – допустимый набор индексов. Теперь представим c_i в виде

$$c_i = \sum_{j \geq 0} \theta_{i,j} p^j = \sum_{\overrightarrow{q} \in \Gamma^*} \left(\sum_{l=1}^{m_{\overrightarrow{q}}} a_{\overrightarrow{q},l} \theta_{\overrightarrow{q},l} \right) \overrightarrow{t}^{\overrightarrow{q}}, \quad a_{\overrightarrow{q},l} \in \mathbb{Z}. \tag{2.6}$$

По лемме 2 любой мультииндекс $\overrightarrow{q} \in \Gamma^*$ появляется в разложении лишь для конечного числа индексов j, значит, и набор коэффициентов при $\overrightarrow{t}^{\overrightarrow{q}}$ конечен.

Рассмотрим наборы мультииндексов

$$\Gamma_l = \left\{ \overrightarrow{q} \in \Gamma^* : l = m_{\overrightarrow{q}} \right\}. \tag{2.7}$$

Заметим, что $\bigcup_{l\geq 1} \Gamma_l = \Gamma^*$ и $\{\Gamma_l, l \geq 1\}$ – допустимое мультимножество наборов индексов.

Таким образом,

$$c_i = \sum_{l\geq 1} \sum_{\overrightarrow{q}\in\Gamma_l} a_{\overrightarrow{q},l}\theta_{\overrightarrow{q},l}\, \overrightarrow{t}^{\,\overrightarrow{q}}. \tag{2.8}$$

Подставим в $f(X)$ значение $X = \overrightarrow{t}^{\,\overrightarrow{r}}$. Получаем

$$\sum_{l\geq 1}\sum_{i\geq 0}\sum_{\overrightarrow{q}\in\Gamma_l} a_{\overrightarrow{q},l}\theta_{\overrightarrow{q},l}\, \overrightarrow{t}^{\,\overrightarrow{q}+i\overrightarrow{r}} = \sum_{l\geq 1}\sum_{\overrightarrow{q}\in\Gamma_\cup^{(l)}} \left(\sum_{j=1}^{m_{\overrightarrow{q},l}} a_{\overrightarrow{q},l,j}\theta_{\overrightarrow{q},l,j} \right) \overrightarrow{t}^{\,\overrightarrow{r}}, \tag{2.9}$$

где $\Gamma_\cup^{(l)} = (\Gamma_l \cup \{\overrightarrow{r}\})^*$ – допустимый набор.

Пусть теперь

$$\Gamma_{l,j} = \left\{ \overrightarrow{q} \in \Gamma_\cup^{(l)} : j = m_{\overrightarrow{q},l} \right\}. \tag{2.10}$$

Легко видеть, что $\{\Gamma_{l,j} : l \geq 1, j \geq 1\}$ – допустимое мультимножество наборов индексов.

Итак, мы получили

$$\sum_{l,j\geq 1}\sum_{\overrightarrow{q}\in\Gamma_{l,j}} a_{\overrightarrow{q},l,j}\theta_{\overrightarrow{q},l,j}\, \overrightarrow{t}^{\,\overrightarrow{q}}, \quad a_{\overrightarrow{q},l,j} \in \mathbb{Z}. \tag{2.11}$$

Представим этот ряд как разность двух рядов аналогичного вида, но с $a_{\overrightarrow{q},l,j} \in \mathbb{N}$. Таким образом придем к рядам вида

$$\sum_{l,j\geq 1}\sum_{\overrightarrow{q}\in\Gamma_{l,j}}\sum_{0\leq w\leq a_{\overrightarrow{q},l,j}} \theta_{\overrightarrow{q},l,j}\, \overrightarrow{t}^{\,\overrightarrow{q}}, \tag{2.12}$$

которые можно переписать как

$$\sum_{l,j,w\geq 1}\sum_{\overrightarrow{q}\in\Gamma_{l,j,w}}\theta_{\overrightarrow{q},l,j}\,\overrightarrow{t}^{\,\overrightarrow{q}}, \tag{2.13}$$

где

$$\Gamma_{l,j,w}=\left\{\overrightarrow{q}\in\Gamma_{l,j}:w=a_{\overrightarrow{q},l,j}\right\}. \tag{2.14}$$

Мультимножество $\{\Gamma_{l,j,w}:l\geq 1,j\geq 1,w\geq 1\}$ допустимо, значит, оба полученных ряда сходятся. □

Лемма 4. *Для любого допустимого набора положительных индексов Ω и семейства рядов $f_{\overrightarrow{r}}(X)\in X\mathbb{Z}_p[[X]]$, $\overrightarrow{r}\in\Omega$, корректна подстановка*

$$\sum_{\overrightarrow{r}\in\Omega}f_{\overrightarrow{r}}(X)\big|_{X=\overrightarrow{t}^{\,\overrightarrow{r}}}. \tag{2.15}$$

Доказательство. Аналогично доказательству предыдущей леммы, раскладываем коэффициенты каждого из рядов $f_{\overrightarrow{r}}(X)=\sum\limits_{i\geq 0}c_{i,\overrightarrow{r}}X^i$ по степеням $\overrightarrow{t}$:

$$c_{i,\overrightarrow{r}}=\sum_{l\geq 1}\sum_{\overrightarrow{q}\in\Gamma_l}a_{\overrightarrow{q},l,\overrightarrow{r}}\theta_{\overrightarrow{q},l,\overrightarrow{r}}\,\overrightarrow{t}^{\,\overrightarrow{q}},$$

приходим к ряду

$$\sum_{\overrightarrow{r}\in\Omega}\sum_{l\geq 1}\sum_{i\geq 0}\sum_{\overrightarrow{q}\in\Gamma_{l,\overrightarrow{r}}}a_{\overrightarrow{q},l}\theta_{\overrightarrow{q},l}\,\overrightarrow{t}^{\,\overrightarrow{q}+i\overrightarrow{r}}=\sum_{l\geq 1}\sum_{\overrightarrow{q}\in\Gamma_{\cup}^{(l)}}\left(\sum_{j=1}^{m_{\overrightarrow{q},l}}a_{\overrightarrow{q},l,j}\theta_{\overrightarrow{q},l,j}\right)\overrightarrow{t}^{\,\overrightarrow{q}},$$

где $\Gamma_{\cup}^{(l)}=(\Gamma_l\cup\Omega)^*$ – допустимый набор.

Продолжая аналогично доказательству леммы 3, получим разность двух сходящихся рядов вида

$$\sum_{l,j\geq 1}\sum_{\overrightarrow{q}\in\Gamma_{l,j,\overrightarrow{r}}}\sum_{0\leq w\leq a_{\overrightarrow{q},l,j,\overrightarrow{r}}}\theta_{\overrightarrow{q},l,j,\overrightarrow{r}}\,\overrightarrow{t}^{\,\overrightarrow{q}},$$

следовательно, подстановка определена корректно. □

2.3 Экспонента Артина-Хассе

Обозначим подполе инерции поля K через T, а его кольцо целых через $\mathfrak{o}$. Возьмем кольцо $\mathfrak{o}\{\{X_1\}\}\{\{X_2\}\}...\{\{X_n\}\}$ и рассмотрим на нем оператор Фробениуса $\triangle$, который на переменные X_i действует как возведение в степень p, а на коэффициенты - как автоморфизм Фробениуса φ из $Gal(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$. На $X_n\mathfrak{o}\{\{X_1\}\}\{\{X_2\}\}...\{\{X_{n-1}\}\}[[X_n]]$ определена экспонента Артина-Хассе

$$E(a) = exp((1 - \frac{\triangle}{p})^{-1}(a)). \tag{2.16}$$

Рассмотрим корректность подстановки элементов максимального идеала в образ мономов относительно экспоненты Артина-Хассе. Сначала докажем, что на мономах с коэффициентом из представителей Тейхмюллера экспоненту можно определить как степенной ряд от монома с целыми p-адическими коэффициентами. В силу определения отображения, это утверждение достаточно проверить на мономах первой степени. Для простоты заменим набор переменных X_i одной переменной X, на которую оператор Фробениуса действует возведением в p-ую степень. Рассмотрим, как автоморфизм Фробениуса влияет на коэффициент:

Лемма 5. *Пусть $\theta \in R$, φ - автоморфизм Фробениуса в поле T. Тогда*

$$\varphi(\theta) = \theta^p. \tag{2.17}$$

Доказательство. Из свойств φ $\varphi(\theta) \equiv \theta^p \mod \mathfrak{M}$, где $\mathfrak{M}$ - максимальный идеал K. При этом $\varphi(\theta) \in R$. Следовательно, представитель $rep(\varphi(\theta)) = \varphi(\theta)$, но $rep(\varphi(\theta)) = rep(\theta^p) = \theta^p$. □

Таким образом, $E(\theta X) = exp(\sum_{i\geq 0} \frac{(\theta X)^{p^i}}{p^i})$. Упростим запись этого ряда, чтобы убедиться в том, что коэффициенты целы.

Лемма 6.

$$(\sum_{i\geq 0}\frac{X^{p^j}}{p^i}) = \prod_{(i,p)=1}(1-X^i)^{-\mu(i)/i}, \tag{2.18}$$

где $\mu(i)$ - функция Мебиуса, причем степень $-\mu(i)/i$ следует рассматривать как p-адическое число.

Доказательство. Введем обозначение

$$\lambda(X) = \sum_{i\geq 0}\frac{X^{p^i}}{p^i}. \tag{2.19}$$

Докажем, что

$$log(1-X) = -\sum_{(i,p)=1}\frac{1}{i}\lambda(X^i). \tag{2.20}$$

В левой части коэффициент при X^i $\frac{-1}{i}$ при $i \geq 1$, коэффициенты при остальных мономах равны 0. Пусть $i = i_0 p^{d_i}$, где $(i_0, p) = 1$. Тогда в правой части слагаемое X^i встречается только в ряде $\lambda(X^{i_0})$ с коэффициентом $\frac{1}{p^{d_i}}$. Итого коэффициент $\frac{-1}{i_0}\frac{1}{p^{d_i}} = \frac{-1}{i}$, следовательно, ряды совпадают.

Докажем, что

$$\lambda(X) = \sum_{(i,p)=1}\frac{-\mu(i)}{i}log(1-X^i). \tag{2.21}$$

Правую часть можно переписать в виде

$$\frac{\mu(i)}{i}\sum_{(j,p)=1}\frac{1}{j}\lambda(X^{ij}) = \sum_{i,j:(ij,p)=1}\frac{\mu(i)}{ij}\lambda(X^{ij}). \tag{2.22}$$

По свойству функции Мебиуса для $n \neq 1$ $\sum_{d|n}\mu(d) = 0$.

Рассмотрим коэффициенты при X^l в левой и правой частях (2.21).

1. $l = p^n$. В $\sum_{i,j:(ij,p)=1}\frac{\mu(i)}{ij}\lambda(X^{ij})$ соответствующее слагаемое встречается

только в $\lambda(X)$, следовательно, коэффициент при нем совпадает с коэффициентом в левой части (2.21);

2. $l = p^n l_0$, $(l_0, p) = 1$, $l_0 \neq 1$. В $\sum_{i,j:(ij,p)=1} \frac{\mu(i)}{ij}\lambda(X^{ij})$ соответствующее слагаемое встречается только в $\lambda(X^{i_0})$, значит, коэффициент при нем $\sum_{d|i_0} \frac{\mu(d)}{i_0}\frac{1}{p^{i_0}} = \frac{1}{i_0 p^{i_0}}\sum_{d|i_0}\mu(d) = 0$, как и в левой части (2.21).

