ГЛАВА I

ЯВНАЯ ФОРМУЛА ДЛЯ ОБОБЩЕННОГО СИМВОЛА ГИЛЬБЕРТА В ЧИСЛОВОМ ЛОКАЛЬНОМ ПОЛЕ С ЧЕТНОЙ ХАРАКТЕРИСТИКОЙ ПОЛЯ ВЫЧЕТОВ

Пусть $F(X,Y)$ - формальная группа Любина-Тэйта, определенная над кольцом целых элементов $\mathcal{O}_0$ поля k_0, являющегося конечным расширением поля $\mathbb{Q}_2$. Для конечного расширения k поля k_0 на максимальном идеале этого поля с помошью формальной группы определяется структура $\mathcal{O}_0$ -модуля. Если корни изогении $[\pi_0^n]$ содержатся в поле k, то корректно определяется обобшенный символ Гильберта, являюшийся спариванием на $k^* \times F(\wp)$. В частном случае мультипликативной формальной группы обобшенный символ Гильберта совпадает с символом норменного вычета. В первой главе решается задача нахождения конструктивной формулы для обобшенного символа Гильберта через разложение элементов поля в ряд по локальной униформизуюшей. В случае $\mathrm{char}\, k \neq 2$ явная формула была получена С.В.Востоковым ([5],[6],[7]). Для этого вводится вспомогательное спаривание $\langle \alpha,\beta \rangle_F$, определяемое формулой $[\mathrm{tr}\,\mathrm{res}\,\Phi_{\alpha,\beta}/s](3)$ где $\Phi_{\alpha,\beta}$ - ряд, зависяший от разложения элементов $\alpha \in k^*$, и $\beta \in F(\wp)$ в ряд по локальной униформизуюшей. Устанавливается инвариантность относительно выбора простого элемента и независимость относительно разложения в ряд по простому элементу введенного спаривания, что, наряду со знанием структуры формального модуля позволяет доказать совпадение этого спаривания с символом Гильберта.

В случае $\mathrm{char}\, k = 2$, который рассматривается в первой главе, формула для спаривания значительно усложняется, она выглядит так: $[\operatorname{tr}\operatorname{res}(\Phi_{\alpha,\beta}+\tilde{\Phi}_{\alpha,\beta})\chi/s](\zeta)$, где $\tilde{\Phi}_{\alpha,\beta}$ - добавочный ряд, χ - многочлен (см. §6-§8). Доказательство инвариантности и независимости требует проведения большого объема вычислений, многие из которых собраны в § 4. В § 3 излагаются сведения о коэффициентах логарифма формальной группы Любина-Тэйта определенного вида, в § 5 рассмотрены арифметические вопросы строения формального модуля $F(\rho)$. Формулы для спаривания различаются в следующих трех подслучаях: I) расширение $k_0/\mathbb{Q}_2$ имеет степень инерции большую единицы; 2) $k_0=\mathbb{Q}_2$; 3) расширение $k_0/\mathbb{Q}_2$ вполне разветвлено. Доказательство требуемых свойств спариваний проводится соответственно в §6, §7 и § 8. В § 9 проверяется невырожденность этих спариваний и в случае мультипликативной формальной группы указывается связь с имеющимися частными формулами для символа Гильберта.

§ I. Основные обозначения и определения

$p=2$

k_0 - конечное расширение $\mathbb{Q}_2$, $\mathcal{O}_0$ - кольцо целых k_0

π_0 - простой элемент в k_0.

k - конечное расширение поля k_0.

π - простой элемент в k

ρ - максимальный идеал кольца целых поля k

e - индекс ветвления расширения k/k_0

e_0 - индекс ветвления расширения $k_0/\mathbb{Q}_2$

T - подполе инерции в расширении k/k_0, $\mathcal{O}$ - кольцо целых элементов поля T

T' – абсолютное подполе инерции поля k

$\mathfrak{o}'$ – кольцо целых элементов поля T'

$q=p^f$, f – степень инерции k_0/Q_2

R – мультипликативная система представителей поля вычетов в поле k

Δ – автоморфизм Фробениуса в T/k_0

S – автоморфизм Фробениуса в T'/Q_2

v – показатель в поле k с условием $v(\pi)=1$.

Через $\mathfrak{o}\{\{X\}\}$ обозначается кольцо рядов $\sum a_i X^i$ с коэффициентами из $\mathfrak{o}$, удовлетворяющих условию: $v(a_i)\to+\infty$ при $i\to-\infty$.

