Д. Г. Бенуа, С. В. Востоков, Норменное спаривание в формальных группах и представления Галуа,
Алгебра и анализ, 1990, том 2, выпуск 6, 69–97

Д.Г.Бенуа, С.В.Востоков

НОРМЕННОЕ СПАРИВАНИЕ В ФОРМАЛЬНЫХ ГРУППАХ И ПРЕДСТАВЛЕНИЯ ГАЛУА

Пусть $F(X,Y)$ - формальная однопараметрическая группа конечной высоты, заданная над кольцом целых неразветвленного расширения k_0 поля p-адических чисел. Для любого конечного расширения k/k_0, содержащего группу μ_F корней изогении F, определен символ Гильберта $(,)_F: k^* \times F(m) \to \mu_F$, где Fm - формальный модуль на максимальном идеале кольца целых поля k. В работе получена явная формула для символа $(,)_F$ и в качестве приложения этого результата вычислены представления группы Галуа локального поля в модулях Тэйта некоторых формальных групп.

Введение

1°. Пусть $F(X,Y)$ - однопараметрическая формальная группа, определенная над кольцом o_0 целых конечного расширения k_0 поля $\mathbb{Q}_p$ p-адических чисел. Предположим, что F имеет конечную высоту h. Тогда для каждого $n \in \mathbb{N}$ группа $\mu_{F,n}$ корней изогении $[p^n]$ изоморфна абелевой группе $(\mathbb{Z}/p^n\mathbb{Z})^{(h)}$.

Пусть k - конечное расширение поля k_0, содержащее группу $\mu_{F,n}$ для некоторого фиксированного n. Обозначим через m максимальный идеал кольца целых поля k. Тогда на m определена структура $F(m)$ формального $\mathbb{Z}_p$-модуля. Возьмем $\alpha \in k^\times$, $\beta \in F(m)$. Тогда найдется такой элемент γ из максимального идеала кольца целых сепарабельного замыкания $\bar{k}$ поля k, что $[p^n](\gamma)=\beta$. Положим

$$(\alpha,\beta)_{F,n} = \gamma^{\theta(\alpha)} - {}_F\gamma,$$

где $\theta: k^\times \to \mathrm{Gal}(k^{ab}/k)$ - отображение взаимности. (См. [10]). Легко проверяется, что $(,)_{F,n}$ является корректно определенным билинейным отображением

$$(,)_{F,n} : k^\times \times F(m) \longrightarrow \mu_{F,n}.$$

Важным свойством $(,)_{F,n}$ является норменность. Иначе говоря, $(\alpha,\beta)_{F,n}=0$ тогда и только тогда, когда α является нормой в расширении $k(\gamma)/k$.

Заметим, что если F - мультипликативная группа, то введенный символ является по существу символом Гильберта. Явная формула для него была получена С.В.Востоковым в терминах разложения элементов α и β по степеням униформизующей поля k (см. [2]).

В работах [3] и [4] С.В.Востоков обобщил этот результат на формальные группы Любина-Тэйта. Случай $p=2$ рассмотрен отдельно в работе [5]. Заметим также, что де Шали [13], используя другие методы, вычислил символ Гильберта для групп

Ключевые слова: кольцо целых локального поля, формальная группа, представление Галуа.

Любина-Тэйта в случае, когда k получено присоединением к полю k_0 корней изогении $[p^n]$.

Норменное спаривание в произвольной формальной группе рассматривалось В. А. Колывагиным [6]. Его результаты позволяют вычислить символ $(\alpha,\beta)_{F,n}$ при некоторых ограничениях на α и β, если известны определенные инварианты представления группы Галуа поля k_0 в модуле Тэйта формальной группы F.

В данной работе явно вычисляется символ $(,)_{F,1}$ для произвольной формальной группы конечной высоты над кольцом целых неразветвленного расширения поля $\mathbb{Q}_p$ ($p\neq 2$). В качестве приложения мы вычисляем представления группы Галуа поля k_0 в модулях Тэйта некоторых формальных групп.

В дальнейшем, для простоты, мы будем писать $(,)_F$ вместо $(,)_{F,1}$.

2^0. Напомним некоторые определения и результаты, относящиеся к формальным группам.

Для всякой формальной группы над o_0 существует степенной ряд $\lambda(X)\equiv X \bmod \deg 2$ с коэффициентами в поле k_0 такой, что

$$F(X,Y) = \lambda^{-1}\circ(\lambda(X)+\lambda(Y)),$$

где λ^{-1} – ряд, обратный к λ относительно операции $\circ$ подстановки ряда в ряд. $\lambda(X)=\sum_{m=1}^{\infty} c_m X^m$ называется логарифмом формальной группы F. Заметим, что для всякого $m\geq 2$ $c_m p^{m-2}$ является целым элементом кольца o_0 (см., например, [3]). Логарифм связывает аддитивную и формальную структуры, в частности для изогении $[p]$ имеет место равенство

$$\lambda\circ[p] = p\lambda.$$

Кроме того, если π_0 – униформизующая поля k_0 и формальная группа F имеет конечную высоту h, то

$$[p] \equiv \sum_{i=1}^{\infty} a_{ip^h} X^{ip^h} \bmod p,$$

причем $a_{p^h}\not\equiv 0 \bmod \pi_0$.

Введем оператор Δ, действующий на степенные ряды с коэффициентами в максимальном неразветвленном расширении поля $\mathbb{Q}_p$. Для каждого такого ряда

$$\varphi = \sum_{i=0}^{\infty} b_i X^i$$

положим

$$\varphi^{\Delta} = \sum_{i=0}^{\infty} b_i^{\mathrm{Fr}} X^{ip},$$

где Fr – абсолютный автоморфизм Фробениуса $\mathbb{Q}_p^{nr}/\mathbb{Q}_p$. Иногда, для удобства, мы будем писать $\Delta\varphi$ вместо φ^{Δ}. Мы будем также рассматривать суммы степеней оператора Δ с коэффициентами в $\mathbb{Q}_p^{nr}$. В частности, в нашей работе важную роль будут играть операторы $\mathcal{A}(\Delta)$ вида

$$\mathcal{A}(\Delta) = \alpha_1\Delta + \alpha_2\Delta^2 + \ldots + \alpha_h\Delta^h,$$

где $\alpha_1,\alpha_2,\ldots,\alpha_h$ принадлежат кольцу o_0, неразветвленному над $\mathbb{Z}_p$, причем $\alpha_1\equiv\alpha_2\equiv\ldots\equiv\alpha_h\equiv 0 \bmod p$, а α_h – единица кольца o_0.

Используя оператор Δ, можно следующим образом сформулировать результат Хонды о классификации формальных групп (см. [11], предл. 3.5).

1. Ряд

$$\lambda_a = (1 - \frac{\mathcal{A}(\Delta)}{p})^{-1}(X)$$

является логарифмом некоторой формальной группы F_a над o_0, которую мы будем называть формальной группой Артина-Хассе (в работе Хонды такие группы назывались p-типическими).

2. В классе изоморфных формальных групп высоты h существует формальная группа Артина-Хассе.

3. Разным операторам $\mathcal{A}(\Delta)$ соответствуют разные классы изоморфных формальных групп.

3^0. Введем основные обозначения работы.

k_0 - неразветвленное расширение поля p-адических чисел,

o_0 - кольцо целых поля k_0,

F - формальная группа высоты h над кольцом o_0,

μ_F - группа корней изогении $[p]$,

$\xi_1, \ldots, \xi_h$ - фиксированный базис μ_F,

k - конечное расширение поля k_0, содержащее группу μ_F,

π - униформизующая поля k,

ν - нормирование поля k такое, что $\nu(\pi)=1$,

m - максимальный идеал кольца целых поля k,

$F(m)$ - формальный $\mathbb{Z}_p$-модуль,

o - кольцо целых максимального неразветвленного подрасширения поля k,

o_1 - неразветвленное расширение $\mathbb{Z}_p$ степени h,

$\mathfrak{K}, \mathfrak{K}_1$ - системы Тейхмюллера колец o и o_1 соответственно

$tr: o \to \mathbb{Z}_p$, $tr_1: o_1 \to \mathbb{Z}_p$ -операторы следа,

e - индекс ветвления $k/\mathbb{Q}_p$,

$$q = p^h, \qquad e_1 = \frac{e}{q-1}, \qquad e_n = e_1/q^{n-1}.$$

Заметим, что $o_1 \subset o$ (см. доказательство леммы 1.2).

4°. Функции E_F и ℓ_F. Если F - формальная группа высоты h над неразветвленным кольцом o_0 и F_a - изоморфная ей группа Артина-Хассе, то ряд $\lambda_0^{-1} \circ \lambda_a$, где λ и λ_a - логарифмы групп F и F_a соответственно, осуществляет изоморфизм между ними и, значит, имеет целые коэффициенты. В конструкции спаривания существенную роль будут играть две взаимно-обратные функции, определенные на множестве степенных рядов из кольца $o^{nr}[[X]]$ без свободного члена

$$E_F(\varphi) = \lambda^{-1} \circ (1 - \frac{\mathcal{A}(\Delta)}{p})^{-1}(\varphi),$$

$$\ell_F(\varphi) = (1 - \frac{\mathcal{A}(\Delta)}{p})(\lambda(\varphi)),$$

где $\varphi \in X o^{nr}[[X]]$.

Для групп Любина-Тэйта эти функции рассматривались в работе [3]. Так же, как

и в § 2 этой работы, проверяются следующие утверждения относительно функций E_F и ℓ_F:

1. Функции E_F и ℓ_F задают степенные ряды с целыми коэффициентами без свободного члена.

2. Имеют место равенства

$$E_F(\varphi+\psi) = E_F(\varphi) +_F E_F(\psi), \quad \ell_F(\varphi+_F\psi) = \ell_F(\varphi) + \ell_F(\psi),$$

$$E_F(a\varphi) = [a] \circ E_F(\varphi), \quad \ell_F([a] \circ \varphi) = a\ell_F(\varphi), \quad a\in\mathbb{Z}_p,$$

$$E_F(\ell_F(\varphi)) = \ell_F(E_F(\varphi)) = \varphi,$$

где $\varphi,\psi\in X\mathcal{O}^{nr}[[X]]$.

4. Если φ - степенной ряд порядка r из кольца $\mathcal{O}^{nr}[[X]]$, то

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

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

$$E_F(a\ell_F(\varphi))|_{X=\pi} \equiv a\varphi(\pi) \bmod \pi^{r+1},$$

где $a\in\mathcal{O}^{nr}$.

Нам потребуется еще функция ℓ_F для мультипликативной формальной группы, а именно положим

$$\ell(\varphi) = \frac{1}{p} \log \varphi^p/\varphi^\Delta,$$

где $\varphi\in X\mathcal{O}^{nr}[[X]]$. Известно (см. [2]), что ряд имеет целые коэффициенты.

5°. В этом пункте мы сформулируем основные результаты работы. Пусть F - формальная группа высоты h над неразветвленным кольцом $\mathcal{O}_0$, λ - логарифм формальной группы F, а $\lambda_a(X)=(1-\frac{a(\Delta)}{p})^{-1}(X)$ - логарифм изоморфной ей формальной группы Артина-Хассе (см. 2°).

Если мы возьмем элемент α из поля k и разложим его по степеням униформизующей π с коэффициентами из кольца $\mathcal{O}$, то этому разложению соответствует ряд из кольца рядов Лорана $\mathcal{O}\{X\}$, который мы будем чаще всего обозначать той же буквой $\alpha(X)$, таким образом $\alpha(\pi)=\alpha$.

Пусть $\xi_1,\dots,\xi_h$ - образующие группы μ_F и $z_1(X)\in\mathcal{O}[[X]]$ - степенной ряд, полученный из разложения корня ξ_1 по степеням униформизующей π с коэффициентами из кольца $\mathcal{O}$, таким образом, $z_1(\pi)=\xi_1$. При этом мы будем считать, что порядок ряда z_1 равен e_1.

Положим

$$s_1(X) = [p](z_1).$$

Будет доказано (см. лемму 1.2), что

$$\xi_j \equiv \theta_{j1}\xi_i \bmod \pi^{2e_1},$$

где элементы $\theta_{i1},\dots,\theta_{ii}=1,\dots,\theta_{hi}$ образуют базис $\mathbb{Z}_p$-модуля $\mathcal{O}_1$ для каждого $i=1,2,\dots,h$.

