Записки научных
семинаров ПОМИ
Том 435, 2015 г.

А. И. Мадунц, Р. П. Востокова

ФОРМАЛЬНЫЕ МОДУЛИ ДЛЯ ОБОБЩЕННЫХ ГРУПП ЛЮБИНА–ТЕЙТА

§1. Обобщенные формальные группы Любина–Тейта и их эндоморфизмы

Данная работа изучает обобщенные формальные группы Любина–Тейта, в частности, арифметику связанного с ними формального модуля. Введем основные обозначения.

Пусть K – локальное поле (конечное расширение поля $\mathbb{Q}_p$), $\mathcal{O}_K$– его кольцо целых, v_K – нормирование, π – произвольный униформизирующий элемент, $\wp$ – максимальный идеал.

Под $\overline{K}$ будем подразумевать поле вычетов K (конечное поле характеристики p с числом элементов $q = p^{f_0}$).

Как обычно, $R[[X_1, \dots, X_n]]$ обозначим множество степенных рядов от n переменных с коэффициентами из некоторого кольца R, а

$$R[[X_1, \dots, X_n]]^o$$

будем обозначать множество рядов без свободного члена.

Для $a(X_1, \dots, X_n), b(X_1, \dots, X_n) \in K[[X_1, \dots, X_n]]$ будем писать

$$a(X_1, \dots, X_n) \equiv b(X_1, \dots, X_n) \bmod \deg n,$$

если все члены степеней, меньших n, у данных рядов совпадают, а для степенных рядов

$$a(X_1, \dots, X_n), b(X_1, \dots, X_n) \in \mathcal{O}_K[[X_1, \dots, X_n]]$$

под $a(X) \equiv b(X) \bmod \pi^s$ подразумеваем, что

$$a(X_1, \dots, X_n) - b(X_1, \dots, X_n) \in \pi^s \mathcal{O}_K[[X_1, \dots, X_n]].$$

Для любого натурального числа m введем также множество

$$\mathcal{F}_\pi = \{f(X) \in \mathcal{O}_K[[X]] : f(X) \equiv \pi X + X^{q^m} \bmod (\pi, \deg 2)\}.$$

Ключевые слова: локальные поля, обобщенные формальные группы Любина–Тейта, формальные модули, символ Гильберта.

Здесь и в дальнейшем вместо $a(X_1,\dots,X_n) \equiv b(X_1,\dots,X_n) \bmod \pi$ и $a(X_1,\dots,X_n) \equiv b(X_1,\dots,X_n) \bmod \deg n$ мы используем обозначение $a(X_1,\dots,X_n) \equiv b(X_1,\dots,X_n) \bmod (\pi, \deg n)$.

Аналогично случаю классических групп Любина–Тейта (см. [2]), верны следующие утверждения.

1.1. Лемма. *Для любых $f(X), g(X) \in \mathcal{F}_\pi$ и $\alpha_1,\dots,\alpha_n \in \mathcal{O}_K$ существует единственный ряд от n переменных*

$$F(X_1,\dots,X_n) \in \mathcal{O}_K[[X_1,\dots,X_n]]$$

такой, что $F(X_1,\dots,X_n) \equiv \alpha_1 X_1 + \dots + \alpha_n X_n \bmod \deg 2$ и

$$f(F(X_1,\dots,X_n)) = F(g(X_1),\dots,g(X_n)).$$

1.1.1. Следствие. *Для любого $f(X) \in \mathcal{F}_\pi$ существует единственная формальная группа $F_f(X,Y)$ над $\mathcal{O}_K$, для которой $f(X)$ является эндоморфизмом.*

1.2. Определение. Формальную группу F_f, полученную таким образом, называют обобщенной формальной группой Любина–Тейта.

1.3. Определение. Формальную группу F_0, ассоциированную с

$$f_0(X) = \pi X + X^{q^m},$$

назовем базисной обобщенной формальной группой Любина–Тейта.

1.3.1. Следствие. *Для любого $\alpha \in \mathcal{O}_K$ существует единственный ряд $[\alpha]_{f,g}(X) \in \mathcal{O}_K[[X]]$ такой, что*

$$[\alpha]_{f,g}(X) \equiv \alpha X \bmod \deg 2$$

и

$$[\alpha]_{f,g} \in \mathrm{End}_{\mathcal{O}_K}(F_g, F_f).$$

Для любых $[\alpha]_{f,g}, [\beta]_{g,h}$ верно

$$[\alpha]_{f,g} \circ [\beta]_{g,h} = [\alpha\beta]_{f,h}$$

и для любых $[\alpha]_{f,g}, [\beta]_{f,g}$ имеем

$$[\alpha]_{f,g} +_F [\beta]_{f,g} = [\alpha+\beta]_{f,g},$$

где под $([\alpha]_{f,g} +_F [\beta]_{f,g})(X)$ подразумевается $F_f([\alpha]_{f,g}(X), [\beta]_{f,g}(X))$.

Множество эндоморфизмов относительной формальной группы Любина–Тейта F_f с операциями

$$[\alpha] \cdot_F [\beta] = [\alpha] \circ [\beta]$$

и

$$[\alpha] +_F [\beta] = F_f([\alpha],[\beta])$$

изоморфно $\mathcal{O}_K$.

1.3.2. Замечание. Очевидно, что ряд $f(X)$ совпадает с эндоморфизмом $[\pi](X) \in \operatorname{End}_{\mathcal{O}_K} F_f$. Будем называть его изогенией обобщенной формальной группы Любина–Тейта. Высотой формальной группы называют высоту ее изогении. Поскольку

$$[\pi](X) \equiv X^{q^m} \bmod \pi,$$

высота обобщенной формальной группы Любина–Тейта равна m.