Сравнение $\varphi\equiv\psi \mod \deg t$ означает, что коэффициенты при степенях, меньших t, совпадают у рядов $\varphi,\psi\in\mathfrak{o}\{\{X\}\}$.

Сравнение $\varphi\equiv\psi \mod (\deg t, \pi_0^r)$ означает, что эти же коэффициенты сравнимы по $\mod \pi_0^r$.

Действие автоморфизмов Фробениуса распространяется на ряды:

$$\varphi^S=\left(\sum a_i X^i\right)^S=\sum a_i^S X^{pi} \quad \text{для } \varphi\in\mathfrak{o}'\{\{X\}\},$$

$$\psi^\Delta=\left(\sum b_i X^i\right)^\Delta=\sum b_i^\Delta X^{qi} \quad \text{для } \psi\in\mathfrak{o}\{\{X\}\}.$$

Пусть $\mathcal{F}_{\pi_0}$ – множество степенных рядов из кольца $\mathfrak{o}_0[[X]]$, удовлетворяющих условиям:

$$f(X)\equiv\pi_0 X \mod \deg 2, \quad f(X)\equiv X^q \mod \pi_0 .$$

Над кольцом $\mathfrak{o}_0$ существует единственная формальная группа такая, что ряд $f(X)$ является ее эндоморфизмом, она называется формальной группой Любина-Тэйта (см., например, [12]). Эндоморфизм $f(X)$ обозначается через

$$[\pi_0](X)=\pi_0 X+X^q+\pi_0\sum_{i\geq 2} a_i X^i\ ,\quad a_i\in\mathcal{O}_0\ .$$

На максимальном идеале $\wp$ вводится структура $\mathcal{O}_0$ -модуля $F(\wp)$ с помощью формальной группы $F(X,Y)$:

$$\alpha +_F \beta = F(\alpha,\beta)$$
$$a\alpha = [a](\alpha)\ ,\qquad \alpha,\beta\in\wp,\ a\in\mathcal{O}_0\ ,$$

где $[a](X)$ - ряд с целыми коэффициентами, являющийся эндоморфизмом формальной группы, соответствующий элементу a.

Если $\lambda(X)$ - логарифм формальной группы, то

$$F(X,Y)=\lambda^{-1}(\lambda(X)+\lambda(Y))$$
$$[a](X)=\lambda^{-1}(a\lambda(X))\ ,\quad a\in\mathcal{O}_0\ .$$

На поле k накладывается условие: все корни изогении $[\pi_0^h]$ содержатся в поле k.

Обобщенный символ Гильберта определяется на элементах $\alpha\in k^*,\ \beta\in F(\wp)$ по формуле

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

где $[\pi_0^h](\rho)=\beta\ ,\ \sigma_\alpha\in Gal(k^{ab}/k)$ соответствует элементу α в силу локальной теории полей классов. В случае мультипликативной формальной группы получается обычный норменный символ Гильберта. Обобщенный символ Гильберта является билинейным и норменным по первому аргументу:

$$(\alpha,\beta)_F=0 \iff \alpha\in Nk(\rho)\ ,\quad \text{где}\ \ [\pi_0^h](\rho)=\beta\ .$$

Большую роль в построении спаривания будут играть функции $\ell, E, \ell_m, \ell_F, E_F$. Для их определения воспользуемся следуюшим утверждением (см. [6], лемма 3): если F_1 и F_2 – две формальные группы Любина-Тэйта из класса $\mathcal{F}_{\pi_0}$ и λ_1, λ_2 – их логарифмы, то ряды $\lambda_1^{-1} \circ \lambda_2$ и $\lambda_2^{-1} \circ \lambda_1$ имеют целые коэффициенты из кольца $\mathcal{O}_0$ и осуществляют изоморфизм F_1 и F_2. В классе изоморфных между собой формальных групп Любина-Тэйта существует формальная группа F_a, логарифмом которой является функция Артина-Хассе $\lambda_a(X) = X + \frac{X^q}{\pi_0} + \frac{X^{q^2}}{\pi_0^2} + \dots$ (см. также § 3). Значит, ряд $\lambda^{-1} \circ \lambda_a$ имеет целые коэффициенты, обозначим его через $\mathcal{E}(X)$.

Пусть $\mathcal{H}_F$ – модуль кривых Картье, т.е. $\mathcal{O}_0$ – модуль степенных рядов без свободного члена с коэффициентами из $\mathcal{O}$, в котором

$$\varphi(X) +_F \psi(X) = F(\varphi, \psi),$$

$$a\varphi = [a](\varphi), \ a \in \mathcal{O}_0,$$

([25]).