Кроме того, мы проверим, что в кольце $\mathcal{O}_1$ найдутся единственные элементы $v_1,\dots,v_h$ такие, что

$$\mathrm{tr}_1(v_i\theta_{ji}) = 0, \quad \text{если } i\neq j,$$

$$\mathrm{tr}_1(v_1\theta_{i1}) = 1.$$

Возьмем элемент α из мультипликативной группы k^x и β из формального модуля $F(\mathfrak{m})$. Пусть

$$\alpha = \theta\pi^a + a_1\pi^{a+1} + \dots, \qquad \beta = b_1\pi + b_2\pi^2 + \dots$$

где $a_i, b_j \in o$, и мы будем считать, чтобы не усложнять формулу, что первый коэффициент θ у элемента α взят из системы Тейхмюллера $\mathfrak{K}$.

Построим спаривание

$$\langle , \rangle_F : k^x \times F(\mathfrak{m}) \longrightarrow \mu_F$$

по следующей формуле

$$\langle \alpha, \beta \rangle_F = \sum_{i=1}^{h} {}_{(F)}[\mathrm{tr}(v_i\gamma_i)](\xi_i),$$

где $\gamma_i = \mathrm{res}\ \Phi_{\alpha,\beta}/s_i$, и при этом

$$\Phi_{\alpha,\beta} = \frac{1}{\alpha_h}\, \ell_F(\beta)\alpha^{-1}d\alpha - \frac{1}{q}\, \ell(\alpha)^{\Delta^{h-1}}\, d\lambda^{\Delta^h}(\beta).$$

Замечание. Для упрощения записи мы пишем $d\varphi$ вместо $\dfrac{d\varphi(X)}{dX}$.

Теорема 1. *Пусть $p \neq 2$. Спаривание $\langle , \rangle_F$ совпадает с символом Гильберта $(,)_F$ и тем самым дает для последнего явную формулу.*

Используя эту теорему, можно получить основные результаты работы [12]. В частности, справедливо следующее утверждение.

Теорема 2. *Пусть $H = \{g \in \mathrm{GL}_h(\mathbb{Z}_p) \mid g \equiv 1 \bmod p\}$ - подгруппа полной линейной группы $\mathrm{GL}_h(\mathbb{Z}_p)$. Предположим, что h делится на степень расширения $k_0/\mathbb{Q}_p$. Для того чтобы H содержалась в образе представления*

$$\rho_F : \mathrm{Gal}\ (\overline{k}_0/k_0) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_F) \simeq \mathrm{GL}_h(\mathbb{Z}_p)$$

группы Галуа поля k_0 в модуле Тэйта T_F формальной группы F, необходимо и достаточно, чтобы элементы $\alpha_1, \alpha_2, \dots, \alpha_{h-1} \not\equiv 0 \bmod p^2$.

6^0. Сформулированные выше теоремы доказываются в последних двух параграфах 6 и 7. В первом параграфе доказывается ряд вспомогательных результатов об изогениях.

Следующий параграф содержит конструкцию специального базиса формального модуля $F(\mathfrak{m})$.

Спаривание $\langle , \rangle_F$ определяется в § 4. Его инвариантность от выбора униформизующей доказывается в § 3; а независимость от способа разложения - в § 5.

§ 1. Изогения формальной группы и ее корни

Пусть F - формальная группа над кольцом o_0. Обозначим через $\mathcal{A}(\Delta) = \alpha_1\Delta + \alpha_2\Delta^2 + \dots + \alpha_h\Delta^h$ оператор, соответствующий F в силу теоремы Хонды (см. Введение, п. 2^0).

Пусть $\tilde{F}$ - формальная группа над кольцом o_0, изоморфная F, с логарифмом $\tilde{\lambda}$ и изогенией $[\tilde{p}]$, имеющей вид

$$[\tilde{p}] = pv(X) + \tilde{f}(X^q),$$

где $v(X)$ - многочлен, степень которого не превосходит $q-1$, а $\tilde{f}(X)$ - обратимый в

смысле суперпозиции ряд. Положим

$$\tilde{\lambda}(\tilde{f}(X)) = \sum_{m=1}^{\infty} b_m X^m,$$

$$\left(1 - \frac{\mathcal{A}(\Delta)}{p}\right) \tilde{\lambda}(\tilde{f}(X)) = \sum_{m=1}^{\infty} b'_m X^m.$$

Заметим, что $\left(1 - \frac{\mathcal{A}(\Delta)}{p}\right) \tilde{\lambda}(\tilde{f}(X)) = \ell_{\tilde{F}}(\tilde{f}(X))$, и поэтому $b'_m \in o_0 (m>1)$.

При доказательстве символьного свойства спаривания $<,>_F$ будет использоваться следующая лемма.

Лемма 1.1. *Коэффициенты b_m и b'_m удовлетворяют сравнениям:*

1. $b_m \cdot m \equiv 0 \bmod p$ *для любого* $m \geq 1$.
2. $b'_m \equiv 0 \bmod p$ *если* $q \mid m$.

Доказательство. Существует ряд $\tilde{v} \in X o_0[[X]]$ такой, что $\tilde{f}(X^q) +_F (p\tilde{v}) = [\tilde{p}]$. Из соотношения $\tilde{\lambda} \circ [p] = p\tilde{\lambda}$ следует, что

$$\tilde{\lambda}(\tilde{f}(X^q)) + \tilde{\lambda}(p\tilde{v}) = p\tilde{\lambda}. \tag{1}$$

Поскольку $\tilde{\lambda}(p\tilde{v}) \equiv 0 \bmod p$, получаем сравнение $\tilde{\lambda}(\tilde{f}(X^q)) \equiv p\tilde{\lambda}(X) \bmod p$. Положим, что $\tilde{\lambda}(X) = \sum_{m=1}^{\infty} c_m X^m$. Тогда последнее сравнение означает, что для любого $m \geq 1$ $b_m \equiv p c_{mq} \bmod p$. Таким образом, достаточно проверить, что $pmc_{mq} \in o_0$ для любого $m \geq 1$. Для групп Артина-Хассе это проверяется непосредственно, а общий случай сводится к нему с помощью формулы $\tilde{\lambda} = \lambda_a \circ E(x)$.

2) Заметим, что $\tilde{\lambda}(p\tilde{v}) \equiv p\tilde{v} \bmod p^2$. Поэтому из равенства (1) следует сравнение

$$\tilde{\lambda}(\tilde{f}(X^q)) + p\tilde{v} \equiv p\lambda \bmod p^2. \tag{2}$$

Применяя к обеим частям сравнения (2) оператор $1 - \frac{\mathcal{A}(\Delta)}{p}$, получаем

$$\left(1 - \frac{\mathcal{A}(\Delta)}{p}\right)\tilde{\lambda}(f(X^q)) + (p - \mathcal{A}(\Delta))\tilde{v} \equiv 0 \bmod p. \tag{3}$$

Так как $\alpha_1, \alpha_2, \ldots, \alpha_{h-1} \equiv 0 \bmod p$, сравнение (3) можно записать в виде

$$\left(1 - \frac{\mathcal{A}(\Delta)}{p}\right)\tilde{\lambda}(f(X^q)) \equiv \alpha_h \tilde{v}^{\Delta^h} \bmod p. \tag{4}$$

Воспользуемся теперь тем, что v является многочленом степени, не превосходящей $q-1$. По определению $\tilde{v}$ имеем

$$p\tilde{v} +_F \tilde{f}(X^q) = pv + f(X^q). \tag{5}$$

Левая часть этого равенства имеет вид

$$p\tilde{v} + \tilde{f}(X^q) + \sum_{i,j \geq 1} a_{ij} (p\tilde{v})^i \tilde{f}(X^q)^j \equiv$$

$$\equiv p\tilde{v} + \tilde{f}(X^q) + p\tilde{v}\sum_{j=1}^{\infty} a_{1j}\tilde{f}(X^q)^j \bmod p^2.$$

Тогда из соотношения (5) получаем сравнение

$$\tilde{v}\left(1 + \sum_{j=1}^{\infty} a_{1j}\tilde{f}(X^q)^j\right) \equiv v \bmod p.$$

Обратный к $1 + \sum_{j=1}^{\infty} a_{1j}\tilde{f}(X^q)^j$ ряд имеет вид $1 + \sum_{j=1}^{\infty} d_j X^{qj}$, поэтому

$$\tilde{v} \equiv v\left(1 + \sum_{j=1}^{\infty} d_j X^{qj}\right) \bmod p.$$

Применяя к обеим частям сравнения оператор Δ^h, имеем

$$\tilde{v}^{\Delta^h} \equiv v^{\Delta^h}\left(1 + \sum_{j=1}^{\infty} d_j^{\Delta^h} X^{q^2 j}\right) \bmod p.$$

Так как степень многочлена v не превосходит $q-1$, коэффициенты ряда, стоящего в правой части, при степенях, делящихся на q^2, равны нулю. Положим $\tilde{v}^{\Delta^h} = \sum_{i=1}^{\infty} r_i X^i$. Тогда для любого $i \in \mathbb{N}$ $r_{iq} \equiv 0 \bmod p$. Перепишем теперь соотношение (4) в виде

$$\sum_{m=1}^{\infty} b'_m X^{mq} \equiv \alpha_h \sum_{i=1}^{\infty} r_i X^i \bmod p.$$

Тогда для всех m, делящихся на q,

$$b'_m \equiv \alpha_h r_{(\frac{m}{q})q^2} \equiv 0 \bmod p.$$

Лемма доказана.

Замечание. Формальные группы F_0 и $F_{\eta,\rho}$ удовлетворяют условиям леммы (см. § 2).

Поле $k_0(\mu_F)$, полученное присоединением к k_0 всех корней изогении $[p]$, является слабо разветвленным расширением k_0, причем индекс ветвления $k_0(\mu_F)/k_0$ равен $q-1$. Кроме того, нам потребуется следующий результат.

Лемма 1.2. *Пусть в группе μ_F выбраны образующие $\xi_1, \ldots, \xi_h$. Тогда существуют элементы $\theta_{ij} \in R_1$ $(1 \le i, j \le h)$ такие, что для любых $1 \le i, j \le h$*

$$\xi_i \equiv \theta_{ij}\xi_j \bmod \pi^{2e_1}.$$

Для каждого $1 \le j \le h$ элементы $\theta_{1j}, \ldots, \theta_{hj}$ образуют базис $\mathbb{Z}_p$-модуля ω_1.

Доказательство. Пусть $[p] = \sum_{i=1}^{\infty} a_i X^i$. Обозначим через $\gamma_1, \ldots, \gamma_{q-1}$ корни уравнения $[p]/X = 0$. Рассмотрим также уравнение $X^{q-1} + \frac{p}{a_q} = 0$ с корнями $\beta_1, \ldots, \beta_{q-1}$. Из сравнения $\frac{1}{a_q X}[p] \equiv X^{q-1} + \frac{p}{a_q} \bmod (p, \deg q)$ следует, что $\nu(\gamma_1^{q-1} + \frac{p}{a_q}) > e$. С другой стороны, $\nu(\gamma_1^{q-1} + \frac{p}{a_q}) = \nu(\gamma_1 - \beta_1) + \ldots + \nu(\gamma_1 - \beta_{q-1})$, и, поскольку $\nu(\gamma_1) = \nu(\beta_j) = e_1$,

найдется единственное k такое, что

$$v(\gamma_1 - \beta_k) > e_1. \tag{6}$$

Далее, равенство

$$v((q-1)\gamma_1^{q-2}) = (q-2)v(\gamma_1) = \sum_{j\geq 2} v(\gamma_1 - \gamma_j)$$

показывает, что для каждого $j\geq 2$ $v(\gamma_1-\gamma_j)=v(\gamma_1)$. Тогда из леммы Краснера (см. предл. 3, гл. 2, [7]) следует, что $k_0(\gamma_1)=k_0(\beta_k)$. Поэтому неравенство (6) означает, что $\gamma_1\equiv\beta_k \bmod \pi^{2e_1}$. Предположим, что корни занумерованы так, что $\xi_i\equiv\beta_i \bmod \pi^{2e_1}$. Очевидно, что существуют такие $\theta_{ij}\in\mathfrak{K}_1$, что $\beta_i=\theta_{ij}\beta_j$. Следовательно, $\xi_i\equiv\theta_{ij}\xi_j \bmod \pi^{2e_1}$, и первая часть леммы доказана. Покажем теперь, что для любого $1\leq j\leq h$ элементы $\theta_{1j},\ldots,\theta_{hj}$ образуют базис $\mathbb{Z}_p$-модуля o_1. Достаточно доказать, что для всякого $\theta\in\mathfrak{K}_1$ найдутся элементы $c_1,\ldots,c_h\in\mathbb{Z}_p$ такие, что

$$\theta \equiv c_1\theta_{1j} + \ldots + c_h\theta_{hj} \bmod p.$$

Возьмем такой элемент $\gamma\in\mu_F$, что $\gamma\equiv\theta\xi_j \bmod \pi^{2e_1}$. Поскольку $\xi_1,\ldots,\xi_h$ образуют базис группы μ_F, существуют $c_1,\ldots,c_h\in\mathbb{Z}_p$ такие, что

$$[c_1](\xi_1) +_F \ldots +_F [c_h](\xi_h) = \gamma.$$

Учитывая, что $\xi_i\equiv\theta_{ij}\xi_j \bmod \pi^{2e_1}$, получаем сравнение

$$(c_1\theta_{1j}+\ldots+c_h\theta_{hj})\xi_j \equiv \theta\xi_j \bmod \pi^{2e_1}.$$

Так как $c_1\theta_{1j}+\ldots+c_h\theta_{hj}$ лежит в кольце целых неразветвленного расширения поля $\mathbb{Q}_p$, из последнего сравнения следует, что $\theta\equiv c_1\theta_{1j}+\ldots+c_h\theta_{hj} \bmod p$. Лемма доказана.