Взяв экспоненту от (2.21), получаем утверждение леммы. □

$\prod_{(i,p)=1}(1-\theta^i X^i)^{-\mu(i)/i}$ - ряд с целыми p-адическими коэффициентами. Поэтому, воспользовавшись этим представлением и леммой 3, получаем следующую теорему:

Теорема 12. *Для любого $\theta \in R\backslash\{0\}$, $\overrightarrow{i} > \overrightarrow{0}$ корректно определен элемент $E(\theta X)|_{X=\overrightarrow{t}^{\overrightarrow{i}}}$ в K, причем выполнено сравнение*

$$E(\theta X)|_{X=\overrightarrow{t}^{\overrightarrow{i}}} \equiv 1 + \theta\overrightarrow{t}^{\overrightarrow{i}} \mod \overrightarrow{t}^{\overrightarrow{i}} + . \tag{2.23}$$

Доказательство.

$$\prod_{(j,p)=1}(1-X^j)^{-\mu(j)/j} \equiv (1-X)^{-1} \equiv 1 + X \mod X^2. \tag{2.24}$$

Значит, сравнение выполнено. □

2.4 Случай поля без p-корней из единицы

Теорема 13. *Пусть n-мерное поле K не содержит корень из единицы степени p. Тогда любую его главную единицу можно представить в виде*

$$\prod_{\overrightarrow{r}\in\Omega} E(\theta_{\overrightarrow{r}}\overrightarrow{X}^{\overrightarrow{r}})^{a_{\overrightarrow{r}}}|_{\overrightarrow{X}=\overrightarrow{t}}, \tag{2.25}$$

где

- Ω — *допустимое множество;*

- $\theta_{\overrightarrow{r}} \in \Re$, $\Re$ - *система представителей базиса последнего поля вычетов как векторного пространства над* $\mathbb{F}_p$
- $a_{\overrightarrow{r}} \in \mathbb{Z}_p$;
- $\overrightarrow{t}$ — *локальные параметры;*
- $0 < \overrightarrow{r} < \frac{p\overrightarrow{v}(p)}{p-1}$;
- $p \not| \overrightarrow{r}$,

однозначно при $v_n(p) > 0$ *и с точностью до множителя из* K^{p^d} *для произвольного натурального* d *при* $v_n(p) = 0$, *причем такое представление канонично по модулю* K^{p^d}.

Сначала изучим, когда система элементов становится мультипликативной порождающей системой главных единиц. Сформулируем теорему из [17]:

Теорема 14. *Пусть для любого* $\overrightarrow{r} > 0$ *и любого* $\theta \in R$ *определен элемент* $a_{\theta,\overrightarrow{r}} \in K$, $a_{\theta,\overrightarrow{r}} \equiv 1 + \theta\overrightarrow{t}^{\overrightarrow{r}}$ *mod* $\overrightarrow{t}^{\overrightarrow{r}}+$. *Тогда для того, чтобы любая главная единица* $\alpha \in K$ *была однозначно представима в виде*

$$\alpha = \prod_{\overrightarrow{r} \in \Omega_\alpha} a_{\theta_{\overrightarrow{r}},\overrightarrow{r}}, \tag{2.26}$$

где Ω_α – *допустимый набор положительных индексов, достаточно выполнения любого из следующих условий:*

1. *множество наборов индексов* $\left\{\Omega_{\theta,\overrightarrow{r}}, \theta \in R, \overrightarrow{r} \in \Omega\right\}$, *где* $\Omega_{\theta,\overrightarrow{r}}$ – *набор индексов из разложения* $a_{\theta,\overrightarrow{r}} - 1$ *по степеням* $\overrightarrow{t}$, *допустимо для любого допустимого* Ω;
2. *ряд* $\sum\limits_{\overrightarrow{r} \in \Omega} (a_{\theta,\overrightarrow{r}} - 1)$ *сходится для любого допустимого набора* Ω.

Доказательство. Для первого из условий теорема доказана в [17]. Фактически это доказательство состоит из двух частей: сначала доказывается, что из

допустимости $\left\{\Omega_{\theta,\overrightarrow{r}}, \theta \in R, \overrightarrow{r} \in \Omega\right\}$ следует сходимость рядов $\sum\limits_{\overrightarrow{r}\in\Omega}(a_{\theta,\overrightarrow{r}} - 1)$, потом (с использованием только этой сходимости) доказывается существование и единственность разложения α в произведение. Таким образом, если нам изначально известно, что такие ряды сходятся для выбранных некоторым специальным образом $a_{\theta,\overrightarrow{r}}$, то утверждение теоремы останется верным.

□

Зафиксируем подмножество представителей Тейхмюллера $\Re$, чьи вычеты образуют базис k над $\mathbb{F}_p$.

В соответствии с теоремой 12 определим для $\theta \in R$

$$a_{\theta,\overrightarrow{r}} = E(\theta X)|_{X=\overrightarrow{t}^{\overrightarrow{r}}}. \tag{2.27}$$

В системе $a_{\theta,\overrightarrow{r}}$ некоторые элементы можно заменить на p-е степени других. В самом деле, выпишем сравнения:

$$(1+\theta\overrightarrow{t}^{\overrightarrow{i}})^p \equiv 1+\theta^p\overrightarrow{t}^{p\overrightarrow{i}} \mod \overrightarrow{t}^{p\overrightarrow{i}}+, \text{ если } \overrightarrow{i} < \overrightarrow{e}_1, \tag{2.28}$$

$$(1+\theta\overrightarrow{t}^{\overrightarrow{i}})^p \equiv 1+(\theta^p+\theta_0\theta)\overrightarrow{t}^{p\overrightarrow{i}} \mod \overrightarrow{t}^{p\overrightarrow{i}}+, \text{ если } \overrightarrow{i} = \overrightarrow{e}_1, \tag{2.29}$$

$$(1+\theta\overrightarrow{t}^{\overrightarrow{i}})^p \equiv 1+\theta_0\theta\overrightarrow{t}^{\overrightarrow{i}+\overrightarrow{e}} \mod \overrightarrow{t}^{\overrightarrow{i}+\overrightarrow{e}}+, \text{ если } \overrightarrow{i} > \overrightarrow{e}_1. \tag{2.30}$$

Из сравнений следует, что на p-е степени других элементов можно заменить $a_{\theta,\overrightarrow{r}}$ для $\overrightarrow{r}$, меньших $p\overrightarrow{e}_1$ и кратных p, равных $p\overrightarrow{e}_1$ или больших $\overrightarrow{e}_1+\overrightarrow{e}$, при условии, что соответствующие отображения коэффициентов индуцируют автоморфизмы поля вычетов k как линейного пространства над $\mathbb{F}_p$. Поле k совершенно, умножение на ненулевой элемент очевидно является автоморфизмом, а отображение $\theta \longrightarrow \theta^p + \theta_0\theta$ автоморфизмом является по следующей лемме.

Лемма 7. *Гомоморфизм $\psi : \theta \to \theta^p + \theta_0\theta$ является изоморфизмом векторных пространств над $\mathbb{F}_p$.*

Доказательство. Инъективность доказана в [31]. Тогда у любого элемента из базиса k над $\mathbb{F}_p$ существует единственный прообраз. Прообраз произвольного элемента k, таким образом, будет линейной комбинацией прообразов элементов базиса, и, значит, ψ – сюръекция. □

Теперь для каждого элемента системы $\{a_{\theta,\overrightarrow{r}}\}$, для которого это возможно, переопределим его как p-ую степень другого элемента, который, в свою очередь, (опять же при возможности это сделать) как p-ую степень третьего, и т. д. Заметим, что нормирование каждого следующего элемента меньше нормирования предыдущего, и при $v_n(p) > 0$ для каждого из исходных $\{a_{\theta,\overrightarrow{r}}\}$ эта цепочка оборвется. При $v_n(p) = 0$ мы для любого фиксированного натурального d можем останавливаться после d переобозначений.

Почему теперь мы можем применить к системе $\{a_{\theta,\overrightarrow{r}}\}$ теорему 14? В случае конечного k это возможно по следующей лемме:

Лемма 8. *Пусть* $a_{\theta,\overrightarrow{r}} = E(\theta X)|_{X=\overrightarrow{t}^{\overrightarrow{r}}}$, *где* $\theta \in R$. *Пусть* $\Omega_{\theta,\overrightarrow{r}}$ – *набор индексов в разложении* $a_{\theta,\overrightarrow{r}}$ *по степеням* $\overrightarrow{t}$, Ω – *допустимый набор положительных индексов. Тогда при конечном* R $\left\{\Omega_{\theta,\overrightarrow{r}} : \theta \in R, \overrightarrow{r} \in \Omega\right\}$ – *допустимое мультимножество наборов положительных индексов.*

Доказательство. Пусть $\overrightarrow{s} \in \mathbb{Z}^n$ – мультииндекс. Заметим, что $\overrightarrow{s}$ встречается в $\Omega_{\theta,\overrightarrow{r}}$ лишь при $\overrightarrow{r} \leq \overrightarrow{s}$, а таких $\overrightarrow{r}$ конечное число. Таким образом, первое из условий допустимости выполнено.

Докажем второе условие. Рассмотрим объединение $\bigcup \Omega_{\theta,\overrightarrow{r}}$ и докажем, что оно является допустимым набором индексов. Зафиксируем $i_{n-k+1}, \ldots, i_n$. Рассмотрим подмножество $\Omega_{\{i_{n-k+1},\ldots,i_n\}} \subset \bigcup \Omega_{\theta,\overrightarrow{r}}$, состоящее из индексов, k последних элементов которых совпадают с $i_{n-k+1}, \ldots, i_n$.

Пусть $\overrightarrow{i_0} \in \Omega_{\{i_{n-k+1},\ldots,i_n\}}$ – некоторый произвольно выбранный фиксированный элемент. Тогда $\Omega_{\{i_{n-k+1},\ldots,i_n\}}$ разбивается на два подмножества, состоящие соответственно из $\overrightarrow{i} \leq \overrightarrow{i_0}$ и $\overrightarrow{i} > \overrightarrow{i_0}$.

Число таких $\Omega_{\theta,\overrightarrow{r}}$, в которых встречаются $\overrightarrow{i} \leq \overrightarrow{i_0}$, конечно, в каждом из этих множеств $(n-k)$-ые компоненты таких $\overrightarrow{i}$ ограничены снизу, значит, и в $\bigcup \Omega_{\theta,\overrightarrow{r}}$ $(n-k)$-ые компоненты $\overrightarrow{i} \leq \overrightarrow{i_0}$ ограничены снизу.

Если же рассмотреть $\overrightarrow{i} > \overrightarrow{i_0}$, то, раз последние k компонент $\overrightarrow{i}$ и $\overrightarrow{i_0}$ совпадают, то для $(n-k)$-ых компонент $i_{n-k} \geq (i_0)_{n-k}$. Таким образом, для всех индексов из $\Omega_{\{i_{n-k+1},\ldots,i_n\}}$ выполняется условие ограниченности $(n-k)$-ой компоненты. □

Замечание. Если множество представителей Тейхмюллера R бесконечно, то $\left\{\Omega_{\theta,\overrightarrow{r}} : \theta \in R, \overrightarrow{r} \in \Omega\right\}$ не является допустимым, так как любой мультииндекс $\overrightarrow{s} \in \mathbb{Z}^n$ встречается в наборах $\Omega_{\theta,\overrightarrow{s}}$ при всех $\theta \in R$.

Тем не менее, так как при нашем выборе $a_{\theta,\overrightarrow{r}}$ ряды $\sum\limits_{\overrightarrow{r}\in\Omega}(a_{\theta,\overrightarrow{r}}-1)$ для любого допустимого Ω сходятся по лемме 4, то и при конечном, и при бесконечном R можно воспользоваться теоремой 14. Заметим также, что каждый из элементов $a_{\theta,\overrightarrow{r}}$ для $\theta \in R$ представляет собой произведение конечного числа элементов $a_{\theta,\overrightarrow{r}}$ с $\theta \in \Re$. Таким образом приходим к утверждению теоремы 13.