Определим функции $E_F : X\mathcal{O}[[X]] \longrightarrow \mathcal{H}_F$ и $\ell_F : \mathcal{H}_F \longrightarrow X\mathcal{O}[[X]]$, являющиеся гомоморфизмами $\mathcal{O}_0$ – модулей, формулами:

$$E_F(\varphi) = \lambda^{-1}\left(\left(1 + \frac{\Delta}{\pi_0} + \frac{\Delta^2}{\pi_0^2} + \dots\right)(\varphi)\right)$$

$$\ell_F(\psi) = \left(1 - \frac{\Delta}{\pi_0}\right)(\lambda(\psi))$$

Действительно, ввиду формальной аддитивности функции E_F, значение $E_F(\varphi) \in \mathcal{H}_F$, так как

$$E_F(\theta X^m) = \mathcal{E}(\theta X^m), \quad \text{если } \theta \in \mathcal{R} \tag{I}$$

Далее, $\ell_F(\psi)$ также является рядом с целыми коэффициентами (см. § 3) и легко проверяется, что функции E_F и ℓ_F осуществляют взаимно обратные изоморфизмы между аддитивным θ_0 -модулем $X\theta[[X]]$ и θ_0 -модулем $\mathcal{H}_F$.

В случае мультипликативной формальной группы $F(X,Y) = X+Y+XY$ получаются функция Шафаревича E (см. [22]) и функция ℓ :

$$E: X\theta'[[X]] \to 1+X\theta'[[X]], \quad \ell: 1+X\theta'[[X]] \to X\theta'[[X]],$$

$$E(\varphi) = \exp\left(\varphi + \frac{\varphi^{\delta}}{p} + \frac{\varphi^{\delta^2}}{p^2} + \ldots\right),$$

$$\ell(\psi) = \left(1 - \frac{\delta}{p}\right)(\log(\psi)) .$$

Для $\varepsilon \in 1+X\theta[[X]]$ введем еше функцию ℓ_m:

$\ell_m(\varepsilon) = \left(1-\frac{\Delta}{q}\right)(\log(\varepsilon(X)))$, ее значения уже не обязательно являются рядами с целыми коэффициентами, но если $\varepsilon \in 1+X\theta'[[X]]$, то

$$p^{f-1}\ell_m(\varepsilon) = (p^{f-1} + p^{f-2}\delta + \ldots + \delta^{f-1})\,\ell(\varepsilon), \tag{2}$$

значит, ряд $p^{f-1}\ell_m(\varepsilon)$ имеет целые коэффициенты.

Определим, наконец, для $\varepsilon \in 1+X\theta'[[X]]$ функцию

$$\sigma(\varepsilon) = (1 + \delta + \delta^2 + \ldots)\,\ell(\varepsilon),$$

для $\beta \in X\theta[[X]]$ функцию

$$\sigma_F(\beta) = (1+\Delta+\Delta^2+\ldots)\,\ell_F(\beta).$$

§ 2. Ряды $s_m(X)$ и многочлен $\chi(X)$.

Пусть $[\pi_0]$ – эндоморфизм формальной группы F, тогда для $\alpha \in \rho$ справедливы следующие сравнения: (см.[6])

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

$$[\pi_0](\alpha) \equiv \pi_0 \alpha \mod \pi^{i+e+1} \quad , \text{ если } v(\alpha) = i > e_1 ; \qquad (3)$$

$$[\pi_0](\alpha) \equiv \pi_0 \alpha + \alpha^q \mod \pi^{qe_1+1} \quad \text{ если } v(\alpha) = i = e_1 ;$$

где $e_1 = e/q-1$, определим также $e_m = e/(q-1)q^{m-1}$.

Пусть ζ – первообразный корень изогении $[\pi_0^n]$, тогда из приведенных формул следует $v(\zeta) = e_n$.

