Записки научных
семинаров ПОМИ
Том 430, 2014 г.

Е. В. Иконникова

КАНОНИЧЕСКИЙ БАЗИС ГЕНЗЕЛЯ–ШАФАРЕВИЧА В ФОРМАЛЬНЫХ МОДУЛЯХ ЛЮБИНА-ТЕЙТА

§1. Введение

В арифметике формальных модулей, построенных на максимальных идеалах полных дискретно нормированных полей с помощью формальных групповых законов, существенную роль играют образующие этих модулей.

Уже создатель теории локальных полей Курт Гензель дал полную систему образующих группы главных единиц полного дискретно нормированного поля характеристики 0 с совершенным полем вычетов ненулевой характеристики. И. Р. Шафаревич в 1950 году определил базис в группе главных единиц поля, содержащего все корни степени p^n из 1, определяющий разложение однозначно с точностью до p^n-ых степеней. Элементы этого базиса строились с использованием функции Артина–Хассе.

С. В. Востоков в статье [1] построил базис $\mathbb{Z}_p$-модуля главных единиц для полного дискретно нормированного поля с произвольным полем вычетов.

Для многомерных локальных полей вопрос построения базиса рассматривался в [10].

В данной работе эти результаты переносятся на случай формальных модулей Любина–Тейта. Сначала рассматривается случай классического локального поля (т.е., полного дискретно нормированного поля с конечным полем вычетов), далее следует обобщение на случай произвольного поля вычетов.

Пусть K_0 – локальное поле, $\mathrm{char}\ K_0 = 0$, 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

Ключевые слова: базис Гензеля–Шафаревича, формальные модули.
Работа поддержана грантом РФФИ 6.15.527.2014. Автор также благодарит Санкт-Петербургский Государственный Университет за финансовую поддержку в рамках НИР.

Любина–Тейта над O_0 (кольцом целых K_0), $F(M)$ – формальный O_0-модуль, натянутый на максимальный идеал кольца O_K.

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

Теорема 1. *Пусть k совершенно. Тогда множество*

$$E(\Theta\pi^s) \cup E(H\pi^{e_m}) \cup E(\Xi\pi^{e_1}),$$

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

$$\beta = \sum\nolimits_F [a_i]\varepsilon_i,$$

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

Теорема 2. *Пусть k несовершенно. Тогда множество*

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

где $s \in S_e$, является системой образующих модуля $F(M)$ над O_T. Т.е., любой элемент $\beta \in F(M)$ 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.

§2. 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;
- $e_i = \frac{e}{(q-1)q^{i-1}}, i \geqslant 1$;
- N – подполе инерции в K/K_0;
- $\widetilde{N}$ – пополнение максимального неразветвленного расширения поля N;
- 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 $g(X)=\sum\limits_{i=0}^{\infty} a_i X^i$

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

- $S_e=\{s\in\mathbb{Z}:1\leqslant s<qe_1,\quad q\nmid s\}$.

§3. Предварительные сведения

3.1. Формальные модули.

Определение 1. 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

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

Пусть $F(M)$ – формальный O_0 -модуль, натянутый на идеал M, т.е.,

$$\alpha,\beta\in F(M)\mapsto \alpha+_F\beta=F(\alpha,\beta)\in F(M),$$
$$a\in O_0,\alpha\in F(M)\mapsto [a]_F\alpha\in F(M).$$

Пусть

$$\mathcal{F}_{\pi_0}=\{g(X)\in O_0[[X]]\mid g(X)\equiv \pi_0X \bmod \deg 2 \text{ и } g(X)\equiv X^q \bmod \pi_0\}.$$

Тогда над кольцом O_0 существует единственная формальная группа F высоты 1, такая, что $g(X)$ – ее эндоморфизм. Данный эндоморфизм в дальнейшем обозначается как $[\pi_0]$. Доказано (см. [6]), 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

$$\lambda(X)=X+c_1X+c_2X^2+\dots .$$

Пусть F_q – изоморфная F O_0-типическая формальная группа и $\lambda_q(X)$ – логарифм F_q. Вообще говоря, F_q определена неоднозначно. Например ([5]), можно выбрать в качестве $\lambda_q(X)$ ряд

$$\lambda_q(X)=X+c_qX^q+c_{q^2}X^{q^2}+\dots .$$

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

Определение 2. Для каждого элемента $\alpha \in \widetilde{N}$ определим ряд, который назовем функцией Артина-Хассе:

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

В работе [3] доказано следующее утверждение.