1.3.3. Замечание. Из доказательства леммы видно, что для корректного построения эндоморфизмов обобщенной формальной группы Любина–Тейта требуется выполнение условия: для любого a из кольца целых

$$a^{q^m} \equiv a \bmod \pi.$$

Обозначим T_m неразветвленное расширение поля K степени m. Для его кольца целых условие выполнено. Пусть $\widetilde{K}$ – пополнение максимального неразветвленного расширения K. Тогда имеются следующие изоморфизмы:

$$\operatorname{End}_{\mathcal{O}_K} F_f \cong \mathcal{O}_K, \qquad \operatorname{End}_{\mathcal{O}_{\widetilde{K}}} F_f \cong \mathcal{O}_{T_m}.$$

§2. Логарифм обобщенной формальной группы Любина–Тейта

Применим к обобщенным формальным группам Любина–Тейта подход Хазевинкеля. Сформулируем функциональную лемму из его работы [1] в нужном нам варианте.

2.1. Лемма. *Выполнены следующие утверждения:*

(1) *для любого ряда* $g(X) \in \mathcal{O}_K[[X]]^o$ *существует единственный ряд* $\lambda_g(X) \in K[[X]]$ *такой, что* $\lambda_g(X) = g(X) + \frac{1}{\pi}\lambda_g(X^{q^m})$, *причем*

$$F(X,Y) = \lambda_g^{-1}(\lambda_g(X) + \lambda_g(Y)) \in \mathcal{O}_K[[X,Y]];$$

(2) *для любых* $\lambda_{g_1}(X), \lambda_{g_2}(X)$ *таких, что*

$$\lambda_{g_1}(X) = g_1(X) + \frac{1}{\pi}\lambda_{g_1}(X^{q^m}), \lambda_{g_2}(X) = g_2(X) + \frac{1}{\pi}\lambda_{g_2}(X^{q^m})$$

имеем $\lambda_{g_1}^{-1}(\lambda_{g_2}(X)) \in \mathcal{O}_K[[X]]$;

(3) *для любых* $g_1(X), h(X) \in \mathcal{O}_K[[X]]^o$ *существует единственный ряд* $g_2(X) \in \mathcal{O}_K[[X]]^o$ *такой, что* $\lambda_{g_1}(h(X)) = \lambda_{g_2}(X)$;

(4) *для любых* $\alpha(X), \beta(X) \in \mathcal{O}_K[[X]]$ *имеем*

$$\alpha(X) \equiv \beta(X) \bmod \pi^n \Leftrightarrow \lambda(\alpha(X)) \equiv \lambda(\beta(X)) \bmod \pi^n;$$

(5) *пусть*

$$\lambda_{g_1}(X) = g_1(X) + \frac{1}{\pi_1}\lambda_{g_1}(X^{q^m}), \lambda_{g_2}(X) = g_2(X) + \frac{1}{\pi_2}\lambda_{g_2}(X^{q^m}),$$

$$F_1(X,Y) = \lambda_{g_1}^{-1}(\lambda_{g_1}(X) + \lambda_{g_1}(Y)), F_2(X,Y) = \lambda_{g_2}^{-1}(\lambda_{g_2}(X) + \lambda_{g_2}(Y)).$$

Тогда $F_1 \cong F_2 \Leftrightarrow \pi_1 = \pi_2$. □

Выберем $g(X) \equiv X \bmod \deg 2$. В этом случае $F(X,Y)$ – формальная группа, а $\lambda(X)$ является ее логарифмом.

2.2. Предложение. *Обобщенные формальные группы Любина–Тейта находятся во взаимно-однозначном соответствии с формальными группами, полученными применением леммы* 2.1.

Доказательство. Для произвольного $g(X) \in \mathcal{O}_K[[X]]^o, g(X) \equiv X \bmod \deg 2$ построим по лемме 2.1 ряд $f(X) = \lambda^{-1}(\pi\lambda(X))$. Легко видеть, что $f \circ F = F \circ f$. По свойству логарифма $\pi\lambda(X) = \pi g(X) + \lambda(X^{q^m})$.

Введем $g_1(X) = \pi g(X), \lambda_1(X) = \pi\lambda(X)$. Очевидно, что

$$\lambda_1(X) = g_1(X) + \frac{1}{\pi}\lambda_1(X^{q^m}).$$

По утверждению (2) леммы 2.1 из этого следует, что

$$f(X) = \lambda^{-1}(\lambda_1(X)) \in \mathcal{O}_K[[X]].$$

Так как $\lambda(X) \equiv X \bmod \deg 2, \lambda^{-1}(X) \equiv X \bmod \deg 2$, имеем

$$f(X) \equiv \pi X \bmod \deg 2.$$

Кроме того, по части (4) леммы 2.1 условие

$$f(X) \equiv X^{q^m} \bmod \deg 2$$

равносильно условию

$$\lambda(f(X)) = \pi\lambda(X) \equiv \lambda(X^{q^m}) \bmod \deg 2,$$

которое выполнено по свойствам логарифма.

Таким образом, $f(X) \in \mathrm{End}_{\mathcal{O}_K} F$ и $f(X) \in \mathcal{F}_\pi$. По единственности в лемме 1.1 формальная группа $F(X,Y)$ совпадает с $F_f(X,Y)$, построенной в предыдущем пункте.

Теперь выберем любое $f_1(X) \in \mathcal{F}_\pi$. По лемме 1.1 существует единственный $[1]_{f,f_1} \in \operatorname{End}_{\mathcal{O}_K}(F_{f_1}, F_f)$. Но $\lambda^{-1}(\lambda_1(X)) \equiv X \bmod \deg 2$, причем согласно части (2) леммы 2.1 имеем $\lambda^{-1}(\lambda_1(X)) \in \operatorname{End}_{\mathcal{O}_K}(F_{f_1}, F_f)$. Значит, $\lambda_1 = \lambda([1]_{f,f_1})$, что по части (3) леммы 2.1 дает $\lambda_1 = \lambda_{g_1}$. $\square$

Логарифм не является эндоморфизмом формальных групп, поскольку его коэффициенты не обязательно целые. Однако верно следующее утверждение.