Пусть $\zeta = c_0 \pi^{e_n} + c_1 \pi^{e_n+1} + \ldots$ – разложение ζ в ряд по униформизующей π с коэффициентами из θ, тогда определены ряды

$$z(X) = c_0 X^{e_n} + c_1 X^{e_n+1} + \ldots ,$$

$$S_m(X) = [\pi_0^m](z(X))$$

Ряд $S_n(X)$ будем обозначать через $s(X)$.
Легко получаются следующие сравнения (см.[6]):

$$s_m \equiv s_{m-1}^{\Delta} \mod \pi_0^m ,$$

$$s_m / s_{m-1} \equiv 0 \mod \deg 0 \qquad (4)$$

Это дает возможность определить ряды

$$u(X) = s(X)/s_{n-1}(X) , \quad h(X) = \frac{s_{n-1}^{\Delta} - s}{\pi_0^n}$$

При задании спаривания конструктивной формулой большое знаif $Y = \alpha(X) = X\eta\varepsilon(X)$ and $s(X) = s_Y(Y) = s_Y(\alpha(X))$, then the corresp. $\chi \equiv \chi_Y(\alpha(X)) \bmod (\pi_0^h, \deg$

BECAUSE: $h \equiv 0 \bmod_{2m+1} (\pi_0, \deg e)$ and

$\chi_{0,Y}^{\Delta_Y^2} + (1 + (\pi_0^{h-1} - 1) s_{h-1,Y}) \chi_{0,Y}^{\Delta_Y} + s_{h-1} \chi_{0,Y} - h_Y \equiv \pi_0 g_1(Y) + Y^e \underbrace{g_2(Y)}_{odd} \bmod (\pi_0, \deg 2e), \Rightarrow$

$\rho_Y(\alpha(X)) = \pi_0 g_1(\alpha(X)) + \eta^e X^e \underbrace{g_2(\eta X)}_{odd} \bmod (\pi_0, \deg 2e)$

чение имеет многочлен $\chi(X)$.

1. Для $q \geqslant 3$ положим $\chi(X) = 1$.

2. Если $e_0 = 1$, $p = q = 2$, то положим

$$\chi \equiv 1 + \pi_0^{h-1} \chi_0^{\Delta} \mod (\pi_0^h, \deg 2e),$$

где многочлен χ_0 задается по $\mod (\pi_0^{*}, \deg e)$ сравнением $(\chi_0 \in X\mathcal{O}[[X]])$:

$$\chi_0^{\Delta^2} + (1 + (\pi_0^{h-1} - 1) s_{h-1}) \chi_0^{\Delta} + s_{h-1} \chi_0 \equiv h \mod_{2m} (\pi_0, \deg 2e) \quad (5)$$

($\mod_{2m}$ означает, что сравнению по $\mod \pi_0$ должны удовлетворять коэффициенты при четных степенях правой и левой части). Таким образом, для $(e-1)$ коэффициента многочлена $\chi_0(X)$ выполняются $(e-1)$ линейных сравнений по $\mod \pi_0$. Так как при нулевой правой части в (5) решение этого сравнения единственно, то можно сделать вывод об однозначной определимости $\chi(X)$. При этом нужно воспользоваться очевидным следствием (4):

$$s_h(X) \equiv X^{q e_1} \mod (\pi_0, \deg (q e_1 + 1)) \quad (6)$$

Это же сравнение показывает, что условие (5) равносильно условию (7) (см.[8]):

коэффициенты ряда

$$G(\chi) = \frac{\chi^{\Delta^2} - (1 + \pi_0^{h-1} h^{\Delta}) \chi^{\Delta}}{s^{\Delta}} + \frac{\chi^{\Delta} - (1 + \pi_0^{2h-2} h^{\Delta}) \chi}{s} \quad (7)$$

при отрицательных степенях, кратных 4, делятся на π_0^h.

Если $h = 1$, то сравнение (5) упрощается:

$$\chi_0^{\Delta} + z\chi_0 \equiv z \mod_{2m} (\pi_0, \deg 2e) \quad (5')$$

if $Y = \alpha(X) = X\eta\varepsilon(X)$ and $s(X) = s_Y(Y) = s_Y(\alpha(X))$, then the corr. $\chi \equiv \chi_Y(\alpha(X)) \mod (\pi_0^n, \deg 2e)$
BECAUSE:
$g_Y(Y) = \text{LHS-RHS} \equiv \pi_0 g_1(X^2) + Y^{2e} \underset{\text{odd}}{g_2}(Y) \mod (\pi_0, \deg$
$\Rightarrow$
$g_Y(\alpha(X)) = \pi_0 g_1(\alpha(X)^2) + \eta^e X^{2e} \underset{\text{odd}}{g_2(\eta X)} \mod (\pi_0, \deg 4e)$

