СЕРИЯ
МАТЕМАТИЧЕСКАЯ
Том 45, № 5, 1981

УДК 519.48

ВОСТОКОВ С. В.

СИМВОЛЫ НА ФОРМАЛЬНЫХ ГРУППАХ

§ 1. Введение

Из K-теории хорошо известна теория непрерывных символов Стейнберга в локальном поле (см., например, [8] или ниже § 4). Напомним, что символом Стейнберга (или мультипликативным символом) в локальном поле k называют непрерывное билинейное спаривание $c(,)$ из мультипликативной группы $k^\times$ в некоторую топологическую группу, которое удовлетворяет соотношению $c(x, 1-x)=0$ для любого отличного от 1 элемента x из $k^\times$. Одним из основных фактов этой теории является существование универсального символа такого, что все остальные символы будут его гомоморфными образами. Таким универсальным символом является символ норменного вычета Гильберта и его явное описание (см. [2], [3]) дает в явном виде универсальный объект в теории мультипликативных символов.

В настоящей работе обобщается теория мультипликативных символов на коммутативные формальные группы. В полном объеме эта теория развивается здесь для формальных групп Любина — Тэйта (см. §§ 5—7) и в этом случае описывается в явном виде универсальный символ (см. § 7), а также проверяется, что модуль значений любого символа является модулем с одной образующей, который изоморфно вкладывается в группу точек формальной группы (см. § 7, теорема 2).

Надо отметить, что развитие теории символов для формальных групп дает, в частности, новый подход к построению явных формул для символа Гильберта, заданного на группе точек формальной группы (см. § 8, а также [4]).

В общем случае коммутативных формальных групп, который рассматривается в § 9, доказывается, что модуль значений конечно порожден своими значениями на парах простого элемента локального поля и примарных элементов группы точек формальной группы. Кроме того, проверяется, что модуль значений символа изоморфно вкладывается в ядро изогении формальной группы.

При изложении мы придерживались той точки зрения, что доказательство вспомогательных утверждений не должно мешать развитию теории и поэтому мы отнесли их в конец статьи (см. §§ 10, 11). Первые

же три параграфа посвящены общим определениям и постановке задачи.

В статье используется раздельная нумерация лемм, предложений и теорем.

§ 2. Формальные групповые законы

1°. Определения и основные факты теории формальных групп, которые мы сейчас будем рассматривать, можно найти в [9].

Пусть $\mathfrak{o}$ — коммутативное кольцо с 1 и $F(X, Y)$ — коммутативный формальный групповой закон над $\mathfrak{o}$, т. е. степенной ряд с коэффициентами из $\mathfrak{o}$, который удовлетворяет условиям

$$F(X, 0)=X, \quad F(0, Y)=Y,$$

$$F(F(X, Y), Z)=F(X, F(Y, Z)), \quad F(X, Y)=F(Y, X).$$

Как обычно, степенной ряд $f(X)$ без свободного члена с коэффициентами из кольца $\mathfrak{o}$ называется гомоморфизмом формальных групповых законов F и G, определенных над $\mathfrak{o}$, если

$$f(F(X, Y))=G(f(X), f(Y)). \tag{1}$$

Групповые законы с гомоморфизмами образуют категорию, если в качестве композиции гомоморфизмов взять подстановку рядов.

2°. Множество эндоморфизмов $\operatorname{End} F$ формального группового закона F имеет структуру кольца (так как F — коммутативный закон) и отображение $c: \operatorname{End} F \to \mathfrak{o}$, где $c(f)=f'(0)$ будет вложением, если характеристика кольца $\mathfrak{o}$ равна нулю (см., например, [6], предложение 1.1). Таким образом, кольцо эндоморфизмов $\operatorname{End} F$, изоморфное образу $c(\operatorname{End} F)$, можно считать подкольцом в $\mathfrak{o}$; если элемент a из кольца $\mathfrak{o}$ принадлежит этому образу $c(\operatorname{End} F)$, то его прообраз будем обозначать через $[a]$ (или $[a]_F$), т. е.

$$[a]=c^{-1}(a). \tag{2}$$

Пусть $\mathfrak{o}_0$ — подкольцо в $\mathfrak{o}$. Групповой закон F называется формальным $\mathfrak{o}_0$-модульным законом над $\mathfrak{o}$, если кольцо $\mathfrak{o}_0$ является подкольцом $c(\operatorname{End} F)$.

3°. Предположим, что кольцо $\mathfrak{o}$ имеет нулевую характеристику и пусть k — поле частных кольца $\mathfrak{o}$ и $\tilde{\mathfrak{o}}$ — локализация кольца $\mathfrak{o}$ по системе $\{1, 2, \ldots\}$. Считаем, что $\mathfrak{o}$ содержится в $\tilde{\mathfrak{o}}$. *Логарифмом* формального закона F будем называть гомоморфизм над $\tilde{\mathfrak{o}}$ закона F в аддитивный закон $F_a=X+Y$, т. е. всякий степенной ряд $\lambda(X)=X+c_2X^2+\ldots$ такой, что $\lambda(F(X, Y))=\lambda(X)+\lambda(Y)$.

Нетрудно проверить, что если F и G — два формальных групповых закона над $\mathfrak{o}$ с логарифмами λ_F и λ_G соответственно и если $f \in \operatorname{Hom}(F, G)$, то

$$\lambda_G(f)=c(f)\lambda_F$$

(напомним, что $c(f)=f'(0)$). Это, в частности, дает для формального $\mathfrak{o}_0$-модульного закона F над $\mathfrak{o}$ равенство

$$[a]_F(X)=\lambda^{-1}(a\lambda(X)), \tag{3}$$

где a — элемент из кольца $\mathfrak{o}_0$, и этим равенством эндоморфизм $[a]_F$ определен однозначно.

4°. Определим теперь понятие высоты эндоморфизма f. Если кольцо $\mathfrak{o}$ имеет простую характеристику $p>1$, то ненулевой эндоморфизм f можно представить в виде степенного ряда $\varphi(X^{p^h})$, где $c(\varphi)\neq 0$, а h — неотрицательное целое число, которое и называется в этом случае *высотой эндоморфизма* f.

Если $\mathfrak{o}$ — локальное кольцо с максимальным идеалом $\mathfrak{m}$ и полем вычетов $k=\mathfrak{o}/\mathfrak{m}$, то высотой эндоморфизма f формальной группы F над $\mathfrak{o}$ будем называть высоту редукции $\bar{f}$ в $k[[X]]$.

5°. Пусть M — коммутативная нильпотентная алгебра над $\mathfrak{o}$ (т. е. некоторая положительная степень каждого элемента из M равна нулю). Тогда формальная группа F определяет групповой закон на множестве элементов из M с помощью отображения $(x, y)\mapsto F(x, y)$ для x, y из M. Вместо $F(x, y)$ мы будем писать в дальнейшем

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

Множество M с таким групповым законом мы обозначим через $A(M)$ (или $A_F(M)$, если надо подчеркнуть формальную группу F). Ясно, что каждый эндоморфизм $f(X)$ формальной группы F определяет эндоморфизм на $A(M)$ благодаря отображению $x\mapsto f(x)$ для всех x из M. Поэтому если F является формальным $\mathfrak{o}_0$-модульным законом, то группу $A(M)$ мы можем также рассматривать как $\mathfrak{o}_0$-модуль, в котором операторы из $\mathfrak{o}_0$ задаются с помощью отображения

$$x\mapsto[a]_F(x)$$

для всех $x\in A(M)$.

§ 3. Формальные групповые законы над дискретно нормированными кольцами

6°. Пусть k — полное относительно дискретного нормирования поле характеристики 0, поле вычетов которого имеет простую характеристику $p>1$.

Пусть F — формальный групповой закон, определенный над $\mathfrak{o}$. Максимальный идеал $\mathfrak{m}$ кольца $\mathfrak{o}$ будет топологическим нильпотентом в том смысле, что большая степень каждого элемента стремится к нулю. Поэтому мы можем рассматривать группу

$$A(\mathfrak{m}),$$

которая как множество совпадает с $\mathfrak{m}$, и сложение в которой задано отображением $(x, y)\mapsto F(x, y)=x+_F y$ для x и y из $\mathfrak{m}$. Эту группу мы будем

называть *группой точек формальной группы F на $\mathfrak{m}$*. Если F — формальный $\mathfrak{o}_0$-модульный закон, то группа точек $A(\mathfrak{m})$ также будет $\mathfrak{o}_0$-модулем, если положить $a\alpha=[a]_F(\alpha)$ для любого a из $\mathfrak{o}_0$ и α из $\mathfrak{m}$.

Пусть K — конечное расширение поля k, тогда оно, как и основное поле k, будет полным и мы можем на максимальном идеале $\mathfrak{M}_K$ кольца целых поля K рассматривать группу точек $A(\mathfrak{M}_K)$. Если же L — алгебраическое расширение поля k, то группой точек $A(\mathfrak{M}_L)$ максимального идеала $\mathfrak{M}_L$ поля L будем считать объединение $\bigcup A(\mathfrak{M}_K)$ по всем конечным расширениям поля k, которые содержатся в L. Если $\bar{k}$ — фиксированное алгебраическое замыкание поля k и $\bar{\mathfrak{m}}$ — максимальный идеал его кольца целых, то через $A(\bar{\mathfrak{m}})$ обозначаем группу точек F на $\bar{\mathfrak{m}}$.

7°. Эндоморфизм f формальной группы F называется изогенией, если индуцированный им гомоморфизм $f: A(\bar{\mathfrak{m}})\to A(\bar{\mathfrak{m}})$ является эпиморфизмом с конечным ядром. Можно проверить, что f является изогенией тогда и только тогда, когда высота h эндоморфизма f конечна. При этом порядок $\ker f$ равен p^h (см. [6, предложение 2.2]).

Пусть эндоморфизм f формального группового закона F является изогенией, и пусть $f^{(n)}$ — n-кратная суперпозиция эндоморфизма f. Обозначим через $\varkappa_{f,n}$ ядро изогении $f^{(n)}: A(\bar{\mathfrak{m}})\to A(\bar{\mathfrak{m}})$. Это ядро будет конечной группой в $A(\bar{\mathfrak{m}})$.

8°. Нас интересует теперь специальный случай формальных групп — группы Любина — Тэйта. Предположим, что k_0 — локальное поле, поле вычетов которого имеет q элементов. Пусть π_0—простой элемент кольца целых $\mathfrak{o}_0$ поля k_0 и $\mathscr{F}_{\pi_0}$ — набор степенных рядов f с коэффициентами из $\mathfrak{o}_0$ таких, что

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

Для каждого ряда f из $\mathscr{F}_{\pi_0}$ существует единственная формальная группа F_f (над $\mathfrak{o}_0$) такая, что f является ее эндоморфизмом (см. [10]). Эту группу называем *формальной группой Любина — Тэйта*.

Формальную группу, ассоциированную с $f_0(X)=\pi_0 X+X^q$, будем называть *базисной группой Любина — Тэйта* и будем обозначать через F_0.

Кольцо эндоморфизмов формальной группы Любина — Тэйта совпадает с $\mathfrak{o}_0$ и отображение $a\mapsto[a]=c^{-1}(a)$ (см. (2)) задает изоморфизм кольца $\mathfrak{o}_0$ в $\operatorname{End} F_f$, при котором $[\pi_0]=f$. Кроме того, для любых двух рядов f_1 и f_2 из $\mathscr{F}_{\pi_0}$ соответствующие им формальные группы Любина — Тэйта F_{f_1} и F_{f_2} изоморфны.

§ 4. Мультипликативные символы в локальном поле

9°. Пусть k — полное дискретно нормированное поле с конечным полем вычетов (локальное поле), и пусть $\mathfrak{A}$ — полная топологическая абелева группа с хаусдорфовой топологией.

Определение 1. Непрерывным символом Стейнберга (или просто символом) на поле k будем называть непрерывное билинейное спаривание

$$c : k^\times \times k^\times \mapsto \mathfrak{A},$$

удовлетворяющее соотношению

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

для любого $x \neq 1$.

Теория символов в локальном поле хорошо известна (см., например, [8]), и мы изложим сейчас кратко основные факты этой теории.

Пусть $\mathfrak{R}$ — мультипликативно замкнутая система представителей поля вычетов поля k, U — группа главных единиц в k и π — простой элемент поля k. Тогда доказывается, что

$$c(\mathfrak{R}, U) = 0, \quad c(\mathfrak{R}, \mathfrak{R}) = 0,$$

$$c(U, U) \subset c(\pi, U).$$

Эти свойства, в частности, означают, что символ $c(k^\times, k^\times)$ порожден значениями $c(\pi, \mathfrak{R})$ и $c(\pi, U)$.

