О согласованных наборах униформизующих элементов в башнях абелевых расширений числовых локальных полей*

Л. В. КУЗЬМИН
Российский научный центр «Курчатовский институт»
e-mail: helltiapa@mail.ru

УДК 519.4

Ключевые слова: формальные группы Любина—Тэйта, башня Любина—Тэйта, точки конечного порядка.

Аннотация

Для числового локального поля K с кольцом целых $\mathcal{O}_K$, полем вычетов $\mathbb{F}_q$ и униформизующим элементом π рассматривается башня Любина—Тэйта $K_\pi = \bigcup\limits_{n\geqslant 0} K_n$, где $K_n = K(\pi_n)$, $f(\pi_0) = 0$ и $f(\pi_{n+1}) = \pi_n$ при $n \geqslant 0$ и $f(X)$ задаёт эндоморфизм $[\pi]$ в группе Любина—Тэйта. Доказано, что при $q \neq 2$ для любого формального степенного ряда $g(X) \in \mathcal{O}_K[[X]]$ справедливо соотношение $\sum\limits_{n=0}^{\infty} \mathrm{Sp}_{K_n/K} g(\pi_n) = -g(0)$. Похожее соотношение справедливо и в случае $q = 2$.

Abstract

L. V. Kuz'min, On coherent families of uniformizing elements in some towers of Abelian extensions of local number fields, Fundamentalnaya i prikladnaya matematika, vol. 14 (2008), no. 8, pp. 151—157.

For a local number field K with the ring of integers $\mathcal{O}_K$, the residue field $\mathbb{F}_q$, and uniformizing π, we consider the Lubin—Tate tower $K_\pi = \bigcap\limits_{n\geqslant 0} K_n$, where $K_n = K(\pi_n)$, $f(\pi_0) = 0$, and $f(\pi_{n+1}) = \pi_n$. Here $f(X)$ defines the endomorphism $[\pi]$ of the Lubin—Tate group. If $q \neq 2$, then for any formal power series $g(X) \in \mathcal{O}_K[[X]]$ the following equality holds: $\sum\limits_{n=0}^{\infty} \mathrm{Sp}_{K_n/K} g(\pi_n) = -g(0)$. One has a similar equality in the case $q = 2$.

Введение

Для фиксированного простого ℓ пусть K — конечное расширение поля рациональных ℓ-адических чисел $\mathbb{Q}_\ell$ и $\{K_n\}_{n\geqslant 0}$ — некоторая возрастающая последовательность абелевых чисто разветвлённых расширений поля K. Существует ряд задач, для решения которых нужно найти набор элементов $\pi_n \in K_n$, где

*Работа выполнена при поддержке РФФИ (проект № 08-01-00777) и гранта «Научные школы».

Фундаментальная и прикладная математика, 2008, том 14, № 8, с. 151—157.

π_n — униформизующий элемент поля K_n, причём эти элементы должны быть определённым образом согласованы. Такие наборы строились и использовались в [2—4] для решения различных задач, связанных со свойствами ℓ-адического логарифма. Например, важным является случай, когда $K_n = \mathbb{Q}_\ell(\zeta_n)$, где ζ_n — первообразный корень из единицы степени ℓ^{n+1} при $\ell \neq 2$ (степени ℓ^{n+2} при $\ell = 2$). В этом случае поле $K_\infty = \bigcup_n K_n$ является круговым $\mathbb{Z}_\ell$-расширением поля K_0.

В разделе 1 мы напоминаем основные результаты, относящиеся к этому случаю. Наиболее важным для приложений является тот факт, что для любого формального степенного ряда $f(X) \in \mathbb{Z}_\ell[[X]]$ при $\ell \neq 2$ справедлива формула

$$f(0) + \sum_{n=0}^{\infty} \mathrm{Sp}_{K_n/\mathbb{Q}_\ell} f(\pi_n) = 0, \tag{1}$$

где Sp — оператор следа, а при $\ell = 2$ справедлива формула

$$f(0) + f(2) + \sum_{n=0}^{\infty} \mathrm{Sp}_{K_n/\mathbb{Q}_\ell} f(\pi_n) = 0. \tag{2}$$

Справедливость этих формул легко следует из того факта, что $\sum_{\zeta^{\ell^m}=1} \zeta = 0$, где ζ пробегает все корни из единицы степени ℓ^m для некоторого $m > 0$. Кажется, что соотношения (1) и (2) характерны только для круговых полей, но это не так.