При доказательстве последней леммы было показано, что поле $k_0(\mu_F)$ получается присоединением к k_0 всех корней многочлена $X^{q-1}+\frac{p}{a_q}=0$. В случае, когда высота h формальной группы делится на степень расширения $k_0/\mathbb{Q}_p$, этот результат можно уточнить.

Предложение 1.3. *Пусть F_0 – формальная группа, изогения которой имеет вид $[p]_0=pX+f_0(X^q)$, где $f_0(X) = \sum_{i=1}^{\infty} a_{qi}X^i$. Предположим, что высота $h=ht(F_0)$ делится на степень расширения $k_0/\mathbb{Q}_p$. Тогда существует обратимый в смысле суперпозиции ряд $h\in o_0[[X]]$ такой, что если β – корень уравнения $\frac{pX}{a_q}+X^q=0$, то $h(\beta)\in\mu_{F_0}$. При этом*

$$h(X) \equiv \frac{X}{a_q} \bmod (p,\ \deg(q+1)). \tag{7}$$

Доказательство. Заметим, что ряды $[p]_0\circ f_0^{-1}$ и $\frac{pX}{a_q}+X^q$ являются изогениями

изоморфных групп Любина-Тейта. Отсюда следует существование ряда h. При этом сравнение (7) проверяется непосредственно.

Следующая лемма легко доказывается с помощью индукции.

Лемма 1.4. Предположим, что $p\neq 2$. Пусть $\mathbb{F}_q$ - конечное поле из q элементов, ряд $\alpha(x)\in\mathbb{F}_q[[X]]$, причем $\alpha(x)\equiv 1 \bmod \deg 1$. Положим

$$\alpha^{-1}\frac{d\alpha}{dX}=\sum_{i=0}^{\infty} d_i X^i.$$

Пусть d'_{q-p^j-1}, d''_{q-p^j-1} $(0\leq j\leq h-1)$ - такие элементы поля $\mathbb{F}_q$, что для каждого $j=0,1,\ldots,h-1$

$$d_{q-p^j-1}=d'_{q-p^j-1}+d''_{q-p^j-1}.$$

Тогда существуют такие ряды $\alpha'(X)$, $\alpha''(X)\in\mathbb{F}_q[[X]]$, что

а) $\alpha=\alpha'\alpha''$;

б) $\alpha'\equiv\alpha''\equiv 1 \bmod \deg 1$;

в) для всякого $0\leq j\leq h-1$ коэффициенты при X^{q-p^j-1} рядов $\alpha'^{-1}\frac{d\alpha'}{dx}$ и $\alpha''^{-1}\frac{d\alpha''}{dx}$ равны α'_{q-p^j-1} и α''_{q-p^j-1} соответственно.

§ 2. Арифметика группы точек

В этом параграфе строится специальный базис формального $\mathbb{Z}_p$-модуля $F(\mathfrak{m})$. Доказательства будут опубликованы в работе [1].

1°. Основную роль в арифметике группы точек играют примарные элементы. Напомним, что элемент ω группы точек $F(\mathfrak{m})$ называется p^n-примарным, если расширение поля k, полученное делением точки ω на изогению $[p^n]$, неразветвлено. В случае мультипликативной формальной группы, а также формальных групп Любина-Тэйта примарные элементы были построены в работах [2,3].

Итак, пусть ξ - некоторый корень изогении $[p^n]$ формальной группы F с логарифмом $\lambda(X)$, а $z(X)$ - степенной ряд, полученный из разложения корня ξ по простому элементу π, таким образом, $\xi=z(\pi)$. Обозначим далее через $s(X)$ ряд $[p^n](z(X))$.

Пусть $\mathcal{A}(\Delta)=\alpha_1\Delta+\alpha_2\Delta^2+\ldots+\alpha_h\Delta^h$ - оператор, соответствующий группе F в силу теоремы Хонды (см. Введение, п. 2^0). Для произвольного элемента $a\in\mathfrak{a}$ положим

$$\mathcal{B}(\Delta)=b_0-\frac{\alpha_1 b_1}{p}\Delta-\ldots-\frac{\alpha_{h-1}b_{h-1}}{p}\Delta^{h-1},$$

где $b_i=a^{\Delta^i}+a^{\Delta^{i+1}}+\ldots+a^{\Delta^{h-1}}$ $(i=0,1,\ldots,h-1)$.

Предложение 2.1. *Элемент*

$$P(a)=E_F(\mathcal{B}(\Delta)\lambda(s))|_{X=\pi},\quad a\in\mathfrak{a}$$

является p^n-примарным элементом, причем

$$(\pi,\ P(a))_{F,n} = [\mathrm{tr}\ a](\xi).$$

В случае $n=1$ вид p-примарного элемента можно значительно упростить. Пусть $\xi\in\mu_F$ - фиксированный корень изогении $[p] = \sum_{i=0}^{\infty} a_i X^i$. Положим $f(X) = \sum_{i=0}^{\infty} d_{q1} X^i$, и пусть $s(z)$ обозначает ряд $[p](z)$.

Предложение 2.2. *Элемент*

$$\omega(a) = E_F(bf(z^q))|_{X=\pi},$$

где $b=a+a^{\Delta}+\ldots+a^{\Delta^{h-1}}$ *является* p*-примарным, причем*

$$(\pi,\omega(a))_F = [\mathrm{tr}\ a](\xi).$$

Замечание. Пусть элементы $\xi_1,\ldots,\xi_h$ образуют базис группы μ_F. Тогда через $\omega_j(a)$, $1\le j\le h$, будем обозначать примарный элемент, связанный с корнем ξ_j.

2°. Арифметика группы точек.

При вычислении норменного спаривания на формальных группах Любина-Тэйта важную роль играют формальные группы с изогениями вида $pX+p\eta X^{p^\rho}+X^q$ (см. [4]). Их конструкцию можно обобщить следующим образом.

Предложение 2.3. *Для каждой формальной группы* F *над кольцом* o_0 *существует изоморфная ей формальная группа* F_0 *с изогенией вида*

$$[p]_0 = pX + f_0(X^q),$$

где $f_0(X) = \sum_{i=1}^{\infty} d_{q1} X^i$ *- обратимый (в смысле суперпозиции) ряд из кольца* $o_0[[X]]$.

2. *Для любых* $\eta\in o_0$, $\rho\in\mathbb{N}$ *существует формальная группа* $F_{\eta,\rho}$, *изоморфная* F, *такая, что*

а) $[p]_{\eta,\rho}=pX+p\eta X^{p^\rho}+f_{\eta,\rho}(X^q)$ *для некоторого ряда* $f_{\eta,\rho}\in o_0[[X]]$.

б) $[p]_{\eta,\rho}\equiv[p]_0+p\eta X^{p^\rho}+(d_q\eta^q-\eta d_q^{p^\rho})X^{qp^\rho}$ mod deg $(qp^\rho+1)$.

Пусть $\lambda_{\eta,\rho}$ и λ_0 - логарифмы формальных групп $F_{\eta,\rho}$ и F_0 соответственно. Положим

$$\mathcal{E}_0(X) = \lambda^{-1}\circ\lambda_0(f_0(X)),$$

$\mathcal{E}_{\eta,\rho}(X) = \lambda^{-1}\circ\lambda_{\eta,\rho}(f_{\eta,\rho}(X))$ для всех $\eta\in\mathbb{R}$, $1\le\rho\le h-1$. Заметим, что $\mathcal{E}_0(X)$ и $\mathcal{E}_{\eta,\rho}(X)$ являются степенными рядами с целыми коэффициентами.

Сформулируем теперь основной результат параграфа.

Предложение 2.4. *Элементы* $\mathcal{E}_0(\theta\pi^i)$, $\mathcal{E}_{\eta,\rho}(\theta\pi^i)(\theta\in\mathbb{R},(i,p)=1)$ *дают вместе с примарными элементами* $\omega_j(a)$, $a\in o$, *полную систему образующих* $\mathbb{Z}_p$*-модуля* $F(\mathfrak{m})$.

Замечание. Базис, построенный в предложении 2.4, является обобщением канонического базиса Шафаревича в группе главных единиц локального поля, а также в формальных модулях Любина-Тэйта (см. [4]).

§ 3. Вспомогательное спаривание и его свойства

1°. В этом параграфе будет строиться спаривание $[,]_F$ между мультипликативной группой $\mathcal{H}_m$ рядов Лорана с коэффициентами из кольца a и формальным $\mathbb{Z}_p$-модулем $\mathcal{H}_F$ и будут доказаны основные его свойства. Опираясь на это спаривание, мы в следующем параграфе определим норменное спаривание, которое и будет играть в дальнейшем основную роль.

Итак, пусть $\mathcal{H}_m$ - мультипликативная группа рядов Лорана, а $\mathcal{H}_F$ - $\mathbb{Z}_p$-модуль степенных рядов без свободного члена с коэффициентами из кольца a, в котором сложение происходит по формальному групповому закону F, т.е. $\varphi(X)+_F\psi(X)=F(\varphi,\psi)$.

Определим спаривание

$$\begin{array}{rccc}[,]_F: & \mathcal{H}_m \times \mathcal{H}_F & \longrightarrow & a \\ & \alpha, \quad \beta & \longmapsto & [\alpha,\beta]_F\end{array}$$

по следующей формуле

$$[\alpha,\beta]_F = \operatorname{res} \Phi_{\alpha,\beta}(X) W^{\Delta^h}(X), \tag{8}$$

где $W(X)$ - некоторый фиксированный ряд из кольца $a\{\{X\}\}$ (относительно этого кольца см. [3]), производная которого делится на p^{n-1}, т.е.

$$\frac{d}{dX} W(X) \equiv 0 \mod p^{n-1} \tag{9}$$

а ряд $\Phi_{\alpha,\beta}(X)$ определен следующим образом:

$$\Phi_{\alpha,\beta}(X) = \ell_F(\beta)\alpha^{-1} \cdot d\alpha - \frac{1}{p} \sum_{i=1}^{h} \alpha_i \ell_i(\alpha) d\lambda(\beta)^{\Delta^i}, \tag{10}$$

при этом

$$\ell_i(\alpha) = \frac{1}{p^i} \log (\alpha^{p^i}/\alpha^{\Delta^i}), \tag{11}$$

$$\ell_F(\alpha) = (1 - \frac{\mathcal{A}(\Delta)}{p})\lambda(\beta) \tag{12}$$

(здесь $\lambda(X)$ - логарифм формальной группы F, а относительно оператора $\mathcal{A}(\Delta)$ см. Введение, п. 2°).

Замечание. В тех местах, где не возникает недоразумений, мы будем писать $d\varphi$ вместо $\frac{d}{dX}\varphi(X)$.

В первую очередь нам надо убедиться, что ряд $\Phi_{\alpha,\beta}(X)$ имеет целые коэффициенты, хотя не все входящие в него функции определены над кольцом a (например, таковой является функция $\ell_i(\alpha)$).

Лемма 3.1. *Ряд $\Phi_{\alpha,\beta}(X)$ является степенным рядом из кольца $a[[X]]$.*

Доказательство. Первое слагаемое в определении ряда имеет целые коэффициенты, согласно п. 4° Введения.

Для доказательства того, что вторая сумма в (10) является рядом с целыми коэффициентами, заметим сперва, что из легко проверяемой формулы

$$dh(X)^{\Delta} = pX^{p-1}(dh(X))^{\Delta}$$

(справедливой для любого ряда Лорана $h(X)$) по индукции вытекает равенство

$$dh(X)^{\Delta^i} = p^i X^{-1}(X dh(X))^{\Delta^i}. \tag{13}$$

Рассмотрим i-е слагаемое во второй сумме в (10)

$$\frac{1}{p}\alpha_i \ell_i(\alpha) d\lambda(\beta)^{\Delta^i} = \frac{1}{p}\alpha_i \left(1+\frac{\Delta}{p}+\ldots+\frac{\Delta^{i-1}}{p^{i-1}}\right)\left(\frac{1}{p}\log \alpha^p/\alpha^\Delta\right) d\lambda(\beta)^{\Delta^i} =$$

$$= \frac{\alpha_i}{p^i}\,(p^{i-1} + p^{i-2}\,\Delta + \ldots + \Delta^{i-1})(\ell(\alpha)) \cdot d(\lambda)\beta)^{\Delta^i}).$$

Осталось заметить, что функция $\ell(\alpha)$ имеет уже целые коэффициенты (см. [2], лемма 2), и воспользоваться равенством (13), согласно которому

$$d(\lambda(\beta)^{\Delta^i}) = p^i X^{-1}(X d\lambda(\beta))^{\Delta^i}$$

(производная логарифма $\lambda(X)$ при этом имеет уже целые коэффициенты см. [10]).