Определение 2. Символ $c : k^\times \times k^\times \mapsto \mathfrak{A}$ называется *ручным*, если $c(k^\times, U) = 0$, и *диким*, если $c(k^\times, \mathfrak{R}) = 0$.

Нетрудно проверить, что любой непрерывный символ на локальном поле однозначно представляется в виде суммы ручного и дикого символов и поэтому изучение символов распадается на изучение отдельно ручных и диких символов.

Определение 3. Символ $c : k^\times \times k^\times \mapsto \mathfrak{A}$ называется *универсальным*, если для любого символа $c' : k^\times \times k^\times \mapsto \mathfrak{A}'$ существует непрерывный гомоморфизм $f : \mathfrak{A} \mapsto \mathfrak{A}'$ такой, что $f \circ c = c'$.

Легко указать универсальный ручной символ

$$c_{\text{ун. ручн.}}(\alpha, \beta) \equiv (-1)^{v(\alpha)v(\beta)} \alpha^{v(\beta)} \beta^{-v(\alpha)} \bmod \mathfrak{m}$$

(здесь $\mathfrak{m}$ — максимальный идеал кольца целых поля k, v — $\mathfrak{m}$-адическое нормирование поля k) и тем самым описать множество всех ручных символов локального поля k.

Значительно сложней обстоит дело с описанием всех диких символов. Если поле k не содержит нетривиальных корней p-ой степени из 1 или характеристика поля k равна p, то любой дикий символ на поле k тривиален. Это утверждение непосредственно следует из определения символа и арифметики локального поля.

Если же k содержит p-ые корни из 1 и ζ — корень максимально возможной степени p^n в k, то можно проверить, что значения дикого символа $c(k^\times, k^\times)$ образуют циклическую группу порядка p^r, $r \leqslant n$, и что p^n-ый символ норменного вычета Гильберта является универсальным диким символом на k.

Тем самым задача явного описания всех диких символов эквивалентна описанию в явном виде символа Гильберта. Эта задача была решена в работах [2] и [3] и построенное в них в явном виде спаривание

$$\delta(\alpha, \beta) = \zeta^{\operatorname{tr} \operatorname{res} \Phi_{\alpha,\beta}/s}$$

является универсальным диким символом на k, совпадающим с символом Гильберта. Здесь степенной ряд $\Phi_{\alpha,\beta}(X)$ однозначно определен элементами α и β, а $s(X)=\zeta(X)^{p^n}-1$, где $\zeta(X)$ — ряд, полученный из разложения корня ζ по степеням π (подробнее см. [2] или [3]).

§ 5. Символы на формальных группах Любина— Тэйта

10°. Обобщим понятие непрерывного символа Стейнберга и зададим его для произвольной формальной группы Любина — Тэйта F, определенной над кольцом $\mathfrak{o}_0$, поле вычетов которого по максимальному идеалу имеет q элементов. Пусть $[\pi_0]$ — эндоморфизм F.

Если $\lambda(X)$ — логарифм формальной группы F, а $\lambda_0(X)$ — логарифм базисной группы Любина — Тэйта F_0, ассоциированной с многочленом $\pi_0 X+X^q$ (см. § 3, п. 8°), то через $\mathscr{E}(X)$ будем обозначать ряд $\lambda^{-1}\circ\lambda_0$, который задает изоморфизм группы F_0 в F (см. (1)).

Пусть $\mathfrak{A}$ — топологический $\mathfrak{o}_0$-модуль, в котором сложение и действие эндоморфизмов из кольца $\mathfrak{o}_0$ индуцировано формальной группой F. Пусть, далее, k — алгебраическое расширение поля частных k_0 кольца $\mathfrak{o}_0$ и $\mathfrak{m}$ — максимальный идеал кольца целых поля k. Рассмотрим группу точек $A(\mathfrak{m})$ формальной группы F (см. § 3, п. 6°).

Определение 4. *Символом* на группе точек $A(\mathfrak{m})$ будем называть непрерывное билинейное спаривание

$$c_F : k^\times \times A(\mathfrak{m}) \mapsto \mathfrak{A},$$

удовлетворяющее соотношению

$$c_F(\alpha, \mathscr{E}(\alpha^m))=0 \tag{4}$$

для любого α из $\mathfrak{m}$ и любого натурального m, не делящегося на q.

Замечание 1. *Билинейность символа c_F означает выполнение следующих равенств*:

$$c_F(\alpha_1\alpha_2, \beta)=c_F(\alpha_1, \beta)+_F c_F(\alpha_2, \beta),$$

$$c_F(\alpha, \beta_1+_F\beta_2)=c_F(\alpha, \beta_1)+_F c_F(\alpha, \beta_2),$$

$$c_F(\alpha,[a](\beta))=ac_F(\alpha, \beta), \quad a\in\mathfrak{o}_0.$$

Замечание 2. *Значения символа c_F образуют $\mathfrak{o}_0$-подмодуль в $\mathfrak{A}$.*

Замечание 3. *Если $q=p$, то условие* (4) *равносильно* $c_F(\alpha, \mathscr{E}(\alpha))=0$.

Определение 5. Символ $c_F : k^\times \times A(\mathfrak{m}) \mapsto \mathfrak{A}$ назовем *универсальным*, если для любого символа $c'_F : k^\times \times A(\mathfrak{m}) \mapsto \mathfrak{A}'$ существует непрерывный гомоморфизм $\sigma : \mathfrak{A} \mapsto \mathfrak{A}'$ такой, что $\sigma\circ c_F = c'_F$.

11°. Если $\mathfrak{R}$ — мультипликативная система представителей в k, то

$$c_F(\mathfrak{R}, A(\mathfrak{m}))=0,$$

так как в $\mathfrak{R}$ возможно извлечение любых степеней p из элементов, а в группе точек $A(\mathfrak{m})$ — деление на любую единицу кольца $\mathfrak{o}_0$.

ЛЕММА 1. *Если натуральное число m не делится на q, то*

$$c_F(\pi, \mathscr{E}(\theta\pi^m)) = 0$$

для любого $\theta \in \mathfrak{R}$. Если же $m = m_0 q^r$, где m_0 не делится на q, то

$$q^r c_F(\pi, \mathscr{E}(\theta\pi^m)) = 0.$$

Доказательство. Проверим первое утверждение леммы. Пусть m не делится на q. Представим m в виде $m = m_1 p^r$, где $(m_1, p) = 1$. Пусть $\theta_1^{p^r} = \theta$, где $\theta_1 \in \mathfrak{R}$. Тогда для элемента $\alpha = \theta_1 \pi^{m_1}$ по определению символа c_F имеем

$$c_F(\alpha, \mathscr{E}(\alpha^{p^r})) = 0,$$

так как по условию m, а значит, и p^r не делятся на q.

Далее,

$$0 = c_F(\alpha, \mathscr{E}(\alpha^{p^r})) = c_F(\theta_1, \mathscr{E}(\alpha^{p^r})) +_F c_F(\pi^{m_1}, \mathscr{E}(\alpha^{p^r})) =$$

$$= m_1 c_F(\pi, \mathscr{E}(\alpha^{p^r})) = m_1 c_F(\pi, \mathscr{E}(\theta\pi^m)).$$

Отсюда следует, что $c_F(\pi, \mathscr{E}(\theta\pi^m)) = 0$, так как m_1 взаимно просто с p. Второе утверждение леммы доказывается аналогично.

Из леммы 1, определения символа c_F и арифметики группы точек $A(\mathfrak{m})$ (см. § 11, п. 32°) непосредственно вытекает следующее

Предложение 1. *Если в группе точек $A(\mathfrak{m})$ нет нетривиальных корней изогении $[\pi_0]$, то любой символ c_F на $A(\mathfrak{m})$ тривиален.*

Пусть теперь в группе точек $A(\mathfrak{m})$ содержатся корни изогении $[\pi_0]$.

ЛЕММА 2. *Модуль значений символа c_F аннулируется изогенией $[\pi_0^r]$ при некотором r, т. е. $\pi_0^r c_F(k^\times, A(\mathfrak{m})) = 0$.*

Доказательство. Группа точек $A(\mathfrak{m})$ имеет в нашем случае следующую систему образующих (см. § 11, п. 32°):

$$\mathscr{E}(\theta\pi^i), \quad \omega_* = \mathscr{E}(\theta_*\pi^{qe_1}), \tag{5}$$

где $\theta, \theta_* \in \mathfrak{R}$, а индекс i принимает натуральные значения, меньшие qe_1, не делящиеся на q (здесь $e_1 = e/(q-1)$, а e — индекс ветвления расширения k/k_0).

Согласно лемме 1, $c_F(\pi, \mathscr{E}(\theta\pi^i)) = 0$. Поэтому значения $c_F(\pi, A(\mathfrak{m}))$ порождены значением $c_F(\pi, \omega_*)$. Далее, если $qe_1 = q^s m_0$, где m_0 не делится на q, то по лемме 1 значение $c_F(\pi, \omega_*)$ аннулируется эндоморфизмом $[q^s]$. Если $q^s = \pi_0^r \varepsilon$, где ε — единица кольца $\mathfrak{o}_0$, то

$$\pi_0^r c_F(\pi, \omega_*) = 0.$$

Таким образом, изогения $[\pi_0^r]$ аннулирует $c_F(\pi, A(\mathfrak{m}))$, а значит, и $c_F(k^\times, A(\mathfrak{m}))$, поскольку мультипликативная группа $k^\times$ порождена произведениями простых элементов. Лемма доказана.

12°. Проверим теперь, что $\mathfrak{o}_0$-модуль $c_F(k^\times, A(\mathfrak{m}))$ имеет одну образующую.

Предложение 2. *Модуль значений символа c_F порожден значением на паре π, ω, где π — произвольный простой элемент, а ω — примарная образующая группы точек $A(\mathfrak{m})$* (см. § 11, п. 31°).

Доказательство. Проверим, что для любого простого элемента π значения $c_F(U, A(\mathfrak{m}))$ содержатся в $c_F(\pi, A(\mathfrak{m}))$ (здесь U — группа главных единиц поля k). Пусть $\varepsilon \in U$ и β — некоторый элемент из $A(\mathfrak{m})$. Тогда найдется главная единица η в поле k такая, что $\beta = \mathscr{E}(\varepsilon - \eta)$.

Из определения символа c_F следует, что $c_F(\varepsilon - \eta, \mathscr{E}(\varepsilon - \eta)) = 0$. Отсюда, используя линейность символа по первому аргументу, получим:

$$c_F(\varepsilon, \beta) = -c_F(1 - \varepsilon^{-1}\eta, \beta).$$

Обозначим $1 - \varepsilon^{-1}\eta$ через α и прибавим к правой части символ $c_F(\alpha, \mathscr{E}(\alpha))$, равный по определению нулю. Тогда

$$c_F(\varepsilon, \beta) = c_F(\alpha, \mathscr{E}(\alpha)) \underset{F}{\frown} c_F(\alpha, \beta) = c_F(\alpha, \beta_1), \tag{6}$$

где через β_1 обозначен элемент $\mathscr{E}(\alpha) \underset{F}{\frown} \mathscr{E}(\varepsilon - \eta)$.

Нетрудно видеть, что порядок элемента β_1 строго больше порядка элемента β, т. е. $v(\beta_1) > v(\beta)$ (здесь v — показатель в поле k). Действительно, имеют место сравнения

$$\mathscr{E}(\alpha) \equiv \alpha \bmod \alpha^2, \quad \beta = \mathscr{E}(\varepsilon - \eta) \equiv \varepsilon\alpha \bmod \alpha^2,$$

откуда, в частности, следует, что $v(\alpha) = v(\beta)$. Далее, из определения формального группового закона $F(X, Y)$ получаем:

$$\beta_1 = \mathscr{E}(\alpha) \underset{F}{\frown} \mathscr{E}(\varepsilon\alpha) \equiv \mathscr{E}(\alpha) - \mathscr{E}(\varepsilon\alpha) \equiv (1 - \varepsilon)\alpha \bmod \alpha^2.$$

Так как ε — главная единица и $v(\alpha) = v(\beta)$, то из последнего сравнения получим $v(\beta_1) > v(\beta)$.