3. В случае $e_0 > 1,\ q = 2$ положим

$$\chi \equiv 1 + \pi_0^{n-1}\chi_0 \mod (\pi_0^n, \deg 2e),$$

где многочлен χ_0 задается по $\mod (\pi_0, \deg 2e)$ сравнением

$$\chi_0^{\Delta^2} + (1 + (\pi_0^{n-1} - 1)s)\chi_0^{\Delta} + s\chi_0 \equiv h^{\Delta} \mod_{2m} (\pi_0, \deg 4e) \qquad (8)$$

Так же как и ранее устанавливается однозначная определимость многочлена $\chi(X)$ и равносильность сравнения (8) условию (9):

$$G_T(\chi) = \frac{\chi^{\Delta^2} - (1 + \pi_0^{n-1}h^{\Delta})\chi^{\Delta}}{s^{\Delta}} + \frac{\chi^{\Delta} - (1 + \pi_0^{2n-2}h^{\Delta})\chi}{s} \equiv 0 \mod_{2m} (\pi_0^n, \deg 0) \qquad (9)$$

При $h = 1$ многочлен χ_0 определяется из более простого сравнения:

$$\chi_0^{\Delta} + s\chi_0 \equiv s \mod_{2m} (\pi_0, \deg 4e) \qquad (8')$$

Наконец, покажем, что из условия (9) следует сравнение (I0):

$$(\chi/s)^{\Delta} + \chi/s + \pi_0/s_{n-1} \equiv 0 \mod_{2(2m+1)} (\pi_0^n, \deg 0) \qquad (I0)$$

где $\mod_{2(2m+1)}$ означает, что сравнение $\mod \pi_0^n$ выполняется для коэффициентов с индексами вида $2(2m+1),\ m \in \mathbb{Z}$.

Для вывода импликации (9) $\Longrightarrow$ (I0) потребуются

ЛЕММА I. Многочлен χ_0, определенный в (8), удовлетворяет сравнению $\chi_0 \equiv h \mod_{2m+1} (\pi_0, \deg e)$.

ДОКАЗАТЕЛЬСТВО. Обозначим левую часть сравнения (8) через $H(\chi_0)$. Пусть

$$\chi_1 \equiv h + h^{\Delta} + h^{\Delta^2} + \ldots \mod \deg 2e$$

тогда многочлен $\chi_2 = \chi_0 - \chi_1$ удовлетворяет сравнению:

$$H(\chi_2) \equiv s\left(h + 2^{n-1}\left(h^{\Delta} + h^{\Delta^2} + \ldots\right)\right) \bmod_{2m} (\pi_0, \deg 4e)$$

Из вида $H(X)$ и сравнения (6) тогда следует

$$H(\chi_2) \equiv 0 \bmod_{2m} (\pi_0, \deg 2e)$$

и значит, $\chi_2 \equiv 0 \bmod (\pi_0, \deg e)$, поэтому

$$\chi_0 = \chi_1 + \chi_2 \equiv \chi_1 \equiv h \bmod_{2m+1} (\pi_0, \deg e)$$

ЛЕММА 2. Если $n > 1$, то

$$\pi_0^{n-1} \chi_0 \equiv \pi_0 s_{n-2} \bmod_{2m+1} (\pi_0^n, \deg e)$$

ДОКАЗАТЕЛЬСТВО. Из леммы I, а также определения s_m и h имеем

$$\pi_0^{n-1} \chi_0 \equiv s_{n-1} + s_{n-1}^2 / \pi_0 + \sum_{i \geq 2} a_i s_{n-1}^i \bmod_{2m+1} (\pi_0^n, \deg e)$$

Используя теперь сравнение (4) при $m = n-1$ получаем, что

$$\pi_0^{n-1} \chi_0 \equiv s_{n-1} \bmod_{2m+1} (\pi_0^n, \deg e)$$

Еще раз используя определение s_m находим, что

$$s_{n-1} \equiv \pi_0 s_{n-2} \bmod_{2m+1} (\pi_0^n, \deg e)$$

Из двух последних сравнений следует утверждение леммы.