Приведем частный случай спаривания $[,]_F$ при n=1, который будет использоваться в дальнейшем.

Лемма 3.2. *При $p\neq 2$ имеет место сравнение*

$$\Phi_{\alpha,\beta} \equiv \ell_F(\beta)\alpha^{-1} \cdot d\alpha - \frac{\alpha_h}{q}\,\ell(\alpha)^{\Delta^{h-1}} \cdot d\lambda(\beta)^{\Delta^h} \bmod p,$$

где α_h - последний коэффициент оператора $A(\Delta)$, а функция $\ell(\alpha)$ имеет вид $\frac{1}{p}\log \alpha^p/\alpha^\Delta$.

Доказательство. Для всех $i=1,2,\ldots,h-1$ согласно (13) имеем сравнение

$$\frac{\alpha_i}{p}\,(1 + \frac{\Delta}{p} + \ldots + \frac{\Delta^{i-1}}{p^{i-1}})(\ell(\alpha)) \cdot d\lambda(\beta)^{\Delta^i} \equiv 0 \bmod p,$$

так как коэффициент α_i/p - целый, функция $\ell(\alpha)$ дает тоже ряд с целыми коэффициентами, а ряд $d\lambda(\beta)^{\Delta^i}$ делится на p^i согласно (13). Последний же член суммы в определении ряда $\Phi_{\alpha,\beta}$ из тех же соображений легко преобразуется к виду $\frac{\alpha_h}{q}\,\ell(\alpha)^{\Delta^{h-1}} \cdot d\lambda(\beta)^{\Delta^h}$, и лемма доказана.

Лемма 3.3. *Пусть $\varphi(X)$ - произвольный степенной ряд с коэффициентами из поля частных кольца o, для которого ряд $\frac{q}{p}\,\varphi(X)$ имеет целые коэффициенты (здесь $q=p^h$). Тогда*

$$\operatorname{res}((d\varphi) \cdot W^{\Delta^h}) \equiv 0 \bmod p^n. \tag{14}$$

Доказательство практически не отличается от доказательства леммы 13 работы [3].

2^0. Отметим теперь простейшие свойства спаривания $[,]_F$. Из аддитивности функций ℓ_i логарифмической производной $\alpha^{-1}d\alpha$ и обычной производной, а также линейности функции ℓ_F (см. Введение, п. 4°) следует билинейность спаривания $[,]_F$, т. е.

$$[\alpha_1\alpha_2,\beta]_F = [\alpha_1\beta]_F + [\alpha_2,\beta]_F, \tag{15а}$$

$$[\alpha,\beta_1 +_F \beta_2] = [\alpha,\beta_1]_F + [\alpha,\beta_2]_F, \tag{15б}$$

$$[\alpha^a,\beta]_F = a[\alpha,\beta]_F, \quad a\in\mathbb{Z}_p, \tag{15в}$$

$$[\alpha,[a](\beta)]_F = a[\alpha,\beta]_F, \quad a\in\mathbb{Z}_p. \tag{15г}$$

Приступим теперь к проверке одного из самым важных свойств спаривания $[\alpha,\beta]_F$ – его инвариантности при замене переменных. А именно пусть имеется следующая замена переменных

$$X = g(Y),$$

где $g(Y)$ – степенной ряд из кольца $o[[X]]$ без свободного члена, первый коэффициент которого обратим в кольце o.

Предложение 3.4. *Пусть* $p\neq 2$. *Спаривание* $[,]_F$ *инвариантно по* mod p^n *относительно замены переменных, т.е.*

$$[\alpha(X),\beta(X)]_F \equiv [\alpha(g(Y)),\ \beta(g(Y))]_F \bmod p^n. \tag{16}$$

Доказательство. Сделаем следующие наблюдения. Во-первых, инвариантность достаточно проверять в случае $\alpha(X)=X$ (рассуждение, что этого достаточно для общего случая, имеется в предл. 4, [3]). Во-вторых, ряд $\beta(X)$ можно представить в виде

$$\beta(X) = E_F(\ell_F(\beta))$$

(см. Введение, п. 4°). Поэтому, используя аддитивность функции E_F (см. Введение, п. 4) и билинейность спаривания $[,]_F$ (см. (15а–15г)), мы видим, что инвариантность достаточно проверять для пары $\alpha=X$, $\beta=E_F(aX^m)$, где $a\in o$, $m\geq 1$.

Прежде чем формулировать соответствующее утверждение, сделаем следующее замечание. Функция E_F зависит (по своему определению) от выбора переменной X. Мы сейчас будем доказывать результат, в котором будем менять одну переменную на другую, поэтому, чтобы не было недоразумений в нижеследующем тексте, мы будем снабжать обозначение эндоморфизма Фробениуса Δ соответствующим индексом, т.е. писать Δ_X. Этим же индексом будем снабжать и функцию E_F.

Итак, нам надо доказать следующее сравнение:

$$[X,\ E_{F,X}(aX^m)]_F \equiv [g(Y),\ E_{F,X}(ag(Y)^m)]_F \bmod p^n. \tag{17}$$

Нетрудно убедиться, как связаны функции $E_{F,X}$ и $E_{F,Y}$ при замене переменных, а именно

$$E_{F,X}(aX^m) = E_{F,Y}((1 - \frac{\mathcal{A}(\Delta_Y)}{p})S),$$

где

$$S = \left(1 - \frac{\mathcal{A}(\Delta_g)}{p}\right)^{-1}(ag^m) = (1 + \frac{\mathcal{A}(\Delta_g)}{p} + \frac{\mathcal{A}(\Delta_g)^2}{p^2} + \dots)(ag^m)$$

(здесь через Δ_g обозначен оператор Фробениуса, который возводит ряд g в степень p, а на элемент a действует как обычный автоморфизм Фробениуса в кольце o).

Действительно, по определению функций $E_{F,X}$ и $E_{F,Y}$ имеем

$$E_{F,Y}\left(\left(1 - \frac{\mathcal{A}(\Delta_Y)}{p}\right)S\right) = \lambda^{-1}\left(\left(1 - \frac{\mathcal{A}(\Delta_Y)}{p}\right)^{-1} \circ \left(1 - \frac{\mathcal{A}(\Delta_Y)}{p}\right)(S)\right) =$$

$$= \lambda^{-1}(S) = \lambda^{-1}\left(\left(1 - \frac{\mathcal{A}(\Delta_g)}{p}\right)^{-1}(ag^m)\right) = E_{F,g}(ag^m) = E_{F,X}(aX^m),$$

так как $X=g(Y)$. Наша проверка корректна, потому что ряд $\left(1 - \frac{\mathcal{A}(\Delta_Y)}{p}\right)(S)$ имеет

целые коэффициенты, в чем можно убедиться, если подробнее расписать этот ряд

$$\left(1 - \frac{\mathcal{A}(\Delta_Y)}{p}\right)(S) = ag^m + \sum_{r=1}^{\infty} \frac{\mathcal{A}(\Delta_g)^{p^r}(ag^m) - \mathcal{A}(\Delta_Y)\circ\mathcal{A}(\Delta_g)^{r-1}(ag^m)}{p^r} \tag{18}$$

и индукцией по r проверить, что любое r-е слагаемое в сумме имеет целые коэффициенты. При этом надо использовать несложно доказываемое сравнение

$$\Delta_g^{r+1}(ag^m) \equiv \Delta_Y\Delta_g^{r+i-1}(ag^m) \bmod p^r.$$

Приступим теперь непосредственно к проверке сравнения (17). По определению спаривания имеем

$$[X, E_{F,X}(aX^m)]_F = \operatorname{res}_X aX^{m-1}W^{\Delta_X^h}(X),$$

$$[g(Y), E_{F,Y}(ag(Y)^m)]_F = \left[g(Y), E_{F,Y}\left(\left(1 - \frac{\mathcal{A}(\Delta_Y)}{p}\right)(S)\right)\right]_F = \operatorname{res}_Y \Psi(Y)W^{\Delta_Y^h}(g(Y)),$$

где

$$\Psi(Y) = \left(1 - \frac{\mathcal{A}(\Delta_Y)}{p}\right)(S) \cdot g^{-1}\frac{d}{dY}g - \frac{1}{p}\sum_{i=1}^{h}\alpha_i\ell_i(g)\frac{d}{dY}S^{\Delta_Y^i},$$

при этом

$$\ell_i(g) = \frac{1}{p^i}\log\left(g^{p^i}/g^{\Delta_Y^i}\right).$$

Представив $\left(1 - \frac{\mathcal{A}(\Delta_Y)}{p}\right)(S)$ в виде (18), мы получим

$$\Psi(Y) = ag^{m-1}\frac{d}{dY}g + \sum_{r=1}^{\infty}\left\{\frac{\mathcal{A}(\Delta_g)^r(ag^m) - \mathcal{A}(\Delta_Y)\circ\mathcal{A}(\Delta_g)^{r-1}(ag^m)}{p^r} + \right.$$

$$\left. + \sum_{i=1}^{h}\alpha_i\ell_i(g)\frac{d}{dY}\frac{\mathcal{A}(\Delta_g)^{r-1}}{p^r}\left((ag^m)^{\Delta_Y^i}\right)\right\}. \tag{19}$$

Мы хотим получить в итоге следующий вид ряда $\Psi(Y)$:

$$\Psi(Y) = ag^{m-1}\frac{d}{dY}g + \sum_{i=1}^{h}\frac{d}{dY}\frac{\psi_i(Y)}{p^{i-1}} \tag{20}$$

при некоторых рядах $\psi_i(Y)$ с целыми коэффициентами. Если мы этого добьемся, то, используя лемму 3.3, легко получить инвариантность, а именно

$$\operatorname{res}_Y\Psi(Y)W^{\Delta_Y^h}(g) \equiv \operatorname{res}_Y\left(ag^{m-1}\frac{d}{dY}g + \frac{d}{dY}\sum_{i=1}^{h}\frac{\psi_i(Y)}{p^{i-1}}\right)W^{\Delta_g^h}(g) \equiv$$

$$\operatorname{res}_Y\left(ag^{m-1}\frac{dg}{dY}\right)W^{\Delta_X^h}(g) =$$

$$= \operatorname{res}_Y ag^{m-1}W^{\Delta_g^h}(g)\cdot\frac{dg}{dY} = \operatorname{res}_X aX^{m-1}W^{\Delta_g^h}(X) \bmod p^n,$$

и это даст нам сравнение (17).