Элемент α можно представить в виде $\alpha = \pi^{a_1}\theta_1\varepsilon_1$, где $a_1 \geqslant 1$, $\theta_1 \in \mathfrak{R}$, ε_1 — главная единица. Тогда из (6) и линейности символа c_F следует:

$$c_F(\varepsilon, \beta) = c_F(\alpha, \beta_1) = a_1 c_F(\pi, \beta_1) + {}_F c_F(\varepsilon_1, \beta_1).$$

Продолжаем процесс с символом $c_F(\varepsilon_1, \beta_1)$ до тех пор, пока не придем к разложению

$$c_F(\varepsilon, \beta) = \sum_{i=1}^{m} {}_{(F)} a_i c_F(\pi, \beta_i) + {}_F c_F(\varepsilon_m, \beta_m),$$

в котором элемент β_m имеет настолько большой порядок, что он будет делиться в группе точек $A(\mathfrak{m})$ на изогению $[\pi_0^r]$, т. е. $\beta_m = [\pi_0^r](\beta'_m)$, где $\beta'_m \in A(\mathfrak{m})$. Тогда $c_F(\varepsilon_m, \beta_m) = \pi_0^r c_F(\varepsilon_m, \beta'_m) = 0$ (напомним, что π_0^r аннулирует $c_F(k^\times, A(\mathfrak{m}))$ и поэтому

$$c_F(\varepsilon, \beta) = c_F(\pi, \beta'),$$

где $\beta' = \sum_{i=1}^{m} [a_i]\beta_i \in A(\mathfrak{m})$. Таким образом, значения символа $c_F(k^\times, A(\mathfrak{m}))$

совпадают со значениями $c_F(\pi, A(\mathfrak{m}))$. Отсюда и из леммы 1 следует утверждение нашего предложения.

Из только что доказанного предложения, а также из леммы 2 вытекает следующее

Предложение 3. *Модуль значений* $c_F(k^\times, A(\mathfrak{m}))$ *изоморфно вкладывается в ядро изогении* $[\pi_0^r]$ *при некотором* r.

Итак, мы проверили, что $\mathfrak{o}_0$-модуль $c_F(k^\times, A(\mathfrak{m})$ имеет одну образующую $c_F(\pi, \omega_*)$ и изоморфно вкладывается в $\varkappa_r$-ядро изогении $[\pi_0^r]$. Нашей ближайшей задачей будет построение универсального символа, а также доказательство того, что $c_F(k^\times, A(\mathfrak{m}))$ изоморфно вкладывается в группу точек $A(\mathfrak{m})$.

§ 6. Спаривание $\langle , \rangle_F$ как символ на группе Любина — Тэйта

В этом и следующем параграфах мы займемся задачей явного описания универсального символа формальной группы Любина — Тэйта. Для этого мы рассмотрим спаривание $\langle,\rangle_F$, впервые построенное в работе [4], и проверим, что оно является символом на F и задает универсальный символ на F (см. ниже теоремы 1 и 3). Мы считаем, что p — нечетное простое число.

13°. Пусть $\varkappa_n$—$\mathfrak{o}_0$-модуль корней изогении $[\pi_0^n]$, содержащийся в группе точек $A(\mathfrak{m})$, и при этом n имеет максимально возможное значение. Рассмотрим спаривание

$$\langle,\rangle_F\colon\ k^\times \times A(\mathfrak{m}) \to \varkappa_n,$$

которое задается при $p \neq 2$ следующим образом. Пусть α — элемент мультипликативной группы $k^\times$, а β — элемент группы точек $A(\mathfrak{m})$, и пусть $\alpha = \pi^a \theta \varepsilon$, где $\theta \in \mathfrak{R}$, а ε — главная единица поля k. Обозначим через $\mathrm{A}(X)$ ряд $X^a \theta \varepsilon(X)$, где $\varepsilon(\pi) = \varepsilon$. Аналогично, через $\beta(X)$ обозначим ряд, получающийся из разложения элемента β по степеням простого элемента π, т. е. $\beta(\pi) = \beta$. Отметим, что при этом коэффициенты ряда $\mathrm{A}(X)$ принадлежат кольцу целых элементов $\mathfrak{o}'$ абсолютного подполя инерции T' поля k, а коэффициенты ряда $\beta(X)$ принадлежат кольцу целых элементов $\mathfrak{o}$ подполя инерции T расширения k/k_0. Ясно, что $\mathfrak{o}' \subset \mathfrak{o}$. Фиксируем образующую ξ модуля $\varkappa_n$, и пусть $z(X)$ — ряд, полученный из разложения ξ по степеням π, т. е. $z(\pi) = \xi$. Через $s(X)$ обозначим ряд $[\pi_0^n] z(X)$.

Пусть δ — автоморфизм Фробениуса поля T', который на поле вычетов действует возведением в степень p, и пусть $\Delta = \delta^f$ — автоморфизм Фробениуса расширения T/k_0. Оператор следа в расширении T/k_0 обозначаем через tr.

Рассмотрим функцию

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

определенную для любого степенного ряда $\varepsilon(X)$ с коэффициентами из кольца $\mathfrak{o}'$, который начинается с 1; а также функцию

$$l_F(\beta) = \left(1 - \frac{\Delta}{\pi_0}\right)\lambda(\beta), \tag{7}$$

определенную для любого степенного ряда $\beta(X)$ без свободного члена из кольца $\mathfrak{o}[[X]]$.

Определим спаривание $\langle,\rangle_F$ по формуле

$$\langle\alpha,\ \beta\rangle_F = [\operatorname{tr}\gamma_{\alpha,\beta}](\xi), \tag{8}$$

где $\gamma_{\alpha,\beta} = \operatorname{res}\Phi_{\alpha,\beta}/s$, а ряд $\Phi_{\alpha,\beta}$ задается в виде

$$\Phi_{\alpha,\beta} = l_m(\varepsilon)\frac{d}{dX}l_F(\beta) - l_m(\varepsilon)\frac{d}{dX}\lambda(\beta) + l_F(\beta)\,\mathrm{A}^{-1}\frac{d\mathrm{A}}{dX}.$$

Замечание 4. Ряд $\Phi_{\alpha,\beta}$ является степенным рядом с коэффициентами из кольца $\mathfrak{o}$, а ряд $\Phi_{\alpha,\beta}/s$ принадлежит кольцу $\mathfrak{o}\{X\}$, которое состоит из всех рядов $\sum_{-\infty}^{\infty} a_i X^i$, $a_i \in \mathfrak{o}$, удовлетворяющих условию: $a_i \to 0$, если $i \to -\infty$ (см. § 1, п. 3°).

Замечание 5. Несложно проверить (см. [4, предложение 4]), что спаривание $\langle,\rangle_F$ является $\mathbf{Z}_p$-линейным по первому аргументу и $\mathfrak{o}_0$-линейным по второму. Это свойство мы будем для простоты называть билинейностью.

Замечание 6. Поскольку на протяжении всего параграфа у нас будет фиксирована формальная группа F, то мы будем обозначать наше спаривание просто $\langle,\rangle$ или $\langle,\rangle_\pi$, если нам надо подчеркнуть простой элемент π, относительно которого было задано спаривание.

14°. Предложение 4. *Значения спаривания $\langle,\rangle$ не зависят от выбора простого элемента π и от способа разложения элементов в степенные ряды по π.*

Доказательство. Утверждение предложения было доказано в теореме 1 работы [4] на множестве $\{\pi, A(\mathfrak{m})\}$. Докажем, что этого достаточно и для общего случая.

Инвариантность от выбора π нужно доказывать, учитывая билинейность лишь для пары главной единицы $\varepsilon \in k^\times$ и произвольного элемента $\beta \in A(\mathfrak{m})$. При этом надо проверить для произвольных простых элементов π и τ следующее равенство:

$$\langle\varepsilon,\ \beta\rangle_\pi = \langle\varepsilon,\ \beta\rangle_\tau. \tag{9}$$

Обозначим через ρ простой элемент $\pi\varepsilon$. Тогда, согласно доказанной в теореме 1 работы [4] инвариантности, имеем:

$$\langle\rho,\ \beta\rangle_\rho = \langle\rho,\ \beta\rangle_\pi, \quad \langle\rho,\ \beta\rangle_\rho = \langle\rho,\ \beta\rangle_\tau.$$

Отсюда и из билинейности спаривания следует:

$$\langle\rho,\ \beta\rangle_\pi = \langle\pi,\ \beta\rangle_\pi +_F \langle\varepsilon,\ \beta\rangle_\pi,$$

$$\langle\rho,\ \beta\rangle_\tau = \langle\pi,\ \beta\rangle_\tau +_F \langle\varepsilon,\ \beta\rangle_\tau = \langle\pi,\ \beta\rangle_\pi +_F \langle\varepsilon,\ \beta\rangle_\tau.$$

Из последних двух равенств вытекает требуемая инвариантность (9).

Проверим теперь независимость спаривания $\langle,\rangle$ от разложения элементов в степенные ряды по простому элементу π. Нам надо проверить независимость отдельно по первому и второму аргументу.

Если первым аргументом является главная единица $\varepsilon\in k^\times$, то из инвариантности следует:

$$\langle\varepsilon, \beta\rangle_\pi = \langle\tau, \beta\rangle_\pi \underset{F}{\sim} \langle\pi, \beta\rangle_\pi = \langle\tau, \beta\rangle_\tau \underset{F}{\sim} \langle\pi, \beta\rangle_\pi,$$

где $\tau=\pi\varepsilon$. Поэтому в этом случае независимость от разложения β в ряд по простому элементу вытекает из уже доказанной в теореме 1 работы [4] независимости на паре простого элемента и β. В общем случае независимость по второму аргументу следует из билинейности спаривания.

Осталось доказать независимость спаривания $\langle,\rangle$ от разложения первого аргумента в степенной ряд по простому элементу π. Иначе говоря, надо проверить, что если $A(X)$ и $A^{(1)}(X)$ — ряды, полученные из двух различных разложений элемента $\alpha\in k^\times$ в ряд по π, то для любого элемента β из $A(\mathfrak{m})$

$$\operatorname{tr}\gamma_{\alpha,\beta} \equiv \operatorname{tr}\gamma^{(1)}_{\alpha,\beta} \bmod \pi_0^n \tag{10}$$

(см. (8)). Обозначим $\operatorname{tr}\gamma_{\alpha,\beta}$ через $\{A(X), \beta(X)\}_X$. Из билинейности спаривания следует, что сравнение (10) равносильно сравнению

$$\{\varepsilon(X), \beta(X)\}_X \equiv 0 \bmod \pi_0^n, \tag{11}$$

где $\varepsilon(X)$ — произвольный степенной ряд с коэффициентами из кольца $\mathfrak{o}'$, начинающийся с 1, и значение которого в точке $X=\pi$ равно 1, т. е. $\varepsilon(\pi)=1$.

Рассмотрим ряд $Y=g(X)=X\varepsilon(X)$. Тогда для ряда $g^{-1}(X)$, так же как и для ряда $g(X)$, выполнено условие

$$g^{-1}(\pi)=\pi$$

(здесь g^{-1} — ряд, обратный к g относительно суперпозиции).

Инвариантность спаривания $\langle,\rangle$ дает сравнение

$$\{g(X), \beta(X)\}_X \equiv \{Y, \beta(g^{-1}(Y))\}_Y \bmod \pi_0^n. \tag{12}$$

Формально заменив Y на X, получаем:

$$\{Y, \beta(g^{-1}(Y))\}_Y = \{X, \beta(g^{-1}(X))\}_X. \tag{13}$$

Из условия $g^{-1}(\pi)=\pi$ следует, что значения рядов $\beta(X)$ и $\beta(g^{-1}(X))$ в точке $X=\pi$ совпадают. Поэтому из независимости спаривания $\langle,\rangle$, доказанной в теореме 1 работы [4], получаем:

$$\{X, \beta(g^{-1}(X))\}_X \equiv \{X, \beta(X)\}_X \bmod \pi_0^n. \tag{14}$$

Наконец, из (12), (13) и (14) следует:

$$\{g(X), \beta(X)\}_X \equiv \{X, \beta(X)\}_X \bmod \pi_0^n.$$

Отсюда и из линейности по первому аргументу вытекает (11), так как $g(X) = X\varepsilon(X)$. Предложение полностью доказано.

15°. ТЕОРЕМА 1. *Спаривание* $\langle,\rangle_F$ (*см.* (8)) *задает непрерывный символ на* F.

Доказательство. В предыдущем предложении была доказана корректность определения спаривания $\langle,\rangle$. Билинейность $\langle,\rangle$ была проверена в [4], предложение 4. Осталось поэтому доказать, что для любого элемента α из максимального идеала $\mathfrak{m}$ поля k имеет место равенство

$$\langle \alpha, \mathscr{E}(\alpha^u)\rangle = 0 \tag{15}$$

для любого натурального числа u, не делящегося на q.