2.3. Предложение. *Пусть*

$$g(X) = X + \sum_{i>1} b_i X^i, \lambda(X) = X + \sum_{i>1} c_i X^i.$$

Тогда $c_i = b_i$, *если* $q^m \nmid i$,

$$c_{q^{mk}} = b_{q^{mk}} + \frac{1}{\pi} b_{q^{m(k-1)}} + \dots + \frac{1}{\pi^{k-1}} b_{q^m} + \frac{1}{\pi^k},$$
$$c_{q^{mk}s} = b_{q^{mk}s} + \frac{1}{\pi} b_{q^{m(k-1)}s} + \dots + \frac{1}{\pi^k} b_s, 2 \leqslant s \leqslant q^m - 1.$$

Доказательство производится непосредственным вычислением с помощью формулы

$$\lambda(X) = g(X) + \frac{1}{\pi}\lambda(X^{q^m}).$$

В частности, получаем $v_K(c_i) \geqslant -\log_{q^m} i$.

2.3.1. Замечание. Ряд, обратный к $\lambda(X)$ в смысле суперпозиции, обозначим $\exp_F X$ и будем называть формальной экспонентой. Таким образом,

$$\exp_F(\alpha X) = [\alpha] \exp_F X$$

и

$$\exp_F(X + Y) = \exp_F X +_F \exp_F Y,$$

где $\alpha \in \mathcal{O}_{T_m}$.

Пусть $\exp_F X = \sum_{i \geqslant 1} a_i X^i$. Используя формулу

$$\exp_F(\pi x) = [\pi] \exp_F x,$$

несложной индукцией можно показать, что

$$v_K(a_i) \geqslant -\frac{i-1}{q^m - 1}.$$

2.4. Определение. В случае $g(X) = X$ имеем $\lambda_a(X) = \sum_{i\geqslant 0} \frac{X^{q^{mi}}}{\pi^i}$. Этот логарифм назовем логарифмом Артина–Хассе. Как мы видим, существует $f_a(X) \in \mathcal{F}_\pi$ такое, что соответствующая обобщенная формальная группа Любина–Тейта $F_{f_a}(X,Y)$ имеет логарифм Артина–Хассе.

§3. Модуль ядра изогении

Пусть L – некоторое расширение поля K, содержащееся в K^{sep} – сепарабельном замыкании K. Обозначим $\wp_L$ максимальный идеал L. Для фиксированной обобщенной формальной группы Любина–Тейта $F_f(X,Y)$ введем операцию формального сложения элементов из $\wp_L$:

$$x +_F y = F(x,y)$$

и умножения элемента $x \in \wp_L$ на элемент $\alpha \in \mathcal{O}_{T_m}$:

$$\alpha \cdot_F x = [\alpha](x)$$

(напомним, что T_m – неразветвленное расширение поля K степени m, а $[\alpha](X) \in \mathrm{End}_{\mathcal{O}_{\widetilde{K}}} F$).

Пусть $\mathcal{M}_L$ – множество $\wp_L$ с данными операциями. Его называют группой точек (со структурой $\mathcal{O}_{T_m}$-модуля). Для каждого $\alpha \in \mathcal{O}_{T_m}$ ищем $x \in \mathcal{M}_L$ такие, что $\alpha \cdot_F x = 0$. Пусть $\alpha = \varepsilon\pi^n$, где $\varepsilon \in \mathcal{O}^*_{T_m}$. Тогда $\alpha \cdot_F x = 0 \Leftrightarrow \pi^n \cdot_F x = 0$. Таким образом, достаточно изучить корни

$$[\pi^n](X), n \in \mathbb{N}.$$

Пусть теперь L содержит все корни изогении $[\pi^n](X)$. Введем обозначение

$$\Lambda_{f,n} = \{\xi \in \mathcal{M}_L : \pi^n \cdot_F x = 0\}.$$

Легко видеть, что это $\mathcal{O}_{T_m}$-подмодуль $\mathcal{M}_L$. Более того, поскольку по следствию 1.3.1 для любых $f(X), g(X) \in \mathcal{F}_\pi$ существует строгий изоморфизм

$$[1]_{g,f}(X) \in \mathrm{End}_{\mathcal{O}_K}(F_g, F_f)$$

такой, что $[1]_{g,f}(f(X)) = g([1]_{f,g}(X))$, поле $K(\Lambda_{f,n}) = K_{\pi,n}$ не зависит от выбора $f(X) \in \mathcal{F}_\pi$.

Возьмем $f_0(X) = \pi X + X^{q^m} = X(\pi + X^{q^m-1})$. Пусть ξ_1 – некоторый корень многочлена Эйзенштейна $\Phi_1(X) = \pi + X^{q^m-1}$. Тогда

$$\Lambda_{f,1} = \{\zeta^k\xi_1, k = 0, \dots, q^m - 1\},$$

где ζ – первообразный корень из единицы степени $q^m - 1$. Наименьшим расширением, его содержащим, является T_m. Получаем цепочку расширений Галуа

$$K \subset T_m = K(\zeta) \subset K_{\pi,1} = T_m(\xi_1),$$

из которых первое является неразветвленным степени m, а второе – куммеровским слаборазветвленным степени $q^m - 1$.

Пусть далее

$$\Phi_s(X) = \frac{[\pi^s](X)}{[\pi^{s-1}](X)} = \pi + ([\pi^{s-1}](X))^{q^m-1}.$$

Данный многочлен неприводим над K и T_m как многочлен Эйзенштейна, причем его степень равна $q^{m(s-1)}(q^m-1)$, а корнями являются первообразные корни $[\pi^s](X)$. Обозначим некоторый такой корень ξ_s. Таким образом, расширение $K_{\pi,s} = T_m(\xi_s)$ вполне разветвлено над T_m. Более того, если выбрать $\xi_{s-1} = [\pi](\xi_s)$, то ξ_s будет корнем

$$\pi X + X^{q^m} - \xi_{s-1},$$

то есть, многочлена Эйзенштейна над K_{s-1} степени q^m. В итоге имеем башню расширений Галуа

$$\begin{gathered} K \subset T_m = K(\zeta) \subset K_{\pi,1} = T_m(\xi_1) \subset K_{\pi,2} = K_{\pi,1}(\xi_2) \subset \dots \\ \subset K_{\pi,n} = K_{\pi,n-1}(\xi_n), \end{gathered}$$

из которых первое является неразветвленным степени m, второе – куммеровским слаборазветвленным степени $q^m - 1$, а все последующие – вполне разветвленными степени q^m.