Итак, разберем формулу (19). Напомним, что оператор $\mathcal{A}(\Delta_g)$ имеет вид

$$\mathcal{A}(\Delta_g) = \alpha_1\Delta_g + \alpha_2\Delta_g^2 + \ldots + \alpha_h\Delta_g^h. \tag{21}$$

Поэтому

$$\mathcal{A}(\Delta_g)^r = \beta_r\Delta_g^r + \beta_{r+1}\Delta_g^{r+1} + \ldots + \beta_{rh}\Delta_g^{rh}$$

при некоторых целых коэффициентах $\beta_r,\dots,\beta_{rh}$. Отсюда следует, что $(r+1)$-е слагаемое в сумме (19) примет вид

$$\frac{\mathcal{A}(\Delta_g)\circ(\mathcal{A}(\Delta_g)^r(ag^m))-\mathcal{A}(\Delta_Y)\circ(\mathcal{A}(\Delta_g)^r(ag^m))}{p^{r+1}}\cdot g^{-1}\frac{dg}{dY}-$$

$$-\sum_{i=1}^{h}\frac{\alpha_i}{p^{r+1}}\ell_i(g)\frac{d}{dY}\mathcal{A}(\Delta_g)^r(ag^m)^{\Delta_Y^i}=$$

$$=\frac{1}{p^{r+1}}\{((\alpha_1\Delta_g+\dots+\alpha_h\Delta_g^h)\circ(\beta_r a^{\Delta^r}g^{p^{r}m}+\dots+\beta_{rh}a^{\Delta^{rh}}g^{p^{rh}m})-$$

$$-(\alpha_1\Delta_Y+\dots+\alpha_h\Delta_Y^h)\circ(\beta_r a^{\Delta^r}g^{p^{r}m}+\dots+\beta_{rh}a^{\Delta^{rh}}g^{p^{rh}m}))\,g^{-1}\cdot\frac{dg}{dY}\}-$$

$$-\frac{1}{p^{r+1}}\sum_{i=1}^{h}\alpha_i\ell_i(g)\frac{d}{dY}(\beta_r a^{\Delta^{r+1}}g^{\Delta_Y^i p^{r}m}+\dots+\beta_{rh}a^{\Delta^{rh+i}}g^{\Delta_Y^i p^{rh}m})=$$

$$=\frac{1}{p^{r+1}}\sum_{1\le i\le h}\ \sum_{r\le j\le rh}\alpha_i\beta_i^{\Delta^i j}a^{\Delta^{i+j}}\left\{(g^{p^{i+j}m}-g^{\Delta^i p_Y^j m})g^{-\frac{dg}{dY}}-\ell_i(g)\frac{d}{dY}g^{\Delta^i p_Y^j m}\right\}\qquad(22)$$

Далее, нетрудно видеть, что

$$\frac{d}{dY}g^{\Delta_Y^i p^j m}=\frac{d}{dY}(g^{\Delta_Y^i})^{p^j m}=p^j m g^{\Delta_Y^i p^j m}\cdot(g^{-\Delta_Y^i}\cdot\frac{d}{dY}g^{\Delta_Y^i})=$$

$$=p^{i+j}mg^{\Delta_Y^i p^j m}(g^{-1}\cdot\frac{dg}{dY}-\ell_i(g)).$$

Мы воспользовались при этом равенством

$$g^{-\Delta_Y^i}\frac{d}{dY}g^{\Delta_Y^i}=p^i(g^{-1}\frac{dg}{dY}-\ell_i(g)).$$

Отсюда следует, что

$$\frac{d}{dY}\left(\frac{g^{p^{i+j}m}-g^{\Delta_Y^i p^j m}}{p^{i+j}m}-g^{\Delta_Y^i p^j m}\ell_i(g)\right)=$$

$$=(g^{p^{i+j}m}-g^{\Delta_Y^i p^j m})\,g^{-1}\frac{dg}{dY}-\ell_i(g)\frac{d}{dY}g^{\Delta_Y^i p^j m}.\qquad(23)$$

Учитывая теперь (22), мы видим, что $(r+1)$-е слагаемое в сумме (19) принимает вид

$$\frac{1}{p^{r+1}}\sum_{1\le i\le h}\ \sum_{r\le j\le rh}\alpha_i\beta_j^i a^{\Delta^{i+j}}\frac{d}{dY}\left(\frac{g^{p^{i+j}m}-g^{\Delta_Y^i p^j m}}{p^{i+j}m}-g^{\Delta_Y^i p^j m}\ell_i(g)\right).$$

Если обозначим ряд, стоящий под производной, через $f_{i,j}(Y)$ и воспользуемся леммой 3.5 ниже, то получим сравнение

$$\frac{f_{i,j}(Y)}{p^{r+1}}\equiv 0 \bmod (mp^j\cdot p)^2/mp^{r+i+j+1}.$$

Ясно, что $(mp^j\cdot p)^2/mp^{r+i+j+1}=mp^{(j-r)-(i-1)}$. Осталось учесть, что у нас $j\ge r$, и мы получаем равенство (20), в котором ряд $\psi_i(Y)/p^{i-1}$ получается суммированием всех $f_{i,j}(Y)/p^{r+1}$ по всем j и r. Итак, инвариантность полностью доказана.

Осталось проверить лемму, на которую мы ссылались при доказательстве инвариантности. Пусть $h(X)$ - произвольный ряд из кольца $o[[X]]$ и Δ - оператор Фробениуса в кольце $o[[X]]$.

Лемма 3.5. *При нечетном простом p имеет место сравнение*

$$h^{mp^i} - h^{m\Delta^i} \equiv mp^i \ell_i(h)^{m\Delta^i} \bmod (mp)^2,$$

где $\ell_i(h) = \frac{1}{p^i} \log (h^{p^i}/h^{\Delta^i})$.

Доказательство. Из определения функции ℓ_i (см. (11)) следует

$$h^{mp^i} / h^{m\Delta^i} = \exp(mp^i \ell_i(h)),$$

так как

$$mp^i \ell_i(h) = m \log h^{p^i}/h^{\Delta^i} = \log h^{mp^i}/h^{m\Delta^i}.$$

Значит,

$$h^{mp^i} - h^{m\Delta^i} = h^{m\Delta^i}(\exp(mp^i \ell_i(h))-1) =$$

$$= mp^i \ell_i(h) h^{m\Delta^i} + h^{m\Delta^i} \sum_{k\geq 2} \frac{(mp)^k}{k!} (p^{i-1}\ell_i(h))^k.$$

Осталось сказать, что ряд $p^{i-1}\ell_i(h)=(p^{i-1}+p^{i-2}\Delta+\ldots+\Delta^{i-1})\ell(h))$ имеет целые коэффициенты, так как $\ell(h)=\frac{1}{p}\log h^p/h^\Delta$ имеет целые коэффициенты (см. Введение, п. 4^0) и, кроме того, число $(mp)^k/k!$ делится на $(mp)^2$, если $p\geq 3$ и $k\geq 2$.

3^0. Символьное свойство спаривания. Пусть $\tilde{F}$ - формальная группа над o_0, изоморфная F, с логарифмом λ и изогенией $[\tilde{p}]$, имеющей вид

$$[\tilde{p}] = pv(X) + \tilde{f}(X^q),$$

где $v(X)$ - многочлен, степень которого не превосходит $q-1$, а $\tilde{f}(X)$ - обратимый в смысле суперпозиции ряд. Пусть

$$\tilde{\mathcal{E}}(X) = \lambda^{-1} \circ \tilde{\lambda} \circ \tilde{f}.$$

Предложение 3.6. *Пусть $p\neq 2$. Спаривание $[,]_F$ обладает по* mod p *символьным свойством, т.е.*

$$[\varphi(X), \tilde{\mathcal{E}}(\varphi(X))]_F \equiv 0 \bmod p.$$

Доказательство. По определению ряда Φ имеем

$$\Phi = \Phi_{\varphi, \tilde{\mathcal{E}}(\varphi)} = \varphi^{-1} \cdot d\varphi \circ \ell_F(\tilde{\mathcal{E}}(\varphi)) - \frac{1}{p} \sum_{i=1}^{h} \alpha_i \ell_i(\varphi) d(\tilde{\lambda} \circ \tilde{f}(\varphi))^{\Delta^i}.$$

Если положить

$$\tilde{\lambda}(\tilde{f}(X)) = \sum_{m\geq 1} b_m X^m; \quad \ell_{\tilde{F}}(\tilde{f}) = \sum_{m\geq 1} b'_m X^m,$$

то ряд Φ примет вид

$$\Phi = \varphi^{-1}d\varphi \sum_{m\geq 1} b'_m\varphi^m + \sum_{i=1}^{h}\sum_{m=1}^{\infty} \frac{b_m^{\Delta^i}\alpha_i}{p}\,(\varphi^{mp^i} - \varphi^{m\Delta^i} - \ell_i(\varphi)d\varphi^{m\Delta^i}).$$

Нам надо показать, что

$$\operatorname{res} \Phi W^{\Delta^h} \equiv 0 \bmod p.$$

Если m не делится на q, то сразу же получаем

$$\operatorname{res}(b'_m\varphi^{m-1}d\varphi\cdot W^{\Delta^h}) = \operatorname{res} d\left(\frac{b'_m}{m}\,\varphi^m\right)\cdot W^{\Delta^h} \equiv 0 \bmod p,$$

так как ряд $\dfrac{qb'_m}{pm}\,\varphi^m$ имеет целые коэффициенты, и мы можем воспользоваться леммой 3.3. Если же q делит m, то в силу леммы 1.1 имеем $b'_m \equiv 0 \bmod p$ и поэтому опять получаем

$$\operatorname{res}\,(b'_m\varphi^{m-1}d\varphi \cdot W^{\Delta^h}) \equiv 0 \bmod p.$$

Положим

$$g_{m,i} = \frac{\varphi^{mp^i} - \varphi^{m\Delta^i}}{p^i m} - \varphi^{m\Delta^i}\ell_i(\varphi).$$

Было доказано (см. (23)), что

$$dg_{m,i} = \varphi^{mp^i} - \varphi^{m\Delta^i} - \ell_i(\varphi)d\varphi^{m\Delta^i}.$$

Из леммы 1.1 следует, что ряд

$$\frac{q}{p}\left(\frac{b_m^{\Delta^i}\alpha_i}{p} \circ g_{m,i}\right) = \alpha_i\frac{g_{m,i}}{pm}\cdot\frac{b_m^{\Delta^i}mq}{p}$$

имеет целые коэффициенты. Следовательно, по лемме 3.3 получаем

$$\operatorname{res}\frac{b_m^{\Delta^i}\alpha_i}{p}\,(\varphi^{mp^i} - \varphi^{m\Delta^i} - \ell_i(\varphi)d\varphi^{m\Delta^i})W^{\Delta^h} =$$

$$= \operatorname{res}\left(\frac{b_m^{\Delta^i}\alpha_i}{p}\,dg_{m,i}\cdot W^{\Delta^h}\right) \equiv 0 \bmod p,$$

и предложение доказано.

§ 4. Определение нормменного спаривания

1°. С помощью вспомогательного спаривания $[,]_F$ мы построим спаривание

$$\langle,\rangle_F : k^\times \times F(\mathfrak{m}) \longrightarrow \mu_F,$$

где k - локальное поле, содержащее k_0, $F(\mathfrak{m})$ - формальный модуль идеала $\mathfrak{m}$ кольца целых поля k, а μ_F - группа корней изогении $[p](X)$ формальной группы F. Это спаривание в итоге даст явную формулу для норменного спаривания Гильберта (см. § 6).

Пусть α - элемент мультипликативной группы $k^\times$, а β - элемент из $F(\mathfrak{m})$. Разложим элементы α и β в степенные ряды по простому элементу π с коэффициентами из кольца o:

$$\alpha = \theta\pi^a + a_1\pi^{a+1} + \ldots; \ \beta = b_1\pi + b_2\pi^2 + \ldots, \ a_i, \ b_j \in o.$$

Замечание 1. Чтобы не усложнять формулу для спаривания $\langle , \rangle_F$, мы всегда будем считать, что первый коэффициент θ в разложении элемента $\alpha \in k^\times$ взят из системы Тейхмюллера $\mathfrak{K}$.

Замечание 2. Построенные по этим элементам ряды $\alpha(X)$ из $\mathcal{H}_\mathfrak{m}$ и $\beta(X)$ из $\mathcal{H}_F$ (обозначения см. в § 3) мы будем обозначать теми же буквами α и β. Таким образом, $\alpha(\pi)=\alpha$, $\beta(\pi)=\beta$.

Пусть $\xi_1, \ldots, \xi_h$ - базис группы μ_F корней изогении $[p]$. Каждому ξ_i соответствует ряд $z_i(X) \in o[[X]]$, для которого, как и выше, $z_i(\pi)=\xi_i$, а также ряд $s_i(X)=[p](z_i)$.

В § 1, лемма 1.2 было доказано, что

$$\xi_j \equiv \theta_{ji}\xi_i \bmod \pi^{2e_1}$$

и для каждого $i=1,2,\ldots,h$ элементы

$$\theta_{1i}, \ldots, \theta_{ii} = 1, \ldots, \theta_{hi} \tag{24}$$

образуют базис $\mathbb{Z}_p$-модуля o_1.

Лемма 4.1. *Пусть элементы $b_1, \ldots, b_{h-1}$ из кольца o_1 вместе с 1 образуют базис $\mathbb{Z}_p$-модуля o_1. Тогда существует единственный элемент b из кольца o_1 такой, что для всех $i=1,2,\ldots,h-1$ имеем*

$$\mathrm{tr}_1(bb_1) = 0, \ \mathrm{tr}_1 b = 1.$$

Доказательство. Известно, что билинейное отображение $k_1^\times \times k_1^\times \longrightarrow \mathbb{Q}_p$, определенное формулой

$$(x,y) \longmapsto \mathrm{tr}_1(xy),$$

осуществляет изоморфизм аддитивной группы поля k_1^+ с группой характеров $\mathrm{Hom}_{\mathbb{Q}_p}(k_1^+, \mathbb{Q}_p)$. Пусть характер χ определен равенствами

$$\chi(b_i) = 0, \ \chi(1) = 1; \ 1 \le i \le h-1.$$

Тогда найдется единственный элемент $b \in k^+$ такой, что

$$\mathrm{tr}_1(bb_1) = 0, \ \mathrm{tr}_1 b = 1, \ 1 \le i \le h-1.$$

Так как элементы $1, b_1, \ldots, b_{h-1}$ образуют базис o_1, то для любого $x \in o_1$ имеем

$$\mathrm{tr}_1(bx) \in \mathbb{Z}_p.$$

Поскольку k_1 неразветвлено над $\mathbb{Q}_p$, то последнее означает, что $b \in o_1$, и лемма доказана.