Пусть $\alpha = \pi^a\theta\varepsilon$, где $\theta \in \mathfrak{R}$, а ε — главная единица поля k. Равенство (15) будет доказано, согласно определению (8), если мы проверим выполнение сравнения

$$\operatorname{tr} \gamma_{\alpha, \mathscr{E}(\alpha^u)} \equiv 0 \bmod \pi_0^n. \tag{16}$$

Ряд $\Phi(X)$, входящий в определение спаривания $\langle,\rangle$, имеет в нашем случае вид:

$$\Phi = l_F(\mathscr{E}(\mathrm{A}^u))\,\mathrm{A}^{-1}\frac{d\mathrm{A}}{dX} - l_m(\varepsilon)\frac{d}{dX}\frac{\Delta}{\pi_0}\lambda(\mathscr{E}(\mathrm{A}^u)).$$

Пусть $\lambda_0(X) = X + c_2X^2 + \ldots$ — логарифм базисной формальной группы Любина — Тэйта F_0, ассоциированной с эндоморфизмом $\pi_0X + X^q$, и пусть

$$c_v' = \begin{cases} c_v, & \text{если } v \text{ не делится на } q, \\ c_v - \dfrac{1}{\pi_0}c_{v/q}, & \text{если } v \text{ делится на } q. \end{cases}$$

Из определения функции l_F (см. (7)) и ряда $\mathscr{E}(X) = \lambda^{-1}\circ\lambda_0$ получаем:

$$l_F(\mathscr{E}(\mathrm{A}^u)) = \left(1 - \frac{\Delta}{\pi_0}\right)\lambda(\mathrm{A}^u) = \sum_{q \nmid v} c_v\mathrm{A}^{uv} + \sum_{v=1}^{\infty}\left(c_{qv}\mathrm{A}^{uvq} - \frac{c_v}{\pi_0}\mathrm{A}^{uv\Delta}\right) =$$

$$= \sum_{v=1}^{\infty} c_v'\mathrm{A}^{uv} + \sum_{v=1}^{\infty}\frac{c_v}{\pi_0}(\mathrm{A}^{uvq} - \mathrm{A}^{uv\Delta}).$$

Аналогично

$$\frac{\Delta}{\pi_0}\lambda(\mathscr{E}(\mathrm{A}^u)) = \sum_{v=1}^{\infty}\frac{c_v}{\pi_0}\mathrm{A}^{uv\Delta}.$$

Поэтому ряд Φ можно переписать в виде

$$\Phi = \sum_{v=1}^{\infty} c'_v \frac{d}{dX} \frac{A^{uv}}{uv} + \sum_{v=1}^{\infty} \frac{c_v}{\pi_0} \left\{ (A^{uvq} - A^{uv\Delta}) A^{-1} \frac{d}{dX} A - l_m(\varepsilon) \frac{d}{dX} A^{uv\Delta} \right\}.$$

Обозначим ряд, стоящий в скобках $\{\ldots\}$, через $f_{u,v}$ и проверим, что для всех $v \geqslant 1$ и всех u, не делящихся на q, имеют место сравнения:

$$\operatorname{tr res} c'_v \left(\frac{d}{dX} \frac{A^{uv}}{uv} \right) / s \equiv 0 \bmod \pi_0^n, \tag{17}$$

$$\operatorname{tr res} \frac{c_v}{\pi_0} f_{u,v}/s \equiv 0 \bmod \pi_0^n. \tag{18}$$

Эти сравнения дадут (16), а значит, и требуемое равенство (15).

Пусть $v = q^s v_0$, где v_0 не делится на q, и пусть $uv = q^r u_0$, где u_0 тоже не делится на q. Заметим, что если $q = p$, то обязательно $r = s$, если же $q \geqslant p^2$, то r может быть равным $s+1$, когда uv_0 делится на q (напомним, что у нас по условию u не делится на q). В любом случае, как будет доказано ниже в (45), элемент

$$c'_v \equiv 0 \bmod \pi_0^r. \tag{19}$$

Если при этом $r \geqslant n$, то сравнение (17) очевидно. Если же $0 \leqslant r < n$, то сравнение (17) следует из (19) и ниже доказываемого сравнения (44), в котором в качестве m надо брать uv.

Для проверки сравнения (18) используем легко проверяемые равенства:

$$\begin{aligned} \frac{d}{dX} h^{\Delta} &= qX^{-1} \left(X \frac{d}{dX} h \right)^{\Delta}, \\ h^{-1} \frac{dh}{dX} &= \frac{d}{dX} l_m(\psi) + h^{-\Delta} \frac{d}{dX} \frac{h^{\Delta}}{q}, \end{aligned} \tag{20}$$

справедливые для любого степенного ряда $h(X)$ с коэффициентами из кольца $\mathfrak{o}'$, если при этом $h = X^a \theta \psi(X)$, где $\theta \in \mathfrak{R}$, а степенной ряд ψ начинается с 1.

Пользуясь этими равенствами, ряд $f_{u,v}$ можно переписать в виде

$$f_{u,v} = \frac{d}{dX} \left(\frac{A^{uvq} - A^{uv\Delta}}{uvq} - l_m(\varepsilon) A^{uv\Delta} \right) = \frac{d}{dX} g_{u,v}.$$

Коэффициенты ряда $\frac{q}{p} g_{u,v}$ делятся на uvq (см. ниже (38)), т. е. делятся на q^{r+1}. С другой стороны, согласно (46) элемент $\pi_0^{r+1} \left(\frac{c_v}{\pi_0} \right)$ будет целым, значит, и ряд $\frac{q}{\pi} \left(\frac{c_v}{\pi_0} \cdot g_{u,v} \right)$ имеет целые коэффициенты. Кроме того, из того же сравнения (38) следует, что ряд $\frac{c_v}{\pi_0} f_{u,v}$ также имеет целые коэффициенты.

Значит, мы можем воспользоваться доказанным в § 11 сравнением (42), из которого следует, что

$$\operatorname{res}\frac{c_v}{\pi_0} f_{u,v}/s = \operatorname{res}\left(\frac{d}{dX}\frac{c_v}{\pi_0} g_{u,v}\right)\Big/ s \equiv 0 \bmod \pi_0^n.$$

Тем самым сравнение (18) доказано. Как уже говорилось, сравнения (17) и (18) дают требуемое равенство (15). Теорема доказана.

§ 7. Универсальный символ для формальной группы Любина — Тэйта

В этом параграфе будет доказано, что $\mathfrak{o}_0$-модуль значений $c_F(k^\times, A(\mathfrak{m}))$ любого символа c_F изоморфно вкладывается в группу точек $A(\mathfrak{m})$. Кроме того, мы проверим, что спаривание $\langle , \rangle_F$ задает универсальный символ для F. Основой, на которой будут доказываться эти утверждения, является невырожденность спаривания $\langle , \rangle_F$ по второму аргументу (см. ниже § 10, теорему 5). Так же как и в § 6, мы предполагаем, что p — нечетное простое число.

16°. Пусть $\varkappa_n$ — модуль корней изогении $[\pi_0^n]$ формальной группы F, содержащийся в группе точек $A(\mathfrak{m})$ с максимально возможным n, и пусть $\varkappa_r = c_F(k^\times, A(\mathfrak{m}))$ — модуль значений символа c_F на F (см. предложение 3).

ТЕОРЕМА 2. *Модуль значений символа c_F формальной группы Любина — Тэйта F изоморфно вкладывается в группу точек $A(\mathfrak{m})$ и, таким образом, выполняется неравенство $r \leqslant n$.*

Доказательство. Пусть ξ — некоторая образующая $\mathfrak{o}_0$-модуля $\varkappa_n$, содержащаяся в группе точек $A(\mathfrak{m})$. Согласно доказанной в теореме 5 невырожденности спаривания $\langle , \rangle_F$ для элемента ξ найдется простой элемент π такой, что значение $\langle \pi, \xi \rangle_F$ является также образующим в $\mathfrak{o}_0$-модуле $\varkappa_n$. Поскольку $\langle \pi, \mathscr{E}(\theta\pi^m) \rangle_F = 0$ для любого m, не делящегося на q, и $\theta \in \mathfrak{R}$ (см. (15)), то в разложение элемента ξ по базису (5) обязательно входит примарный элемент ω_* с некоторым единичным коэффициентом.

Меняя, если нужно, образующую ξ, мы можем считать этот коэффициент равным 1. Поэтому

$$\xi = \sum_{\substack{1 \leqslant m < qe_1 \\ q \nmid m}} [r_m]\, \mathscr{E}(\theta_{r,m}\pi^m) +_F \omega_* = \beta' +_F \omega_*,$$

где $r_m \in \mathfrak{o}_0$. Для символа c_F значение $c_F(\pi, \mathscr{E}(\theta\pi^m))$ равно нулю, если m не делится на q и $\theta \in \mathfrak{R}$ (см. лемму 1), значит,

$$c_F(\pi, \xi) = c_F(\pi, \beta') +_F c_F(\pi, \omega_*) = c_F(\pi, \omega_*).$$

Таким образом, $c_F(\pi, \xi)$, как и $c_F(\pi, \omega_*)$, является образующим элементом $\mathfrak{o}_0$-модуля значений символа c_F. Но

$$\pi_0^n c_F(\pi, \xi) = c_F(\pi, [\pi_0^n](\xi)) = c_F(\pi, 0) = 0.$$

Отсюда сразу следует, что $r \leqslant n$, и теорема вытекает теперь из предложения 2.

17°. Модуль значений спаривания $\langle , \rangle_F$ совпадает с ядром изогении $[\pi_0^n]$, при этом n — максимально возможное число, для которого ядро $\varkappa_n$ содержится в группе точек $A(\mathfrak{m})$. С другой стороны, $\mathfrak{o}_0$-модуль значений любого символа c_F изоморфен $\varkappa_r$, где $r \leqslant n$, по только что доказанной теореме. Отсюда немедленно вытекает следующая

ТЕОРЕМА 3. *Спаривание $\langle , \rangle_F$ является универсальным символом при $p \neq 2$ для формальной группы Любина — Тэйта F.*

§ 8. Явная форма символа Гильберта

Мы используем теперь теорию символов на формальных группах Любина — Тэйта, которая была развита в предыдущих параграфах, для получения явной формы символа Гильберта на формальной группе F (см. также [4]). Мы проверим также, что символ Гильберта на F будет (наряду со спариванием $\langle , \rangle_F$) являться универсальным символом, невырожденным по второму аргументу (см. замечание 7).

18. Напомним определение и основные свойства символа Гильберта на формальной группе Любина — Тэйта F (см. [9], [4], [6]). Пусть в группе точек $A(\mathfrak{m})$ содержатся все корни изогении $[\pi_0^n]$, т. е. $\varkappa_n \subset A(\mathfrak{m})$. Тогда для любого β из $A(\mathfrak{m})$ расширение K поля k, полученное делением точки β на изогению $[\pi_0^n]$, будет абелевым над k. Если ρ — один из корней уравнения $[\pi_0^n](X) = \beta$, то отображение $\sigma \mapsto \rho^{\sigma} \underset{F}{\smile} \rho$ является вложением группы Галуа $G(K/k)$ в $\varkappa_n$, которое не зависит от выбора ρ.

Под символом Гильберта на формальной группе F понимаем спаривание

$$(,)_F : k^{\times} \times A(\mathfrak{m}) \mapsto \varkappa_n,$$

которое задается равенством

$$(\alpha, \beta)_F = \rho^{\sigma_\alpha} \underset{F}{\smile} \rho,$$

где σ_α — элемент группы Галуа, соответствующий элементу α в силу локальной теории полей классов.

Это спаривание $\mathbf{Z}_p$-линейно по первому аргументу и $\mathfrak{o}_0$-линейно по второму ($\mathfrak{o}_0$ — кольцо, над которым определена F). Ядро спаривания по второму аргументу равно $[\pi_0^n]A(\mathfrak{m})$. Спаривание $(\alpha, \beta)_F$ равно 0 тогда и только тогда, когда элемент α является нормой в расширении K/k, полученном делением β на изогению $[\pi_0^n]$. Наконец, если G — формальная группа над $\mathfrak{o}_0$, изоморфная F, и ряд $f(X)$ задает этот изоморфизм, т. е. $f : F \mapsto G$, то

$$f((\alpha, \beta)_F) = (\alpha, f(\beta))_G. \tag{21}$$

Это равенство вытекает непосредственно из определения символа Гильберта, так как формальный групповой закон G имеет вид $G(X, Y) = f(F(f^{-1}(X), f^{-1}(Y)))$, изогения $[\pi_0^n]_G$ группы G выражается через изогению $[\pi_0^n]_F$ группы F в виде $[\pi_0^n]_G = f \circ [\pi_0^n]_F \circ f^{-1}$ и группа корней изогении $[\pi_0^n]_G$ есть множество $f(\varkappa_n)$.