Заметим, что $[\pi^n](X) = X\Phi_1(X)\dots\Phi_n(X)$. Кроме того, легко видеть, что

$$\Lambda_{f,n} \cong \mathcal{O}_{T_m}/\pi^n\mathcal{O}_{T_m}$$

(доказательство аналогично приведенному в [2]).

§4. Изоморфизмы степенных рядов

Пусть T – неразветвленное расширение поля K, $\mathcal{O}_T$ – его кольцо целых, Δ – автоморфизм Фробениуса T/K. Продолжим данный автоморфизм на множество степенных рядов без свободного члена

$\mathcal{O}_T[[X]]^o$ по формуле:

$$\Delta\left(\sum_{i\geqslant 1} a_i X^i\right) = \sum_{i\geqslant 1} a_i^{\Delta} X^{qi}.$$

По основному соотношению для логарифма из леммы 2.1 и предложению 2.2 для любой обобщенной формальной группы Любина–Тейта $F(X,Y)$ имеем

$$l_F(X) = \left(1 - \frac{\Delta^m}{\pi}\right)(\lambda(X)) \in \mathcal{O}_K[[X]]^o.$$

Заметим, что случай $g(X) = X$ дает логарифм Артина–Хассе $\lambda_a(X)$ и

$$l_F(X) = \lambda_a^{-1}(\lambda(X)) = [1]_{f_a,f}.$$

Отображение, обратное к l_F в смысле суперпозиции, обозначим E_F (см. [7]). Очевидно, что

$$E_F(X) = \lambda^{-1}\left(\sum_{\mathbf{i}\geqslant 0} \frac{\Delta^{mi}(X)}{\pi^i}\right).$$

Поскольку $E_F(X) = \lambda^{-1}(\lambda_a(X)) = [1]_{f,f_a}$, коэффициенты данного ряда целые. Кроме того,

$$E_F(X) \equiv X \bmod \deg 2, l_F(X) \equiv X \bmod \deg 2.$$

Действие введенных отображений естественным образом продолжается на $\mathcal{O}_T[[X]]^o$, то есть, для любого $\varphi(X) \in \mathcal{O}_T[[X]]^o$ имеем

$$l_F(\varphi) = \left(1 - \frac{\Delta^m}{\pi}\right)(\lambda(\varphi)), E_F(\varphi) = \lambda^{-1}\left(\sum_{\mathbf{i}\geqslant 0} \frac{\Delta^{mi}(\varphi)}{\pi^i}\right).$$

Через $\mathcal{H}_F^0$ обозначим $\mathcal{O}_{T_m}$-модуль рядов без свободного члена над $\mathcal{O}_T$ со следующими операциями:

$$\varphi +_F \psi = F(\varphi,\psi), \alpha \cdot_F \varphi = [\alpha](\varphi), \alpha \in \mathcal{O}_{T_m}.$$

Аналогично [3] получаем, что

$$E_F(\varphi + \psi) = E_F(\varphi) +_F E_F(\psi), E_F(\alpha\varphi) = [\alpha]E_F(\varphi)$$

и

$$l_F(\varphi +_F \psi) = l_F(\varphi) + l_F(\psi), l_F([\alpha]\varphi) = \alpha l_F(\varphi).$$

Таким образом, функции E_F и l_F осуществляют взаимно-обратные изоморфизмы между аддитивным $\mathcal{O}_{T_m}$-модулем $\mathcal{O}_T[[X]]^o$ и $\mathcal{O}_{T_m}$-модулем $\mathcal{H}_F^0$. В работе [3] также доказано, что для ряда φ порядка r (то есть, $\varphi(X)=\sum_{i\geqslant r}a_iX^i$) из кольца $\mathcal{O}_T[[X]]^o$ верно

$$E_F(\varphi)\equiv\varphi \bmod \deg(r+1), l_F(\varphi)\equiv\varphi \bmod \deg(r+1),$$

из чего следует, что для ряда φ порядка r при всех $\alpha\in\mathcal{O}_{\widetilde{K}}$ имеем $E_F(\alpha l_F(\varphi)|_{X=\pi}\equiv\alpha\varphi(\pi) \bmod \pi^{r+1}$.

§5. Примарные элементы

Здесь и в дальнейшем L будет конечным расширением K, содержащим все корни изогении $[\pi^n](X)$. Согласно результатам пункта 3, это означает, что $K_{\pi,n}=T_m(\xi_n)\subset L$, где ξ_n – первообразный корень $[\pi^n](X)$, причем $K_{\pi,n}/T_m$ – вполне разветвленное расширение степени $q^{m(n-1)}(q^m-1)$ и T_m/K – неразветвленное степени m.

Пусть v_L – нормирование L, а π_L – униформизующая L. Обозначим e_L индекс ветвления, а f_L – степень инерции L/K. Тогда

$$e_n=\frac{e_L}{q^{m(n-1)}(q^m-1)}\in\mathbb{Z}, e_1=\frac{e_L}{q^m-1}\in\mathbb{Z}, f_1=\frac{f_L}{m}\in\mathbb{Z}.$$

Разложим ξ_n в степенной ряд по простому элементу π_L с коэффициентами из кольца $\mathcal{O}_T$, где T – подполе инерции L/K. Имеем

$$\xi_n=\sum_{i\geqslant 0}c_i\pi_L^{i+e_n}.$$

Введем ряды $z(X)=\sum_{i\geqslant 0}c_iX^{i+e_n}$ и $s_k(X)=[\pi^k](z(X))$, причем $s_n(X)$ будем обозначать $s(X)$.