Из доказанной леммы следует, что для элементов θ_{ji} (см. (24)) существуют единственные элементы $v_1, v_2, \ldots, v_h \in o_1$ такие, что для каждого $i=1,2,\ldots,h$

$$\mathrm{tr}_1(v_i\theta_{ji}) = 1, \quad i \neq j,$$

$$\mathrm{tr}_1(v_i\theta_{ii}) = \mathrm{tr}_1(v_i) = 1.$$

Напомним, что через ℓ_F и ℓ у нас обозначались функции

$$\ell_F(\varphi) = \left(1 - \frac{\mathcal{A}(\Delta)}{p}\right)\lambda(\varphi), \quad \ell(\varphi) = \frac{1}{p}\log \psi^p/\psi^\Delta.$$

Мы готовы теперь определить спаривание

$$<,>_F : k^\times \times F(\mathfrak{m}) \longrightarrow \mu_F. \tag{25}$$

Пусть $p \neq 2$, тогда

$$<\alpha,\beta>_F = \sum_{i=1}^{h} {}_{(F)}[\mathrm{tr}(v_i\gamma_i)](\xi_1),$$

где $\gamma_i = \mathrm{res}\ \Phi_{\alpha,\beta}/s_i$, и при этом

$$\Phi_{\alpha,\beta} = \frac{1}{\alpha_h}\ell_F(\beta)\alpha^{-1}d\alpha - \frac{1}{q}\ell(\alpha)^{\Delta^{h-1}}\alpha\lambda(\beta)^{\Delta^h} \tag{26}$$

(напомним, что мы пишем $d\varphi$ вместо $\frac{d\varphi}{dX}$).

Прежде чем сформулировать и доказать основные свойства спаривания $<,>_F$, введем еще несколько обозначений. Для изогении $[p] = \sum_{i\geq 1} a_i X^i$ формальной группы F положим

$$f(X) = \sum_{i=1}^{\infty} a_{iq}X^i.$$

Заметим, что первый коэффициент ряда $f(X)$ является единицей кольца o_0, а ряд $[p](X) - f(X^q)$ делится на p (см. Введение).

Пусть $\tilde{F}$ - формальная группа над o_0, изоморфная F, с логарифмом $\tilde{\lambda}(X)$ и изогенией $[\tilde{p}]$, имеющей вид

$$[\tilde{p}] = pv(X) + \tilde{f}(X^q),$$

где многочлен $v(X)$ имеет степень, не превосходящую $q-1$, а ряд $\tilde{f}(X)$ обратим в смысле суперпозиции.

В качестве группы $\tilde{F}$ мы будем использовать группы F_0 и $F_{\eta,\rho}$ (см. § 2, предл. 2.3).

Обозначим далее через $\tilde{\varepsilon}(X)$ ряд

$$\tilde{\mathcal{E}}(X) = \lambda^{-1} \circ \tilde{\lambda} \circ \tilde{f}.$$

Основные свойства спаривания $\langle , \rangle_F$ сформулируем в виде следующего предложения.

Предложение 4.2. *Спаривание $\langle , \rangle_F$ является $\mathbb{Z}_p$-линейным по обоим аргументам, инвариантным относительно выбора простого элемента π, независимым от способа разложения элементов в степенные ряды по π, и обладает символьным свойством, т.е. для любого элемента α из максимального идеала $\mathfrak{m}$ кольца целых поля k имеет место равенство*

$$\langle \alpha, \tilde{\mathcal{E}}(\alpha) \rangle_F = 0. \tag{27}$$

Замечание. Все свойства, кроме $\mathbb{Z}_p$-линейности, мы проверяем при $p \neq 2$.

Свойства $\mathbb{Z}_p$-линейности, инвариантности, а также символьное свойство непосредственно вытекают из соответствующих свойств вспомогательного спаривания $[,]_F$ (см. § 3), а свойство независимости спаривания $[,]_F$ проверим ниже в § 5, предл. 5.1.

При проверке совпадения построенного спаривания $\langle , \rangle_F$ с норменным спариванием Гильберта $(,)_F$ в § 6 нам потребуется символьное свойство в следующем виде.

Лемма 4.3. *Для любого α из максимального идеала кольца целых поля k имеет место сравнение*

$$\langle \alpha, \tilde{\mathcal{E}}(\theta\alpha^i) \rangle_F = 0,$$

где $\theta \in \mathfrak{R}$, $(i, p)=1$.

Доказательство. Используем символьное свойство спаривания $\langle , \rangle_F$:

$$\langle \alpha, \tilde{\mathcal{E}}(\theta\alpha^i) \rangle_F = \left[\frac{1}{i}\right] \langle \theta\alpha^i, \tilde{\mathcal{E}}(\theta\alpha^i) \rangle_F = 0,$$

и лемма доказана.

§ 5. Доказательство независимости спаривания

1°. В этом параграфе мы будем доказывать независимость спаривания $\langle , \rangle_F$, действуя по схеме, разработанной в [2,3]. Мы следуем обозначениям, введенным в этих работах. А именно если ξ - некоторый корень изогении μ_F, то $z(X)$ будет обозначать ряд, полученный из разложения этого корня по степеням простого элемента π, таким образом, $z(\pi)=\xi$. Далее, обозначим через $u(X)$ ряд $[p](z)/z$.

Сделаем сперва несколько несложных наблюдений. Во-первых, для любого ряда $\varphi(X)$ из кольца $o[[X]]$ имеет место сравнение

$$\varphi(X)^{\Delta} \equiv \varphi(X)^p \bmod p,$$

и поэтому $z(X)^{\Delta^h} \equiv z(X)^q \bmod p$, где $q=p^h$. Во-вторых, $[p](z) \equiv a_q z^q + \ldots + \bmod p$ (см. Введение, п. 2^0), и поэтому

$$1/[p] \equiv /a_q z^q \equiv 1/a_q z^{\Delta^h} \bmod (p, \deg 0). \tag{28}$$

Действительно, по определению ряда $[p]$ имеем $[p](z)=pz+\ldots+a_q z^q+\ldots$, где все коэффициенты a_i, $1 \leq i \leq q-1$, делятся на p (см. Введение, п. 2^0). Поэтому $[p](z) \equiv a_q z^q + \ldots \bmod p$. Отсюда немедленно вытекает сравнение (28).

Замечание. Полученное сравнение дает возможность заменять ряд $1/[p]$ в определении спаривания $\langle , \rangle_F$ либо на ряд $1/a_q z^q$, либо на ряд $1/a_q z^{\Delta^h}$.

Предложение 5.1. *Пусть $p \neq 2$. Спаривание $\langle \ \rangle_F$ не зависит от способа разложения элементов в степенные ряды по простому элементу π.*

Доказательство. В предл. 4, [4] было доказано, что независимость спаривания достаточно проверять для пары π, β, где $\beta \in F(m)$.

Таким образом, нам надо проверить, что

$$\operatorname{tr} [X, \beta(X)]_F \equiv 0 \bmod p,$$

если ряд $\beta(X)$ обращается в нуль в точке $X=\pi$ (см., например, (54), с.790, [3]). В этом случае ряд $\beta(X)$ можно представить в виде

$$\beta(X) = u(X)\psi(X),$$

где $\psi(x)$ - некоторый степенной ряд из кольца $o[[X]]$ (см. лемму 6, § 3, [2]).

Воспользуемся теперь определением спаривания

$$[X, \beta(X)]_F = \operatorname{res} X^{-1} \ell_F(u\psi)/[p] \equiv \operatorname{res} X^{-1} \ell_F(u\psi)/a_q Z^q \equiv \operatorname{res} X^{-1} \ell_F(u\psi)/a_q Z^{\Delta^h} \bmod p$$

(мы использовали еще предыдущее замечание).

Таким образом, для проверки утверждения нашего предложения нам надо проверить выполнение следующего сравнения:

$$\operatorname{tr} \operatorname{res} X^{-1} \ell_F(u\psi)/[p] \equiv 0 \bmod p. \tag{29}$$

Функция $\ell_F(u\psi)$ по определению имеет вид

$$\ell_F(u\psi) = \lambda(u\psi) - \sum_{i=1}^{h-1} \frac{\alpha_i}{p} \lambda(u\psi)^{\Delta^i} - \frac{\alpha_h}{p} \lambda(u\psi)^{\Delta^h}.$$

Мы отдельно вычислим теперь вычеты от каждого слагаемого. Ниже будут проверены следующие сравнения:

$$\lambda(u\psi)/a_q z^q \equiv \psi/z \quad \bmod (p, \deg 1), \tag{30}$$

$$\lambda(u\psi)^{\Delta^i}/a_q z^q \equiv 0 \quad \bmod (p, \deg 1), \tag{31}$$

$$\frac{1}{p} \lambda(u\psi)^{\Delta^h}/z^q \equiv (\psi/z)^{\Delta^h} \bmod (p, \deg 1). \tag{32}$$

Из этих сравнений немедленно вытекает сравнение

$$\ell_F(u\psi)/a_q z^q \equiv \psi/z - \frac{\alpha_h}{a_q} (\psi/z)^{\Delta^h} =$$

$$= (1 - \frac{\alpha_h}{a_q} \Delta^h)(\psi/z) \quad \bmod (p, \deg 1)$$

(мы учли, что α_i/p - целый элемент, если $1 \leq i \leq h-1$, и поэтому сравнение (31) отбрасывает средние члены по модулю p). Осталось заметить, что $\alpha_h/a_q \equiv 1 \bmod p$ (см. лемму 5.2 ниже), откуда

$$\operatorname{tr} \operatorname{res} X^{-1} \ell_F(u\psi)/[p] \equiv \operatorname{tr} (1-\Delta^h) b \equiv 0 \bmod p,$$

где b - свободный член ряда ψ/z.

Сравнение (29), а вместе с ним и наше утверждение доказаны.

2°. Доказательство сравнений (30)-(32).

A. Ряд $u(z)$ имеет по определению вид

$$u(z) = p + a_2 z + \ldots + a_q z^{q-1} + \ldots = p\varphi(z) + a_q z^{q-1}.$$

Отсюда следует, что

$$u\psi/a_q z^q = p\varphi\psi/a_q z^q + \psi/z + (\text{степенной ряд от } X) \equiv \psi/z \bmod (p, \deg 1). \tag{33}$$

Пусть $\lambda(X) = X + c_2 X^2 + \ldots$ - логарифм формальной группы F. Учитывая, что элемент $p^{m-2} c_m$ - целый при $m \geq 2$ (см. Введение, п. 2°), получаем

$$c_m u^m \psi^m / a_q z^q = c_m (p\varphi(z) + a_q z^q + \ldots)^m \psi^m / a_q z^q.$$

Заметим, что $(a_q z^{q-1} + \ldots)^i \eta(X)/a_q z^q$ является степенным рядом от X при $i \geq 2$. Поэтому для $2 \leq i \leq m$ имеем

$$c_m C_m^i (a_q z^q + \ldots)^i \ (p\varphi)^{m-i} \psi^m / a_q z^q \equiv 0 \bmod \deg 1.$$

Наконец,

$$c_m (p\varphi(z))^m \psi^m / a_q z^q = (p^{m-2} c_m) p^2 (\varphi\psi)^m / a_q z^q \equiv 0 \bmod p.$$

Из этих двух сравнений следует, что

$$c_m u^m \psi / a_q z^q \equiv 0 \mod (p, \deg 1), \quad m \geq 2. \tag{34}$$

Последнее сравнение и (33) дают сравнение (30).

B. Приступим теперь к доказательству сравнения (31). Имеем

$$\lambda(u\psi)^{\Delta^i} / a_q z^q = u^{\Delta^i} \psi^{\Delta^i} / a_q z^q + \sum_{m \geq 2} c_m u^{m\Delta^i} \ \psi^{m\Delta^i} / a_q z^q. \tag{35}$$

Из определения ряда $u(z)$ получаем

$$u^{\Delta^i} \psi^{\Delta^i} / a_q z^q = p\varphi^{\Delta^i} \ \psi^{\Delta^i} / a_q z^q + (a_Q z^{\Delta^i (q-1)} + \ldots) / a_q z^q.$$

Первое слагаемое в правой части делится на p. Относительно второго слагаемого нужно заметить, что ряд $z(X)$ начинается с члена порядка e_1 (см. Введение, п. 5°), и поэтому ряд $z^{\Delta^i (q-1)}$ начинается с члена порядка $p^i (q-1) e_1$, а значит, ряд $z^{\Delta^i (q-1)} / z^q$ является степенным, который начинается с члена порядка $(p^i (q-1) - q) e_1 \geq 1$. Все сказанное в наших обозначениях принимает вид

$$(a_q z^{\Delta^i (q-1)} + \ldots) / a_q z^q \equiv 0 \mod \deg 1,$$

и значит,

$$u^{\Delta^i} \psi^{\Delta^i} / a_q z^q \equiv 0 \mod (p, \deg 1).$$

Точно так же, как (34), доказывается сравнение

$$c_m u^{m\Delta^i} \psi^{m\Delta^i} / a_q z^q \equiv 0 \mod (p, \deg 1).$$

Поэтому отсюда и из (35) получаем (31).