Лемма 9. *Полученное разложение определено однозначно.*

Доказательство. Предположим противное. Докажем, что из неоднозначности разложения следует наличие в поле корня из единицы степени p. В самом деле, если есть неоднозначное разложение, то есть нетривиальное разложение единицы. Запишем его:

$$\prod_{\overrightarrow{r}\in\Omega} E(\theta_{\overrightarrow{r}}\overrightarrow{t}^{\overrightarrow{r}})^{a_{\overrightarrow{r}}} = 1 \qquad \text{при } v_n(p) > 0, \tag{2.31}$$

$$\beta^{p^d}\prod_{\overrightarrow{r}\in\Omega} E(\theta_{\overrightarrow{r}}\overrightarrow{t}^{\overrightarrow{r}})^{a_{\overrightarrow{r}}} = 1 \qquad \text{при } v_n(p) = 0. \tag{2.32}$$

Если все $a_{\overrightarrow{r}}$ делятся на p, то, поделив показатели на p, мы получим сходящееся разложение для корня из единицы степени p, т.е. он лежит в поле K. Значит, есть лексикографически наименьший $\overrightarrow{j}$, такой, что $a_{\overrightarrow{j}}$ не делится на p (множество индексов Ω допустимо, значит, наименьший существует). Тогда мы

можем переписать наше выражение в виде

$$\prod_{\vec{r}\geq\vec{j}} E(\theta_{\vec{r}}\overrightarrow{t}^{\vec{r}})^{a_{\vec{r}}} = \varepsilon^p \tag{2.33}$$

для некоторой (главной!) единицы ε. Пусть $\varepsilon \equiv 1 + \eta\overrightarrow{t}^{\vec{i}} \mod \overrightarrow{t}^{\vec{i}}+$. Так как

$$E(\theta_{\vec{j}}\overrightarrow{t}^{\vec{j}})^{a_{\vec{j}}} \equiv 1 + a_{\vec{j}}\theta_{\vec{j}}\overrightarrow{t}^{\vec{j}} \mod \overrightarrow{t}^{\vec{j}}+, \tag{2.34}$$

то

$$1 + a_{\vec{j}}\theta_{\vec{j}}\overrightarrow{t}^{\vec{j}} \equiv (1 + \eta\overrightarrow{t}^{\vec{i}})^p \mod \overrightarrow{t}^{\vec{j}} + . \tag{2.35}$$

Но все такие единицы представлены в нашем базисе p-ми степенями других элементов, значит, $a_{\vec{j}}$ делится на p. Противоречие. □

2.5 Элемент $\omega(a)$

Определим на $1 + X_n\mathfrak{o}\{\{X_1\}\}\{\{X_2\}\}...[[X_n]]$ функцию

$$l(a) = (1 - \frac{\triangle}{p})(\log(a)). \tag{2.36}$$

Лемма 10. *E является $\mathbb{Z}_p$-изоморфизмом из $X_n\mathfrak{o}\{\{X_1\}\}\{\{X_2\}\}...[[X_n]]$ в $1 + X_n\mathfrak{o}\{\{X_1\}\}\{\{X_2\}\}...[[X_n]]$, а l - обратный изоморфизм.*

Доказательство. Доказательство аналогично Proposition (2.2) Ch.VI в [31]. □

Для $a \in \mathfrak{o}$ существует α в $\hat{T}$ – пополнении T, такое что $\varphi(\alpha) - \alpha = a$ ([31], Proposition (1.8) Ch. IV).

Пусть теперь поле K содержит корень из 1 p-ой степени. Обозначим m наибольшее число, такое, что K содержит корень из 1 p^m-ой степени. Сам этот корень мы обозначим ζ.

Обозначим $z(\overrightarrow{X})$ из $R\{\{X_1\}\}\{\{X_2\}\}...\{\{X_{n-1}\}\}[[X_n]]$, такой, что

$$z(\overrightarrow{t}) = \zeta. \tag{2.37}$$

Его можно получить, например, из разложения ζ в ряд по локальным параметрам с коэффициентами из представителей Тейхмюллера. Определим ряд

$$s(\overrightarrow{X}) = z(\overrightarrow{X})^{p^m} - 1. \tag{2.38}$$

Рассмотрим следующую подстановку:

$$\omega(a) = E(as(\overrightarrow{X}))|_{\overrightarrow{X}=\overrightarrow{t}}. \tag{2.39}$$

Из определения ряда s и леммы 3 следует ее корректность. Найдем условие, при котором полученный элемент лежит в K^{p^m}. Докажем цепочку лемм, ведущих к соответствующему утверждению.

Лемма 11. *Элемент*

$$H(a) = E(p^m\varphi(\alpha)l(z(\overrightarrow{X})))|_{\overrightarrow{X}=\overrightarrow{t}} \tag{2.40}$$

корректно определен в K. При этом

$$H(a) \in K^{p^m} \Longleftrightarrow Tr_{T/\mathbb{Q}_p}a \equiv 0 \mod p^m. \tag{2.41}$$

Доказательство. По лемме 10 элемент корректно определен.

Пусть $f = f(T/\mathbb{Q}_p)$, тогда автоморфизм Фробениуса поля T φ_T совпадает с φ^f и

$$\varphi^{f+1}(\alpha) - \varphi(\alpha) = \varphi(1 + \varphi + ... + \varphi^{f-1})(\varphi(\alpha) - \alpha) = (\varphi + \varphi^2... + \varphi^f)(a). \tag{2.42}$$

Теперь заметим, что

$$(\varphi + \varphi^2... + \varphi^f)(a) = Tr_{T/\mathbb{Q}_p}a. \tag{2.43}$$

Следовательно,

$$\varphi_T E(\varphi(\alpha)l(z(\overrightarrow{X})))|_{\overrightarrow{X}=\overrightarrow{t}} = E((Tr_{T/\mathbb{Q}_p}a + \varphi(\alpha))l(z(\overrightarrow{X})))|_{X=\pi} = \\ = E(\varphi(\alpha)l(z(\overrightarrow{X})))|_{\overrightarrow{X}=\overrightarrow{t}}\zeta^{Tr_{T/\mathbb{Q}_p}a}. \tag{2.44}$$

Тем самым второе утверждение теоремы доказано. Так как

$$\varphi_T H(a) = H(a)\zeta^{p^m Tr_{T/\mathbb{Q}_p}a} = H(a), \tag{2.45}$$

то $H(a)$ лежит в K. □

Теперь преобразуем $H(a)$. Поскольку

$$(1 - \frac{\triangle}{p})(\alpha \log z) = \alpha \log z - \varphi(\alpha)\frac{\triangle}{p}\log z = \\ = (\alpha - \varphi(\alpha))\log z + \varphi(\alpha)l(z) = \varphi(\alpha)l(z) - a\log z, \tag{2.46}$$

а также

$$E(p^m(1 - \frac{\triangle}{p})\alpha \log z) = \exp(p^m \alpha \log z), \tag{2.47}$$

получаем

$$E(p^m\varphi(\alpha)l(z)) = E(p^m a \log z)\exp(p^m\alpha\log z). \tag{2.48}$$

Подстановка в рассмотренные ряды $\overrightarrow{X} = \overrightarrow{t}$ корректна, так как log - ряд с целыми p-адическими коэффициентами, как и ряд $\exp(p^m\overrightarrow{X})$. При этом

$$\exp(p^m\alpha\log z(\overrightarrow{X}))|_{\overrightarrow{X}=\overrightarrow{t}} = \exp(\alpha\log z(\overrightarrow{X})^{p^m})|_{\overrightarrow{X}=\overrightarrow{t}} = \exp(\alpha\log\zeta^{p^m}) = 1. \tag{2.49}$$

То есть,

$$H(a) = E(p^m\varphi(\alpha)l(z(\overrightarrow{X}))|_{\overrightarrow{X}=\overrightarrow{t}}) = E(p^m a\log z(\overrightarrow{X})|_{\overrightarrow{X}=\overrightarrow{t}}. \tag{2.50}$$

Поскольку $p^m \log z = \log(s+1)$, получим

$$E(p^m a \log z) = E(as)E(a(\log(1+s) - s)). \tag{2.51}$$

Докажем, что подстановка $E(a(\log(1 + s(\overrightarrow{X})) - s(\overrightarrow{X})))|_{\overrightarrow{X}=\overrightarrow{t}}$ дает элемент K^{p^m}. Тогда будет получена следующая теорема:

Теорема 15. *Для $a \in \mathfrak{o}$ элемент*

$$\omega(a) = E(as(\overrightarrow{X}))|_{\overrightarrow{X}=\overrightarrow{t}} \tag{2.52}$$

корректно определен, и

$$\omega(a) \in K^{p^m} \Longleftrightarrow Tr_{T/\mathbb{Q}_p} a \equiv 0 \mod p^m. \tag{2.53}$$

Доказательство. Для обоснования второго утверждения теоремы заметим, что $\omega(a)$ отличается от $H(a)$ на множитель из K^{p^m}. □

Поскольку $\overrightarrow{v}(\zeta - 1) = \overrightarrow{e}/(p-1)p^{n-1} = e_\zeta$, ряд $z(\overrightarrow{X}) = 1 + \theta\overrightarrow{X}^{\overrightarrow{e}_\zeta} + ...$ Будем в дальнейшем рассматривать только такой ряд и соответствующий ему ряд $s(\overrightarrow{t}) \equiv \theta_1 \overrightarrow{t}^{\overrightarrow{e}_1} \mod \overrightarrow{t}^{\overrightarrow{e}_1}+$. Отметим, что ряд, соответствующий разложению ζ по локальным параметрам с коэффициентами из представителей Тейхмюллера удовлетворяет этому условию.

Лемма 12. *Подстановка $E(a(\log(1 + s(\overrightarrow{X})) - s(\overrightarrow{X})))|_{\overrightarrow{X}=\overrightarrow{t}}$ корректна, и ее результат является элементом K^{p^m}.*

Доказательство. Перепишем $E(a(\log(1 + s(\overrightarrow{X})) - s(\overrightarrow{X})))$ как

$$\exp(a(\log(1 + s(\overrightarrow{X})) - s(\overrightarrow{X})) \exp(\sum_{i\geq 1} \triangle^i (a(\log(1 + s(\overrightarrow{X})) - s(\overrightarrow{X}))/p^i) \tag{2.54}$$

Заметим, что

$$\exp(a(\log(1 + s(\overrightarrow{X})) - s(\overrightarrow{X}))|_{\overrightarrow{X}=\overrightarrow{t}} = 1, \tag{2.55}$$

так как подстановка корректна по лемме 3 и $s(\overrightarrow{t}) = 0$. Одновременно, так как

$$\log(1+s) - s = \sum_{k\geq 2}(-1)^{k+1}s^k/k, \tag{2.56}$$

то

$$\exp(\sum_{i\geq 1}\triangle^i(a(\log(1+s)-s)/p^i) = \exp(\sum_{i\geq 1}\sum_{k\geq 2}(-1)^{k+1}\triangle^i(as^k)/kp^{i+m})^{p^m}. \tag{2.57}$$

Для корректности выделения степени p^m достаточно доказать, что аргумент экспоненты после подстановки имеет нормирование хотя бы $\overrightarrow{e}$, поскольку ряд $\exp(pX)$ является рядом с целыми p-адическими коэффициентами. Аналогично одномерному случаю ([31], Ch.6, (4.2)) выполняется неравенство

$$\overrightarrow{v}(\triangle^k s(\overrightarrow{t})) > \overrightarrow{e}(1+\max(k,m)). \tag{2.58}$$

Тогда $\overrightarrow{v}(\triangle^i(as^k)/kp^{i+m}) > \overrightarrow{e}(k(1+\max(m,i))-i-m-(k-1)) \geq \overrightarrow{e}$, поскольку $k \geq 2$, $\overrightarrow{v}(m) \leq (m-1)\overrightarrow{e}$ при натуральном m. □

2.6 Случай поля с p-корнями из единицы

Пусть теперь поле K содержит корень из 1 p-ой степени. Докажеи следующую теорему:

Теорема 16. *Пусть K –n-мерное поле , и наибольшее m, такое, что поле содержит корень из единицы степени p^m, больше нуля. Обозначим этот корень за ζ. Тогда любую главную единицу поля K можно представить в виде*

$$\prod_{\overrightarrow{r}\in\Omega} E(\theta_{\overrightarrow{r}}\overrightarrow{X}^{\overrightarrow{r}})^{a_{\overrightarrow{r}}} E(as(X))^b|_{\overrightarrow{X}=\overrightarrow{t}}, \tag{2.59}$$

где

- Ω — *допустимое множество;*

- $\theta_{\overrightarrow{r}} \in \Re$;
- $a_{\overrightarrow{r}}, b \in \mathbb{Z}_p$;
- $\overrightarrow{t}$ — *локальные параметры;*
- $0 < \overrightarrow{r} < p\overrightarrow{v}(p)/(p-1)$;
- $p \not| \overrightarrow{r}$;
- a — *целый элемент подполя инерции, такой, что* $Tr_{T/\mathbb{Q}_p} a \equiv 1 \mod p^m$;
- $z(\overrightarrow{X}) \in R\{\{X_1\}\}\{\{X_2\}\}...\{\{X_{n-1}\}\}[[X_n]]$, *причем* $z(\overrightarrow{t}) = \zeta_{p^m}$, *первообразному корню из единицы степени* p^m;
- $s = z^{p^m} - 1$,

с точностью до множителя из K^{p^m}. *При этом базис является каноническим по модулю* K^{p^m}, *т.е. для двух элементов поля, отличающихся множителем из* K^{p^m}, *соответствующие показатели в представлении сравнимы по модулю* p^m.

Подобно случаю без p-корней, любой элемент поля представим в виде произведения $E(\theta_{\overrightarrow{r}} \overrightarrow{t}^{\overrightarrow{r}})$ по допустимому множеству. Переопределим, как и раньше, некоторые элементы базиса как p-ые степени других элементов, но так, чтобы в итоге степень не превысила p^m.