В дальнейшем нам потребуется ряд

$$\frac{1}{s(X)}=\widetilde{s}(X).$$

Непосредственным вычислением проверяется, что

$$\widetilde{s}(X)=\sum_{i\geqslant -q^{nm}e_n}d_iX^i,$$

причем

$$\frac{d\widetilde{s}(X)}{dX}\equiv 0 \bmod \pi^n.$$

Элемент группы точек $x \in \mathcal{M}_L$ называют π^n-примарным, если расширение поля K, полученное делением x на изогению $[\pi^n]$, неразветвлено. Примарные элементы играют важную роль в задании обобщенного символа Гильберта, который сопоставляет упорядоченной паре

$$\alpha \in L^*, \beta \in \mathcal{M}_L$$

элемент ядра изогении $\Lambda_{f,n}$ по формуле:

$$(\alpha, \beta)_F = \rho^{\sigma_\alpha} -_F \rho,$$

где $\beta = [\pi^n](\rho)$, а σ_α – изоморфизм из группы Галуа $\mathrm{Gal}(L/K)$, соответствующий α в силу локальной теории полей классов (см. [8]).

Для $a \in \mathcal{O}_T$ выберем $A \in \mathcal{O}_{\widetilde{K}}$ такое, что $A^{\Delta^m} - A = a$ (напомним, что $\widetilde{K}$ – пополнение максимального неразветвленного расширения над T, а Δ здесь – продолжение автоморфизма Фробениуса T/K на $\widetilde{K}$). Подобно случаю классических формальных групп Любина–Тейта (см. [3]), введем $H(a) = E_F(\pi^n A^{\Delta^m} l_F(z(X)))\big|_{X=\pi_L}$ и $\omega(a) = E_F(as(X))|_{X=\pi_L}$.

5.1. Теорема. *Элементы $H(a), \omega(a)$ являются корректно определенными π^n-примарными, причем*

$$(\pi_L, H(a))_F = (\pi_L, \omega(a))_F = [\mathrm{tr}_{T/T_m} a](\xi_n).$$

Доказательство. В работе [9] для классических формальных групп Любина–Тейта доказано, что $H(a)$ и $\omega(a)$ корректно определены (то есть, используемые ряды при подстановке элемента π_L сходятся). Аналогично, заменив Δ на Δ^m, получаем корректность определения соответствующих элементов в случае обобщенных формальных групп Любина–Тейта.

Пусть $\widetilde{\Delta} = \Delta^{mf_1}$ – автоморфизм Фробениуса $\widetilde{K}/T$ (заметим, что он дает σ_{π_L}, а $\rho = E_F(A^{\Delta^m} l_F(z(X)))\big|_{X=\pi_L}$).

Поскольку $A^{\Delta^m \widetilde{\Delta}} = A^{\Delta^m} + \mathrm{tr}_{T/T_m} a$, имеем

$$\begin{aligned} E_F(A^{\Delta^m} l_F(z(X)))^{\widetilde{\Delta}} &= E_F(A^{\Delta^m} l_F(z(X))) +_F E_F((\mathrm{tr}_{T/T_m} a) l_F(z(X))) \\ &= (\mathrm{tr}_{T/T_m} a) l_F(z(X) E_F(A^{\Delta^m} l_F(z(X))) +_F [\mathrm{tr}_{T/T_m} a](z(X)). \end{aligned}$$

Таким образом,

$$\begin{aligned} H(a)^{\widetilde{\Delta}} &= H(a) +_F [\pi^n \mathrm{tr}_{T/T_m} a](z(\pi_L)) \\ &= H(a) +_F [\mathrm{tr}_{T/T_m} a]([\pi^n] z(\pi_L)) = H(a), \end{aligned}$$

что дает примарность, и $\rho^{\widetilde{\Delta}} = \rho +_F [\mathrm{tr}_{T/T_m}\, a](\xi_n)$, из чего получаем формулу $(\pi_L, H(a))_F = [\mathrm{tr}_{T/T_m}\, a](\xi_n)$.

Преобразовав соответствующим образом результат из [9], связывающий $H(a)$ и $\omega(a)$, получаем

$$H(a) = \omega(a) +_F [\pi^n]\left(\sum\nolimits_{F\, i=2}^{+\infty} \sum\nolimits_{F\, j=0}^{+\infty} \exp_F \frac{a^{\Delta^{im}} c_j s^{j\Delta^{im}}(\pi_L)}{\pi^{n+i}}\right),$$

где $\lambda(X) = \sum_{j\geqslant 1} c_j X^j$. Следовательно, $H(a)$ и $\omega(a)$ отличаются на элемент, делящийся на изогению $[\pi^n]$ в группе точек. Это дает как примарность $\omega(a)$, так и формулу $(\pi_L, \omega(a))_F = [\mathrm{tr}_{T/T_m}\, a](\xi_n)$.

§6. Образующие Шафаревича

Дальнейшей задачей является обобщение на случай обобщенных формальных групп Любина–Тейта понятия базиса Шафаревича (см. [10]). Обозначим $\mathcal{R}$ множество представителей Тейхмюллера в L.

6.1. Лемма. *Пусть для каждого $\theta \in \mathcal{R}$ и для натуральных i с условием*

$$1 \leqslant i < q^m e_1, q^m \nmid i; i = q^m e_1$$

выбран элемент $\varepsilon_i(\theta)$ из группы точек $\mathcal{M}_L$ такой, что

$$\varepsilon_i(\theta) \equiv \theta_i \pi_L^i \bmod \pi_L^{i+1}.$$

Тогда любой элемент β из группы точек можно представить в виде

$$\beta = \sum\nolimits_{F\, i,r} [\pi^r](\varepsilon_i(\theta_{i,r})),$$

где r пробегает все целые неотрицательные числа.