C. Докажем, наконец, последнее сравнение (32). Проверим сперва, что

$$\frac{1}{p} \lambda(u\psi)/z \equiv \psi/z \mod (p, \deg 1). \tag{36}$$

Действительно,

$$\frac{1}{p}\lambda(u\psi)/z = \frac{1}{p}u\psi/z + \sum_{m\geq 2}\frac{1}{p}c_m u^m\psi^m/z.$$

Ряд $u(z)$ имеет вид $p\varphi+a_q z^{q-1}+\ldots=(pz+p\varphi_1)+a_q z^{q-1}+,\ldots,$ где $\varphi_1(z)$ как ряд от z начинается со второй степени. Поэтому

$$\frac{1}{p}u\psi/z = \psi/z + (\text{степенной ряд}) \equiv \psi/z \bmod \deg 1.$$

Далее, так же как (34), доказывается сравнение

$$\frac{1}{p}c_m u^m\psi^m/z = \frac{1}{p}c_m(p\varphi + a_q z^{q-1}+\ldots)^m\psi^m/z \equiv 0 \bmod (p, \deg 1).$$

Из этих двух сравнений получаем (36).

Чтобы получить сравнение, (32) осталось подействовать на обе части сравнения (36) оператором Δ^h и воспользоваться сравнением $1/z^q\equiv 1/z^{\Delta^h} \bmod p$.

3°. Пусть, как и ранее,

$$[p] = pX + \ldots + a_q X^q + \ldots, \qquad q=p^h,$$

- изогения формальной группы F высоты h.

Пусть

$$\lambda_a(X) = (1 - \frac{\mathcal{A}(\Delta)}{p})^{-1}(X) = (1 + \frac{\mathcal{A}(\Delta)}{p} + \ldots)(X)$$

- логарифм формальной группы F_a, изоморфной группе F. Здесь оператор $\mathcal{A}(\Delta)$ имеет вид

$$\mathcal{A}(\Delta) = \alpha_1\Delta + \ldots + \alpha_h\Delta^h,$$

при этом $\alpha_1,\ldots,\alpha_{h-1}$ делятся на p, а α_h - единица кольца o_0 (см. Введение, п. 2°).

Лемма 5.2. *Имеет место сравнение*

$$a_q \equiv \alpha_h \bmod p. \tag{37}$$

Доказательство. Рассмотрим сперва формальную группу F_0 с изогенией $[p]_0=pX+a_qX^q+\ldots$ (см. предл. 2.3) Из равенства $\lambda_0\circ[p]=p\lambda_0$ легко получаются следующие соотношения для коэффициентов логарифма:

$$c_2=\ldots=c_{q-1}=0,$$

$$(p-p^q)c_q=a_q. \tag{38}$$

Далее, как известно, ряд

$$\ell_{F_0}(X) = (1 - \frac{\mathcal{A}(\Delta)}{p})\lambda_0(X) = \lambda_0(X) - \frac{\mathcal{A}(\Delta)}{p}\lambda_0(X)$$

имеет целые коэффициенты (см. Введение, п. 4°). Так как коэффициент при X^q в этом ряде равен $c_q - \frac{\alpha_h}{p}$, выполняется сравнение

$$\alpha_h \equiv pc_q \bmod p^2. \tag{39}$$

Отсюда и из (38) следует сравнение леммы для формальной группы F_0.

Если теперь F - произвольная группа из класса изоморфных группе Артина-Хассе F_a формальных групп и $[p]=pX+a'_2X^2+\ldots+a'_qX^q+\ldots$ - ее изогения, то имеет место сравнение

$$a_q \equiv a'_q \bmod p. \tag{40}$$

Действительно, формальные группы F и F_0 изоморфны, поэтому существует ряд $\varphi(X)=X+\ldots$ с целыми коэффициентами такой, что

$$\varphi \circ [p]_0 = [p] \circ \varphi.$$

Рассматривая коэффициент при X^q в обеих частях этого равенства, мы легко получаем сравнение (40), из которого следует сравнение нашей леммы. Лемма доказана.

§ 6. Явная формула для норменного спаривания

Пусть F – формальная группа над o_0 с изогенией $[p]=\sum_{i=1}^{\infty} a_i X^i$. Положим $f(X)=\sum_{i=1}^{\infty} a_{iq} X^i$. Оказывается, что норменное спаривание $(,)_F$ является f-символом.

Предложение 6.1. *Для любого* $\alpha\in\mathfrak{m}$ $(\alpha, f(\alpha))_F=0$.

Доказательство. На множестве формальных степенных рядов введем операции γ и τ с помощью равенств

$$\gamma\Big(\sum_{i=0}^{\infty} b_i X^i\Big) = \sum_{i=0}^{q-1} b_i X^i,$$

$$\tau\Big(\sum_{i=0}^{\infty} b_i X^i\Big) = \sum_{i=q}^{\infty} b_i X^{i-q}.$$

Возьмем $\beta\in\mathfrak{m}$ и рассмотрим уравнение $[p]-\beta=0$. По подготовительной теореме Вейерштрасса существуют многочлен $h=X^q+u_{q-1}X^{q-1}+\ldots+u_0$ и обратимый ряд $\varepsilon(X)$ такие, что $[p]-\beta=h\cdot\varepsilon$. Многочлен h можно вычислить по формуле

$$h = \frac{[p]-\beta}{\tau([p])}\,(1 + \tau \circ \frac{\gamma([p]-\beta)}{\tau([p])})^{-1} \quad (1)$$

(см. доказательство теоремы 4.1, гл. 12, [8]).

Свободный член ряда h является многочленом от β с коэффициентами в кольце o_0. Обозначим его через $g(X)$. Так как p нечетно, $g(\beta)$ является нормой корня уравнения $[p]-\beta=0$, а значит, $(g(\beta),\beta)_F=0$ для всякого $\beta\in\mathfrak{m}$. Из определения ряда f и сравнения $[p]\equiv f(X^q) \bmod p$ следует, что

$$\frac{\gamma([p]-\beta)}{\tau([p])} \equiv \frac{\gamma(f(X^q)-\beta)}{\tau(f(X^q))} + p\sum_{q\nmid i} r_i X^i \bmod p^2, \quad (41)$$

где r_i – некоторые элементы кольца целых поля k. Так как коэффициенты ряда $\frac{\gamma(f(X^q)-\beta)}{\tau(f(X^q))}$ при степенях, не делящихся на q, сравнимы с нулем по модулю p, из (41) получаем сравнение

$$\Big(1+\tau \circ \frac{\gamma([p]-\beta)}{\tau([p])}\Big)^{-1}(1) \equiv \Big(1+\tau \circ \frac{\gamma(f(X^q)-\beta)}{\tau(f(X^q))}\Big)^{-1}(1) + p\sum_{q\nmid i} u_i X^i \bmod p^2$$

для некоторых целых u_i. Поэтому свободный член ряда

$$-\frac{\beta}{a_q}\Big(1 + \tau \circ \frac{\gamma([p]-\beta)}{\tau([p])}\Big)^{-1}(1)$$

сравним со свободным членом ряда

$$-\frac{\beta}{a_q}\left(1+\tau\circ\frac{\gamma(f(X^q)-\beta)}{\tau(f(X^q))}\right)^{-1}(1) \qquad (42)$$

по модулю p^2. Но свободный член ряда (42) равен норме корня уравнения $f(X^q)-\beta=0$, т.е. $f^{-1}(\beta)$. Таким образом, получаем сравнение $g(X)\equiv f^{-1}(X) \bmod p^2$. Так как f и g обратимы в смысле суперпозиции,

$$g^{-1}(X) \equiv f(X) \bmod p^2.$$

Возьмем произвольный элемент $\alpha\in\mathfrak{m}$ и положим $\beta=g^{-1}(\alpha)$. Тогда $(\alpha, f(\alpha))_F=(g(\beta),\beta)_F=0$, так как $v(p^2)>qe_1$. Предложение доказано.

Теперь мы можем вычислить значения $(\pi,)_F$ на базисе модуля $F(\mathfrak{m})$, построенном в § 2.

Предложение 6.2. *Пусть* $\eta\in\mathfrak{K}$, $1\le\rho\le h-1$. *Тогда для всех* $\theta\in\mathfrak{K}$, $(i,p)=1$

$$(\pi, \mathcal{E}_{\eta,\rho}(\theta\pi^i))_F = (\pi, \mathcal{E}_0(\theta\pi^i))_F=0.$$

Доказательство. Пусть $(,)_{\eta,\rho}$ – нормменное спаривание на формальной группе $F_{\eta,\rho}$ (см. предл. 2.3). Тогда, в силу предложения 6.1

$$(\pi,\ f_{\eta,\rho}(\theta\pi^i))_{\eta,\rho} = \left[\frac{1}{1}\right]\circ(\pi^i,\ f_{\eta,\rho}(\theta\pi^i))_{\eta,\rho} + {}_F(\theta,\ f_{\eta,\rho}(\theta\pi^i))_{\eta,\rho}=0.$$

Но тогда $(\pi, \mathcal{E}_{\eta,\rho}(\theta\pi^i))_F=(\pi, f_{\eta,\rho}(\theta\pi^i))_{\eta,\rho}=0$.

Аналогично доказывается, что $(\pi, \mathcal{E}_0(\theta\pi^i))_F=0$.

Предложение доказано.

Обозначим через z_i ряд с коэффициентами в a, полученный в результате разложения элемента ξ_i по степеням униформизующей, и положим $s_i=[p](z_i)$.

В § 4 мы построили спаривание $<,>_F: k^\times F(\mathfrak{m}) \longrightarrow \mu_F$ по формуле

$$<\alpha,\beta>_F = \sum_{i=1}^{h}{}_{(F)}\ [\mathrm{tr}(v_i\gamma_i)](\xi_i),$$

где $\gamma_i=\mathrm{res}\ \Phi_{\alpha,\beta}/s_i$, причем

$$\Phi_{\alpha,\beta} = \ell_F(\beta)\alpha^{-1}d\alpha - \frac{\alpha_n}{q}\ell(\alpha)^{\Delta^{h-1}}\cdot d\lambda^{\Delta^h}(\beta),$$

а $v_1,\dots,v_h$ – элементы, построенные по базису $\xi_1,\dots,\xi_h$ группы μ_F в § 4.

Теперь мы можем сформулировать основной результат работы.

Теорема 1. *Пусть* $p\ne2$. *Спаривание* $<,>_F$ *совпадает с символом Гильберта* $(,)_F$ *и тем самым дает для последнего явную формулу.*

Доказательство. В силу предложения 4.2 $<,>_F$ является корректно определенным спариванием, причем из предложения 4.3 следует, что для любых $(i,p)=1$, $\theta\in\mathfrak{K}$

$$<\pi, \mathcal{E}(\theta\pi^i)>_F = <\pi, \mathcal{E}_{\eta,\rho}(\theta\pi^i)>_F = 0.$$

Подставляя $\alpha=\pi$, $\beta=\omega_j(a)$ в формулу для γ_i, получаем, что $\gamma_i\equiv\theta_{ji}(a+\dots+a^{\Delta^{h-1}}) \bmod p$. Тогда из определения элементов v_i следует, что $\mathrm{tr}(v_i\gamma_i)=\delta_{ij}\mathrm{tr}\ a$, где δ_{ij} – символ Кронекера. Следовательно,

$$<\pi,\omega_j(a)>_F = [\mathrm{tr}\ a](\xi_j).$$

Мы показали, что символ $\langle \pi, \rangle_F$ совпадает с символом Гильберта на базисе $\mathbb{Z}_p$-модуля $F(\mathfrak{m})$ для любой униформизующей π поля k. Следовательно, они совпадают всюду.

Теорема доказана.

