

На правах рукописи

Иконникова Елена Валерьевна

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

01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
кандидата физико-математических наук

Санкт-Петербург — 2022

Работа выполнена на кафедре высшей алгебры и теории чисел Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет».

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

Официальные оппоненты:

Кузьмин Леонид Викторович, доктор физико-математических наук, ведущий научный сотрудник Института информационных технологий Федерального государственного бюджетного учреждения «Национальный исследовательский центр “Курчатовский институт”».

Шабат Георгий Борисович, доктор физико-математических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный гуманитарный университет», профессор.

Ведущая организация: Федеральное государственное бюджетное учреждение науки Математический институт им. В. А. Стеклова Российской академии наук.

Защита состоится «____» _____ 2022 г. в ____ часов на заседании диссертационного совета Д 002.202.02 на базе ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук по адресу: 191023, Санкт-Петербург, наб. р. Фонтанки, д. 27.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук, <http://www.pdmi.ras.ru>.

Автореферат разослан «____» _____ 2022 г.

Ученый секретарь
диссертационного совета,
доктор физико-математических наук

Пономаренко И. Н.

Общая характеристика работы

Тема исследования и ее актуальность

Исследования формальных групп связаны со многими активно развивающимися разделами математики.

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). Построение формальных групп помогает в изучении эллиптических кривых.

Формальные группы также постоянно возникают в алгебраической топологии при изучении обобщенных теорий когомологий. 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.

Формальные группы также 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 Э. Куммером был доказан результат, который в современных терминах является явной формулой для символа Гильберта между определёнными элементами кругового расширения поля p -адических чисел. Явные формулы несколько иного типа впервые появляются у Артина и Хассе. 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. Иваса-

вой, в произвольном локальном поле — Ш. Сенем. Также изучался символ Гильберта, определённый относительно формальной группы. А. Уайлс получил формулу типа Артина-Хассе для формальных групп Любина-Тейта для поля деления изогении $[\pi^m]$, А. В. Колывагин — для полей, содержащих поле деления изогении $[\pi^m]$. В мультипликативном случае и в случае формальных групп Любина-Тейта продвижения были также получены Р. Коулманом. Выдвинутая им гипотеза о виде формулы в общем случае формальных групп Любина-Тейта была доказана А. Де Шалитом. Ф. Детрам обобщил формулы Сена на случай формальных групп Любина-Тейта, а Д. Бенуа — на случай p -делимых групп.

Изучение формул Куммеровского типа было продолжено в работе И. Р. Шафаревича "Общий закон взаимности". С помощью теоремы Гензеля 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 и Г. Брюкнером. 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 обычно системой образующих Гензеля или базисом Шафаревича (построение проводится по аналогии с методом, использованным Шафаревичем для построения базиса).
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 фор-

мального 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, относительных формальных групп Любина-Тейта, формальных групп Хонды, для обобщенных формальных групп Любина-Тейта 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 \mathfrak{R} 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

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

где ζ_{p^m} — первообразный корень 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, теоретическая и практическая значимость

Работа носит теоретический характер. Использовались методы алгебраической теории чисел и теории формальных групп. Результаты могут быть использованы в дальнейших теоретических исследованиях в области алгебраической теории чисел, в частности, для нахождения явных формул для символа Гильбера.

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 трех статьях в журналах, входящих в список рекомендованных ВАК для соискателей ученой степени кандидата и доктора наук. Все журналы входят в наукометрическую базу данных SCOPUS.

1. *Иконникова Е. В., Шавердова Е. В.* Базис Шафаревича в многомерном локальном поле. // Записки научных семинаров ПОМИ – 2013 – Т. 430, стр. 115–133.
2. *Иконникова Е. В.* Канонический базис Гензеля–Шафаревича в формальных модулях Любина–Тейта. // Записки научных семинаров ПОМИ – 2014 – Т. 430, стр. 186–201.
3. *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.

Статья 1 написана в соавторстве, диссертанту принадлежат леммы 2 и 3 из §1 и доказательство теоремы 5. Статья 3 написана в соавторстве, диссертанту принадлежит раздел 3.1.

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

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

где

- Ω — допустимое множество;
- $\theta_{\vec{r}} \in \mathfrak{R}$, \mathfrak{R} — система представителей базиса последнего поля вычетов как векторного пространства над \mathbb{F}_p ;
- $a_{\vec{r}} \in \mathbb{Z}_p$;
- \vec{t} — локальные параметры;
- $0 < \vec{r} < \frac{p\vec{v}(p)}{p-1}$;
- $p \nmid \vec{r}$,

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

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

где

- Ω — допустимое множество;
- $\theta_{\vec{r}} \in \mathfrak{R}$;

- $a_{\vec{r}}, b \in \mathbb{Z}_p$;
- \vec{t} — локальные параметры;
- $0 < \vec{r} < p\vec{v}(p)/(p-1)$;
- $p \nmid \vec{r}$;
- a — целый элемент подполя инерции, такой, что $\text{Tr}_{T/\mathbb{Q}_p} a \equiv 1 \pmod{p^m}$;
- $z(\vec{X}) \in R\{\{X_1\}\}\{\{X_2\}\}\dots\{\{X_{n-1}\}\}[[X_n]]$, причем $z(\vec{t}) = \zeta_{p^m}$, 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 .

Рассмотрим теперь построение системы образующих для формальных модулей Любина-Тейта. Опишем рассматриваемую ситуацию. Пусть 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 .