Доказательство. Несложной индукцией можно доказать (см. мультипликативный случай из [10] и случай классической формальной группы Любина–Тейта в [3]), что всякий элемент β из группы точек представим в виде

$$\beta = \sum\nolimits_{F\, i=1}^{\infty} \varepsilon_i(\theta_i),$$

где

$$\varepsilon_i(\theta_i) \in \mathcal{M}_L, \varepsilon_i(\theta_i) \equiv \theta_i \pi_L^i \bmod \pi_L^{i+1}, \theta_i \in \mathcal{R}.$$

Для произвольного элемента $\alpha \in \mathcal{M}_L, v_L(\alpha) = i$ имеются очевидные соотношения

$$[\pi](\alpha) \equiv \alpha^{q^m} \bmod \pi_L^{q^m i+1}, i < e_1,$$
$$[\pi](\alpha) \equiv \pi\alpha \bmod \pi_L^{i+e_L+1}, i > e_1.$$

Пусть γ – первый коэффициент в разложении π по π_L. Тогда

$$[\pi]\varepsilon_{i-e}(\gamma^{-1}\theta_i) \equiv \pi_L^{e_L}\gamma\gamma^{-1}\theta_i\pi_L^{i-e_L} \equiv \theta_i\pi_L^i \bmod \pi_L^{i+1}.$$

После замены в разложении из леммы 6.1 элементов $\varepsilon_i(\theta_i), i > q^m e_1$ на $[\pi]\varepsilon_{i-e_L}(\gamma^{-1}\theta_i)$ остаются значения i между 1 и $q^m e_1$.

Затем элементы $\varepsilon_i(\theta_i), i = q^m j, 1 \leqslant i < q^m e_1$ заменяем на $[\pi]\varepsilon_j(\theta_i^{\frac{1}{q^m}})$, избавляясь от индексов, кратных q^m.

В результате имеем

$$\beta = \sum\nolimits_{F\, i,r}[\pi^r](\varepsilon_i(\theta_{i,r})),$$

где индекс i принимает значения между 1 и $q^m e_1$, не делящиеся на q^m, а также значение $i = q^m e_1$, индекс r пробегает целые неотрицательные числа.

6.1.1. Следствие. *Всякий элемент β из группы точек $\mathcal{M}_L$ можно представить в виде*

$$\beta = H(b) +_F E_F(w_\beta)|_{X=\pi_L},$$

где $w_\beta(X) = \sum_i b_i X^i$, причем $b, b_i \in \mathcal{O}_T$, а индекс i пробегает значения между 1 и $q^m e_1$, взаимно простые с q^m. При этом след элементов b, b_i определен однозначно по модулю π^n.

Доказательство. Поскольку

$$E_F(\theta_i\pi_L^i) \in \mathcal{M}_L, E_F(\theta_i\pi_L^i) \equiv \theta_i\pi_L^i \bmod \pi_L^{i+1}$$

и

$$H(\theta) \in \mathcal{M}_L, H(\theta) \equiv \theta_0\pi_L^{q^m e_1} \bmod \pi_L^{q^m e_1+1},$$

применяя лемму 6.1 к системе

$$H(\theta), E_F(\theta_i\pi_L^i), 1 \leqslant i < q^m e_1, q^m \nmid i,$$

получим

$$\beta = \sum\nolimits_{F\, r}([\pi^r]H(\theta_r) +_F \sum\nolimits_{F\, i}[\pi^r]E_F(\theta_{i,r}\pi_L^i)) = H(b) +_F \sum\nolimits_{F\, i} E_F(b_i\pi_L^i).$$

6.1.2. Замечание. Учитывая, что примарный элемент $\omega(b)$ отличается от $H(b)$ на элемент, делящийся на изогению $[\pi^n]$, можно в каноническом разложении заменить $H(b)$ на $\omega(b)$.

Основываясь на идее, использованной в [6] для классических формальных групп Любина–Тейта, построим еще одну систему образующих, которая потребуется в дальнейшем для вычисления обобщенного символа Гильберта.

Напомним, что в классе изоморфных $F(X,Y)$ формальных групп есть базисная $F_0(X,Y)$ с изогенией

$$[\pi]_0 = \pi X + X^{q^m}.$$

Кроме того, для произвольных $\eta \in \mathcal{R}, 1 \leqslant \rho < mf_0$, где $q = p^{f_0}$, введем изоморфную $F(X,Y)$ обобщенную формальную группу Любина–Тейта $F_{\rho,\eta}(X,Y)$ с изогенией

$$[\pi]_{\rho,\eta}(X) = \pi X + X^{q^m} + \pi\eta X^{p^\rho}.$$

Соответствующие логарифмы обозначим $\lambda_0(X)$ и $\lambda_{\rho,\eta}(X)$. Тогда ряды

$$\varepsilon(X) = \lambda^{-1}(\lambda_0(X)), \varepsilon_{\rho,\eta}(X) = \lambda^{-1}(\lambda_{\rho,\eta}(X)),$$

задающие изоморфизмы из F_0 и $F_{\rho,\eta}$ в F, имеют целые коэффициенты.

6.2. Теорема. *Элементы*

$$\varepsilon(\theta\pi_L^i), \varepsilon_{\rho,\eta}(\theta\pi_L^i),$$

где $\theta, \eta \in \mathcal{R}, 1 \leqslant \rho < mf_0$, а индекс i пробегает все натуральные взаимно простые с p значения, меньшие $q^m e_1$, дают вместе с примарным элементом $\omega(b)$ полную систему образующих группы точек.