Предложение 1. *Для любых $\xi \in F(M), \alpha \in O_{\widetilde{N}}$ 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*

$$E_F((\alpha+\beta)\xi) = E_F(\alpha\xi) +_F E_F(\beta\xi), \quad \alpha, \beta \in O_{\widetilde{N}},$$
$$E_F(a\alpha\xi) = [a]_F(E_F(\alpha\xi)), \quad \alpha \in O_{\widetilde{N}}, a \in O_0,$$
$$E_F(\alpha\xi) \equiv \alpha\xi \bmod (\alpha\xi)^2.$$

3.2. Примарные элементы в формальном модуле. Предположим, что K содержит ядро изогении $[\pi_0^n]$.

Определение 3. 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 [2] (§3.1, стр.775) была определена функция

$$H_\zeta(\alpha) = E_F(\pi_0^n A\xi).$$

Предложение 2. ([3]) *$H_\zeta(\alpha)$ – 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.*

3.3. Действие изогении $[\pi_0]$.

Предложение 3. ([2], §1.2, стр. 774) *Для $\alpha \in M$*

$$[\pi_0](\alpha) \equiv \alpha^q \bmod (\pi^{qi+1}) \text{ при } v(\alpha) = i < e_1,$$
$$[\pi_0](\alpha) \equiv \pi_0\alpha \bmod (\pi^{i+e_1+1}) \text{ при } v(\alpha) = i > e_1,$$
$$[\pi_0](\alpha) \equiv \pi_0\alpha + \alpha^q \bmod (\pi^{qe_1+1}) \text{ при } v(\alpha) = e_1.$$

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

Замечание. Более того, второе сравнение можно заменить на

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

где $\theta_0 \in O_N$ определяется из равенства

$$\pi_0 \equiv -\theta_0 \pi^e \bmod \pi^{e+1}.$$

§4. Случай конечного поля вычетов

4.1. 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 [2] (§4.1, стр. 781) был дан критерий для системы образующих $F(M)$:

Лемма 1. *Пусть для каждого i с условием: $i \not\equiv 0 \bmod q$, $1 \leqslant i < qe_1$, 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 $\epsilon_i(\theta) \equiv \theta\pi^i \bmod \pi^{i+1}$. Тогда любой элемент $\beta \in F(M)$ можно представить в виде*

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

Теорема 3. *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*

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

Доказательство. Существование такого разложения следует из леммы 1: для каждого $i \in S_e$, и для каждого $\theta \in \mathfrak{R}$ 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:

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

Пусть i_0 – минимальное i, такое, что $a_i \neq 0$. Тогда $a_{i_0}\pi^{i_0} \equiv 0 \bmod \pi^{i_0+1}$. Противоречие. $\square$

4.2. 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 $\underline{\alpha}(\pi) = \alpha$.

Обозначим $s_j(X) := [\pi_0^j](\underline{\zeta}); s := s_n, u = \frac{s}{s_{n-1}}$.

В работе [2] (§1.4, стр. 773) проверено, что

$$s \equiv s_{n-1}^{\triangle} \bmod \pi_0^n.$$

Определим на $XO_N[[X]]$ функцию

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

Предложение 4. ([2], стр. 780) *Для любого* $a \in O_N$

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

является π_0^n*-примарным в* $F(M)$.

Теорема 4. ([2], §4.3, стр. 783) *Всякий элемент* $\beta \in F(M)$ *можно представить в виде*

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

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

§5. Случай совершенного поля вычетов

Пусть теперь k – совершенное поле, не обязательно являющееся конечным. Выберем в k какой-нибудь базис $\overline{\Theta} = \{\overline{\theta}_i, i \in I\}$ над k_0, и пусть $\Theta = \{\theta_i, i \in I\}$ – множество представителей этого базиса в O_K.

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

$$e_1 \leqslant q^{\mu_s} s < qe_1.$$

5.1. Случай $e \not\equiv 0 \bmod (q-1)$**.**

Предложение 5. *Пусть* $s \in S_e$.