В разделе 2 мы в качестве последовательности $\{K_n\}$ рассматриваем башню абелевых расширений произвольного локального числового поля K, полученных с помощью теории Любина—Тэйта. Таким образом, последовательность $\{K_n\}$ образует башню абелевых расширений поля K и $\bigcup_n K_n = K_\pi$, где K_π — максимальное чисто разветвлённое абелево расширение поля K, определённое, например, в [1]. В этом случае также можно определить набор согласованных униформизующих элементов $\pi_n \in K_n$, и достаточно неожиданным обстоятельством является то, что в этом случае также справедлив аналог соотношений (1) и (2) (теорема 2.1). Эта теорема составляет основной результат работы. По-видимому, она означает, что такие результаты об ℓ-адических логарифмах, как, например, основная теорема работы [2], обобщаются также на случай логарифмов формальных групп Любина—Тэйта. Это обобщение мы надеемся рассмотреть в одной из последующих работ.

1. Круговые $\mathbb{Z}_\ell$-расширения

Пусть $K = \mathbb{Q}_\ell$ и $K_n = K(\zeta_n)$, $n \geqslant 0$, где ζ_n — первообразный корень из единицы степени ℓ^{n+1} (степени ℓ^{n+2} при $\ell = 2$). Таким образом, поле $K_\infty = \bigcup_n K_n$ является круговым $\mathbb{Z}_\ell$-расширением поля K_0. Мы предполагаем, что корни ζ_n согласованы условием $\zeta_{n+1}^\ell = \zeta_n$ для всех n. Следующее утверждение проверяется непосредственно.

Предложение 1.1. *Положим* $\pi_n = 1 - \zeta_n$. *Тогда* π_n *является униформизующим элементом поля* K_n *при* $n \geqslant 0$, *элементы* π_n *согласованы относительно нормы, т. е.* $N_{K_{n+1}/K_n}(\pi_{n+1}) = \pi_n$ *для всех* $n \geqslant 0$, *и* $\pi_{n+1}^{\ell} \equiv \pi_n \pmod{\ell\pi_{n+1}}$.

Пусть $\mathbb{Q}_{\ell,\infty}$ — круговое $\mathbb{Z}_\ell$-расширение поля $\mathbb{Q}_\ell$ и $\mathbb{Q}_{\ell,n}$ — единственное промежуточное подполе расширения $\mathbb{Q}_{\ell,\infty}/\mathbb{Q}_\ell$ степени ℓ^n над $\mathbb{Q}_\ell$. Положим

$$\Delta = \mathrm{Gal}(\mathbb{Q}_{\ell,\infty}(\zeta_0)/\mathbb{Q}_{\ell,\infty}) \cong \mathrm{Gal}(\mathbb{Q}_\ell(\zeta_n)/\mathbb{Q}_{\ell,n}).$$

Таким образом, Δ — циклическая группа порядка $\ell - 1$ при $\ell \neq 2$ (порядка 2 при $\ell = 2$). Следующее утверждение также проверяется непосредственно.

Предложение 1.2. *Для любого* $n \geqslant 0$ *элемент* $\rho_n = N_\Delta(\pi_n)$, *где* N_Δ — *норма относительно* Δ, *является униформизующим элементом поля* $\mathbb{Q}_{\ell,n}$, *причём элементы* ρ_n *согласованы относительно нормы и удовлетворяют сравнениям* $\rho_{n+1}^{\ell} \equiv \rho_n \pmod{\ell\rho_{n+1}}$.

Пусть теперь K — произвольное конечное расширение поля $\mathbb{Q}_\ell$, $K_\infty = K\cdot\mathbb{Q}_{\ell,\infty}$, $K_n = K\cdot\mathbb{Q}_{n,\infty}$, H — максимальное неразветвлённое подполе поля K_∞ и $\mathcal{O}_H$ — кольцо целых поля H. Пусть $R = \mathcal{O}_H[[T]]$ — кольцо формальных степенных рядов одной переменной с коэффициентами из $\mathcal{O}_H$. Определим действие автоморфизма Фробениуса φ поля H на R по правилу

$$\varphi\Big(\sum_{i=0}^{\infty} b_i T^i\Big) = \sum_{i=0}^{\infty} \varphi(b_i) T^i.$$

Для многочлена $F(X) = F(X,T) \in R[X]$ и целого n мы обозначаем через $F^{(n)}(X,T)$ многочлен, полученный из $F(X,T)$ действием φ^n на коэффициенты.