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

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

где ε_i пробегает все упомянутые множества, кроме элемента $\eta_* \in \text{Ker}\psi$, $a_i, a_* \in \mathcal{O}_0$. 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 \mathcal{O}_T . Т.е., любой элемент $\alpha \in F(M)$ представим в виде

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

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 униформизирующей 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

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

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

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

где $\theta \in \mathcal{R}$, $a \in \mathcal{O}_K^*$, $1 \leq \rho < fh$, $p \nmid i$, $0 < i_n \leq e_* = p^h e_n / (p^h - 1)$, \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 75 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.

Содержание работы

Канонический базис для многомерного локального поля

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

Будем придерживаться следующих обозначений:

- K - n -мерное локальное поле над совершенным полем k , $\text{char } K = 0$, $\text{char } k = p$, $\vec{t} = (t_1, t_2, \dots, t_n)$ - набор локальных параметров в K ;
- R - система представителей Тейхмюллера поля вычетов k ;
- $\vec{t}^{\vec{i}} := t_1^{i_1} t_2^{i_2} \dots t_n^{i_n}$;
- $\vec{t}^{\vec{i}_1} \equiv \vec{t}^{\vec{i}_2} \pmod{\vec{t}^{\vec{r}_1} +} \iff \exists \vec{r}_1 > \vec{r} : \vec{t}^{\vec{i}_1} \equiv \vec{t}^{\vec{i}_2} \pmod{\vec{t}^{\vec{r}_1}}$.

Определение 2. Набор индексов Ω будем называть допустимым, если для любых $i_n, \dots, i_{n-k+1} \in \mathbb{Z}$ найдется $i_{n-k} \in \mathbb{Z}$ такое, что для каждого $\vec{r} \in \Omega$ с $r_n = i_n, \dots, r_{n-k+1} = i_{n-k+1}$, выполняется неравенство $r_{n-k} \geq i_{n-k}$

Обозначим подполе инерции поля K через T , а его кольцо целых – через \mathfrak{o} . Возьмем кольцо $\mathfrak{o}\{\{X_1\}\}\{\{X_2\}\}\dots\{\{X_n\}\}$ и рассмотрим на нем оператор Фробениуса Δ , 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 $X_n\mathfrak{o}\{\{X_1\}\}\{\{X_2\}\}\dots\{\{X_{n-1}\}\}[[X_n]]$ определена экспонента Артина-Хассе

$$E(a) = \exp\left(\left(1 - \frac{\Delta}{p}\right)^{-1}(a)\right).$$

Теорема 6 (Жуков, Мадунц, 2000). Пусть для любого $\vec{r} > 0$ и любого $\theta \in R$ определен элемент $a_{\theta, \vec{r}} \in K$, $a_{\theta, \vec{r}} \equiv 1 + \theta \vec{t}^{\vec{r}} \pmod{\vec{t}^{\vec{r}+}}$. Тогда для того, чтобы любая главная единица $\alpha \in K$ была однозначно представима в виде

$$\alpha = \prod_{\vec{r} \in \Omega_\alpha} a_{\theta, \vec{r}},$$

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

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

Зафиксируем подмножество представителей Тейхмюллера \mathfrak{R} , такое что вычеты его элементов образуют базис k над \mathbb{F}_p . Определим для $\theta \in R$

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

В системе $a_{\theta, \vec{r}}$ можно заменить на p -е степени других элементов $a_{\theta, \vec{r}}$ для \vec{r} , меньших $p\vec{e}_1$ и кратных p , равных $p\vec{e}_1$ или больших $\vec{e}_1 + \vec{e}$, при условии, что соответствующие отображения коэффициентов индуцируют автоморфизмы поля вычетов k как линейного пространства над \mathbb{F}_p .

Мы можем применить к системе $\{a_{\theta, \vec{r}}\}$ теорему 6, так как при нашем выборе $a_{\theta, \vec{r}}$ ряды $\sum_{\vec{r} \in \Omega} (a_{\theta, \vec{r}} - 1)$ для любого допустимого Ω сходятся ввиду следующей леммы.

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

$$\sum_{\vec{r} \in \Omega} f_{\vec{r}}(X) \Big|_{X=\vec{t}^{\vec{r}}}.$$

Канонический базис для формальных модулей Любина-Тейта

В данном разделе мы начинаем с того, что строим системы представителей “ступеней” формального модуля вида $F(M^s) \setminus F(M^{s+1})$. Далее из их числа выбираем систему образующих для всего формального модуля.

Канонический базис для формальных модулей Хонды

Предложение 1. Пусть F – p -типическая формальная группа над \mathcal{O}_K типа $u = \pi - a_h B \Delta^h$, $B \in 1 + \mathcal{D}\Delta$, и пусть $\lambda_1(X) = (\pi u^{-1}(\Delta))(X)$, 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 $[\pi a_h^{-1}]_{F, F_1} \in \text{Hom}_{\mathcal{O}_K}(F, F_1)$, такой что

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

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

Таким образом мы получаем следующую последовательность формаль-

ных групп и гомоморфизмов f_i :

$$F \rightarrow F_1 \rightarrow \dots \rightarrow F_N.$$

Предложение 2.

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

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

Определим многочлены Эньяра:

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

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

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 7. Элементы

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

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

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

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

Из этого результата уже легко получить систему образующих для $F(\mathfrak{M})$.