Ниже будет доказано еще одно важное свойство символа Гильберта — невырожденность по второму аргументу (см. замечание 7).

19°. Пусть $\lambda(X)$ — логарифм формальной группы F, а $\lambda_0(X)$ — логарифм базисной группы Любина — Тэйта F_0, ассоциированной с эндоморфизмом $[\pi_0]_0 = \pi_0 X + X^q$. Как и раньше, ряд $\lambda^{-1} \circ \lambda_0$ обозначаем через $\mathscr{E}(X)$.

ЛЕММА 3. *Для любого элемента α из группы точек $A(\mathfrak{m})$ и любого натурального m, взаимно простого с p, имеет место равенство*

$$(\alpha, \mathscr{E}(\alpha^m))_F = 0. \tag{22}$$

Доказательство. Для формальной группы F_0 элемент α является, очевидно, мультипликативной нормой в расширении поля k, полученном делением точки α на изогению $[\pi_0^n]$, так как ряд $[\pi_0^n]_0$ является унитарным многочленом. Значит, $(\alpha, \alpha)_{F_0} = 0$ для всех $\alpha \in \mathfrak{m}$ (см. п. 18°). Далее, ряд $\mathscr{E} = \lambda^{-1} \circ \lambda_0$ задает изоморфизм из группы F_0 в F, поэтому

$$(\alpha, \mathscr{E}(\alpha))_F = \mathscr{E}((\alpha, \alpha)_{F_0}) = \mathscr{E}(0) = 0$$

(см. (21)). Равенство (22) следует теперь из того, что m — единица кольца $\mathfrak{o}_0$. Лемма доказана.

Предложение 5. *Символ Гильберта $(,)_F$ является универсальным символом для формальной группы Любина — Тэйта F, если $q = p$.*

Доказательство. Из непрерывности, билинейности символа Гильберта (которые вытекают непосредственно из определения), а также леммы 3 следует, что символ Гильберта $(,)_F$ является символом на F в смысле определения 4 § 5.

Пусть в группе точек $A(\mathfrak{m})$ содержится ядро изогении $[\pi_0^n]$ формальной группы F и при этом n — максимально возможное число. Значение $(\pi, \omega)_F$, где ω — π_0^n-примарный элемент в $A(\mathfrak{m})$, является образующим ядра $\varkappa_n$ изогении $[\pi_0^n]$ (см. [4], [5]). Значит, модуль значений символа Гильберта совпадает с ядром $\varkappa_n$. Отсюда, так же как и в теореме 3, следует универсальность символа Гильберта. Предложение доказано.

20°. В этом пункте будет доказана лемма, принадлежащая Ги Эньяру (Guy Henniart). Автор глубоко признателен профессору Эньяру, который сообщил ему об этом результате.

Рассмотрим группу Любина — Тэйта $F_{\rho,\eta}$, которая построена по эндоморфизму $[\pi_0]_{\rho,\eta} = \pi_0 X + \pi_0 \eta X^{p^\rho} + X^q$, где η — элемент мультипликативной системы $\mathfrak{R}$, а ρ принимает значения 1, 2, ..., f—1 (напомним,

что $q=p^f$). Пусть $\mathscr{E}_{\rho,\eta}(X)$ — степенной ряд, задающий изоморфизм из формальной группы $F_{\rho,\eta}$ в данную группу Любина — Тэйта F.

ЛЕММА 4. *Элементы*

$$\mathscr{E}(\theta\pi^i), \quad \mathscr{E}_{\rho,\eta}(\theta\pi^i), \tag{23}$$

где θ, $\eta\in\mathfrak{R}$, $1\leqslant\rho\leqslant f-1$, *а индекс* i *пробегает все натуральные взаимно простые с* p *значения, меньшие* qe_1, *дают вместе с примарным элементом* $\omega(a)$ (см. § 11, п. 31°) *полную систему* $\mathfrak{o}_0$*-образующих группы точек* $A(\mathfrak{m})$. *При этом*

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

Доказательство. Достаточно проверить, очевидно, утверждение леммы для базисной формальной группы Любина — Тэйта F_0 (см. § 3, п. 8°), т. е. для $F=F_0$. Из вида эндоморфизмов групп $F_{\rho,\eta}$ и F_0 легко следует сравнение

$$\mathscr{E}_{\rho,\eta}(X)\equiv X+\frac{\eta}{1-\pi_0^{p^\rho-1}}X^{p^\rho} \bmod X^{p^{\rho+1}}.$$

Отсюда получаем:

$$\mathscr{E}_{\rho,\eta}(X)\underset{F_0}{\sim}X\equiv\frac{\eta}{1-\pi_0^{p^\rho-1}}X^{p^\rho} \bmod X^{p^{\rho+1}}$$

и, значит,

$$\mathscr{E}_{\rho,\eta}(\theta\pi^i)\underset{F_0}{\sim}(\theta\pi^i)\equiv\eta\theta^{p^\rho}\pi^{ip^\rho} \bmod \pi^{ip^{\rho+1}}.$$

Поэтому (см. § 11, п. 32°) эти элементы вместе с $\theta\pi^i$ и примарным элементом $\omega(a)$ дают полную систему образующих группы точек $A_{F_0}(\mathfrak{m})$ (при соответствующих условиях на индексы i и ρ). Мы получаем тем самым первое утверждение леммы.

Далее, поскольку $[\pi_0^n]_{\rho,\eta}$ является унитарным многочленом, то для символа Гильберта группы $F_{\rho,\eta}$ имеет место равенство $(\alpha, \alpha)_{F_{\rho,\eta}}=0$ для любого α из $\mathfrak{m}$ (см. п. 18°). Тогда

$$(\alpha, \mathscr{E}_{\rho,\eta}(\alpha))_{F_0}=0$$

(см. (21)). Отсюда получаем второе утверждение леммы. Лемма доказана.

21°. Найдем теперь явную формулу для символа Гильберта.

ТЕОРЕМА 4. *Символ Гильберта* $(,)_F$ *совпадает со спариванием* $\langle,\rangle_F$, *если* $p\neq2$, *и, значит,*

$$(\alpha, \beta)_F=[\operatorname{tr}\operatorname{res}\Phi_{\alpha,\beta}/s](\xi)$$

(*относительно рядов* $\Phi_{\alpha,\beta}(X)$ *и* $s(X)$ *см.* § 6, *п.* 13°).

Доказательство. Случай $q=p$. Символ Гильберта $(,)_F$ и спаривание $\langle,\rangle_F$ являются универсальными символами на F (см. тео-

рему 3 и предложение 5). При этом значения обоих символов совпадают на паре π, $\omega(a)=E_F(as)\,|_{x=\pi}$ (см. (36)). Поскольку значения $(\pi, \omega)_F$ и $\langle\pi, \omega\rangle_F$ являются образующими в модуле $\varkappa_n$, то это дает совпадение самих символов $(,)_F$ и $\langle,\rangle_F$.

Общий случай. Мы используем доказанную в теореме 1 работы [4] инвариантность и независимость спаривания $\langle,\rangle_F$ на множестве $\{\pi, A(\mathfrak{m})\}$, а также лемму 4. Надо отметить, что мы будем сейчас практически повторять доказательство теоремы 2 работы [4].

Проверим сперва равенство

$$(\pi, \beta)_F=\langle\pi, \beta\rangle_F \tag{24}$$

для любого элемента β из $A(\mathfrak{m})$. Из независимости спаривания $\langle,\rangle_F$ от разложения элементов группы точек $A(\mathfrak{m})$ в степенные ряды по простому элементу π (см. предложение 4) следует, что для элемента β мы можем взять такое представление его в виде ряда от π, которое соответствует разложению β по базису (23).

Для образующих этого базиса мы имеем равенства

$$(\pi, \mathscr{E}(\theta\pi^i))_F=0, \quad (\pi, \mathscr{E}_{\rho,\eta}(\theta\pi^i))_F=0 \tag{25}$$

(см. лемму 4). С другой стороны, как было проверено в теореме 1,

$$\langle\pi, \mathscr{E}(\theta\pi^i)\rangle_F=0$$

и, действуя так же как и при доказательстве равенства (15) в теореме 1, используя при этом соотношения (45) для логарифма группы $F_{\rho,\eta}$ (см. § 11, п. 38°), мы получим:

$$\langle\pi, \mathscr{E}_{\rho,\eta}(\theta\pi^i)\rangle_F=0.$$

Наконец, $(\pi, \omega(a))_F=\langle\pi, \omega(a)\rangle_F$ (см. (36)). Отсюда и из (25) следует (24).

Пусть теперь ε — главная единица поля k. Из инвариантности спаривания $\langle,\rangle_F$ и равенства (24) получаем:

$$\langle\varepsilon, \beta\rangle_\pi = \langle\pi\varepsilon, \beta\rangle_\pi \mathbin{\widetilde{F}} \langle\pi, \beta\rangle_\pi = \langle\tau, \beta\rangle_\tau \mathbin{\widetilde{F}} \langle\pi, \beta\rangle_\pi=$$

$$= (\tau, \beta)_F \mathbin{\widetilde{F}} (\pi, \beta)_F = (\varepsilon, \beta)_F$$

(здесь $\tau=\pi\varepsilon$). Общий случай следует теперь из билинейности символа Гильберта и спаривания $\langle,\rangle_F$. Теорема доказана.

Замечание 7. *Из совпадения символа Гильберта со спариванием $\langle,\rangle_F$ следует его универсальность как символа на группе точек $A(\mathfrak{m})$ формальной группы F, а также его невырожденность по второму аргументу* (см. теоремы 3 и 5).

Замечание 8. *Несомненно, что нельзя ожидать невырожденности символа Гильберта по первому аргументу. Например, в мультипликативном случае примарные элементы из $k^\times$ будут ортогональны всей группе точек $A(\mathfrak{m})$. Было бы интересно выяснить ядро символа Гильберта по первому аргументу в общем случае.*

§ 9. Символы на коммутативной формальной группе

Перейдем теперь к теории символов для произвольных коммутативных формальных групп. Доказательства основных утверждений будут даны конспективно, так как мы надеемся закончить и дать более подробные доказательства в другой статье.

22°. Итак, пусть F — коммутативная формальная группа, заданная над полным дискретно нормированным кольцом $\mathfrak{o}$ с конечным полем вычетов по максимальному идеалу. Пусть при этом F является $\mathfrak{o}_0$-модульным групповым законом относительно некоторого подкольца $\mathfrak{o}_0$ кольца $\mathfrak{o}$ (см. § 2, п. 2°). Если $\mathfrak{m}$ — максимальный идеал кольца целых элементов некоторого алгебраического расширения поля частных k_0 кольца $\mathfrak{o}_0$, то, как и раньше, через $A(\mathfrak{m})$ обозначаем группу точек формальной группы F. Пусть, наконец, $f=[\pi_0]$ — изогения формальной группы F (π_0 — простой элемент в $\mathfrak{o}_0$) и $\varphi(X)=X+d_2X^2+\ldots$ — произвольный степенной ряд с коэффициентами из кольца $\mathfrak{o}_0$.

Для мультипликативной группы $k^\times$, группы точек $A(\mathfrak{m})$ формальной группы F и некоторого топологического $\mathfrak{o}_0$-модуля $\mathfrak{A}$, в котором сложение и действие эндоморфизмов из кольца $\mathfrak{o}_0$ индуцировано формальной группой F, определим φ-символ $c_{F,f}$ следующим образом.

Определение 6. *Непрерывным φ-символом на группе точек $A(\mathfrak{m})$ с изогенией f будем называть непрерывное билинейное спаривание*

$$c_{F,f}: k^\times \times A(\mathfrak{m}) \mapsto \mathfrak{A},$$

удовлетворяющее соотношению

$$c_{F,f}(\alpha,\ \varphi(\alpha^m))=0$$

для любого α из $\mathfrak{m}$ и любого натурального m, не делящегося на $q=p^h$, где h — высота изогении f.

Определение 7. *φ-символ $c_{F,f}: k^\times \times A(\mathfrak{m}) \mapsto \mathfrak{A}$ назовем универсальным, если для любого φ-символа $c'_{F,f}: k^\times \times A(\mathfrak{m}) \mapsto \mathfrak{A}'$ существует непрерывный гомоморфизм $\sigma: \mathfrak{A} \mapsto \mathfrak{A}'$ такой, что $\sigma \circ c_{F,f} = c'_{F,f}$.*

23°. Так же как и в лемме 1, доказываются для произвольного θ из $\mathfrak{R}$ равенства: $c_{F,f}(\pi,\ \varphi(\theta\pi^m))=0$, если m не делится на q, и $f^{(r)}c_{F,f}(\pi,\ \varphi(\theta\pi^m))=0$ при произвольном m и некоторой суперпозиции $f^{(r)}$ изогении f.