Покажем теперь, что из (9) вытекает (IO). В случае $n=1$ ((8)) это следует из (8$'$). При $n > 1$ достаточно проверить, что

$$\pi_0^{n-1} h^{\Delta} \chi^{\Delta} / s^{\Delta} + \chi^{\Delta} / s \equiv \pi_0 / s_{n-1} \bmod_{2(2m+1)} (\pi_0^n, \deg 0)$$

а это сравнение сводится к

$n>1$: $(s^{\Delta} \equiv s_{n-1}^{\Delta^2} \bmod \pi_0^n)$

$$\frac{\chi^{\Delta}}{s^{\Delta}} + \frac{\chi}{s} - \frac{\pi_0^{n-1} h^{\Delta} \chi^{\Delta}}{s^{\Delta}} - \frac{\chi^{\Delta}}{s} \equiv \pi_0^{n-1}\left(\frac{\chi_0^{\Delta}}{s^{\Delta}} + \frac{\chi_0}{s} + \frac{h^{\Delta}}{s^{\Delta}} + \frac{\chi_0^{\Delta}}{s} + \left(\frac{\chi_0^{\Delta^2}}{s^{\Delta}}\right)\right) \equiv 0 \bmod_{2(2m+1)} (\pi_0^n, \deg 0)$$

$$\nabla \Rightarrow \frac{\pi_0^{n-1}\chi_0}{s_{n-1}} + \frac{\pi_0 s_{n-2}}{s_{n-1}} \equiv 0 \mod_{2m+1}(\pi_0^n, \deg 0) \quad \text{since } s_{n-1}^2 = (s_{n-2}^{\Delta} + \pi_0^{n-1}h)^2 \; *$$

$$\Rightarrow \frac{\pi_0^{n-1}h\chi}{s} + \frac{\chi}{s_{n-1}} - \frac{\pi_0}{s_{n-2}} \equiv \frac{\pi_0^{n-1}h\cancel{\chi}}{s} + \frac{1}{s_{n-1}} + \frac{\pi_0 s_{n-2}}{s_{n-1}} - \frac{\pi_0}{s_{n-2}} \mod_{2m+1}(\pi_0^n, \deg 0) \quad \text{and}$$

$$\cdot \; \frac{\pi_0^{n-1}h}{s} \equiv \frac{\pi_0^{n-1}h}{s_{n-1}^2} \underset{*}{\equiv} -\frac{s}{\pi_0 s_{n-1}^2} \equiv -\frac{1}{s_{n-1}} \mod_{2m+1}(\pi_0^n, \deg 0); \quad \frac{\pi_0 s_{n-2}}{s_{n-1}} - \frac{\pi_0}{s_{n-2}} = \frac{\pi_0(s_{n-2}^2 - s_{n-1})}{s_{n-2}s_{n-1}} \equiv \frac{-\pi_0^2}{s_{n-2}^{\Delta}} - \frac{\pi_0^2 \sum a_i s_{n-2}^{i-1}}{s_{n-2}^{\Delta}} \equiv 0 \mod_{2m+1}(\pi_0^n, \deg 0)$$

$$\nabla \; \left(\pi_0^{n-1}\chi_0 + \pi_0 s_{n-2}\right) s_{n-2}^{\Delta} \equiv 0 \mod_{2m+1}(\pi_0^n, \deg 2e),$$

последнее же есть немедленное следствие леммы 2.

§ 3. Логарифм формальной группы Любина-Тэйта

ПРЕДЛОЖЕНИЕ I. Ряд $\lambda(X) = X + c_2X^2 + \ldots$ с коэффициентами из кольца $\mathcal{O}_0$ является логарифмом формальной группы Любина-Тэйта тогда и только тогда, когда ряд $\left(1 - \frac{\Delta}{\pi_0}\right)\lambda(X)$ имеет целые коэффициенты.

ДОКАЗАТЕЛЬСТВО. I. Предположим, что ряд $\lambda(X) - \lambda(X^q)/\pi_0$ имеет целые коэффициенты, это означает, что $c_i \in \mathcal{O}_0$, если $q \nmid i$ и $c_i - \frac{c_{i/q}}{\pi_0} \in \mathcal{O}_0$ в противном случае. Тогда

$$\pi_0^r c_i \in \mathcal{O}_0, \quad \text{если} \quad i = q^r s, \; q \nmid s. \tag{II}$$

Рассмотрим в кольце $k_0[[X]]$ следующее уравнение:

$$\lambda(f(X)) = \pi_0 \lambda(X)$$

Оно имеет единственное решение - обозначим его через $f(X)$. Тогда $f(X) \equiv \pi_0 X \mod \deg 2$. Обозначая $f_i(X) = f(X)^i - X^{qi}$ получаем следующее соотношение:

$$\sum_{i \geq 1} c_i f_i(X) = \sum_{q \nmid i} \pi_0 c_i X^i + \sum_{q \mid i} \pi_0\left(c_i - \frac{c_{i/q}}{\pi_0}\right) X^i$$