Отметим, что теперь отображение $\theta \to \theta^p + \theta_0\theta$ изоморфизмом поля вычетов не является. Таким образом, теперь в поле K есть элементы, сравнимые с $1 + \theta\overrightarrow{t}^{p\overrightarrow{e}_1} \mod \overrightarrow{t}^{p\overrightarrow{e}_1}+$, которые не лежат в K^p.

По построению $E(as(\overrightarrow{t})) \equiv 1 + \varphi(a)\theta_1\overrightarrow{t}^{p\overrightarrow{e}_1} \mod \overrightarrow{t}^{p\overrightarrow{e}_1}$, где θ_1 - некоторый фиксированный представитель Тейхмюллера. Поскольку φ - автоморфизм T, в таком виде мы можем получить любой элемент $a_{\theta,p\overrightarrow{e}_1}$. Рассмотрим аддитивный гомоморфизм $\psi : T \longrightarrow \langle\zeta\rangle$:

$$\psi(a) = \zeta^{Tr_{T/\mathbb{Q}_p} a}. \tag{2.60}$$

Его ядро составляют те a, у которых $Tr_{T/\mathbb{Q}_p} a \equiv 0 \mod p^m$. С другой стороны, из теоремы 15 известно, что это ровно те a, для которых $\omega(a) \in K^{p^m}$. Следовательно, элемент $\omega(b)$ с $Tr_{T/\mathbb{Q}_p} b \equiv 1 \mod p^m$ порождает

$$\langle \omega(a) | a \in T \rangle / \langle \omega(a) | a \in T \rangle \bigcap K^p.$$

Поэтому для получения базиса достаточно добавить к порождающим элементам $\omega(b)$ и его степени, определив ими соответствующие $a_{\theta,\vec{r}}$, а также их произведения с уже определенными как p-ые степени $a_{\theta,\vec{r}}$.

Заметим, что теперь в разложении к произведению старого вида добавился множитель вида $\omega(b)$ в p-адической степени, который определен корректно, значит, и все произведение сходится.

Теперь докажем, что полученное разложение канонично по модулю K^{p^m}.

Лемма 13. *Полученное разложение канонично по модулю K^{p^m}.*

Доказательство. Докажем индукцией по m. База: $m = 1$.

Если уществует неоднозначное разложение произвольного элемента, то существует и нетривиальное разложение единицы:

$$\varepsilon_0^p \prod E(\theta \overrightarrow{t}^{\vec{r}})^{a_{\vec{r}}} \omega(a)^b = 1. \tag{2.61}$$

Сначала докажем, что все $a_{\vec{r}}$ делятся на p. Если это не так, то существует лексикографически наименьший $\vec{j}$, такой, что $a_{\vec{j}}$ не делится на p (множество индексов допустимо, значит, наименьший существует). Тогда мы можем записать, что

$$\prod_{\vec{r} \geq \vec{j}} E(\theta \overrightarrow{t}^{\vec{r}})^{a_{\vec{r}}} = \varepsilon^p \omega(a)^{-b} \tag{2.62}$$

для некоторой единицы ε. Значит,

$$E(\theta_j \overrightarrow{t}^{\vec{j}})^{a_{\vec{j}}} \equiv 1 + a_{\vec{j}} \theta \overrightarrow{t}^{\vec{j}} \equiv \varepsilon^p \omega(a)^{-b} \mod \overrightarrow{t}^{\vec{j}} + . \tag{2.63}$$

Рассмотрим два случая:

1. $\overrightarrow{v}(\varepsilon^p - 1) < \overrightarrow{v}(\omega(a)^{-b} - 1)$ Тогда $E(\theta \overrightarrow{t}^{\overrightarrow{j}})^{a_{\overrightarrow{j}}} \equiv \varepsilon^p$ является главной единицей вида, описанного в сравнениях. Но все такие единицы представлены в нашем базисе p-ми степенями других элементов, значит, $a_{\theta, \overrightarrow{j}}$ делится на p.

2. $\overrightarrow{v}(\varepsilon^p - 1) \geq \overrightarrow{v}(\omega(a)^{-b} - 1)$ Тогда $\overrightarrow{j} \geq p\overrightarrow{e}_1$, что противоречит построению.

Итак, все $a_{\theta, \overrightarrow{r}}$ делятся на p. Теперь докажем, что b кратно p. Пусть это не так. Тогда $\omega_(a) \in K^p$, что противоречит выбору этого элемента.

Переход от $m-1$ к m:

Пусть у нас есть нетривиальное разложение единицы с точностью до множителя степени p^m. Тогда по базе индукции все показатели делятся на p. Разделив их, мы получим разложение для некоторого корня p-ой степени из 1 до множителя степени p^{m-1}. Его же разложение можно получить, возведя в p^{m-1}-ю степень разложение ζ_{p^m}. У этого разложения все показатели будут делиться на p^{m-1}. По индукционному предположению показатели определены однозначно по модулю p^{m-1}. Значит, у разложения ζ_p, полученного из разложения единицы, все показатели тоже делятся на p^{m-1}, поэтому у разложения единицы все показатели делятся на p^m, что и требовалось доказать. $\square$

Глава 3

Канонический базис для формальных модулей Любина-Тейта

3.1 Обозначения

Пусть

- π_0 – простой элемент K_0;
- π – простой элемент K;
- $O_0 = O_{K_0}$, $O = O_K$ — кольца целых полей K_0, K соответственно;
- $M = M_K$ – максимальный идеал в O_K;
- $v : K \to \mathbb{Z} \cup \{\infty\}$ – нормирование K;
- $e = e(K/K_0)$ =индекс ветвления;
- $e_i = \frac{e}{(q-1)q^{i-1}}, i \geq 1$;
- N – подполе инерции в K/K_0;

- $\widetilde{N}$ – пополнение максимального неразветвленного расширения поля T;
- O_N и $O_{\widetilde{N}}$ — кольца целых полей N и $\widetilde{N}$ соответственно;
- φ – автоморфизм Фробениуса поля N и его продолжение на $\widetilde{N}$;
- $\triangle$ – оператор Фробениуса на O_N: для $g(X) = \sum\limits_{i=0}^{\infty} a_i X^i$

$$\Delta(g(X)) = \sum_{i=0}^{\infty} \varphi(a_i) X^{qi}; \tag{3.1}$$

- $S_e = \{1 \leq s < qe_1, \quad q \nmid s\}$.

3.2 Предварительные сведения

3.2.1 Формальные модули

Определение 12. Формальную группу $F(X, Y)$ над кольцом O с логарифмом $\lambda(X) \in K_0[[X]]$ назовем формальной O_0-модульной группой, если определен кольцевой гомоморфизм

$$\begin{gathered} {}_F : O_0 \to \mathrm{End}_O(F), \\ a \mapsto [a]_F(X) = \lambda^{-1}(a\lambda(X)). \end{gathered} \tag{3.2}$$

Пусть $F(M)$ — формальный O_0 -модуль, натянутый на идеал M, т.е., операции сложения и умножения заданы следующим образом:

$$\alpha, \beta \in F(M) \mapsto \alpha +_F \beta = F(\alpha, \beta) \in F(M), \tag{3.3}$$

$$a \in O_0, \alpha \in F(M) \mapsto [a]_F \alpha \in F(M). \tag{3.4}$$

Введем обозначение

$$\mathcal{F}_{\pi_0} = \{g(X) \in O_0[[X]] \mid g(X) \equiv \pi_0 X \mod \deg 2 \text{ и } g(X) \equiv X^q \mod \pi_0\}. \tag{3.5}$$

Тогда над кольцом O_0 сушествует единственная формальная группа F высоты 1, такая, что $g(X)$ — ее эндоморфизм. Данный эндоморфизм в дальнейшем обозначается как $[\pi_0]$. Доказано (см. [36]), что для любых двух $g_1, g_2 \in \mathcal{F}_{\pi_0}$ соответствующие формальные группы Любина-Тейта изоморфны над O_0.

С этого момента $F(X, Y)$ — формальная группа Любина-Тейта с логарифмом

$$\lambda(X) = X + c_1 X + c_2 X^2 + \ldots \tag{3.6}$$

Пусть F_q — изоморфная F O_0-типическая формальная группа и $\lambda_q(X)$ — логарифм F_q. Вообще говоря, F_q определена неоднозначно. Например ([32]), можно выбрать в качестве $\lambda_q(X)$ ряд

$$\lambda_q(X) = X + c_q X^q + c_{q^2} X^{q^2} + \ldots \tag{3.7}$$

Тогда ряд $(\lambda^{-1} \circ \lambda_q)(X)$ задает изоморфизм из F в F_q.

Определение 13. Для каждого элемента $\alpha \in \widetilde{N}$ определим ряд, который назовем функцией Артина-Хассе:

$$E_F(\alpha X) = \lambda^{-1}(\alpha X + c_q \varphi(\alpha) X^q + c_{q^2} \varphi^2(\alpha) X^{q^2} + \ldots). \tag{3.8}$$

В работе [14] доказано следующее утверждение:

Предложение 3. *Для любого $\xi \in F(M), \alpha \in O_{\widetilde{N}}$ элемент $E_F(\alpha\xi)$ корректно определен и задает элемент из $F(\widetilde{M})$, где $\widetilde{M}$ — максимальный идеал в кольце целых поля $K\widetilde{N}$. При этом*

$$E_F((\alpha + \beta)\xi) = E_F(\alpha\xi) +_F E_F(\beta\xi), \quad \alpha, \beta \in O_{\widetilde{N}}, \tag{3.9}$$

$$E_F(a\alpha\xi) = [a]_F(E_F(\alpha\xi)), \quad \alpha \in O_{\widetilde{N}}, a \in O_0, \tag{3.10}$$

$$E_F(\alpha\xi) \equiv \alpha\xi \mod (\alpha\xi)^2. \tag{3.11}$$

3.2.2 Примарные элементы в формальном модуле.

Предположим, что K содержит ядро изогении $[\pi_0^n]$.

Определение 14. Элемент $\omega \in F(M)$ назовем π_0^n-примарным, если расширение $K\left(\frac{1}{[\pi_0^n]_F}\omega\right)/K$ неразветвлено, где $\frac{1}{[\pi_0^n]_F}\omega$ — любое решение уравнения $[\pi_0^n]_F(X) = \omega$.

Предположим, что K содержит ядро изогении $[\pi_0^n]$. Пусть ζ – некоторый первообразный корень этой изогении, то есть $[\pi_0^n]_F(\zeta) = 0, [\pi_0^{n-1}]_F(\zeta) \neq 0$. Из определения E_F следует существование $\xi \in F(M)$ — такого элемента, что $\zeta = E_F(\xi)$.

Пусть $\alpha \in O_T$, и A – элемент из кольца целых $O_{\widetilde{T}}$ такой, что $A^\varphi - A = \alpha$. В работе [4] (§3.1, стр.775) была определена функция

$$H_\zeta(\alpha) = E_F(\pi_0^n A\xi). \tag{3.12}$$

Предложение 4. *([14]) $H_\zeta(\alpha)$ – π_0^n-примарный элемент формального O_0-модуля $F(M)$, т.е., $H_\zeta(\alpha) \in K$ и расширение $K\left(\frac{1}{[\pi_0^n]}H_\zeta(\alpha)\right)/K$ неразветвлено. Кроме того, $H_\zeta(\alpha)$ не зависит от выбора A.*

3.2.3 Действие изогении $[\pi_0]$

Предложение 5. *([4], §1.2, стр. 774) Для $\alpha \in M$*

$$[\pi_0](\alpha) \equiv \alpha^q \mod (\pi^{qi+1}) \text{ при } v(\alpha) = i < e_1, \tag{3.13}$$

$$[\pi_0](\alpha) \equiv \pi_0\alpha \mod (\pi^{i+e_1+1}) \text{ при } v(\alpha) = i > e_1, \tag{3.14}$$

$$[\pi_0](\alpha) \equiv \pi_0\alpha + \alpha^q \mod (\pi^{qe_1+1}) \text{ при } v(\alpha) = e_1. \tag{3.15}$$

Из этих формул, в частности, следует, что если $\alpha \equiv 0 \mod (\pi^{qe_1+1})$, то $\alpha = [\pi_0](\rho), \rho \in F(M)$.

Замечание. Более того, второе сравнение можно заменить на

$$[\pi_0](\alpha) \equiv -\theta_0\alpha\pi^e \mod (\pi^{i+e+1}) \text{ при } v(\alpha) = i > e_1, \tag{3.16}$$

где $\theta_0 \in O_N$ определяется из равенства

$$\pi_0 \equiv -\theta_0\pi^e \mod \pi^{e+1}. \tag{3.17}$$

3.3 Случай конечного поля вычетов

3.3.1 Случай отсутствия нетривиальных корней изогении $[\pi_0^n]$

Рассмотрим случай, когда K не содержит нетривиальных корней изогении $[\pi_0^n]$.