Базисом ступени $F(M^{q^{\mu} s}) \setminus F(M^{q^{\mu} s+1}), 0 \leqslant \mu \leqslant \mu_s$, *являются множества*
$$[\pi_0^{q^{\mu}}]E(\Theta\pi^s) \equiv E(\Theta^{q^{\mu}}\pi^{q^{\mu} s}) \bmod F(M^{q^{\mu} s+1}).$$

Базисом ступени $F(M^{q^{\mu_s} s+\mu e}) \setminus F(M^{q^{\mu_s} s+\mu e+1}), \mu > 0$, *являются множества*
$$[\pi_0^{\mu+\mu_s}]E(\Theta\pi^s) \equiv E(\theta_0^{\mu}\Theta^{q^{\mu_s}}\pi^{q^{\mu_s} s+e\mu}) \bmod F(M^{q^{\mu_s} s+\mu e+1}).$$

Доказательство. Ясно из предложения 3. □

5.2. Случай $e \equiv 0 \bmod (q-1)$**.** Пусть $m-1$ – максимальная степень q, на которую делится e:
$$e_m = \frac{e}{(q-1)q^{m-1}} \in \mathbb{Z}, \quad e_{m+1} \notin \mathbb{Z}.$$

Определим гомоморфизм
$$\psi : k \to k,$$
$$\overline{\varepsilon} \mapsto \overline{\varepsilon}^{q^m} - \overline{\theta_0}\overline{\varepsilon}^{q^{m-1}}.$$

5.2.1. *Случай* $\operatorname{Ker}\psi = \{0\}$. Определим
$$\beta_i = \theta_i^{q^m} - \theta_0\theta_i^{q^{m-1}}, \quad i \in I,$$
и обозначим
$$\mathfrak{B} = \{\beta_i, i \in I\}.$$

Лемма 2. *Если* $\operatorname{Ker}\psi = \{0\}$, *то* $\overline{\mathfrak{B}} = \{\overline{\beta}_i, i \in I\}$ *– базис* k *над* k_0.

Доказательство. Пусть
$$\sum_{j=1}^{l} a_j\overline{\beta}_{i_j} = 0,$$
тогда
$$\sum_{j=1}^{l} \Big((a_j\overline{\theta}_{i_j})^{q^m} - \theta_0(a_j\overline{\theta}_{i_j})^{q^{m-1}} \Big) = 0.$$

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

Предложение 6. *Пусть* $e \equiv 0 \bmod (q-1)$, $\operatorname{Ker}\psi = \{0\}$ *и* $s \in S_e$.

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

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

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

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

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

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

Доказательство. Используем предложение 3 (для ступени qe_1) и лемму 2. □

5.2.2. *Случай* $\operatorname{Ker}\psi \neq \{0\}$. В этом случае поле K содержит все корни изогении $[\pi_0^n]$. Заметим, что $n \leqslant m$. Пусть ζ_n – первообразный корень.

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

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

Пусть $H_0 = \{\eta_i, i \in I_0\}$ – система представителей в O_K базиса $k \setminus \operatorname{Ker}\psi$, т.е., дополнение $\overline{\eta}_*$ до базиса поля k над k_0. Получаем $\overline{H} = \overline{H_0} \cup \{\overline{\eta}_*\}$ – базис k.

Можно также заметить, что

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

– линейно независимая система в k (т.к., 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:

$$\overline{\Theta} = \{\overline{\theta}_i, i \in I\}, \quad \overline{H} = \{\overline{\eta_*}, \overline{\eta}_i, i \in I_0\},$$

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

Отсюда получаем

Предложение 7. *Пусть* $s \in S_e, s \neq e_m$. *Тогда базисами ступеней*

$$F(M^{q^\mu s}) \setminus F(M^{q^\mu s+1}), \quad 0 \leqslant \mu \leqslant \mu_s$$

$$\text{и} \;\; F(M^{q^{\mu_s} s+\mu e}) \setminus F(M^{q^{\mu_s} s+\mu e+1}), \quad \mu > 0,$$

будут соответствующие системы из предложения 6.

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

$$F(M^{q^\mu e_m}) \setminus F(M^{q^\mu e_{m+1}+1}), \quad 0 \leqslant \mu \leqslant m,$$

будет система

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

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

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

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

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

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

Теорема 5. *В случае отсутствия нетривиальных корней изогении* π_0^n *множество*

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

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:*

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

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

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

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

Доказательство. $\{\varepsilon_{i,s} | i \in I, s \in S_e\}$ является системой образующих для $F(M)$ по лемме 1.