Из сделанного предположения о ряде $\lambda(X)$ следует сравнение

$$\sum_{i \geq 1} c_i f_i(X) \equiv 0 \mod \pi_0$$

Покажем теперь, что

$$f_1(X) \equiv 0 \mod \pi_0$$

Для этого проверим, что если $f_1(X) \equiv 0 \mod (\pi_0, \deg m)$, то при $i \geq 2$ $c_i f_i(X) \equiv 0 \mod (\pi_0, \deg m+1)$

Действительно, если $i = q^r s$, $q \nmid s$, то запишем

$$c_i f_i(X) = \sum_{j>0} f_1(X)^j X^{q(i-j)} C_i^j c_i = \sum x_j$$

В случае $j \geq r+1$ ввиду (II) и предположения о $f_1(X)$ заключаем $x_j \equiv 0 \mod (\pi_0, \deg m+1)$. В случае $j \leq r$ легко проверить, что $C_i^j c_i \in \mathcal{O}_0$ и поэтому

$$x_j \equiv \pi_0^j \bar{f}_1(X)^j X^{q(i-j)} C_i^j c_i \equiv 0 \mod (\pi_0, \deg m+1),$$

где $f_1(X) \equiv \pi_0 \bar{f}_1(X) \mod \deg m.$

В результате, проводя индукцию по m, получаем, что $f_1(X) \equiv 0 \mod \pi_0$. Итак, установлено, что решение $f(X)$ удовлетворяет следующим условиям: $f(X) \in \mathcal{O}_0[[X]]$, $f(X) \equiv \pi_0 X \mod \deg 2$, $f(X) \equiv X^q \mod \pi_0$. Поэтому $f(X)$ является эндоморфизмом некоторой формальной группы Любина-Тэйта с логарифмом $\tilde{\lambda}(X)$, причем $\tilde{\lambda}(X)$ тоже удовлетворяет уравнению

$$\tilde{\lambda}(f(X)) = \pi_0 \tilde{\lambda}(X),$$

значит $\lambda = \tilde{\lambda}$.

2. Пусть $\lambda(X)$ - логарифм формальной группы Любина-Тэйта F. Из установленного только что результата следует, что ряд $\lambda_a(X) = X + \frac{X^q}{\pi_0} + \frac{X^{q^2}}{\pi_0^2} + \dots$ является логарифмом формальной группы Любина-Тэйта F_a. Поскольку F и F_a изоморф-

ны над $\mathcal{O}_0$ (см. [6], § 2), существует ряд $\psi(X) \in \mathcal{O}_0[[X]]$ такой, что $\lambda = \lambda_a \circ \psi$. Имеем:

$$\lambda_a \circ \psi - \frac{\Delta}{\pi_0}(\lambda_a \circ \psi) = \sum_{i \geq 0} \left(\frac{\psi(X)^{q^i}}{\pi_0^i} - \frac{\psi(X)^{q^{i-1}\Delta}}{\pi_0^i} \right) -$$

ряд с целыми коэффициентами, так как

$$\psi(X)^{q^i} \equiv \psi(X)^{q^{i-1}\Delta} \mod \pi_0^i$$

Значит, $\lambda(X) - \frac{\lambda(X^q)}{\pi_0} \in \mathcal{O}_0[[X]]$. Предложение доказано.

Из доказательства следует обоснование свойств функций E_F и ℓ_F, определенных в § I.

Возьмем в классе $\mathcal{F}_{\pi_0}$ формальную группу F_ρ с эндоморфизмом $[\pi_0]_\rho = \pi_0 X + \pi_0 X^{p^\rho} + X^q$, где $1 \leq \rho < f$, а если $\rho = 0$, то считаем $[\pi_0]_0 = \pi_0 X + X^q$. Пусть λ_ρ - логарифм формальной группы F_ρ. Положим

$$\ell_{F_\rho}(-X) = \left(1 - \frac{\Delta}{\pi_0}\right)\lambda_\rho(-X) = -X + c_2' X^2 + \ldots + c_m' X^m + \ldots$$

Формальные группы F_ρ играют большую роль в построении базиса формального модуля $F(\wp)$ (см. § 5) и явных вычислений значений спариваний, определенных в §§ 6-8. При этом будет использоваться информация о коэффициентах c_m'.