Теорема 1.1. *Пусть* $f(T) \in R$ — *произвольный формальный степенной ряд от* T *с коэффициентами в* $\mathcal{O}_H$. *Пусть* $K_n = H(\zeta_n)$ *и* $\pi_n = 1 - \zeta_n$ — *униформизующий элемент в* K_n. *Тогда при* $\ell \neq 2$ *справедливо соотношение* (1), *а при* $\ell = 2$ *справедливо соотношение* (2).

Доказательство. Достаточно доказать теорему для случая, когда $f(T)$ — многочлен. Но любой многочлен от T является многочленом от $X = 1 - T$, поэтому достаточно проверить теорему для случая $f(T) = (1-T)^k$, где k — любое целое неотрицательное число. В этом случае $f(\pi_n) = \zeta_n^k$, и левая часть соотношений (1) и (2) превращается в $\sum\limits_{\zeta} \zeta^k$, где ζ пробегает все корни из единицы порядка ℓ^m. Очевидно, что при фиксированном k эта сумма равна 0 для всех достаточно больших m. Теорема доказана. □

2. Расширения Любина—Тэйта

Пусть K — произвольное конечное расширение поля $\mathbb{Q}_\ell$, $\mathcal{O}_K$ — кольцо целых поля K и π — фиксированный униформизующий элемент поля K. Пусть

q — число элементов поля вычетов поля K. Зафиксируем некоторый многочлен Любина—Тэйта

$$f(X) = X^q + a_{q-1}X^{q-1} + \ldots + a_1 X, \tag{3}$$

где $a_i \in \pi\mathcal{O}_K$ и $a_1 = \pi$. Как хорошо известно [1, гл. VI, § 3], максимальное абелево расширение поля K можно получить следующей конструкцией. Пусть π_0 — корень неприводимого многочлена $X^{-1}f(X)$ степени $q-1$. Далее, если π_n уже определён, мы определяем π_{n+1} как корень неприводимого многочлена $f(X) - \pi_n$. Отметим, что все рассматриваемые многочлены неприводимы в силу критерия Эйзенштейна. Положим $K_n = K(\pi_n)$ для $n \geqslant 0$ и $K_\infty = K_\pi = \bigcup\limits_n K_n$. Тогда согласно теории Любина—Тэйта K_0 является абелевым над K чисто разветвлённым ручным расширением поля K степени $q-1$ (в частности, $K_0 = K$ при $q = 2$), и для любого $n \geqslant 0$ поле K_{n+1} является абелевым чисто разветвлённым расширением K_n степени q. Поле K_π является максимальным чисто разветвлённым абелевым расширением поля K, и $K^{\mathrm{ab}} = K^{\mathrm{un}} \cdot K_\pi$, где K^{ab} — максимальное абелево расширение поля K и K^{un} — максимальное неразветвленное расширение поля K. Ситуация, рассмотренная в разделе 1, соответствует случаю, когда $K = \mathbb{Q}_\ell$, $\pi = \ell$ и $f(X) = \ell X + \binom{\ell}{2}X^2 + \ldots + \ell X^{\ell-1} + X^\ell$. Оказывается, что в случае произвольной башни расширений Любина—Тэйта справедлив точный аналог теоремы 1.1.

Теорема 2.1. *Пусть K — произвольное конечное расширение поля $\mathbb{Q}_\ell$ с кольцом целых $\mathcal{O}_K$, полем вычетов $\mathbb{F}_q$ из q элементов и фиксированным униформизующим элементом π. Пусть $f(X)$ — многочлен Любина—Тэйта вида* (3) *и $K \subset K_0 \subset K_1 \subset \ldots \subset K_n \subset \ldots$ — определённая выше башня абелевых расширений поля K, причём для любого $n \geqslant 0$ в поле K_n зафиксирован определённый выше униформизующий элемент π_n. Пусть $g(T) \in \mathcal{O}_K[[T]]$. При $q \neq 2$ положим*

$$\widetilde{\mathrm{Sp}}(g) = g(0) + \sum_{n=0}^{\infty} \mathrm{Sp}_{k_n/K}\, g(\pi_n).$$

При $q = 2$ положим

$$\widetilde{\mathrm{Sp}}(g) = g(0) + g(\pi) + \sum_{n=1}^{\infty} \mathrm{Sp}_{K_n/K}\, g(\pi_n).$$

Тогда $\widetilde{\mathrm{Sp}}(g) = 0$.