Докажем единственность разложения. Пусть

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

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

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

$$0 = \sum_{i,s} [a_{i,s}]\varepsilon_{i,s} = \sum_{s \in S_e} \sum_{c \geqslant 1} \varepsilon_s^{(c)},$$

$$\text{где } \varepsilon_s^{(c)} = \sum_{i \in I_s^{(c)}} [a_{i,s}]\varepsilon_{i,s}.$$

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

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

– противоречие. □

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

Теорема 6. *Объединение множеств*

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

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

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

$$\alpha = \sum [a_i]\varepsilon_i,$$

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 следующей леммы.

Лемма 3. *$\alpha \in K$ тогда и только тогда принадлежит (π_0^n), когда все коэффициенты в разложении $\alpha = \sum [a_i]\varepsilon_i$ делятся на π_0^n.*

Доказательство. Достаточность очевидна. Докажем необходимость. Пусть v_0 – нормирование на K_0 и $\nu = \min\{v_0(a_i)\}$. 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 $\omega \equiv \gamma\pi^{i_0} \bmod \pi^{qe_1+1}$, 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, $\omega \not\equiv 0 \bmod \pi^{qe_1}$ и расширение $K(\frac{1}{[\pi_0^{\nu+1}]}\alpha)/K$ будет нетривиальным, что противоречит условию $\alpha \in (\pi_0^n)$. □

□

§6. Случай несовершенного поля вычетов

Определение 4. 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 $l \geqslant 1$.

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

Для мультииндекса (k):

(1) $l_1 \leqslant (k) \leqslant l_2$, если $l_1 \leqslant k_i \leqslant l_2$ для всех i,

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

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

Пусть A – система представителей элементов из k в O.

Лемма 4.
$$A = A^{p^l} + A^{p^l}[\widetilde{T}_l] = \sum_{0 \leqslant i \leqslant n} A^{p^l}[T_{l-i}^{p^i}].$$

Доказательство. Индукцией по l из определения p-базиса получаем
$$k = k^{p^l} + k^{p^l}[\overline{\widetilde{T}_l}] = \bigoplus_{0 \leqslant i \leqslant n} k^{p^l}[\overline{T}_{l-i}^{p^i}].$$ □

Следствие.
$$A = A^{q^l} + A^{q^l}[\widetilde{T}_{lf}] = \sum_{0 \leqslant i \leqslant lf} A^{q^f}[T_{lf-i}^{p^i}].$$

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

6.1. Случай $e \neq 0 \bmod (q-1)$**.**

Лемма 5. *Пусть* $s \in S_e$*. Полной системой представителей ступени* $F(M^s) \setminus F(M^{s+1})$ *является множество*

$$E(A\pi^s).$$

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

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

Доказательство. Ясно из леммы 3. □

Лемма 6. *Пусть* $s \in S_e$*. Полной системой представителей ступени*

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

является множество

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

Полной системой представителей ступени

$$F(M^{q^\mu s} + \mu e) \setminus F(M^{q^\mu s+\mu e+1})$$

является множество

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

Доказательство. Применяем лемму 5 и следствие из леммы 4. □

6.2. Случай $e \equiv 0 \bmod (q-1)$**.** Аналогично случаю совершенного поля вычетов определяем гомоморфизм $\psi : k \to k$.

6.2.1. $\operatorname{Ker}\psi = \{0\}$.

Лемма 7. *Полной системой представителей ступени*

$$F(M^{q^\mu s}) \setminus F(M^{q^\mu s+1}), s \in S_e, 0 \leqslant \mu \leqslant \mu_s,$$

является множество

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

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
$$E\Big(\Big(\theta_0^\mu\sum_{i=0}^{\mu_s}A^{q^{\mu_s}}[T_i^{p^{\mu_s f-i}}]\Big)\pi^{q^{\mu_s}s+\mu e}\Big).$$
Полной системой представителей ступени
$$F(M^{qe_1+\mu e})\setminus F(M^{qe_1+\mu e+1}),\quad s\in S_e,\quad s\neq e_m,$$
является множество
$$E(\theta_0^\mu\mathfrak{B}\pi^{qe_1+\mu e}),$$
где $\mathfrak{B}=\sum\limits_{i=0}^{m-1}\mathfrak{B}_i$,
$$\begin{aligned}\mathfrak{B}_i&=A^{q^m}\Big[T^{p^{mf-i}}\Big]-\theta_0A^{q^{m-1}}\Big[T^{p^{mf-i-1}}\Big]\\&=\Big\{a^{q^m}\Big[T^{p^{mf-i}}\Big]-\theta_0a^{q^{m-1}}\Big[T^{p^{mf-i-1}}\Big]\,:\,a\in A\Big\}.\end{aligned}$$