ЛЕММА 3 ([8]). Пусть $m = q^2 s$, где $q \nmid s$. Тогда $c_m' \equiv 0 \mod \pi_0^2$ за исключением следующих случаев:

$$q \geq p^2 : \quad c_q' \equiv \frac{2}{\pi_0} \mod \pi_0;$$

$$q = p, e_0 > 1 : \quad c_2' \equiv 1 \mod \pi_0, \; c_4' \equiv \pi_0 \mod \pi_0^2;$$

Кроме того, если $q \geq p^2$ и $q \nmid m$, то для $m \neq 1, p^\rho$

$$c_m' \equiv 0 \mod \pi_0,$$

если $q=p,\ e_0=1,\ p\nmid m,$ то

$$C_m^1 \equiv 1 \mod \pi_0$$

если $q=p,\ e_0>1,\ p\nmid m,$ то для $m\neq 1$

$$C_m^1 \equiv 0 \mod \pi_0 .$$

ДОКАЗАТЕЛЬСТВО. Указанные соотношения на коэффициенты логарифма доказываются индукцией по m с использованием (II) и следующего соотношения, вытекающего из определения λ_ρ :

$$(1-\pi_0^{m-1})c_m = \sum \frac{i!}{i_1!\, i_2!\,(i-i_1-i_2)!}\ \pi_0^{i_1+i_2-1} c_i$$

где суммирование ведется по $i_1, i_2,\ i\neq m$, удовлетворяющим условию $i_1+p^\rho i_2+q(i-i_1-i_2)=m$.

Доказательство леммы удобно проводить раздельно для случая $q\geq p^2$; $q=p=2, e_0=1$; $q=p=2, e_0>1$.
Подробный ход рассуждений см. в [8], § 4.

§ 4. Вспомогательные результаты.

В этом параграфе собраны утверждения, которые понадобятся при доказательстве инвариантности и независимости спариваний, определенных в §§ 6-8.

I°. Если $\varphi(X)\in \theta\{\{X\}\}$, то непосредственно проверяется, что

$$\operatorname{tr}\operatorname{res} X^{-1}\varphi^\Delta = \operatorname{tr}\operatorname{res} X^{-1}\varphi \tag{I2}$$

$$\frac{d}{dX}\varphi^\Delta = qX^{-1}\left(X\frac{d\varphi}{dX}\right)^\Delta \tag{I3}$$

$$\operatorname{tr}\operatorname{res}\frac{d}{dX}\frac{\Delta}{q}\varphi/s_i^{\Delta}=\operatorname{tr}\operatorname{res}\frac{d}{dX}\varphi/s_i\,, \tag{I4}$$

где res означает коэффициент при X^{-1}.

Из сравнения (4) и (I3) индукцией по m выводим, что

$$\frac{d}{dX}s_m\equiv\frac{d}{dX}\left(1/s_m\right)\equiv 0 \mod \pi_0^m \tag{I5}$$

Проверим, что если $\frac{q}{\pi_0}\varphi\in\mathfrak{o}\{\{X\}\}$ и $\frac{d\varphi}{dX}\in\mathfrak{o}\{\{X\}\}$, то

$$\operatorname{res}\frac{d\varphi}{dX}/s\equiv 0 \mod \pi_0^n \tag{I6}$$

Действительно, применяя (I3) и (I5), получаем

$$\operatorname{res}\frac{d\varphi}{dX}/s\equiv\operatorname{res}\frac{d\varphi}{dX}/s_{n-1}^{\Delta}=-\operatorname{res}\varphi\frac{d}{dX}\left(1/s_{n-1}^{\Delta}\right)=$$

$$=\operatorname{res}-q\varphi X\left(X^{-1}\frac{d}{dX}\left(1/s_{n-1}\right)\right)^{\Delta}\equiv 0 \mod \pi_0^n$$

В случае $e_0=1$, $\varphi\in\mathfrak{o}\{\{X\}\}$ из вида многочлена $\chi(X)$ аналогичными рассуждениями выводим, что

$$\operatorname{res}\frac{d\varphi}{dX}\chi/s\equiv 0 \mod \pi_0^n \tag{I7}$$

А в общем случае из (I6) и (I4) следует

$$\operatorname{tr}\operatorname{res}\pi_0\frac{d}{dX}\frac{\Delta}{q}\varphi\,\chi/s\equiv 0 \mod \pi_0^n \tag{I8}$$

Если φ и ψ - ряды с целыми коэффициентами, для которых выполняется сравнение

$$\varphi/s\equiv\psi/s \mod (\pi_0^n,\deg\hat{\mathfrak{o}})$$