Из этих равенств и арифметики группы точек $A(\mathfrak{m})$ получаем, с одной стороны, утверждение о тривиальности φ-символа $c_{F,f}$, когда $A(\mathfrak{m}) \cap \bigcap \ker f=(0)$, а с другой стороны, теорему о том, что модуль значений $c_{F,f}(k^\times,\ A(\mathfrak{m}))$ аннулируется некоторой суперпозицией изогении f.

Группа точек $A(\mathfrak{m})$, кроме образующих вида $\varphi(\theta\pi^i)$, где $\theta \in \mathfrak{R}$, а натуральное число i не делится на $q=p^h$, имеет еще конечный набор примарных образующих вида $\omega_s=\varphi(\theta\pi^{t_s})$, $1 \leqslant s \leqslant m$, где t_s — константы, связанные с многоугольником Ньютона изогении f (см. [1, предложение 2.1]). При этом сами примарные элементы ω_s получаются из корней изогении f, содержащихся в группе точек $A(\mathfrak{m})$.

Практически без всяких изменений, так же как и в предложении 2, доказывается, что модуль значений $c_{F,f}(k^\times, A(\mathfrak{m}))$ порожден значениями на парах $c_{F,f}(\pi, \omega_s)$. Отсюда следует вложение модуля $c_{F,f}(k^\times, A(\mathfrak{m}))$ в ядро изогении $f^{(r)}$ при некотором r.

Для окончания теории φ-символов нам надо доказать существование универсального φ-символа, а также проверить вложение модуля $c_{F,f}(k^\times, A(\mathfrak{m}))$ в группу точек $A(\mathfrak{m})$. Автор видит в настоящий момент единственный путь к проверке этих утверждений — построить универсальный φ-символ, доказать его невырожденность и затем, используя способ, данный в теореме 2, доказать вложение модуля $c_{F,f}(k^\times, A(\mathfrak{m}))$ в группу точек $A(\mathfrak{m})$.

§ 10. Невырожденность спаривания $\langle , \rangle_F$

24° В этом параграфе проверяется невырожденность спаривания $\langle,\rangle_F$ (см. (8)) по второму аргументу. Пусть k_0 — поле, над кольцом целых элементов $\mathfrak{o}_0$ которого определена формальная группа F, и T — подполе инерции в расширении k/k_0, оператор следа в расширении T/k_0 обозначим через tr, а степень этого расширения—через j. Пусть, далее, δ — автоморфизм Фробениуса поля T, который на поле вычетов действует как возведение в степень p, а $\Delta=\delta^f$ — автоморфизм Фробениуса в расширении T/k_0 (здесь f — степень инерции $k_0/\mathbf{Q}_p$). Наконец, через π_0, как и раньше, обозначаем простой элемент поля k_0.

ЛЕММА 5. *Если для всех x из кольца целых элементов $\mathfrak{o}$ поля T выполнено сравнение*

$$\mathrm{tr}\,(c_0x + c_1x^{\delta} + \cdots + c_{f-1}x^{\delta^{f-1}}) \equiv 0 \bmod \pi_0,$$

где $c_0, c_1, \ldots, c_{f-1}$ взяты из $\mathfrak{o}$, то коэффициенты $c_0, c_1, \ldots, c_{f-1}$ делятся на π_0.

Доказательство. Сравнение леммы при переходе к полю вычетов будет означать выполнение следующего равенства:

$$\sum_{s=0}^{f-1}\sum_{r=0}^{j-1} \bar{c}_s^{\Delta^r}\bar{x}^{\Delta^r\delta^s} = 0,$$

где $\bar{c}_s$ и $\bar{x}$ — вычеты элементов c_s и x. Из теоремы Артина о линейной независимости автоморфизмов (см. [7, с. 238]) получаем теперь, что все $\bar{c}_s$ равны нулю в поле вычетов. Лемма доказана.

25°. Возьмем образующую ξ группы корней изогении $[\pi_0^n]$ формальной группы F. Элемент ξ имеет порядок $e_n=e/q^{n-1}(q-1)$ в группе точек $A(\mathfrak{m})$ (см. п. 31°). Пусть $z(X)$ — степенной ряд, полученный из разложения ξ по степеням простого элемента π поля k с коэффициентами из кольца $\mathfrak{o}$, т. е. $z(\pi)=\xi$. Будем считать, что разложение элемента ξ начинается с члена степени e_n. Для ряда $s(X)=[\pi_0^n]z(X)$ имеет место сравнение (см. [4, (17)])

$$1/s(X) \equiv 1/z(X)^{\Delta^n} \bmod \pi_0.$$

Поэтому ряд $1/s$ представляет собой по $\bmod \pi_0$ ряд Лорана со степенями, делящимися на q, и начинающийся с члена степени $(-qe_1)$, т. е.

$$1/s \equiv c_0 X^{-qe_1} + c_1 X^{-qe_1+q} + \cdots \bmod \pi_0. \tag{26}$$

26°. Пусть теперь имеются два натуральных числа m и m', меньших qe_1 и не делящихся на q, и пусть $m=p^r\bar{m}$, $m'=p^{r'}\bar{m}'$, где $\bar{m}$ и $\bar{m}'$ — взаимно простые с p числа. Возьмем, далее, главную единицу ε поля k, представленную в виде

$$\varepsilon = E_p(xX^\mu)\,|_{X=\pi} = \exp\left(x\pi^\mu + \frac{x^{\delta}\pi^{p\mu}}{p} + \frac{x^{\delta^2}\pi^{p^2\mu}}{p^2} + \cdots\right), \tag{27}$$

где $\mu=(qe_1-m)/p^r$, а x — произвольный элемент из кольца $\mathfrak{o}$.

ЛЕММА 6. *Имеет место сравнение*

$$\operatorname{res}\left(aX^{m'}\frac{d}{dX}\log\varepsilon(X)\right)/s \equiv \mu a c x^{\delta^{r'}} \bmod \pi_0,$$

где $a\in\mathfrak{o}$, *а* c — *коэффициент при степени* — $(m'+p^{r'}\mu)$ *в сравнении* (26).

Доказательство. Из определения единицы ε имеем равенство

$$aX^{m'}\frac{d}{dX}\log\varepsilon(X) = X^{-1}\sum_{\alpha=0}^{\infty}\mu a x^{\delta^\alpha} X^{m'+p^\alpha\mu}.$$

Степень $m'+p^\alpha\mu$ может делиться на $q=p^f$ только в случае, когда $\alpha=r'$. Ряд $1/s$ имеет ненулевые коэффициенты по $\bmod \pi_0$ лишь при степенях, делящихся на q. Отсюда и из (26) следует сравнение леммы.

27°. Рассмотрим для произвольного элемента β из группы точек $A(\mathfrak{m})$ его каноническое разложение (см. [4, (40)]), построенное с помощью простого элемента π:

$$\beta = E_F(w_\beta(X))\,|_{X=\pi} +_F \omega(a_\beta), \tag{28}$$

где $w_\beta(X)$ — многочлен, для которого степень каждого его одночлена не делится на q и меньше чем qe_1, а $\omega(a_\beta)$ — π_0^n-примарный элемент. Отметим, что

$$\beta \in [\pi_0]A(\mathfrak{m}) \Leftrightarrow \begin{cases} w_\beta(X) \equiv 0 \bmod \pi_0, \\ \operatorname{tr} a_\beta \equiv 0 \bmod \pi_0 \end{cases} \tag{29}$$

(см. [4, предложение 2]).

28°. В этом пункте мы будем считать, что в каноническом разложении (28) элемента β отсутствует примарный элемент и элемент β не делится в группе точек $A(\mathfrak{m})$ на изогению $[\pi_0]$. Тогда его каноническое разложение по $\bmod [\pi_0]A(\mathfrak{m})$ будет иметь вид

$$\beta = E_F(w_\beta)\,|_{X=\pi} \tag{30}$$

и

$$w_\beta = a_1 X^{m_1} + a_2 X^{m_2} + \cdots + a_t X^{m_t},$$

где все a_i не делятся на π_0, а все степени $m_i < qe_1$ и не делятся на q.

Пусть, далее, α — первый индекс, для которого степень m_α имеет наименьший среди всех m_i порядок входящего в него простого числа p. Если ввести обозначения

$$m_i = p^{r_i}\bar{m}_i, \quad (\bar{m}_i, p) = 1,$$

то при нашем выборе α имеем:

$$\begin{cases} r_\alpha \leqslant r_i & \text{для всех } i \geqslant \alpha, \\ r_\alpha < r_i & \text{для всех } i < \alpha. \end{cases} \tag{31}$$

Заметим также, что при всех i степени

$$r_i \leqslant f-1, \tag{32}$$

так как m_i не делится на $q = p^f$.

Пусть $\mu = (qe_1 - m_\alpha)/p^{r_\alpha}$. Тогда для единицы ε вида (27) будет иметь место следующее сравнение:

$$\operatorname{res}\left(w_\beta \frac{d}{dX}\log \varepsilon\right)\Big/ s \equiv a'_\alpha x^{\delta^{r_\alpha}} + \sum_{i=1}^{\alpha-1} a'_i x^{\delta^{r_i}} \bmod \pi_0, \tag{33}$$

где $a_\alpha' = \mu a_\alpha c_0$, а коэффициент a_i' при $i \neq \alpha$ получается перемножением чисел μ, a_i и коэффициента при степени $-(m_i + p^{r_i}\mu)$ в сравнении (26).

Сравнение (33) вытекает непосредственно из леммы 6, если заметить, что члены с $i \geqslant \alpha$ не войдут в сумму правой части, так как при этом $m_i + p^{r_i}\mu$ будет больше qe_1.

29°. Пусть выполнены предположения предыдущего пункта. Проверим, что тогда имеет место следующее сравнение:

$$\operatorname{res}\left(l_m(\varepsilon)\frac{d}{dX}\left(\frac{\Delta}{\pi_0}\lambda(\beta)\right)\right)\Big/ s \equiv 0 \bmod \pi_0, \tag{34}$$

где $l_m(\varepsilon) = \left(1 - \frac{\Delta}{q}\right)\log \varepsilon$, а $\lambda(X)$ — логарифм формальной группы F.

Легко проверить выполнение следующего равенства:

$$l_m(\varepsilon)\frac{d}{dX}\frac{\Delta}{\pi_0}\lambda(\beta) = \frac{p}{\pi_0}(p^{f-1}l_m(\varepsilon))\,X^{-1}\left(X\frac{d}{dX}\lambda(\beta)\right)^{\Delta}.$$

Из вида единицы ε (см. (27)) получаем:

$$p^{f-1}l_m(\varepsilon) = (p^{f-1} + p^{f-2}\delta + \cdots + \delta^{f-1})\left(\left(1 - \frac{\delta}{p}\right)\log \varepsilon\right) \equiv$$
$$\equiv x^{\delta^{f-1}} X^{p^{f-1}\mu} \bmod \pi_0.$$

Поэтому

$$l_m(\varepsilon)\frac{d}{dX}\frac{\Delta}{\pi_0}\lambda(\beta)\equiv X^{-1}\left\{\frac{p}{\pi_0}x^{\delta f-1}X^{p^f-1}\mu\left(X\frac{d}{dX}\lambda(\beta)\right)^{\Delta}\right\}\bmod\pi_0. \tag{35}$$

Если многочлен $w_\beta(X)$ (см. (30)) имеет степени, взаимно простые с p, то $(m_\alpha, p)=1$ и, значит, $p^f-1\mu$ не делится на q. Отсюда следует, что в скобках $\{\ldots\}$ правой части сравнения (35) стоит ряд, у которого нет членов со степенями, делящимися на q. Но все члены ряда $1/s$ по $\bmod\pi_0$ имеют степени, делящиеся на q, значит,

$$\operatorname{res}X^{-1}\{\ldots\}/s\equiv 0\bmod\pi_0$$

и сравнение (34) в этом случае доказано.

Если же в многочлене $w_\beta(X)$ все степени делятся на p, то его можно представить в виде $w_\beta(X)=h(X)^\delta$, где $h(X)$ — многочлен с целыми коэффициентами. Тогда

$$\lambda(\beta)=w_\beta+\frac{w_\beta^\Delta}{\pi_0}+\cdots=\left(\sum_{i=0}^{\infty}\frac{h^{\Delta^i}}{\pi_0^i}\right)^\delta$$

и поэтому

$$\frac{d}{dX}\lambda(\beta)=pX^{p-1}\left(\frac{d}{dX}\sum\frac{h^{\Delta^i}}{\pi_0^i}\right)^\delta.$$

Отсюда и из (35) получаем:

$$l_m(\varepsilon)\frac{d}{dX}\frac{\Delta}{\pi_0}\lambda(\beta)\equiv$$

$$\equiv X^{-1}\left\{\frac{p^2}{\pi_0}x^{\delta f-1}X^{p^f-1}\mu\left(X\frac{d}{dX}\sum\frac{h^{\Delta^i}}{\pi_0^i}\right)^{\Delta\delta}\right\}\bmod\pi_0.$$

Производная ряда $\sum h^{\Delta^i}/\pi_0^i$ имеет, очевидно, целые коэффициенты. Значит, ряд, стоящий в правой части, $\equiv 0\bmod\pi_0$. Отсюда и в этом случае получаем сравнение (34).