Везде в формулировках теорем под суммированием понимается суммирование с помощью формального закона F, сам же символ F опускается во избежание излишнего загромождения формул. Также будем писать $E(X)$ вместо $E_F(X)$.

В работе [4] (§4.1, стр. 781) был дан следующий критерий для системы образующих $F(M)$.

Лемма 14. *Пусть для каждого i с условием: $i \not\equiv 0 \mod q$, $1 \le i < qe_1$, а также для $i = qe_1$, и для каждого $\theta \in \mathfrak{R}$ (множества представителей Тейхмюллера) выбран элемент $\varepsilon_i(\theta)$ в $F(M)$, удовлетворяющий условию $\epsilon_i(\theta) \equiv \theta\pi^i$*

$\mod \pi^{i+1}$. *Тогда любой элемент* $\beta \in F(M)$ *можно представить в виде*

$$\beta = \sum_{r\in\mathbb{N},i} [\pi_0^r](\varepsilon_i(\theta_{i,r})). \tag{3.18}$$

Теорема 17. *Пусть в поле* K *не содержится нетривиальных корней изогении* $[\pi_0^n]$. *Тогда любой элемент* $\beta \in F(M)$ *можно единственным образом представить в виде*

$$\beta = \sum_{i\in S_e} E(a_i\pi^i). \tag{3.19}$$

Доказательство. Существование такого разложения следует из леммы 14: для каждого $i \in S_e$, и для каждого $\theta \in \Re$ выбран элемент $\varepsilon_i(\theta) = E(\theta\pi^i)$. Применяя формальную аддитивность функции E, получаем требуемое разложение.

Докажем его единственность. Предположим противное. Тогда должно существовать нетривиальное представление нуля:

$$\sum_{i\in S_e} E_F(a_i\pi^i) = 0. \tag{3.20}$$

Пусть i_0 – минимальное i, т.ч. $a_i \neq 0$. Тогда $a_{i_0}\pi^{i_0} \equiv 0 \mod \pi^{i_0+1}$. Противоречие. □

3.3.2 Случай наличия нетривиальных корней изогении $[\pi_0^n]$

Пусть ζ – первообразный элемент ядра изогении $[\pi_0^n]$.

Для элемента $\alpha \in F(M)$ обозначим через $\underline{\alpha}$ любой ряд из $O_N[[X]]$, такой что $\underline{\alpha}(\pi) = \alpha$. Введем также обозначения $s_j(X) := [\pi_0^j](\underline{\zeta})$, $s := s_n$, $u = \frac{s}{s_{n-1}}$.

В работе [4] (§1.4, стр. 773) проверялось, что

$$s \equiv s_{n-1}^{\triangle} \mod \pi_0^n. \tag{3.21}$$

Определим на $XO_N[[X]]$ функцию

$$l_F(g(X)) = \left(1 - \frac{\triangle}{\pi_0}\right) \lambda(g(X)). \tag{3.22}$$

Предложение 6. *Для любого $a \in O_N$ элемент*

$$\omega(a) = E(a\pi_0^n(\underline{\zeta}))|_{X=\pi} \tag{3.23}$$

является π_0^n-примарным в $F(M)$.

Теорема 18. *([4], §4.3, стр. 783)) Всякий элемент $\beta \in F(M)$ можно представить в виде*

$$\beta = \omega(a) + \sum_{i \in S_e} E(a_i \pi_0^i), a, a_i \in O_0. \tag{3.24}$$

При этом a_i определены однозначно по $\mod \pi_0^n$.

3.4 Случай совершенного поля вычетов

Пусть теперь k — совершенное поле, не обязательно являющееся конечным. Выберем в k какой-нибудь базис $\overline{\Theta} = \{\overline{\theta}_i, i \in I\}$, и пусть $\Theta = \{\theta_i, i \in I\}$ – представители этого базиса в O_K.

Для каждого $s \in S_e$ определим $\mu_s \in \mathbb{Z}$, такое, что

$$e_1 \leq q^{\mu_s} s < q e_1. \tag{3.25}$$

3.4.1 Случай $e \not\equiv 0 \mod (q-1)$

Предложение 7. *Пусть $s \in S_e$.*

Базисом ступени $F(M^{q^\mu s}) \setminus F(M^{q^\mu s+1}), 0 \leq \mu \leq \mu_s$, является множество

$$[\pi_0^{q^\mu}] E(\Theta \pi^s) \equiv E(\Theta^{q^\mu} \pi^{q^\mu s}) \mod F(M^{q^\mu s+1}). \tag{3.26}$$

Базисом ступени $F(M^{q^{\mu_s}s+\mu e})\setminus F(M^{q^{\mu_s}s+\mu e+1}), \mu > 0$, *является множество*

$$[\pi_0^{\mu+\mu_s}]E(\Theta\pi^s) \equiv E(\theta_0^{\mu}\Theta^{q^{\mu_s}}\pi^{q^{\mu_s}s+e\mu}) \mod F(M^{q^{\mu_s}s+\mu e+1}). \tag{3.27}$$

Доказательство. Ясно из предложения 5. □

3.4.2 Случай $e \equiv 0 \mod (q-1)$

Пусть $m-1$ — максимальная степень q, на которую делится e:

$$e_m = \frac{e}{(q-1)q^{m-1}} \in \mathbb{Z}, \quad e_{m+1} \notin \mathbb{Z} \tag{3.28}$$

Определим гомоморфизм

$$\begin{gathered} \psi : k \to k, \\ \overline{\varepsilon} \mapsto \overline{\varepsilon}^{q^m} - \overline{\theta_0}\overline{\varepsilon}^{q^{m-1}}. \end{gathered} \tag{3.29}$$

Случай $Ker\psi = \{0\}$**.**

Определим

$$\beta_i = \theta_i^{q^m} - \theta_0\theta_i^{q^{m-1}}, i \in I, \tag{3.30}$$

и обозначим

$$\mathfrak{B} = \{\beta_i, i \in I\}. \tag{3.31}$$

Лемма 15. *Если* $Ker\psi = \{0\}$*, то* $\overline{\mathfrak{B}} = \{\overline{\beta}_i, i \in I\}$ *— базис* k*.*

Доказательство. Пусть

$$\sum_{j=1}^{l} a_j\overline{\beta}_{i_j} = 0, \tag{3.32}$$

тогда

$$\sum_{j=1}^{l}\left((a_j\overline{\theta}_{i_j})^{q^m}-\theta_0(a_j\overline{\theta}_{i_j})^{q^{m-1}}\right)=0. \tag{3.33}$$

Взяв $\overline{\rho}=\sum\limits_{j=1}^{l}a_j\overline{\theta}_{i_j}$, получаем $\overline{\rho}^{q^m}-\overline{\theta}\overline{\rho}^{q^{m-1}}=0$. Таким образом, $\overline{\rho}\in Ker\psi$, а значит, $\sum\limits_{j=1}^{m}a_j\overline{\theta}_{i_j}=0$. Из линейной независимости системы Θ следует $a_j=0, j=1,\ldots,l$. □

Предложение 8. *Пусть* $e\equiv 0 \mod (q-1), Ker\psi=\{0\}$ *и* $s\in S_e$.

Базисом ступени $F(M^{q^\mu s})\setminus F(M^{q^\mu s+1}), 0\le\mu\le\mu_s$, *является множество*

$$E(\Theta^{q^\mu}\pi^{q^\mu s}). \tag{3.34}$$

Базисом ступени $F(M^{q^{\mu_s}s+\mu e})\setminus F(M^{q^{\mu_s}s+\mu e+1}), \mu>0$, *является множество*

$$E(\theta_0^\mu\Theta^{q^{\mu_s}}\pi^{q^{\mu_s}s+e\mu}). \tag{3.35}$$

Базисом ступени $F(M^{qe_1+\mu e})\setminus F(M^{qe_1+\mu e+1}), \mu\ge 0$, *является множество*

$$E(\theta_0^\mu\mathfrak{B}\pi^{qe_1+\mu e}). \tag{3.36}$$

Доказательство. Используем предложение 5 (для ступени qe_1) и лемму 15. □

Случай $Ker\psi\neq\{0\}$**.**

В этом случае поле K содержит все корни изогении $[\pi_0^n]$. Заметим, что $n\le m$. Пусть ζ_n — первообразный корень.

Пусть $\eta_*\in O_K^*$ — такой элемент, что $\overline{\eta_*}\in Ker\psi$. Таким образом,

$$\eta_*^{q^m}-\theta_0\eta_*^{q^{m-1}}\equiv 0 \mod \pi. \tag{3.37}$$

Пусть $H_0 = \{\eta_i, i \in I_0\}$ — система представителей в O_K базиса $k \setminus Ker\psi$, т.е., дополнение $\overline{\eta}_*$ до базиса поля k. Получаем $H = \overline{H_0} \cup \{\overline{\eta}_*\}$ — базис k.

Можно также заметить, что

$$\{\psi(\overline{\eta}_i), i \in I_0\} \subset Im\psi \tag{3.38}$$

— линейно независимая система в k (так как является образом линейно независимой системы). Дополним ее до базиса. Пусть $\Xi = \{\xi_j, j \in J\}$ — система представителей дополнения. Таким образом, мы имеем три разных базиса поля k над k_0:

$$\overline{\Theta} = \{\overline{\theta}_i, i \in I\}, \tag{3.39}$$

$$\overline{H} = \{\overline{\eta_*}, \overline{\eta}_i, i \in I_0\}, \tag{3.40}$$

$$\psi(\overline{H}_0) \cup \overline{\Xi} = \{\psi(\overline{\eta}_i), \overline{\xi}_j, i \in I_0, j \in J\}. \tag{3.41}$$

Отсюда получаем следующий результат.

Предложение 9. *Пусть $s \in S_e, s \neq e_m$. Тогда базисами ступеней*

$$F(M^{q^\mu s}) \setminus F(M^{q^\mu s+1}), 0 \leq \mu \leq \mu_s \tag{3.42}$$

$$u\ F(M^{q^{\mu_s} s+\mu e}) \setminus F(M^{q^{\mu_s} s+\mu e+1}), \mu > 0, \tag{3.43}$$

будут соответствующие системы из предложения 8.

Пусть $s = e_m \in S_e$. Тогда базисом ступени

$$F(M^{q^\mu e_m}) \setminus F(M^{q^\mu e_{m+1}+1}), 0 \leq \mu \leq m, \tag{3.44}$$

будет система

$$E(H^{q^\mu} \pi^{q^\mu e_m}). \tag{3.45}$$

Базисом ступени $F(M^{qe_1+\mu e}) \setminus F(M^{qe_1+\mu e+1}), \mu \geq 0$, *будет система*

$$E(\theta^{\mu}\Psi\pi^{qe_1+\mu e}) \cup E(\theta^{\mu}\Xi\pi^{qe_1+\mu e}), \tag{3.46}$$

где Ψ *— система представителей* $\psi(\overline{H}_0)$.

3.4.3 Базис формального модуля $F(M)$ в случае совершенного поля вычетов

Случай отсутствия нетривиальных корней изогении $[\pi_0^n]$

Теорема 19. *В случае отсутствия нетривиальных корней изогении* π_0^n *множество*

$$\{\varepsilon_{i,s} | i \in I, s \in S_e\}, \tag{3.47}$$

где $\varepsilon_{i,s} = E(\theta_i\pi^s)$, *является* O_0*-базисом формального модуля* $F(M)$, *т.е. любой элемент* $\alpha \in F(M)$ *однозначно представляется в виде*

$$\alpha = \sum_{i\in I, s\in S_e} [a_{i,s}]E(\theta_i\pi^s), \tag{3.48}$$

где $a_{i,s} \in O_0$ *и множество индексов*

$$I_{s,c} = \{i \in I | v(a_{i,s}) \leq c\} \tag{3.49}$$

конечно для любого $c \geq 0$ *и любого фиксированного* s.

Доказательство. $\{\varepsilon_{i,s} | i \in I, s \in S_e\}$ является системой образующих для $F(M)$ по лемме 14.

Докажем единственность разложения. Пусть

$$\sum_{i,s} [a_{i,s}]\varepsilon_{i,s} = 0. \tag{3.50}$$

Надо доказать, что $a_{i,s} = 0$ для всех пар (i, s).