Доказательство. Очевидно, что утверждение достаточно проверить для случая $F = F_0$. Поскольку

$$\lambda_{\rho,\eta} \circ [\pi]_{\rho,\eta} = \pi\lambda_{\rho,\eta},$$

непосредственным вычислением убеждаемся, что

$$\varepsilon_{\rho,\eta}(X) \equiv X + \frac{\eta}{1 - \pi^{p^\rho - 1}} X^{p^\rho} \mod \deg(p^\rho + 1).$$

Следовательно,

$$\varepsilon_{\rho,\eta}(X) -_F X \equiv \frac{\eta}{1 - \pi^{p^\rho - 1}} X^{p^\rho} \mod \deg(p^\rho + 1)$$

и потому

$$\varepsilon_{\rho,\eta}(X) -_F \theta\pi_L^i \equiv \eta\theta^{p^\rho}\pi_L^{ip^\rho} \mod \pi_L^{ip^\rho+1}.$$

Остается применить лемму 6.1.

§7. Универсальный символ $\langle\, , \rangle_F$

Пусть k – локальное поле, $\mathcal{U}$ – полная топологическая абелева группа с хаусдорфовой топологией. Напомним (см. [6]), что символом на поле k называется непрерывное билинейное спаривание

$$c : k^* \times k^* \to \mathcal{U},$$

удовлетворяющее соотношению

$$c(x, 1-x) = 0$$

для любого $x \neq 1$.

Символ $c : k^* \times k^* \to \mathcal{U}$ называется универсальным, если для любого символа $\widetilde{c} : k^* \times k^* \to \widetilde{\mathcal{U}}$ существует непрерывный гомоморфизм

$$f : \mathcal{U} \to \widetilde{\mathcal{U}}$$

такой, что $f \circ c = \widetilde{c}$.

Построим спаривание $\langle\, , \rangle_F$ между мультипликативной группой L^* и группой точек $\mathcal{M}_L$ со значениями в группе корней изогении $[\pi^n]$.

Пусть первый аргумент спаривания имеет вид $\alpha = \pi_L^k \theta\varepsilon$, где

$$\theta \in \mathcal{R}, \varepsilon \in U_1,$$

причем $\varepsilon = 1 + a_1\pi_L + a_2\pi_L^2 + \dots, a_i \in \mathcal{R}$, а U_1 – множество главных единиц. Обозначим

$$\varepsilon(X) = 1 + a_1X + a_2X^2 + \dots, A(X) = X^a\theta\varepsilon(X).$$

Второй аргумент $\beta \in \mathcal{M}_L, \beta = b_1\pi_L + b_2\pi_L^2 + \dots$. Обозначим $\beta(X)$ ряд $b_1X + b_2X^2 + \dots$.

Введем функцию

$$l_m(\varepsilon(X)) = \left(1 - \frac{\Delta^m}{q^m}\right) \log \varepsilon(X),$$

где $\log(1+X) = \sum_{i\geqslant 1}(-1)^{i-1}\frac{X^i}{i}$. Она определена для любого степенного ряда $\varepsilon(X)$ с коэффициентами из кольца целых абсолютного подполя инерции поля L, который начинается с 1. Введем также функцию

$$l_F(\beta(X)) = \left(1 - \frac{\Delta^m}{\pi}\right) \lambda(\beta(X)),$$

определенную для любого степенного ряда $\beta(X)$ без свободного члена с коэффициентами из кольца целых поля инерции расширения L/K.

Формула для спаривания такова:

$$\langle \alpha, \beta \rangle_F = [\mathrm{tr}_{T/T_m} \gamma_{\alpha,\beta}](\xi),$$

где $\gamma_{\alpha,\beta} = \mathrm{res}\, \Phi_{\alpha,\beta}(X)/s(X)$, а ряд $\Phi_{\alpha,\beta}$ задается в виде

$$\Phi_{\alpha,\beta}(X) = \frac{l_F(\beta)}{A}\frac{dA}{dX} - l_m(\varepsilon)\frac{d}{dX}\frac{\Delta^m}{\pi}\lambda(\beta)$$

(ряд $s(X)$ определен в начале п. 5).

Легко видеть, что $\Phi_{\alpha,\beta}(X) \in \mathcal{O}_T\{\{X\}\}$, где

$$\mathcal{O}_T\{\{X\}\} = \left\{ \sum_{i\in\mathbb{Z}} d_i X^i, d_i \in \mathcal{O}_T, \lim_{i\to-\infty} d_i = 0 \right\}.$$

Аналогично случаю классических формальных групп Любина–Тейта (см. [3]) доказывается, что для любого нечетного простого p данное спаривание билинейно, инвариантно относительно выбора простого элемента π_L и не зависит от способа разложения элементов в ряды по π_L. Более того, оно является универсальным символом для обобщенной формальной группы Любина–Тейта при всех $p \neq 2$.

§8. Явная форма обобщенного символа Гильберта

И, наконец, докажем явную формулу обобщенного символа Гильберта для обобщенных формальных групп Любина–Тейта.

8.1. Теорема. *При всех нечетных простых p для любых $\alpha \in L^*, \beta \in \mathcal{M}_F$ имеет место формула*

$$(\alpha, \beta)_F = [\mathrm{tr}\, \gamma](\xi),$$

где

$$\gamma = \mathrm{res}_X \left(\frac{l_F(\beta)}{A}\frac{dA}{dX} - l_m(\varepsilon)\frac{d}{dX}\frac{\Delta^m}{\pi}\lambda(\beta) \right) / s(X)$$

(обозначения здесь совпадают с введенными в пункте 7).

Доказательство. Проверим, что для образующих базиса из теоремы 6.2 верны формулы

$$(\pi_L, \varepsilon(\theta\pi_L^i))_F = 0, (\pi_L, \varepsilon_{\rho,\eta}(\theta\pi_L^i))_F = 0.$$

Известно, что $(\alpha, \beta)_F = 0$ тогда и только тогда, когда элемент α является нормой в расширении L, полученном делением β на изогению $[\pi^n]$. Поскольку $[\pi^n]_{\rho,\eta}$ является унитарным многочленом, для символа

Гильберта формальной группы $F_{\rho,\eta}$ имеет место равенство $(\alpha,\alpha)_{F_{\rho,\eta}} = 0$ при $\alpha \in \wp_L$. Тогда

$$\varepsilon_{\rho,\eta}((\alpha,\alpha)_{F_{\rho,\eta}}) = (\alpha, \varepsilon_{\rho,\eta}(\alpha))_{F_0} = 0,$$

что и дает нужный результат.