Доказательство. Первые два утверждения получаем по аналогии с леммой 6. Последнее утверждение получаем, воспользовавшись леммой 1 и тем, что $A=\mathfrak{B}\bmod M$, а значит, $\mathfrak{B}$ – полная система представителей k в O. $\square$

6.2.2. $\operatorname{Ker}\psi\neq\{0\}$. Пусть $\operatorname{Ker}\psi$ 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:
$$\Big(\overline{A}_0^{q^m}-\overline{\theta}_0\overline{A}_0^{q^{m-1}}\Big)+\mathfrak{B}.$$
Обозначим $\Gamma=\{\gamma\in O\mid\overline{\gamma}\in k\setminus\operatorname{Im}\psi\}$.

Лемма 8. *Полной системой представителей ступени*
$$F(M^{q^\mu s})\setminus F(M^{q^\mu s+1}),\ s\in S_e,\ 0\leqslant\mu\leqslant\mu_s,$$
является множество
$$E\Big(\Big(\sum_{i=0}^{\mu}A^{q^\mu}[T_i^{q^\mu f-i}]\Big)\pi^{q^\mu s}\Big).$$
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

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

Полной системой представителей ступени

$$F(M^{qe_1+\mu e}) \setminus F(M^{qe_1+\mu e+1}))$$

является множество

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

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

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

Теорема 7. *Множество*

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

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

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

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

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

конечно для любого $c \geqslant 0$ *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

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

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

$$\sum_{(s,\mu)} \Big(\sum_{c \geqslant 1} \alpha_{s,\mu,c}\Big) = 0,$$

то либо все $\beta_{s,\mu,c}$ 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. □

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

Теорема 8. *Множество*

$$E(A^{q^\mu}[T_{q^\mu}]\pi^{q^\mu s}) \cup E(\Gamma\pi^{q e_1}),$$

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*

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

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

Доказательство. Доказательство единственности разложения повторяет случай совершенного поля. □

Литература

1. С. В. Востоков, *Канонический базис Гензеля–Шафаревича в полных дискретно-нормированных полях.* — Зап. научн. семин. ПОМИ **394** (2011), 174–193
2. С. В. Востоков, *Норменное спаривание в формальных модулях.* — Известия АН СССР. Сер.матем. **43** (1979), No. 4, 706–794.
3. С. В. Востоков, И. Л. Климовицкий, *Примарные элементы в формальных модулях.* — Совр. пробл. матем. **17** (2013), 153–163.
4. I. B. Fesenko, S. V. Vostokov, *Local fields and their extensions.* AMS Bookstore, 2002.
5. M. Hazewinkel, *Formal Groups and Applications.* Pure Appl. Math. **78** 1978.
6. J. Lubin, J. Tate, *Formal complex multiplication in local fields.* — Ann. Math. Second Series **81** (1965) 380–387,
7. Д. Г. Бенуа, С. В. Востоков, *Норменное спаривание в формальных группах и представления Галуа.* — Алгебра и Анализ **2**, No. 6 (1990), 69–97.
8. О. В. Демченко, *Формальные группы Хонды: арифметика группы точек.* — Алгебра и Анализ **12**, No. 1 (2000), 132–149.
9. H. Hasse, *Die Gruppe der* $\mathfrak{p}^n$*-primären Zahlen für einem Primteiler* $\mathfrak{p}^n$ *von* p. — J. Reine Angew. Math. **176** (1936), 174–183.
10. Е. В. Иконникова, Е. В. Шавердова, *Базис Шафаревича в многомерном локальном поле.* — Зап. научн. семин. ПОМИ **413** (2013), 115–133.

Ikonnikova E. V. Hensel-Shafarevich canonical basis in Lubin-Tate formal modules.

In this paper we present a generalization of the Hensel–Shafarevich basis for Lubin–Tate formal modules over a local field. These formal modules are constructed on the maximal ideal of some extension of this field. We

study both the case when the extension has perfect residue field and the case with an imperfect residue field.

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия
E-mail: elena.mm112@gmail.com

Поступило 24 сентября 2014 г.