Для $s \in S_e$ и $c \geq 1$, определим $I_c^{(s)} \subset I$ как множество индексов, для которых $v(a_{i,s}) = c$. Заметим, что это множество конечно. Тогда

$$\begin{gathered} 0 = \sum_{i,s} [a_{i,s}]\varepsilon_{i,s} = \sum_{s \in S_e} \sum_{c \geq 1} \varepsilon_s^{(c)}, \\ \text{где } \varepsilon_s^{(c)} = \sum_{i \in I_s^{(c)}} [a_{i,s}]\varepsilon_{i,s}. \end{gathered} \tag{3.51}$$

Для каждой фиксированной пары (s, c) сумма $\sum\limits_{i \in I_s^{(c)}} [a_{i,s}]\varepsilon_{i,s}$ либо равна 0, когда все $a_{i,s} = 0, i \in I_c$, либо все слагаемые, отличные от 0, лежат в одной ступени. При этом для разных пар (s, c) и (s', c') ступени, в которых лежат $\varepsilon_s^{(c)}$ и $\varepsilon_{s'}^{(c')}$, не совпадают.

Если не все $a_{i,s}$ равны нулю, то найдется пара (s, c), для которой $\varepsilon_s^{(c)}$ принадлежит ступени $F(M^r) \setminus F(M^{r+1})$ с наименьшим номером r. Тогда

$$0 = \sum_{i,s} [a_{i,s}]\varepsilon_{i,s} = \sum_{s \in S_e} \sum_{c \geq 1} \varepsilon_s^c \in F(M^r) \setminus F(M^{r+1}) \tag{3.52}$$

– противоречие. □

Случай наличия нетривиальных корней изогении $[\pi_0^n]$

Теорема 20. *Множества*

$$E(\Theta\pi^s), s \in S_e, s \neq e_m, \tag{3.53}$$

$$E(H\pi^{e_m}), \tag{3.54}$$

$$\text{и } E(\Xi\pi^{e_1}) \tag{3.55}$$

являются системой образующих модуля $F(M)$ над O_0. Т.е, любой элемент $\alpha \in F(M)$ представим в виде

$$\alpha = \sum [a_i]\varepsilon_i, \tag{3.56}$$

где ε_i пробегает все упомянутые множества. При этом a_i определены однозначно по модулю π_0^n.

Доказательство. Существование доказывается аналогично предыдущей теореме. Единственность разложения по модулю π_0^n вытекает из следуещей леммы:

Лемма 16. *$\alpha \in K$ тогда и только тогда принадлежит (π_0^n), когда все коэффициенты в разложении*

$$\alpha = \sum [a_i]\varepsilon_i \tag{3.57}$$

делятся на π_0^n.

Доказательство. Достаточность очевидна. Докажем необходимость. Пусть v_0 — нормирование на K_0 и $\nu = \min\{v_0(a_i), v_0(a_*)\}$. Предположим, что теорема неверна. Тогда $\nu < n$. Пусть $i_0 = \min\{i, v_0(a_i) = \nu\}$. Рассмотрим элемент $\omega = \frac{1}{[\pi_0^\nu]}\alpha$. Получим, что $\omega \equiv \gamma\pi^{i_0} \mod \pi^{qe_1+1}$, где γ — линейная комбинация элементов из H при $i_0 = e_m$, элементов из Ξ при $i_0 = e_m$, элементов из Θ в прочих случаях. Таким образом, $\omega \not\equiv 0 \mod \pi^{qe_1}$ и расширение $K(\frac{1}{[\pi_0^{\nu+1}]}\alpha)/K$ будет нетривиальным, что противоречит условию $\alpha \in (\pi_0^n)$. □

□

3.5 Случай несовершенного поля вычетов

Определение 15. Элементы $\{\bar{t}_r, r \in R\}$ образуют p-базис поля k, если $k = k^p[\{\bar{t}_r\}]$ и $(k^p[\bar{t}_1, \dots \bar{t}_n] \colon k^p) = p^n$ для любых попарно различных $\bar{t}_1, \dots \bar{t}_n$

Замечание. Таким образом, $k = k^{p^l}[\{\bar{t}_r\}]$ для любого $l \geq 1$.

Пусть $\{t_r, r \in R\}$ — система представителей в O p-базиса $\{\bar{t}_r, r \in R\}$ Обозначим $t_{(r)}^{(k)} = t_{r_1}^{k_1} \dots t_{r_l}^{k_l}$.

Для мультииндекса (k) будем использовать следующие обозначения:

- $l_1 \leq (k) \leq l_2$, если $l_1 \leq k_i \leq l_2$ для всех i,

- $p \nmid (k)$, если $p \nmid k_i$ для всех i.

Введем обозначение $\widetilde{T}_l = \{t^{(k)}_{(r)} \mid 1 \leq (k) \leq l\}$, $\widetilde{T}_l := \{1\}$. Пусть $T_l = \{t^{(k)}_{(r)} \in \widetilde{T}_l, p \nmid t^{(k)}_{(r)}\}$ при $l > 0$ и $T_0 := \widetilde{T}_0$.

Пусть A — система представителей элементов из k в O.

Лемма 17.

$$A = A^{p^l} + A^{p^l}[\widetilde{T}_l] = \sum_{0 \leq i \leq n} A^{p^l}[T^{p^i}_{l-i}]. \tag{3.58}$$

Доказательство. Индукцией по l из определения p-базиса получаем

$$k = k^{p^l} + k^{p^l}[\overline{\widetilde{T}_l}] = \bigoplus_{0 \leq i \leq n} k^{p^l}[\overline{T}^{p^i}_{l-i}]. \tag{3.59}$$

□

Следствие 2.

$$A = A^{q^l} + A^{q^l}[\widetilde{T}_{lf}] = \sum_{0 \leq i \leq lf} A^{q^f}[T^{p^i}_{lf-i}]. \tag{3.60}$$

Доказательство. При $q = p^f$ заменяем l на lf. □

3.5.1 Случай $e \neq 0 \mod (q-1)$

Лемма 18. *Пусть $s \in S_e$. Полной системой представителей ступени $F(M^s) \setminus F(M^{s+1})$ является множество*

$$E(A\pi^s). \tag{3.61}$$

Полной системой представителей ступени $F(M^{\mu e+s}) \setminus F(M^{\mu e+s+1})$ является множество

$$E(\theta_0^\mu A\pi^{s+\mu e}). \tag{3.62}$$

Доказательство. Ясно из леммы 5. □

Лемма 19. *Пусть* $s \in S_e$.

Полной системой представителей ступени $F(M^{q^\mu s}) \setminus F(M^{q^\mu s+1}), 0 \le \mu \le \mu_s$, *является множество*

$$E((\sum_{0\le i\le \mu} A^{q^\mu}[T_i^{p^{\mu f-i}}])\pi^{q^\mu s}). \tag{3.63}$$

Полной системой представителей ступени $F(M^{q^\mu s}+\mu e) \setminus F(M^{q^\mu s+\mu e+1})$ *является множество*

$$E((\theta^\mu \sum_{0\le i\le \mu} A^{q^{\mu_s}}[T_i^{p^{\mu_s f-i}}])\pi^{p^{\mu_s} s+\mu e}). \tag{3.64}$$

Доказательство. Применяем лемму 18 и следствие из леммы 17. □

3.5.2 Случай $e \equiv 0 \pmod{q-1}$

Аналогично случаю совершенного поля вычетов определяем гомоморфизм $\psi : k \to k$.

$Ker\psi = \{0\}$

Лемма 20. *Полной системой представителей ступени* $F(M^{q^{\mu_s}}) \setminus F(M^{q^{\mu_s}s+1}), s \in S_e, 0 \le \mu \le \mu_s$, *является множество*

$$E((\sum_{i=0}^{\mu} A^{q^\mu}[T_i^{q^{\mu f-i}}])\pi^{q^\mu s}). \tag{3.65}$$

Полной системой представителей ступени $F(M^{q^\mu s+\mu e}) \setminus F(M^{q^\mu s+\mu e+1}), s \in S_e, s \ne e_m$, *является множество*

$$E((\theta_0^\mu \sum_{i=0}^{\mu_s} A^{q^{\mu_s}}[T_i^{p^{\mu_s f-i}}])\pi^{q^{\mu_s} s+\mu e}). \tag{3.66}$$

Полной системой представителей ступени $F(M^{qe_1+\mu e}) \setminus F(M^{qe_1+\mu e+1}), 0s \in S_e, s \neq e_m$, *является множество*

$$E(\theta_0^{\mu}\mathfrak{B}\pi^{qe_1+\mu e}), \tag{3.67}$$

где $\mathfrak{B} = \sum_{i=0}^{m-1} \mathfrak{B}_i$, $\mathfrak{B}_i = A^{q^m}[T^{p^{mf-i}}] - \theta_0 A^{q^{m-1}}[T^{p^{mf-i-1}}]$.

Доказательство. Первые два утверждения получаем по аналогии с леммой 19. Последнее утверждение получаем, воспользовавшись леммой 14 и тем, что $A = \mathfrak{B} \mod M$, а значит, $\mathfrak{B}$ — полная система представителей k в O. □

$Ker\psi \neq \{0\}$

Пусть $Ker\psi$ порождено $\overline{\alpha}_0 \in \overline{A}$. Так как $\psi(\overline{A}) = \overline{A}^{q^m} - \overline{\theta}_0\overline{A}^{q^{m-1}}$, то, обозначив $A_0 = A \setminus \{\alpha_0\}$, получим систему представителей $\psi(A)$ в O:

$$(\overline{A}_0^{q^m} - \overline{\theta}_0\overline{A}_0^{q^{m-1}}) + \mathfrak{B}. \tag{3.68}$$

Обозначим $\Gamma = \{\gamma \in O \mid \overline{\gamma} \in k \setminus Im\psi\}$.

Лемма 21. *Полной системой представителей ступени* $F(M^{q^{\mu}s}) \setminus F(M^{q^{\mu}s+1}), s \in S_e, 0 \leq \mu \leq \mu_s$, *является множество*

$$E((\sum_{i=0}^{\mu} A^{q^{\mu}}[T_i^{q^{\mu}f-i}])\pi^{q^{\mu}s}). \tag{3.69}$$

Полной системой представителей ступени $F(M^{q^{\mu}s+\mu e}) \setminus F(M^{q^{\mu}s+\mu e+1}), s \in S_e, s \neq e_m$, *является множество*

$$E((\theta_0^{\mu}\sum_{i=0}^{\mu_s} A^{q^{\mu_s}}[T_i^{p^{\mu_s}f-i}])\pi^{q^{\mu_s}s+\mu e}). \tag{3.70}$$

Полной системой представителей ступени $F(M^{qe_1+\mu e}) \setminus F(M^{qe_1+\mu e+1}))$ *яв-*

ляется множество

$$E(\theta_0^{\mu}(A_0^{q^m} - \theta_0 A_0^{q^{m-1}}\pi^{e_1+\mu e})) \cup E(\theta_0^{\mu}\mathfrak{B}\pi^{qe_1+\mu e}) \cup E(\theta_0^{\mu}\Gamma\pi^{qe_1+\mu e}). \tag{3.71}$$

3.5.3 Базис формального модуля $F(M)$ в случае несовершенного поля вычетов.

Случай отсутствия нетривиальных корней изогении $[\pi_0^n]$

Теорема 21. *Множество*

$$E(A^{q^{\mu}}[T_{q^{\mu}}]\pi^{q^{\mu}s}), \tag{3.72}$$

где $s \in S_e, 0 \leq \mu \leq \mu_s$, является O_0-базисом формального модуля $F(M)$, т.е. любой элемент $\beta \in F(M)$ однозначно представляется в виде

$$\beta = \sum_{s,\mu,(k),(r)} [a_{\alpha,\beta}]E(\alpha^{q^{\mu}} t_{(r)}^{(k)} \pi^{q^{\mu}s}), \tag{3.73}$$

при этом (r) пробегает конечное число наборов индексов из R, и

$$I_{s,c} = \{\alpha \in A, (k), (r) | v(a_{\alpha,\beta}) \leq c\} \tag{3.74}$$

конечно для любого $c \geq 0$ и любых фиксированных s и μ.