Следствие. *Пусть* $k=k_0(\mu)$. *Тогда*

$$(\alpha,\beta)_F = \sum_{i=1}^{h} [\mathrm{tr}(v_i\gamma_i)](\xi_i),$$

где

$$\gamma_i = \frac{1}{\alpha_h} \operatorname{res} (\alpha^{-1} d\alpha \ell_F(\beta)/z_i^q).$$

Доказательство. Легко видеть, что в этом случае вычет от второго слагаемого в формуле для $\Phi_{\alpha,\beta}$ равен нулю.

§ 7. Представления Галуа

Пусть

$$\rho_F : \mathrm{Gal}(\bar{k}_0/k_0) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_F) \simeq \mathrm{GL}_h(\mathbb{Z}_p)$$

– представление группы Галуа поля k_0 в модуле Тэйта T_F формальной группы F (см. [10]). Рассмотрим в $\mathrm{GL}_h(\mathbb{Z}_p)$ подгруппу $H=\{g\in \mathrm{CL}_h(\mathbb{Z}_p) \mid g\equiv 1 \mod p\}$. В этом параграфе мы докажем следующий результат.

Теорема 2. *Пусть высота* h *формальной группы* F *делится на степень расширения* $k_0/\mathbb{Q}_p (p\neq 2)$. *Для того чтобы подгруппа* H *содержалась в образе представления* ρ_F, *необходимо и достаточно, чтобы элементы*

$$\alpha_1, \alpha_2, \ldots, \alpha_{h-1} \not\equiv 0 \mod p^2.$$

Для доказательства нам потребуются две вспомогательные леммы.

Лемма 7.1. *Пусть* $v_1, \ldots, v_h$ – *элементы, построенные в* § 4 *по базису группы* μ_F. *Тогда*

1. *Существуют* $\theta_1, \ldots, \theta_h \in \mathfrak{K}_1$ *такие, что для всех* $1\le i\le h$ $\xi_i \equiv \theta_i \pi \mod \pi^2$, *где* $\pi = \sqrt[q-1]{-p/a_q}$ – *униформизующая поля* k.

2. *Пусть* $x\in o_1$ – *такой элемент, что для всех* $1\le i\le h$ $\mathrm{tr}_1\left(\frac{v_i x}{\theta_i}\right) = 0$.

Тогда $x=0$.

Доказательство. Первое утверждение леммы следует из доказательства леммы 1.2, причем $\theta_1, \ldots, \theta_h$ образуют базис o_1.

Пусть $x = \sum_{j=1}^{h} \gamma_j v_j$, $(\gamma_i \in \mathbb{Z}_p)$ – разложение элемента x по этому базису. Тогда для любого i имеем

$$\mathrm{tr}_1\left(\frac{v_i x}{\theta_i}\right) = \sum_{j=1}^{h} \gamma_j \mathrm{tr}_1\left(\frac{v_i \theta_j}{\theta_i}\right) = \gamma_i.$$

Следовательно, все элементы γ_i равны нулю.

Лемма 7.2. *Сохраним обозначения леммы* 7.1. *Для всех* $1\le k,\ell,j,i\le h$ *положим*

$$B_{h(k-1)+i,h(j-1)+\ell} = \mathrm{tr}_1\left(\frac{v_i\theta^{p^{\ell-1}}\theta_j}{\theta_i}\right).$$

Тогда $h^2\times h^2$*-матрица* B *обратима по модулю* p.

Доказательство. Покажем, что столбцы матрицы B линейно независимы по модулю p. Предположим, что для всех $1\le k,i\le h$

$$\sum_{1\le j,\ \ell\le h} s_{h(j-1)+\ell}\, B_{h(k-1)+i,h(j-1)+\ell} \equiv 0 \bmod p.$$

Тогда из леммы 7.1 следует, что для каждого $1\le k\le h$ элемент $\sum_{1\le j,\ \ell\le h} \theta_k^{p^{\ell-1}}\theta_j$ $s_{h(j-1)+\ell}$ сравним с нулем по модулю p. Положим теперь

$$y_\ell = \sum_{j=1}^{h} s_{h(j-1)+\ell}\,\theta_j \qquad (1\le\ell\le h).$$

Тогда получаем систему линейных сравнений

$$\sum_{\ell=1}^{h} \theta_k^{p^{\ell-1}} y_\ell \equiv 0 \bmod p.$$

Эта система имеет единственное решение $y_1\equiv\ldots\equiv y_h \bmod p$, так как ее определитель является дискриминантом расширения $a_1/\mathbb{Z}_p$ и поэтому отличен от нуля. Теперь из линейной независимости элементов θ_j получаем, что $s_{h(j-1)+\ell}\equiv 0 \bmod p$ для всех $1\le j,\ \ell\le h$. Лемма доказана.

Перейдем к доказательству теоремы. Пусть L - расширение поля k_0, полученное присоединением к k_0 группы $\mu_{F,2}$ корней изогении $[p^2]$. Поле L является композитом вполне разветвленных абелевых расширений L_j/k $(1\le j\le h)$, каждое из которых получается присоединением к k корней уравнения $[p](X)=\xi_j$. Пусть N_j - норменная подгруппа расширения L_j/k. Из работы Фонтэна [9] следует, что для доказательства теоремы достаточно показать, что степень расширения L/k равна p^{h^2}. В силу локальной теории полей классов это условие принимает вид

$$(N_1\cap N_2\cap\ \ldots\cap N_{m-1}\cap N_{m+1}\cap\ \ldots\ \cap N_h)N_m = k^\times$$

для любого $m=1,\ldots,h$.

Пусть, для определенности, $m=1$. Тогда достаточно показать, что для всякого $\alpha\in k^\times$ существуют элементы $\alpha',\alpha''\in k^\times$ такие, что

1а) $\alpha = \alpha'\alpha''$,

1б) $(\alpha',\xi_1)_F=0$,

1в) $(\alpha'',\xi_k)_F=0$ для всех $2\le k\le h$, где $(,)_F$ - норменное спаривание в поле $k=k_0(\mu_F)$.

Выберем в поле k униформизующую $\pi=\sqrt[q-1]{-p/a_q}$. Заметим, что представления Галуа в модулях Тэйта изоморфных формальных групп изоморфны, поэтому можно

считать, что $F=F_0$ (см. предл. 2.3). Тогда из предложения 1.3 и леммы 5.2 следует, что

$$\ell_F(z_k) \equiv \theta_k X + \sum_{\ell=2}^{h} \left(\frac{\alpha_{\ell-1}}{p} \right) \theta_k^{p^{\ell-1}} X^{p^{\ell-1}} \bmod (p, \deg q). \tag{43}$$

Будем искать разложения элементов α' и α'' в виде

$$\alpha'(X) = X^a \theta \varepsilon'(X), \quad \alpha''(X) = \varepsilon''(X),$$

где $\varepsilon' \equiv \varepsilon'' \equiv 1 \bmod \deg 1$. Положим теперь

$$d \ln \varepsilon = \sum_{m=0}^{\infty} d_m X^m, \quad d \ln \varepsilon' = \sum_{m=0}^{\infty} d'_m X^m, \quad d \ln \varepsilon'' = \sum_{m=0}^{\infty} d''_m X^m.$$

Тогда, подставляя (43) в формулу для норменного спаривания (см. следствие теоремы 1), получаем соотношения

2а) $d'_{q-p^{\ell-1}} + d''_{q-p^{\ell-1}} = d_{q-p^{\ell-1}}$ для всех $0 \le \ell \le h-1$,

2б) $\operatorname{tr}\left(\frac{v_i}{\alpha_h} \left(\frac{d'_{q-2}\theta_1}{\theta_i} - \sum_{\ell-2}^{h} \left(\frac{\alpha_{\ell-1}}{p} \right) \frac{\theta_1^{p^{\ell-1}}}{\theta_i} d'_{q-p^{\ell-1}} \right) \right) \equiv b_{1j} \bmod p$,

где $1 \le i \le h$.

2в) $\operatorname{tr}\left(\frac{v_i}{\alpha_h} \left(\frac{d''_{q-2}\theta_k}{\theta_i} - \sum_{\ell=2}^{h} \left(\frac{\alpha_{\ell-1}}{p} \right) \frac{\theta_k^{p^{\ell-1}}}{\theta_1} d''_{q-p^{\ell-1}} \right) \right) \equiv 0 \bmod p$,

где $2 \le k \le h$, $1 \le i \le h$, а b_{11} - некоторые элементы кольца o_1.

Обратно, если мы найдем элементы $d'_{q-p^{\ell-1}}$, $d''_{q-p^{\ell-1}}$, удовлетворяющие условиям 2а)-2в), то по лемме 1.4 найдутся элементы α' и α'', для которых выполняются условия 1а)-1в). Подставляя 2а) в 2в), получаем систему сравнений

$$\operatorname{tr}\left(\frac{v_i}{\alpha_h} \left(\frac{d'_{q-2}\theta_k}{\theta_i} - \sum_{\ell=2}^{h} \left(\frac{\alpha_{\ell-1}}{p} \right) \frac{\theta_k^{p^{\ell-1}}}{\theta_1} d'_{q-p^{\ell-1}} \right) \right) \equiv b_{ki} \bmod p, \tag{44}$$

где $1 \le k, i \le h$, а $b_{k,i}$ - некоторые элементы кольца o_1.

Положим

$$\frac{d'_{q-2}}{\alpha_i} = \sum_{j=1}^{h} x_{1j}\theta_j \qquad \text{для } \ell = 0,$$

$$\frac{\alpha_{\ell-1}\, d'_{q-2^{\ell-1}}}{\alpha_h p} = \sum_{j=1}^{h} x_{\ell j}\theta_j \qquad \text{для } 1 \le \ell \le h-1, \tag{45}$$

где элементы $x_{\ell j} \in \mathbb{Z}_p$.

Подставляя эти формулы в (44), получаем систему линейных сравнений с матрицей B такой, что

$$B_{h(k-1)+i,\ h(j-1)+\ell} = \operatorname{tr}_1\left(\frac{v_i \theta_k^{p^{\ell-1}} \theta_j}{\theta_i} \right).$$

Теперь из леммы 7.2 следует, что эта система однозначно разрешима по модулю

p. Так как по условию $\alpha_1, \alpha_2, \ldots, \alpha_{h-1} \not\equiv 0 \pmod{p^2}$, элементы $\alpha'_{q-p^{\ell}-1}$ $(0 \le \ell \le h-1)$ можно найти, используя формулы (45).

Обратно, для того чтобы система (44) была разрешима при любых $d_{q-p^{\ell}-1}$ $(0 \le \ell \le h-1)$, необходимо, чтобы ее определитель не был равен нулю. Следовательно, условие $\alpha_1, \alpha_2, \ldots, \alpha_{h-1} \not\equiv 0 \pmod{p^2}$ является необходимым. Теорема доказана.

Список литературы

[1] Бенуа Д.Г., Востоков С.В. Арифметика группы точек формальной группы // Кольца и модули. Предельные теоремы теории вероятностей, вып.3. Л.: ЛГУ, 1991.

[2] Востоков С.В. Явная форма закона взаимности // Изв. АН СССР. Сер.Мат. 1978. Т.42, N 6. С.1287-1320.

[3] Востоков С.В. Нормменное спаривание в формальных модулях // Изв. АН СССР. Сер. мат. 1979. Т. 43, N 4. С.765-794.

[4] Востоков С.В. Символы на формальных группах // Изв. АН СССР. Сер. мат. 1981. Т.45, N 5. С.985-1014.

[5] Востоков С.В., Фесенко И.Б. Символ Гильберта для формальных групп Любина-Тэйта II // Зап. науч. семинаров ЛОМИ. 1983. Т.132. С.85-96.

[6] Колывагин В.А. Формальные группы и символ норменного вычета // Изв. АН СССР. Сер. мат. 1979. Т.43, N 5. С.1054-1120.

[7] Ленг С. Алгебраические числа. М.: Мир, 1969. 225 с.

[8] Ленг С. Введение в теорию модулярных форм. М.: Мир, 1979. 254 с.

[9] Fontaine J.-M. Points d'ordre fini d'un groupe formel sur une extension non ramifiee de $\mathbb{Z}_p$ // Bull.Soc.Math. France. 1974. Memoire 37. P.75-79.

[10] Fröhlich A. Formal groups. Lect. Notes in Math. Vol.74. Heidelberg: Springer, 1968. 139 p.

[11] Honda T. On the theory of commutative formal groups //J. Math. Soc. Japan. 1970. Vol.22. P.213-243.

[12] Nakamura T. On torsion points of formal groups over a ring of Witt vectors // Math.Zeit. 1986. Bd 193. S.397-404.

[13] de Shalit E. The explicit reciprocity law in local class field theory // Duke Math.J. 1986. Vol.53, N 1. P.163-176.

198904, Ленинград, Петродворец,
Библиотечная площадь, д.2
Математико-механический факультет
Ленинградского университета
кафедра высшей алгебры

Поступило 20 июня 1990 г.