Доказательство. Достаточно доказать теорему для случая $g(X) = X^k$, где k — произвольное целое неотрицательное число. Рассмотрим сначала случай $k = 0$, т. е. $g(X) = 1$. В этом случае при $q > 2$ мы имеем

$$\widetilde{\mathrm{Sp}}(1) = 1 + \sum_{n=0}^{\infty} [K_n : K] = 1 + (q-1) + (q-1)q + \ldots + (q-1)q^n + \ldots = 0.$$

В случае $\ell = 2$ имеем

$$\widetilde{\mathrm{Sp}}(1) = 1 + 1 + \sum_{n=1}^{\infty}[K_n : K] = 2 + \sum_{n=1}^{\infty} 2^n = 0.$$

Пусть теперь $1 \leqslant k < q$. Из теоремы о симметрических функциях вытекает следующая лемма.

Лемма 2.1. *Пусть $E(X) = X^q + a_{q-1}X^{q-1} + \ldots + a_1X + a_0$ — многочлен степени q, коэффициенты которого принадлежат некоторому полю F. Пусть $\alpha_1, \ldots, \alpha_q$ — все корни этого многочлена. Тогда для любого k, такого что $0 < k < q$, выполняется равенство*

$$\sum_{i=1}^{q} \alpha_i^k = P_k(a_{q-1}, \ldots, a_{q-k}),$$

где P_k — некоторый многочлен с коэффициентами из $\mathbb{Z}$ от k переменных, не зависящий от $E(X)$.

Итак, при $0 < k < q$ и $n \geqslant 0$ мы имеем

$$\mathrm{Sp}_{k_n/K}(\pi_n^k) = \mathrm{Sp}_{K_{n-1}/K}\big(\mathrm{Sp}_{K_n/K_{n-1}}(\pi_n^k)\big), \tag{4}$$

где полагаем, что $K_{-1} = K$.

Применяя лемму 2.1 для вычисления величины $A_n = \mathrm{Sp}_{K_n/K_{n-1}}(\pi_n^k)$, мы получаем при $n \geqslant 1$, что $A_n = P_k(a_{q-1}, \ldots, a_{q-k})$, где $a_{q-1}, \ldots, a_{q-k}$ — коэффициенты многочлена (3). Если $n = 0$ и $q > 2$, то уравнение $f(X) = 0$ имеет q корней, один из которых равен 0, а остальные корни — это все числа, сопряжённые с π_0. Поэтому и в этом случае $A_0 = \mathrm{Sp}_{K_0/K}(\pi_0^k) = P_k(a_{q-1}, \ldots, a_{q-k})$. Таким образом, числа A_n не зависят от n, и, обозначая их общее значение через A и используя (4), мы получаем

$$\widetilde{\mathrm{Sp}}(X^k) = A\left(1 + \sum_{n=0}^{\infty}[K_n : K]\right) = 0.$$

Случай $q = 2$ рассматривается аналогично.

Предположим теперь, что $k \geqslant q$ и мы уже доказали, что $\widetilde{\mathrm{Sp}}(X^i) = 0$ для всех $i < k$. Пусть $B = \mathcal{O}_K[Y]$, где Y — формальная переменная. Рассмотрим многочлен $P(X, Y) = f(X) - Y \in B[X]$. Для любого многочлена F, зависящего от X и Y, мы будем обозначать через $\deg_X F$ и $\deg_Y F$ степень F относительно переменных X и Y соответственно. Поскольку коэффициент при старшем члене (относительно X) многочлена $P(X, Y)$ равен 1, мы можем в кольце $B[X]$ делить любой элемент этого кольца на $P(X, Y)$ с остатком. В частности, существует и единственно представление

$$X^k = P(X, Y)Q(X, Y) + R(X, Y), \tag{5}$$

где $\deg_X R(X, Y) < q$.

Лемма 2.2. *Справедливо неравенство*

$$\deg_Y R(X,Y) < k.$$

Доказательство. Рассмотрим подробнее алгоритм деления с остатком. Положим $E_1(X,Y) = X^k$ и $Q_1(X,Y) = X^{k-q}$. Предположим, что многочлены $E_i(X,Y)$ и $Q_i(X,Y)$ уже определены. Тогда мы полагаем $E_{i+1}(X,Y) = E_i(X,Y) - P(X,Y)Q_i(X,Y)$ и $Q_{i+1}(X,Y) = X^{k-q-i}H_{i+1}(Y)$, где $H_{i+1}(Y)$ — коэффициент при старшей степени X в $E_{i+1}(X,Y)$. При этом не исключается случай $H(Y) = 0$. Таким образом, мы получаем, что $\deg_X E_i(X,Y) \leqslant k-i+1$. Следовательно, $\deg_X E_{k-q+2}(X,Y) \leqslant q-1$, т. е. после $k-q+1$ шагов алгоритм остановится, и мы получим