Доказательство. Существование разложения следует из теоремы Гензеля. Докажем единственность. Если есть неоднозначность разложения, то существует и нетривиальное представление нуля. Пусть

$$\beta_{s,\mu,c} = \sum [a_{\alpha,\beta}]E(\alpha^{q^{\mu}} t_{(r)}^{(k)} \pi^{q^{\mu}s}), \tag{3.75}$$

где $(k), (r), \alpha$ пробегают все наборы, для которых $v(a_{\alpha,\beta}) = c$. Тогда, если

$$\sum_{(s,\mu)}(\sum_{c\geq 1}\alpha_{s,\mu,c}) = 0, \tag{3.76}$$

то либо все $\alpha_{s,\mu,c}$ равны нулю, либо для некоторой тройки (s,μ,c) $\beta_{s,\mu,c}$ лежит в ступени $M^r \setminus M^{r+1}$ с наименьшим r. Из этого следует, что $1 \in M^r \setminus M^{r+1}$ – противоречие. □

Случай наличия нетривиальных корней изогении $[\pi_0^n]$

Теорема 22. *Множество*

$$E(A^{q^\mu}[T_{q^\mu}]\pi^{q^\mu s}) \cup E(\Gamma\pi^{qe_1}), \tag{3.77}$$

где $s \in S_e$, являются системой образующих модуля $F(M)$ над O_0. Т.е, любой элемент $\alpha \in F(M)$ представим в виде

$$\beta = \sum_{s,\mu,(k),(r)}[a_{\alpha,\beta}]E(\alpha^{q^\mu}t_{(r)}^{(k)}\pi^{q^\mu s}) + \sum[b_{\gamma,\beta}]E(\gamma\pi^{e_1}). \tag{3.78}$$

При этом $a_{\alpha,\beta}, b_{\gamma,\beta}$ определены однозначно по модулю π_0^n.

Доказательство. Доказательство единственности разложения повторяет случай совершенного поля. □

Глава 4

Канонический базис для формальных модулей Хонды

В этой главе мы рассмотрим случай формальных модулей Хонды.

4.1 Обозначения

Сначала введем следующие обозначения:

- k – локальное поле характеристики 0;
- $\bar{k} = \mathbb{F}_q$, $q = p^f$, $p \neq 2$;
- k'/k – конечное неразветвленное расширение с униформизующей π;
- K – n-мерное локальное поле, т.е., цепочка полей

$$K = K_n, K_{n-1}, \ldots, K_1, K_0, \tag{4.1}$$

где $K_1 = k'$, $K = k'((t_2))\ldots((t_n))$, в которой каждое следующее поле является полем вычетов предыдущего;

- L – конечное расширение K, имеющее вид

$$L = L_1((T_2)) \dots ((T_n)), \tag{4.2}$$

L_1 – конечное расширение K_1 с простым элементом Π и $L_i = L_1((T_2)) \dots ((T_i)))$;

- $\mathfrak{M}$ – максимальный идеал в L

Зададим также отображение $\sigma : K \to K$, действующее на системе локальных параметров как

$$\sigma(t_i) = t_i^p, \tag{4.3}$$

а на k' σ совпадающее с автоморфизмом Фробениуса. Тогда на степенных рядах $K[[X]]$ можно определить оператор $\triangle$:

$$\triangle(\sum c_i X^i) = \sum \sigma(c_i) X^{pi}. \tag{4.4}$$

Введя на множестве степенных рядов от $\triangle$ с коэффициентами из $\mathcal{O}_K$ умножение по правилу $\triangle \cdot a = \sigma(a) \cdot \triangle$, мы получим структуру кольца. Данное кольцо будем обозначать $\mathcal{D}$.

4.2 Предварительные сведения

Тип формальной группы

Пусть $F(X, Y) \in \mathcal{O}_K[[X, Y]]$ – формальная группа.

Теорема 23 (Картье)**.** *Если R – $\mathbb{Z}_p$-алгебра, для любой формальной группы над R существует изоморфная ей p-типическая формальная группа.*

Значит, F строго изоморфна p-типической формальной группе F_p с логарифмом $\lambda_p(X) = \sum\limits_{i=0}^{\infty} c_i X^{p^i}$.

Предложение 10. *Пусть F_p – p-типическая формальная группа. Тогда существует единственный $u_p(\triangle) \in \pi + \mathcal{D}\triangle$ (тип группы F_p), т.ч. $\lambda_p(X) = (\pi u_p^{-1}(\triangle))(X)$.*

Доказательство. По теории Хонды существует $u(\Delta) \in \pi + \mathcal{D}\Delta$, такой что $u(\Delta) \circ \lambda_p(X) \equiv 0 \mod \pi$. Тогда $u \circ \Lambda = \pi\varepsilon(\Delta)$, и $\varepsilon \in 1 + \mathcal{D}\Delta$. Теперь можно взять $u_p = \varepsilon^{-1} \circ u$. □

Предложение 11. *Пусть $u \in \pi + \mathcal{D}\Delta$. Тогда ряд $\lambda(X) = (\pi u_p^{-1}(\triangle))(X)$ является логарифмом некоторой p-типической формальной группы над $\mathcal{O}_K$.*

Доказательство. Достаточно заметить, что ряд удовлетворяет условию $u(\Delta) \circ \lambda(X) \equiv 0 \mod \pi$. Тогда он будет являться логарифмом некоторой p-типической формальной группы. □

Оператор $\mathcal{A}$

Из теории Хонды вытекает следующее предложение.

Предложение 12. *В классе изоморфных формальных групп высоты h можно выделить канонический представитель – группу Артина-Хассе F_c с логарифмом $\lambda_c(X) = \pi u_c^{-1}(\Delta) \circ X$.*

Предложение 13. *Пусть (F, u) и (F', u') – формальные группы и соответствующие специальные элементы. Для $c \in \mathcal{O}_K$ существует гомоморфизм $f(X) \equiv cX \mod X^2$ из F в F' тогда и только тогда, когда существует $s \in \mathcal{D}\Delta$, такой что $u'c = su$.*

Предложение 14. *Пусть F – p-типическая формальная группа над $\mathcal{O}_K$ типа $u = \pi - a_h B\triangle^h$, $B \in 1 + \mathcal{D}\triangle$, и пусть $\lambda_1(X) = (\pi u^{-1}(\triangle))(X)$, где $u_1 = u^{\sigma^h} \circ B^{-1}$. Тогда*

1. *λ_1 является логарифмом некоторой p-типической формальной группы F_1 над $\mathcal{O}_K$;*

2. *существует* $[\pi a_h^{-1}]_{F,F_1} \in Hom_{\mathcal{O}_K}(F, F_1)$, *такой что*

$$[\pi a_h^{-1}]_{F,F_1}(X) \equiv X^{p^h} \mod \pi; \tag{4.5}$$

3. *если* u_c – *канонический тип* F, *то* $a_h^{-1} u_c a_h$ – *канонический тип* F_1.

Доказательство. 1. $u_1 = u^{\sigma^h} \circ B^{-1} \in \pi + \mathcal{D}\Delta$. Следовательно, по предложению 11 ряд λ_1 будет логарифмом некоторой формальной группы F_1 над $\mathcal{O}_K$.

2. Проверим, что условиям удовлетворяет гомоморфизм

$$[\pi a_h^{-1}]_{F,F_1} = [\pi a_h^{-1}]_{F,F_1'} \circ [1]_{F_1',F_1}, \tag{4.6}$$

где $u_1' = Bu_1$, а F_1' – формальная группа с логарифмом $\lambda_{\prime 1} = \pi u_{\prime 1}^{-1} \circ X$.

По теореме 13 группа F_1' строго изоморфна F. Проверим, что $\pi a_h u = u_1' \circ (\pi a_h^{-1})$. По определению u_1'

$$u_1' a_h^{-1} = B(\pi - a_h^{\sigma^h} B^{\sigma^h} \Delta^h) B^{-1} a_h^{-1}. \tag{4.7}$$

По дистрибутивности, учитывая, что $\Delta^h B = B^{\sigma^h} \Delta^h$, получим

$$u_1' a_h^{-1} = a_h^{-1}\pi - B\Delta^h = a_h^{-1} u. \tag{4.8}$$

Поскольку $\pi a_h u = u_1' \circ (\pi a_h^{-1})$ по предложению 13, существует гомоморфизм $[\pi a_h^{-1}]_{F,F_1'} \equiv \pi a_h^{-1} X \mod X^2$. Благодаря строгой изоморфности F_1' и F_1

$$[\pi a_h^{-1}]_{F,F_1'} \circ [1]_{F_1',F_1} \equiv \pi a_h^{-1} X \mod X^2. \tag{4.9}$$

Теперь нам нужно доказать, что

$$[\pi a_h^{-1}]_{F,F_1'} \circ [1]_{F_1',F_1} \equiv X^{p^h} \mod \pi. \tag{4.10}$$

Сначала заметим, что

$$\begin{aligned}\pi a_h^{-1}\lambda(X) = \pi a_h^{-1}(\pi u^1(\Delta)\circ X) = (a_h^{-1}u + B\Delta^h)(\pi u^1(\Delta)\circ X = \\ = \pi a_h^{-1}X + \pi B u^{-\sigma^h}\Delta^h \circ X = \pi u_1^{-1}\circ X^{p^h} \equiv \lambda_1(X^{p^h}) \mod \pi\mathcal{O}_K\end{aligned} \tag{4.11}$$

Так как

$$[\pi a_h^{-1}]_{F,F_1} = \lambda_1^{-1}\circ\pi a_h^{-1}\circ\lambda, \tag{4.12}$$

то

$$\lambda_1([\pi a_h^{-1}]_{F,F_1}) \equiv \lambda_1(X^{p^h}) \mod \pi\mathcal{O}_K[[X]]. \tag{4.13}$$

Такое возможно лишь при $[\pi a_h^{-1}]_{F,F_1} \equiv X^{p^h} \mod \pi$.

□

Таким образом мы получаем следующую последовательность формальных групп и гомоморфизмов f_i:

$$\begin{aligned}F \to F_1 \to \ldots \to F_N \\ f^{(m)} = f_{m-1}\circ\ldots\circ f_1\circ f.\end{aligned} \tag{4.14}$$

Отображение Артина-Хассе

Определим

- отображение $E_F : K[[X]]_0 \to F(K[[X]]_0)$, заданное формулой

$$E_F(\varphi) = \lambda^{-1}(\pi u_0^{-1}\circ\varphi) \tag{4.15}$$

- отображение $l_F : F(K[[X]]_0) \to K[[X]]_0$, заданное формулой

$$l_F(\psi) = \frac{u_0}{\pi}\circ\lambda(\psi). \tag{4.16}$$

Лемма 22. *E_F и l_F задают обратные друг другу изоморфизмы $\mathcal{O}_K$-модулей $\mathcal{O}_K[[X]]_0$ и $F(\mathcal{O}_K[[X]]_0)$, а также $K[[X]]_0$ и $F(K[[X]]_0)$.*

Примарные элементы

Определение 16. Элемент $\omega \in F_N(\mathfrak{M})$ называется примарным, если $K(\widetilde{\omega})/K$ неразветвлено (где $f^{(N)}(\widetilde{\omega}) = \omega$).

Введем следующие обозначения:

- $W_F^N = Ker[\pi^N]_F \subset F(\mathfrak{M})$
- $\{z_1, \ldots, z_h\}$ – множество образующих W_F^N (как модуля над $\mathcal{O}_K$),
- $s = f^{(N)} \circ \underline{z}$, где $\underline{z}$ – ряд, соответствующий разложению произвольной фиксированной образующей из $\{z_1, \ldots, z_h\}$ по степеням Π,
- $\widehat{b} = b + b^{\triangle} + \ldots + b^{\triangle^{h-1}}$

Предложение 15.

$$\omega(b) = E_N(\widehat{b}\lambda_N(s))|_{X=\Pi} \tag{4.17}$$

– корректно определенный элемент множества $F_N(\mathfrak{M})$, и, более того, этот элемент является примарным.

Доказательство. Доказательство аналогично доказательству предложения 1.9.1 [2] □

4.2.1 Основные результаты

Определим многочлены Эньяра:

$$g_0 = \pi_{N-1}X + X^{p^h}, \tag{4.18}$$

$$g_{\rho,a} = \pi_{N-1}X + \pi_{N-1}aX^{p^\rho} + X^{p^h}, a \in \mathcal{O}_K, 1 \leq \rho < fh. \tag{4.19}$$

Пусть u_{N-1} – канонический тип группы F_{N-1}. Тогда существуют единственные (с точностью до изоморфизма) формальные группы G_0, $G_{\rho,a}$, для которых g_0, $g_{\rho,a}$ являются допустимыми изогениями в группы G'_0, $G'_{\rho,a}$ соответственно. Тогда u_N – тип групп G'_0, $G'_{\rho,a}$, следовательно, они изоморфны F_N. Обозначим соответствующие изоморфизмы через $\mathcal{E}_N^0$, $\mathcal{E}_N^{\rho,a}$.