30°. Приступим теперь к доказательству основного результата этого параграфа.

ТЕОРЕМА 5. *Для любого элемента* β *из группы точек* $A(\mathfrak{m})$, *не делящегося в* $A(\mathfrak{m})$ *на изогению* $[\pi_0]$, *найдется простой элемент* π *из поля* k *такой, что значение* $\langle\pi,\beta\rangle$ *является образующей* $\mathfrak{o}_0$*-модуля* $\varkappa_n=\langle k^\times, A(\mathfrak{m})\rangle$.

Доказательство. Если в каноническом разложении (28) элемента β для коэффициента a_β выполнено условие: $\operatorname{tr}a_\beta\not\equiv 0\bmod\pi_0$, то для простого элемента π будем иметь (см. (36))

$$\langle\pi,\beta\rangle=\langle\pi,\omega(a_\beta)\rangle=[\operatorname{tr}a_\beta](\xi)$$

и при этом элемент $[\operatorname{tr}a_\beta](\xi)$ будет снова образующей $\mathfrak{o}_0$-модуля $\varkappa_n$.

Если $\operatorname{tr} a_\beta \equiv 0 \bmod \pi_0$, то элемент β, рассматриваемый по $\bmod [\pi_0] A(\mathfrak{m})$, будет иметь вид (30) (см. (29)).

Рассмотрим в этом случае для элемента β единицу ε, построенную в п. 26°. Тогда по определению спаривания получим (см. (8)):

$$\langle \varepsilon, \beta \rangle = [\operatorname{tr} \gamma_{\varepsilon,\beta}](\xi),$$

где

$$\gamma_{\varepsilon,\beta} = \operatorname{res}\left(l_F(\beta) \frac{d}{dX} \log \varepsilon - l_m(\varepsilon) \frac{d}{dX} \frac{\Delta}{\pi_0} \lambda(\beta) \right).$$

Отметим, что согласно определению функции l_F (см. (7)) имеем $l_F(\beta) = w_\beta(X)$, и поэтому из (33) и (34) получаем:

$$\operatorname{tr} \gamma_{\varepsilon,\beta} \equiv \operatorname{tr} \left(a'_\alpha x^{\delta^{r_\alpha}} + \sum_{i=1}^{\alpha-1} a'_i x^{\delta^{r_i}} \right) \bmod \pi_0.$$

Все степени r_i строго больше r_α и меньше f, а коэффициент a_α' обратим в кольце $\mathfrak{o}$ (см. (31), (32), (33)). Поэтому, согласно лемме 5, найдется x из кольца $\mathfrak{o}$, для которого правая часть последнего сравнения не будет делиться на π_0, значит, для этого x (и тем самым для единицы ε) будем иметь:

$$\operatorname{tr} \gamma_{\varepsilon,\beta} \not\equiv 0 \bmod \pi_0.$$

В этом случае значение $\langle \varepsilon, \beta \rangle$, равное $[\operatorname{tr} \gamma_{\varepsilon,\beta}](\xi)$, будет снова образующей $\mathfrak{o}_0$-модуля $\varkappa_n$.

Для окончания доказательства теоремы возьмем простой элемент $\tau = \pi\varepsilon$, для которого значение

$$\langle \tau, \beta \rangle = \langle \pi, \beta \rangle +_F \langle \varepsilon, \beta \rangle \equiv \langle \varepsilon, \beta \rangle \bmod [\pi_0] \varkappa_n$$

будет образующей в $\varkappa_n$. Теорема доказана.

§ 11. Вспомогательные утверждения

31°. Примарные элементы группы точек $A(\mathfrak{m})$. Пусть F — формальная группа Любина — Тэйта, определенная над кольцом $\mathfrak{o}_0$. Если k — алгебраическое расширение поля отношений k_0 кольца $\mathfrak{o}_0$, то через e обозначаем индекс ветвления расширения k/k_0, $\mathfrak{m}$ — максимальный идеал кольца целых k, $\mathfrak{o}$ — кольцо целых элементов подполя инерции T расширения k/k_0 и, наконец, $q = p^f$ — число элементов поля вычетов поля k_0.

В предложении 1 работы [4] были построены π_0^n-примарные элементы группы точек $A(\mathfrak{m})$ (т. е. элементы, дающие неразветвленное расширение поля k при делении их на изогению $[\pi_0^n]$). А именно, если ξ — фиксированная образующая $\mathfrak{o}_0$-модуля корней изогении $[\pi_0^n]$ и $z(X)$ — степенной ряд, полученный из разложения ξ по степеням π с коэффициентами из $\mathfrak{o}$, т. е. $z(\pi) = \xi$, то π_0^n-примарные элементы в $A(\mathfrak{m})$

имеют вид

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

где $a\in\mathfrak{o}$, $s(X)=[\pi_0^n](z)$ (подробнее см. [4], [5]).

Для π_0^n-примарного элемента $\omega(a)$ выполнены равенства

$$(\pi,\ \omega(a))_F=\langle\pi,\ \omega(a)\rangle_F=[\operatorname{tr}a](\xi), \tag{36}$$

где tr — оператор следа в T/k_0, а также сравнение

$$\omega(a)\equiv a\xi^{q^n} \bmod \pi^{qe_1+1}$$

(см. [4, предложение 1 и § 4]). Образующая ξ имеет порядок $e_n=e/q^{n-1}(q-1)$. Поэтому получаем:

$$\omega(a)\equiv\theta_a\pi^{qe_1} \bmod \pi^{qe_1+1}$$

при некотором θ_a из $\mathfrak{R}$.

32°. Арифметика группы точек $A(\mathfrak{m})$. В работе [4, § 4] был указан критерий для системы образующих в группе точек $A(\mathfrak{m})$: пусть для каждого натурального i, которое не делится на q и не превосходит qe_1, а также для $i=qe_1$ и для каждого $\theta\in\mathfrak{R}$ выбран элемент $\varepsilon_i(\theta)$ в $\mathfrak{o}_0$-модуле $A(\mathfrak{m})$, удовлетворяющий условию $\varepsilon_i(\theta)\equiv\theta\pi^i \bmod \pi^{i+1}$. Тогда элементы $\varepsilon_i(\theta)$ являются системой образующих для $\mathfrak{o}_0$-модуля $A(\mathfrak{m})$.

Отметим, что в качестве элементов $\varepsilon_i(\theta)$ мы можем брать элементы вида $\varphi(\theta\pi^i)$, где $\varphi(X)=X+\ldots$ — произвольный степенной ряд с коэффициентами из кольца $\mathfrak{o}$, а в качестве элемента последней ступени $i=qe_1$ можем брать либо π_0^n-примарный элемент $\omega(a)$, либо $\varphi(\theta\pi^{qe_1})$.

33°. При тех же обозначениях, что и в п. 31° этого параграфа, пусть T' — подполе инерции в $k/\mathbf{Q}_p$ и $\mathfrak{o}'$ — кольцо целых элементов поля T'. Таким образом, $\mathfrak{o}'\subset\mathfrak{o}$. Через δ обозначим автоморфизм Фробениуса в T', который на поле вычетов действует как возведение в степень p, а через $\Delta=\delta^f$ — автоморфизм Фробениуса в расширении T/k_0.

Пусть имеется ряд $g(X)$ из кольца $\mathfrak{o}\{X\}$, которое состоит из всех рядов $\sum_{-\infty}^{\infty} a_iX^i$, $a_i\in\mathfrak{o}$, удовлетворяющих условию: $a_i\to 0$, если $i\to-\infty$ (подробнее см. [4, §1, п. 3°]).

Если $m=q^rm_0$, где $q\nmid m_0$, то несложная индукция по r показывает, что

$$g^{mq}\equiv g^{m\Delta} \bmod \pi_0^{r+1}. \tag{37}$$

Далее, пусть $h(X)$ — произвольный степенной ряд без свободного члена с коэффициентами из кольца $\mathfrak{o}'$. Запишем его в виде $h=X^q\theta\varepsilon(X)$, где θ — элемент мультипликативной системы $\mathfrak{R}$, а $\varepsilon(X)$ — степенной ряд, начинающийся с 1, и проверим выполнение следующе-

го сравнения в кольце $\mathfrak{o}'[[X]]$ при $p \geqslant 3$:

$$h^{mq} - h^{m\Delta} \equiv mql_m(\varepsilon)\, h^{m\Delta} \bmod (mp)^2, \tag{38}$$

где $m \geqslant 1$, а $l_m(\varepsilon) = \left(1 - \frac{\Delta}{q}\right)\log \varepsilon$.

Действительно,

$$h^{mq-m\Delta} = \varepsilon^{mq-m\Delta} = \exp(mq\, l_m(\varepsilon)).$$

Поэтому

$$h^{mq} - h^{m\Delta} = h^{m\Delta}(\exp mql_m(\varepsilon) - 1) =$$

$$= mqh^{m\Delta} l_m(\varepsilon) + h^{m\Delta} \sum_{i=2}^{\infty} \frac{(mp)^i}{i!} \left(\frac{q}{p}\, l_m(\varepsilon)\right)^i. \tag{39}$$

Если $p \geqslant 3$, то легко видеть, что коэффициент $(mp)^i/i!$ делится в $\mathbf{Z}_p$ на число $(mp)^2$. Кроме того, ряд

$$\frac{q}{p}\, l_m(\varepsilon) \in \mathfrak{o}'[[X]],$$

так как $\frac{q}{p}\, l_m(\varepsilon) = (p^{i-1} + p^{i-2}\delta + \cdots + \delta^{i-1})\left(\left(1 - \frac{\delta}{p}\right)\log \varepsilon\right)$ и при этом ряд $l(\varepsilon) = \left(1 - \frac{\delta}{p}\right)\log \varepsilon$ имеет целые коэффициенты (см. [2, лемма 2]). Значит, каждое слагаемое в сумме (39) делится на $(mp)^2$, что дает (38).

Замечание 9. *Можно показать, что сравнение* (38) *справедливо для любого ряда* $h(X)$ *из кольца* $\mathfrak{o}'\{X\}$.

Далее, из очевидных соображений для любого ряда $g(X)$ из кольца $\mathfrak{o}\{X\}$ имеет место сравнение

$$\operatorname{tr} \operatorname{res} X^{-1} g^{\Delta} = \operatorname{tr} \operatorname{res} X^{-1} g. \tag{40}$$

34°. Рассмотрим ряд $s_i = [\pi_0^i] z(X)$ (см. п. 31°). Для ряда s_i имеют место сравнения

$$1/s_i \equiv 1/s_{i-1}^{\Delta} \bmod \pi_0^i, \qquad \frac{d}{dX}(1/s_i) \equiv 0 \bmod \pi_0^i \tag{41}$$

(см. [4, (20), (18)]). Поэтому для любого ряда $g(X)$ из кольца $T[[X]]$ такого, что ряды $\frac{d}{dX}\, g(X)$ и $\frac{q}{p} g(X)$ имеют уже целые коэффициенты из кольца $\mathfrak{o}$, выполнено сравнение

$$\operatorname{res}\left(\frac{d}{dX}\, g\right)/s_i \equiv 0 \bmod \pi_0^i \tag{42}$$

(см. [4, лемма 13]). Наконец, если $g(X) \in \mathfrak{o}\{X\}$, то

$$\operatorname{tr} \operatorname{res}\left(\frac{d}{dX}\, \frac{g^{\Delta}}{q}\right)/s_i^{\Delta} = \operatorname{tr} \operatorname{res} X^{-1}\left(\left(X \frac{d}{dX}\, g\right)/s_i\right)^{\Delta} = \operatorname{tr} \operatorname{res}\left(\frac{d}{dX}\, g\right)/s_i \tag{43}$$

(мы использовали при этом (40) и (20)).