Кроме того, аналогично [6] можно доказать, что

$$\langle \pi_L, \varepsilon(\theta\pi_L^i)\rangle_F = 0, \langle \pi_L, \varepsilon_{\rho,\eta}(\theta\pi_L^i)\rangle_F = 0.$$

Поскольку спаривание $\langle\,,\,\rangle_F$ не зависит от разложения элементов группы точек в степенные ряды по простому элементу π_L, разложим β по базису из 6.2. Только что доказанные формулы и равенство

$$(\pi_L, \omega(a))_F = \langle \pi_L, \omega(a)\rangle_F = [\mathrm{tr}\, a](\xi)$$

дают формулу

$$(\pi_L, \beta)_F = \langle \pi_L, \beta\rangle_F$$

для всех $\beta \in \mathcal{M}_F$.

Теперь проверим, что

$$(\varepsilon, \beta)_F = \langle \varepsilon, \beta\rangle_F,$$

где $\beta \in \mathcal{M}_F$, а первый аргумент является главной единицей. Легко видеть, что

$$\begin{aligned}\langle \varepsilon, \beta\rangle_{\pi_L} = \langle \pi_L\varepsilon, \beta\rangle_{\pi_L} -_F \langle \pi_L, \beta\rangle_{\pi_L} = \langle \pi_L\varepsilon, \beta\rangle_{\pi_L\varepsilon}\\ -_F \langle \pi_L, \beta\rangle_{\pi_L} = (\pi_L\varepsilon, \beta)_F -_F (\pi_L, \beta)_F = (\varepsilon, \beta)_F,\end{aligned}$$

где индекс в спаривании $\langle , \rangle$ указывает, при помощи какого элемента оно построено.

И, наконец, для общего случая по свойствам спариваний имеем

$$\langle \alpha, \beta\rangle_F = [k]\langle \pi_L, \beta\rangle_F +_F \langle \varepsilon, \beta\rangle_F = [k](\pi_L, \beta)_F +_F (\varepsilon, \beta)_F = (\alpha, \beta)_F,$$

что и доказывает теорему.

8.1.1. Замечание. В частности, из полученного равенства следует, что обобщенный символ Гильберта является универсальным на группе точек обобщенной формальной группы Любина–Тейта.

Случай $p = 2$ для классической формальной группы Любина–Тейта подробно разобран в работах [4] и [5]. Применив результат к обобщенной формальной группе Любина–Тейта (которую есть смысл рассматривать лишь при $m > 1$), получаем следующее утверждение.

8.2. Теорема. *Если $p = 2$ и K разветвлено над $\mathbb{Q}_p$, явная формула для обобщенного символа Гильберта имеет тот же вид, что и при нечетном p.*

Если же $p = 2$ и K неразветвлено над $\mathbb{Q}_p$, то имеет место формула

$$(\alpha, \beta)_F = [\operatorname{tr}\gamma](\xi),$$

где

$$\gamma = \operatorname{res}_X \left(\frac{l_F(\beta)}{A} \frac{dA}{dX} - l_m(\varepsilon) \frac{d}{dX} \frac{\Delta^m}{\pi} \lambda(\beta) \right) / s(X) + \frac{2}{\pi} \frac{d}{dX} \frac{\Delta^m}{q^m} \Phi^{(1)}_{\alpha,\beta}(X)$$

и

$$\Phi^{(1)}_{\alpha,\beta}(X) = a l_F(\beta) + \frac{(1 + \delta + \delta^2 + \dots)(l_F(\varepsilon))}{A^{-1}(\alpha A)} \frac{d\lambda(\beta)}{dX}.$$

Здесь $\alpha = \pi^a \theta \varepsilon$, а δ – автоморфизм Фробениуса абсолютного подполя инерции поля K.

Литература

1. M. Hazewinkel, *Formal groups and applications.* N-Y., Academic press (1978), 573.
2. J. Lubin, J. Tate, *Formal complex multiplication in local fields.* — Ann. Math. (2), **81**, No. 2 (1985), 380–387.
3. С. В. Востоков, *Норменное спаривание в формальных модулях.* — Изв. АН СССР, сер. мат. **45**, No. 5 (1981), 985–1014.
4. С. В. Востоков, *Символ Гильберта для формальных групп Любина–Тейта. I.* — Зап. научн. семин. ЛОМИ **114** (1982), 77–95.
5. С. В. Востоков, И. Б. Фесенко, *Символ Гильберта для формальных групп Любина–Тейта. II.* — Зап. научн. сем. ЛОМИ **132** (1983), 85–96.
6. С. В. Востоков, *Символы на формальных группах.* — Изв. АН СССР, сер. мат. **45**, No. 5 (1981), 9–23.
7. С. В. Востоков, *Явная форма закона взаимности.* — Изв. АН СССР, сер. мат. **42**, No. 6 (1978), 1288–1321.
8. К. Ивасава, *Локальная теория полей классов.* М., Мир (1983), 180.
9. А. И. Мадунц, *О сходимости рядов над локальными полями.* — Труды Санкт-Петербургского мат. общ. **3** (1995), 260–282.
10. И. Р. Шафаревич, *Общий закон взаимности.* — Матем. сб. **26(68)**, No. 1 (1950), 113–146.

Madunts A. I., Vostokova R. P. Formal modules for generalized Lubin–Tate groups.

We study generalized Lubin–Tate formal groups: their structure, the ring of endomorphisms of the point group. We investigate the primary elements and prove an explicit formula for the generalized Hilbert symbol.

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия
E-mail: madunts@mail.ru

Балтийский университет (военмех)
E-mail: rvostokova@yandex.ru

Поступило 7 сентября 2015 г.