Теорема 24. *Элементы*

$$\omega_i(b), b \in \mathcal{O}_K, \quad 1 \le i \le h, \tag{4.20}$$

$$\mathcal{E}_N^0(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}), \tag{4.21}$$

$$\mathcal{E}_N^{\rho,a}(\theta \Pi^{i_1} T_2^{i_2} \dots T_n^{i_n}), \tag{4.22}$$

где $\theta \in \mathcal{R}$, $a \in \mathcal{O}_K^*$, $1 \le \rho < fh$, $p \nmid \overrightarrow{i}$, $0 < i_n \le e_* = p^h e_n/(p^h - 1)$, *являются множеством образующих для* $F_N(\mathfrak{M})$.

Доказательство. Достаточно проверить это утверждение для одной формальной группы типа u, например, $F = \mathcal{A}^{-M+1} G_0$. Обозначим логарифм G_0 за λ_0 и логарифм $G_{\rho,a}$ за μ. Тогда

$$(B_{n-1} \lambda_0^{\Delta^h}) \circ g_0 = \pi_{n-1} \lambda_0, \tag{4.23}$$

$$(B_{n-1} \mu^{\Delta^h}) \circ g_{\rho,a} = \pi_{n-1} \mu, \tag{4.24}$$

то есть

$$(B_{n-1} \lambda_0^{\Delta^h})(\pi_{n-1} x) \equiv \pi_{n-1} \lambda_0(x) \mod \deg p^\rho + 1, \tag{4.25}$$

$$(B_{n-1} \mu^{\Delta^h})(\pi_{n-1} x) \equiv \pi_{n-1} \mu(x) \mod \deg p^\rho + 1. \tag{4.26}$$

Таким образом, если мы определим V как элемент, удовлетворяющий усло-

вию

$$V - V^{\Delta^h}\pi_{n-1}^{p^\rho-1} = a, \tag{4.27}$$

то $\mu \equiv \lambda_0 + Vx^{p^\rho}$. Рассмотрев логарифмы $\mathcal{A}G_0$ и $\mathcal{A}G_{\rho,a}$, делаем вывод, что

$$\begin{aligned} E_M^{\rho,a}(\theta\Pi^{i_1}T_2^{i_2}\dots T_n^{i_n}) - \theta\Pi^{i_1}T_2^{i_2}\dots T_n^{i_n} \equiv \\ \equiv V^{\Delta^h}\theta^{p^\rho}\Pi^{ip^\rho}T_2^{i_2}\dots T_n^{i_n} \mod \Pi^{ip^{\rho+1}}T_2^{i_2}\dots T_n^{i_n}. \end{aligned} \tag{4.28}$$

Теперь заметим, что достаточно добавить примарные элементы, чтобы получить полную систему образующих. □

Теорема 25. *Элементы*

$$\widetilde{\omega}_i(b), b \in \mathcal{O}_K, \quad 1 \le i \le h, \tag{4.29}$$

$$\widetilde{\mathcal{E}}_N^0(\theta\Pi^{i_1}T_2^{i_2}\dots T_n^{i_n}), \tag{4.30}$$

$$\widetilde{\mathcal{E}}_N^{\rho,a}(\theta\Pi^{i_1}T_2^{i_2}\dots T_n^{i_n}), \tag{4.31}$$

где $\theta \in \mathcal{R}$, $a \in \mathcal{O}_K^*$, $1 \le \rho < fh$, $p \nmid \overrightarrow{i}$, $0 < i_n \le e_* = p^h e_n/(p^h - 1)$, *являются множеством образующих для* $F(\mathfrak{M})$.

Доказательство. Следует из предыдущей теоремы и того, что

$$[\pi^M/\pi_1^{(M)}]_{F_M,F}\mathcal{E}_M^0(\theta\Pi^{i_1}T_2^{i_2}\dots T_n^{i_n}) = \widetilde{\mathcal{E}}^0(\theta\Pi^{i_1}T_2^{i_2}\dots T_n^{i_n}), \tag{4.32}$$

$$[\pi^M/\pi_1^(M)]_{F_N,F}\mathcal{E}_M^{\rho,a}(\theta\Pi^{i_1}T_2^{i_2}\dots T_n^{i_n}) = \widetilde{\mathcal{E}}^{\rho,a}(\theta\Pi^{i_1}T_2^{i_2}\dots T_n^{i_n}). \tag{4.33}$$

□

Заключение

Таким образом, мы построили системы образующих для многомерного локадьного поля и двух классов формальных модулей: формальных модулей Любина-Тейта и формальных модулей Хонды. Это открывает перспектиы по изучению символа Гильберта в описанных ситуациях, в частности, по построению явных формул типа Куммера.

В работе [25] были рассмотрены так называемые π_0-критические формальные модули – класс формальных модулей, несколько более широкому, чем формальные модули Хонды и построена их система образующих. Построение явных формул для этого класса формальных модулей также может представлять интерес для дальнейшего изучения.

Список литературы

[1] *Адамс Дж. Ф.* Стабильные гомотопии и обобщенные гомологии. – М.: Изд-во МЦНМО, 2013.

[2] *Бондарко М. В., Востоков С. В., Лоренц Ф.* Спаривание Гильберта для формальных групп над σ-кольцами.// Зап. научн. сем. ПОМИ. – 2004. – Т. 319. – С. 5-58

[3] *Бухштабер В. М.* Характер Чженя–Дольда в кобордизмах. I. – Матем. сб. – 1970 – Т. 83 (125), №4 (12) – С. 575-595

[4] *Востоков С. В.* Норменное спаривание в формальных модулях // Изв. АН СССР, Сер. матем. — 1979. — Т. 43, № 4. — С. 765-794.

[5] *Востоков С. В.* Символы на формальных модулях // Изв. АН СССР, Сер. матем. — 1981. — Т. 45, № 5. — С. 985-1014.

[6] *Востоков С. В.* Символ Гильберта для формальных групп Любина-Тэйта I. // Зап. научн. семин. ЛОМИ. — 1982. — Т. 114. — С. 77-95.

[7] *Востоков С. В., Фесенко И. Б.* Символ Гильберта для формальных групп Любина-Тэйта II. // Зап. научн. семин. ЛОМИ. — 1983. — Т. 132. — С. 85-96.

[8] *Востоков С. В., Демченко О. В.* Явная форма спаривания Гильберта для относительных формальных групп Любина–Тэйта // Зап. научн. сем. ПОМИ. — 1995. — Т. 227. — С. 41-44.

[9] *Востоков С. В., Бенуа Д. Г.* Норменное спаривание в формальных группах и представления Галуа // Алгебра и анализ. — 1990. — Т. 2, № 6. — С. 69—79.

[10] *Востоков С. В., Демченко О. В.* Явная формула спаривания Гильберта для формальных групп Хонды // Зап. научн. сем. ПОМИ. — 2000. — Т. 272. — С. 86-128.

[11] *Востоков С.В.* Канонический базис Гензеля–Шафаревича в полных дискретно-нормированных полях. // Зап. научн. сем. ПОМИ. – 2011. – Т. 394. – С. 174-193

[12] *Востоков С. В.* Явная форма закона взаимности // Изв. АН СССР, Сер. матем. — 1978. — Т. 42, № 6. — С. 1288-1321.

[13] *Востоков С.В., Востокова Р.П., Иконникова Е.В.* Канонический базис Гензеля - Шафаревича для формальных модулей Хонды. // Чебышевский сборник. – 2020 – Т. 21(1).– С. 368-373.

[14] *С. В. Востоков, И. Л. Климовицкий.* Примарные элементы в формальных модулях. // Математика и информатика, 2, К 75-летию со дня рождения Анатолия Алексеевича Карацубы, Совр. пробл. матем. – 2013.– Вып. 17. – С. 153-163.

[15] *О. В. Демченко.* Новое в отношениях формальных групп Любина-Тейта и формальных групп Хонды. // Алгебра и анализ – 1998. – Т.10, вып. 5. – С. 77-84.

[16] *Демченко О.В.* Формальные группы Хонды: арифметика группы точек. // Алгебра и Анализ – 2000 – Т. 12, вып.1, – С.132-149.

[17] *Жуков И. Б., Мадунц А. И.* Аддитивные и мультипликативные разложения в многомерных локальных полях. // Зап. научн. сем. ПОМИ. – 2000. – Т. 272. – С. 186-196

[18] *Иконникова Е. В., Шавердова Е. В.* Базис Шафаревича в многомерном локальном поле.// Записки научных семинаров ПОМИ – 2013 – Т. 430, стр. 115-133.

[19] *Иконникова Е. В.* Канонический базис Гензеля–Шафаревича в формальных модулях Любина–Тейта.// Записки научных семинаров ПОМИ – 2014 – Т. 430, стр. 186-201.

[20] *Колывагин В. А.* Формальные группы и символ норменного вычета // Изв. АН СССР, Сер. матем. — 1979. — Т. 43. — С. 1054-1120.

[21] *Мадунц А. И., Востокова Р. П.* Формальные модули для обобщенных групп Любина–Тейта // Зап. научн. сем. ПОМИ. — 2015. — Т. 435. — С. 95-112.

[22] *Новиков С. П.* Методы алгебраической топологии с точки зрения теории кобордизмов. // Изв. АН СССР, Сер. матем. – 1967 – Т. 31б вып. 4 – С. 855-951.

[23] *Фесенко И. Б.* Обобщенный символ Гильберта в 2-адическом случае // Вестник Ленингр. унив., матем., мех., астрон. — 1985. — Т. 18. — С. 88-91.

[24] *Шафаревич И. Р.* Общий закон взаимности // Матем. сб. — 1950. — Т. 26(68), No 1. — С. 113-146.

[25] *Afanaseva S.S., Ikonnikova E.V.* Arithmetic of π_0-critical module.// Lobachevskii Journal of Mathematics. – 2017. – Vol. 38 (1) – Pp. 131-136.

[26] *Artin E., Hasse H.* Die beiden Erganzungssatze zum Reziprozitatsgesetz der l^n-ten Potenzreste im Korper der l^n-ten Einheitswurzeln // Abh. Mathem. Seminar, Hamburg. — 1928. — Jg. 6. — S. 146-162.

[27] *Benois D.* Periodes p-adiques et lois de reciprocite explicites // J. reine und angew. Math. — 1997. — T. 493. — P. 115-151.

[28] *Bruckner H.* Explizites Reziprozitatsgesetz und Anwendungen // Vorlesungen aus dem Fachbereich Mathematik der Universitat Essen. — 1979.

[29] *Coleman R.* The dilogarithm and the norm residue symbol // Bull. Soc. Math. France. — 1981. — Vol. 109. — Pp. 373-402.

[30] *Destrempes F.* Explicit reciprocity laws for Lubin-Tate modules // J. reine und angew. Math. — 1995. — Vol. 463. — Pp. 27-47.

[31] *Fesenko I. B., Vostokov S. V.* Local Fields and Their Extensions. – 2nd Edition. – Providence, R. I. : Amer. Math. Soc., 2002. – 345 pp.

[32] *Hazewinkel M.* Formal Groups and Applications, Pure Appl. Math., 78, Academic Press, New York, 1978.

[33] *Hensel K.* Die multiplicative Dars ellung der algebraischen Zahlen fur den Bereich eines beliebigen Prin teil // Journ. fur die reine und a gew. Math. — 1916. — Jg. 136.

[34] *Iwasawa K.* On explicit formulas for the norm residue symbol // J. Math. Soc. Japan. — 1968. — Vol. 20. — Pp. 151-164.

[35] *Kummer E.* Uber die allgemeinen Reziprozitatsgesetze der Potenzreste // J. reine und angew. Math. — 1858. — Jg. 56. — S. 270–279.

[36] *Lubin J., Tate J.* Formal complex multiplication in local fields. // Annals of Mathematics, Second Series. – 1965. – Vol. 81, No. 2. – Pp. 380-387.

[37] *Milne, J.S.* Class Field Theory (v4.03) // Available at www.jmilne.org.

[38] *Quillen D.* On the formal group laws of unoriented and complex cobordism theory. // Bull. Amer. Math. Soc. – 1975 – 75 (6) – Pp. 1293-1298.

[39] *Sen S.* On explicit reciprocity laws I, II // J. reine und angew. Math. — 1981. — Vol. 323. — Pp. 69-87.

[40] *Shalit E. de* The explicit reciprocity law in local class field theory // Duke Math. J. — 1986. — Vol. 53. — Pp. 163-176.

[41] *Silverman J.H.* The Arithmetic of Eliptic Curves. Springer-Verlag New York, 2009.

[42] *Wiles A.* Higher reciprocity laws // Ann. Math. — 1978. — Vol. 107. — Pp. 235-254.