35°. Пусть, как и в п. 33°, взят произвольный степенной ряд $h(X)$ без свободного члена с коэффициентами из кольца $\mathfrak{o}'$, и пусть $m=q^r m_0$, где $0\leqslant r<n$, а число m_0 не делится на q. Имеет место сравнение:

$$\operatorname{tr}\operatorname{res}\left(\frac{d}{dX}\frac{h^m}{m}\right)\Big/s\equiv 0 \bmod \pi_0^{n-r}. \tag{44}$$

Проверим это сравнение индукцией по r. Если m не делится на q, т. е. $r=0$, то ряд $\frac{q}{p}\frac{h^m}{m}$ имеет целые коэффициенты и, значит, из (42) для $i=n$ будет следовать (44).

Если m делится на q, то ряд $\frac{q}{mp}\left(h^m-h^{\frac{m}{q}\Delta}\right)$ имеет целые коэффициенты из кольца $\mathfrak{o}'$ (см. (37), (38)). Поэтому (см. 42)

$$\operatorname{res}\left(\frac{d}{dX}\frac{h^m-h^{\frac{m}{q}\Delta}}{m}\right)\Big/s\equiv 0 \bmod \pi_0^n$$

и, значит, отсюда, а также из (41), (43) получим:

$$\operatorname{tr}\operatorname{res}\left(\frac{d}{dX}\frac{h^m}{m}\right)\Big/s\equiv \operatorname{tr}\operatorname{res}\left(\frac{d}{dX}\frac{h^{\frac{m}{q}\Delta}}{m}\right)\Big/s\equiv$$

$$\equiv \operatorname{tr}\operatorname{res}\left(\frac{d}{dX}\frac{h^{\frac{m}{q}\Delta}}{m}\right)\Big/s^{\Delta}_{n-1}=\operatorname{tr}\operatorname{res}\left(\frac{d}{dX}\frac{h^{m/q}}{m/q}\right)\Big/s_{n-1} \bmod \pi_0^{n-1}.$$

Применяя теперь индукционное предположение, получаем (44).

36°. Пусть $\lambda_0(X)=X+c_2X^2+\ldots$ — логарифм базисной формальной группы Любина—Тэйта F_0, которая построена по эндоморфизму $[\pi_0]_0=\pi_0X+X^q$. Обозначим через c'_m коэффициент c_m в $\lambda_0(X)$, если m не делится на q, и $c'_m=c_m-\frac{1}{\pi_0}c_{m/q}$, если $q\,|\,m$. Кроме того, через ν_0 обозначаем показатель в поле k_0. В этом и следующем пунктах мы займемся проверкой неравенств

$$\nu_0(c'_m)\geqslant\begin{cases} r, & \text{если } q=p \text{ и } m=p^r m_0, \text{ где } p\nmid m_0, \quad (45а)\\ r+1, & \text{если } q\geqslant p^2 \text{ и } m=q^r m_0, \text{ где } q\nmid m_0. \quad (45б)\end{cases}$$

Из условий (45а, б) итерацией получаем:

$$\nu_0(c_m)\geqslant\begin{cases} -r, & \text{если } q=p \text{ и } m=p^r m_0,\ p\nmid m_0, \quad (46а)\\ -(r-1), & \text{если } q\geqslant p^2 \text{ и } m=q^r m_0,\ q\nmid m_0. \quad (46б)\end{cases}$$

Прежде всего докажем следующую лемму о биномиальных коэффициентах.

ЛЕММА 7. *Пусть даны натуральные числа* $m=q^r s$ *и* $i=q^{r-1}s+a(q-1)=q^r s'$, *где* s *и* s' *не делятся на* q, *а число* $a\geqslant 0$. *Для* $q\geqslant 3$ *имеют место следующие соотношения*:

а) *если* $j\leqslant r$, *то* C_m^j *делится на* π_0^{r+1-j}, *т. е.*

$$v_0(C_m^j)\geqslant r+1-j;$$

б) *если* $a\geqslant 1$ *и при* $a=1$ *число* i *делится на* q (*т. е.* $r'\geqslant 1$), *то*

$$v_0(C_i^{aq})\geqslant\left(r+r'-\frac{aq}{2}\right)e_0f_0;$$

в) *если* $a=1$ *и число* i *не делится на* q (*т. е.* $r'=0$), *но при этом* $r\geqslant 2$, *то*

$$v_0(C_i^q)\geqslant(r-2)e_0f_0$$

(*здесь* e_0 *и* f_0 — *индекс ветвления и степень инерции расширения* $k_0/\mathbf{Q}_p$).

Доказательство. Заметим, что в а) из условия $j\leqslant r$ следует $j<q^r$. Поэтому простое число p входит в биномиальный коэффициент $C_{q^rs}^j$ лишь в множитель q^rs/j. Очевидно, что число j делится самое большее на p^{j-1}. Поэтому

$$v_0(C_m^j)=v_0(m)-v_0(j)\geqslant(r-(j-1))e_0\geqslant r+1-j.$$

Рассмотрим теперь C_i^{aq}. Степень простого числа p, входящего в знаменатель $(aq)!$ коэффициента C_i^{aq}, равна $\left[\frac{aq}{p}\right]+\left[\frac{aq}{p^2}\right]+\cdots$. Поэтому $v_0((aq)!)\leqslant\left[\frac{aq}{p-1}\right]e_0\leqslant\frac{aq}{2}e_0f_0$, если $q\geqslant 3$. Числитель C_i^{aq} делится как на число $i=q^rs'$, так и на $q^{r-1}s$. Кроме того, нетрудно проверить, что среди оставшихся $aq-2$ сомножителей числителя найдется число, делящееся на q. Поэтому числитель коэффициента C_i^{aq} делится на $q^{r+r'}$, откуда следует б).

Последний пункт в) проверяется аналогично.

37°. Приступим теперь к проверке условий (37а, б) для логарифма $\lambda_0(X)$. Коэффициенты логарифма λ_0 однозначно определяются из равенства $[\pi_0]_0=\lambda_0^{-1}\pi_0\lambda_0$ (см. (3)) или, что то же самое, из равенства $\pi_0\lambda_0(X)=\lambda_0(\pi_0X+X^q)$. Несложно проверить, что коэффициент c_m логарифма $\lambda_0(X)$ отличен от нуля только, если m делится на $q-1$. Учитывая это, напишем для c_m определяющее рекуррентное соотношение:

$$(1-\pi_0^{m-1})c_m=\sum_{\substack{\frac{m}{q}\leqslant i<m\\ i\equiv 1 \bmod(q-1)}}c_iC_i^{i'q-m'+1}\pi_0^{i'q-m'}=\sum_i x_i, \tag{47}$$

где $m'=(m-1)/(q-1)$, $i'=(i-1)/(q-1)$.

Условия (45а, б) будем проверять индукцией. Эту проверку проведем для $q=p$. Случай $q\geqslant p^2$ разбирается аналогично, только вместо индукционного предположения (45а) и (46а) надо использовать (45б) и (46б), а также вместо неравенств $q=p\geqslant 3$ — неравенства $q\geqslant p^2\geqslant 9$.

Случай $p\nmid m$. Надо доказать, что при этом элемент $c'_m=c_m$ является целым. Рассмотрим i-ое слагаемое x_i в сумме (47). Если $p\nmid i$, то эле-

мент c_i — целый по индукционному предположению и непосредственно проверяется, что $i'p-m' \geqslant 0$. Поэтому элемент x_i — целый.

Если i делится на p и, например, $i=p^r s'$, где $p \nmid s'$, то по индукционному предположению $v_0(c_i) \geqslant -r'$ (см. (46а)). Если для слагаемого x_i суммы (47) выполнено неравенство $i'p-m' \geqslant r'$, то, очевидно, что x_i — целый. Если же $i'p-m'+1 \leqslant r'$, то, используя лемму 7(а) для биномиального коэффициента $C_{i^{'p-m'+1}}$, получим

$$v_0(x_i) \geqslant -r' + (r'+1-(i'p-m'+1)) + i'p-m' = 0$$

и поэтому x_i опять будет целым элементом. Таким образом, мы проверили, что в сумме (47) все слагаемые — целые, а значит, и коэффициент c_m — целый.

Случай $p \mid m$. Пусть $m=p^r s$, где s не делится на p. Тогда индекс суммирования i в сумме (47) можно написать в виде $i=\frac{m}{p}+a(p-1)$, где $a \geqslant 0$, и тем самым сумма (47) перепишется следующим образом:

$$(1-\pi_0^{m-1})c'_m = \pi_0^{m-2}c_{m/p} + \sum_{1 \leqslant a < \frac{m}{p}} c_i C_i^{ap} \pi_0^{ap-1} = \sum_a x_a, \qquad (48)$$

где $i = \frac{m}{p} + a(p-1)$.

Проверим, что все слагаемые суммы (48) делятся на π_0^r.

Слагаемое $x_0=\pi_0^{m-2}c_{m/p}$ делится на π_0^r, так как по индукционному предположению $v_0(c_{m/p}) \geqslant -(r-1)$ (см. (46а)) и, значит,

$$v_0(x_0) \geqslant (m-2)-(r-1) \geqslant 3^r - r - 1 \geqslant r.$$

Рассмотрим теперь слагаемое x_a в сумме (48), когда $a>1$. Пусть при этом $i=p^r s'$, где $(s', p)=1$. Тогда по индукционному предположению $v_0(c_i) \geqslant -r'$ (см. (46а)). Если $ap-1 \geqslant r'+r$, то $v_0(x_a) \geqslant v_0(c_i)+(ap-1) \geqslant r$, что и требуется. Если же $ap \leqslant r'+r$, то, используя лемму 7(б), получаем:

$$v_0(x_a) \geqslant v_0(c_i) + v_0(C_i^{ap}) + ap - 1 \geqslant -r' + \left(r'+r-\frac{ap}{2}\right) e_0 f_0 + (ap-1) =$$

$$= (r'+r-ap)(e_0 f_0 - 1) + \left(\frac{ap}{2} e_0 f_0 - 1\right) + r \geqslant \left(\frac{3}{2} - 1\right) + r \geqslant r.$$

Таким образом, и в этом случае x_a делится на π_0^r.

Пусть теперь взято слагаемое x_1 и, значит, $i=p^{r-1}s+(p-1)=p^{r'}s'$. Если при этом $r=1$ и $r'=0$, то $ap-1=(p-1) \geqslant r'+r=1$ и поэтому $v_0(x_1) \geqslant v_0(c_i)+(ap-1) \geqslant -r'+(p-1) \geqslant r$, т. е. x_1 делится на π_0^r. Остальные случаи разбираются аналогично с использованием леммы 7, б, в.

Итак, во всех случаях слагаемое x_a в сумме (48) делится на π_0^r, а значит, и элемент c'_m делится на π_0^r. Условие (45а, б) доказано.

38°. Пусть теперь $\lambda_{\rho,\eta}(X)$ — логарифм формальной группы Любина—Тэйта $F_{\rho,\eta}$, построенной по эндоморфизму $\pi_0 X + \pi_0 \eta X^{p^\rho} + X^q$, где $\eta \in \mathfrak{R}$,

$1 \leqslant \rho \leqslant f-1$. Действуя аналогично доказательству условий (45а, б) для логарифма $\lambda_0(X)$, получаем такие же неравенства на коэффициенты логарифма $\lambda_{\rho,\eta}(X)$.

Литература

1. *Башмаков М. И., Кириллов А. Н.* Фильтрация Лютц формальных групп.— Изв. АН СССР. Сер. матем., 1975, т. 39, № 6, с. 1228—1239.
2. *Востоков С. В.* Явная форма закона взаимности.— Изв. АН СССР. Сер. матем., 1978, т. 42, № 6, с. 1288—1321.
3. *Востоков С. В.* Символ Гильберта в дискретно нормированном поле.— Зап. науч. семинаров Ленингр. отд. Мат. ин-та АН СССР, 1979, т. 94, с. 50—69.
4. *Востоков С. В.* Норменное спаривание в формальных модулях.— Изв. АН СССР: Сер. матем., 1979, т. 43, № 4, с. 766—794.
5. *Востоков С. В., Лецко В. А.* Каноническое разложение в группе точек формальной группы Любина — Тэйта.— Зап. науч. семинаров. Ленингр. отд. Мат. ин-та АН СССР, 1980, т. 103, с. 52—57.
6. *Колывагин В. А.* Формальные группы и символ норменного вычета.— Изв. АН СССР. Сер. матем., 1979, т. 43, № 5, с. 1054—1120.
7. *Ленг С.* Алгебра. М.: Мир, 1968, 564 с.
8. *Милнор Дж.* Введение в алгебраическую K-теорию. М.: Мир, 1974, 196 с.
9. *Fröhlich A.* Formal groups.— Lect. Notes Math., 1968, v. 74, 140 p.
10. *Lubin J., Tate J.* Formal complex multiplication in local fields.—Ann. Math., 1965, v. 81, p. 380—387.

Поступила в редакцию
20.II.1981