$$R(X,Y) = E_{k-q+2}(X,Y), \quad Q(X,Y) = \sum_{i=0}^{k-q} Q_i(X,Y).$$

Так как $\deg_Y X^k = 0$, $\deg_Y P(X,Y) = 1$ и $\deg_Y H_{i+1}(Y) \leqslant \deg_Y E_{i+1}(X,Y)$ для любого i, мы получаем, что $\deg_Y E_{i+1}(X,Y) \leqslant \deg_Y E_i(X,Y)+1$. Следовательно,

$$\deg_Y R(X,Y) = \deg_Y E_{k-q+2}(X,Y) \leqslant k-q+1 < k.$$

Лемма доказана. □

Вернёмся к доказательству теоремы. Согласно лемме 2.2 при $k \geqslant q$ для X^k существует представление (5), причём $R(0,0) = 0$, $\deg_X R(X,Y) < q$ и $\deg_Y R(X,Y) < k$. Из этого следует, что для любого $n \geqslant 0$ справедливо равенство $\pi_n^k = R(\pi_n, \pi_{n-1})$, где при $n = 0$ мы полагаем $\pi_{-1} = 0$ по определению.

Представим многочлен $R(X,Y)$ в виде суммы двух многочленов $R(X,Y) = R_1(X) + R_2(X,Y)$, где $R_1(X)$ зависит только от X и $R_2(X,Y)$ делится на Y. Из этого, в частности, следует, что $R_2(\pi_0, \pi_{-1}) = 0$. Таким образом, в случае $q > 2$ мы имеем $\widetilde{\mathrm{Sp}}(x^k) = A + B$, где

$$A = \sum_{n=0}^{\infty} \mathrm{Sp}_{K_n/K}\big(R_1(\pi)\big),$$

$$B = \sum_{n=0}^{\infty} \mathrm{Sp}_{K_n/K}\big(R_2(\pi_n, \pi_{n-1})\big) = \sum_{n=1}^{\infty} \mathrm{Sp}_{K_n/K}\big(R_2(\pi_n, \pi_{n-1})\big).$$

Поскольку $\deg_X R_1(X) < q$, в силу уже доказанной части теоремы мы имеем $A = 0$. Пусть X^bY^c — одночлен, входящий в $R_2(X,Y)$ с некоторым ненулевым коэффициентом. Чтобы доказать, что $B = 0$, достаточно проверить, что для всех таких одночленов

$$\sum_{n=1}^{\infty} \mathrm{Sp}_{K_n/K}\, \pi_n^b \pi_{n-1}^c = 0.$$

Для любого $n \geqslant 1$ мы имеем

$$\mathrm{Sp}_{K_n/K}(\pi_n^b \pi_{n-1}^c) = \mathrm{Sp}_{K_{n-1}/K}\big(\pi_{n-1}^c \,\mathrm{Sp}_{K_n/K_{n-1}}(\pi_n^b)\big).$$

Поскольку $b < q$, в силу леммы 2.1 при $n \geqslant 0$ имеем $\mathrm{Sp}_{K_n/K_{n-1}}(\pi_n^b) = a \in \mathcal{O}_K$, где a не зависит от n (при $n = 0$ мы полагаем $K_{-1} = K$). Таким образом,

$$\sum_{n=1}^{\infty} \mathrm{Sp}_{K_n/K}(\pi_n^b \pi_{n-1}^c) = a \sum_{n=0}^{\infty} \mathrm{Sp}_{K_n/K}(\pi_n^c) = a\widetilde{\mathrm{Sp}}(X^c) = 0,$$

поскольку $c < k$ и мы можем воспользоваться предположением индукции.

Случай $q = 2$ разбирается аналогично. Нужно заметить только, что в этом случае $P(\pi, 0) = 0$ и, следовательно, $\pi^k = R(\pi, 0)$. Теорема доказана. □

Литература

[1] Касселс Дж., Фрёлих А. Алгебраическая теория чисел. — М., 1969.

[2] Кузьмин Л. В. Новое доказательство одной теоремы двойственности о l-адических логарифмах локальных единиц // Итоги науки и техн. Сер. Совр. мат. и её прил. Т. 45. — М.: ВИНИТИ, 1997. — С. 72—81.

[3] Кузьмин Л. В. Некоторые замечания о l-адическом регуляторе. III // Изв. РАН. Сер. мат. — 1999. — Т. 63, № 6. — С. 29—82.

[4] Кузьмин Л. В. Об одном свойстве l-адических логарифмов единиц локальных неабелевых полей // Изв. РАН. Сер. мат. — 2006. — Т. 70, № 5. — С. 97—122.