СЕРИЯ
МАТЕМАТИЧЕСКАЯ
Том 43, № 4, 1979

УДК 519.48

С. В. ВОСТОКОВ

НОРМЕННОЕ СПАРИВАНИЕ В ФОРМАЛЬНЫХ МОДУЛЯХ

Введение

1. Общий закон взаимности в поле алгебраических чисел выражает в явной форме отношение символов степенных вычетов n-ой степени $\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1}$ через числа α и β. Эта задача сводится (см. ([1])) к вопросу о нахождении явного выражения символа норменного вычета Гильберта в локальном поле (конечном расширении поля p-адических чисел $\mathbf{Q}_p$). Такое выражение для символа Гильберта, задающее его через разложение элементов α и β в ряды по локальной униформизирующей, было найдено в работе ([11]).

В настоящей работе обобщаются доказанные в ([11]) результаты на группу точек формальной группы Любина—Тэйта. Кратко эти результаты были сформулированы в ([9]).

В простом идеале $\mathfrak{p}$ локального поля вводится структура группы точек с помощью формального группового закона $F(X, Y)$ Любина—Тэйта, т. е.

$$\alpha \underset{F}{+} \beta = F(\alpha, \beta), \quad \alpha, \beta \in \mathfrak{p}.$$

Далее, в полученной группе точек $F(\mathfrak{p})$ рассматривается аналог символа норменного вычета Гильберта $(\alpha, \beta)_F$ (см. ниже п. 4). Этот символ обладает норменным свойством, т. е. равен нулю тогда и только тогда, когда элемент α является мультипликативной нормой в расширении, полученном делением точки β на изогению.

Основная задача, решаемая в этой статье,—задание обобщенного символа Гильберта в явном виде через разложение элементов α и β в ряды по локальной униформизирующей.

Частные случаи для обобщенного символа Гильберта в расширениях локального поля (над кольцом целых элементов которого определена формальная группа F), полученных присоединением корня изогении, были разобраны в ([8]), ([10]) (в мультипликативном случае такие расширения в точности соответствуют круговым расширениям поля $\mathbf{Q}_p$). В этих работах результаты Ивасавы (см. ([5])) переносятся на группу точек.

Изложим кратко содержание работы. В первых двух параграфах даются основные определения, обозначения и доказываются несколько вспомогательных утверждений.

В следующих двух параграфах изучается арифметика группы точек $F(\mathfrak{p})$. В § 3 строятся примарные элементы, т. е. элементы, задающие неразветвленное расширение при делении их на изогению. В § 4 задается канонический базис группы точек $F(\mathfrak{p})$, являющийся обобщением канонического базиса Шафаревича группы главных единиц локального поля (см. [3]).

В §§ 5, 6 задается в явном виде спаривание $\langle \alpha, \beta \rangle_F$ между мультипликативной группой локального поля и группой точек $F(\mathfrak{p})$ со значениями в корнях изогении и доказываются основные свойства этого спаривания. В § 5 проверяется билинейность и инвариантность спаривания относительно выбора локальной униформизирующей, а в § 6 — независимость относительно разложения заданных элементов α и β в ряды по этой униформизирующей.

Наконец, в последнем параграфе, используя доказанные ранее свойства спаривания $\langle \alpha, \beta \rangle_F$, проверяется совпадение спаривания $\langle \alpha, \beta \rangle_F$ с обобщенным символом Гильберта $(\alpha, \beta)_F$ (при этом предполагается, что поле, над кольцом целых элементов которого определена формальная группа F, вполне разветвлено над $\mathbf{Q}_p$). Это дает нам явное выражение для обобщенного символа Гильберта на группе точек.

2. Введем основные обозначения статьи.

k_0 — локальное поле (конечное расширение поля $\mathbf{Q}_p$),

$\mathfrak{o}_0$ — кольцо целых элементов поля k_0,

π_0 — простой элемент в $\mathfrak{o}_0$,

k — конечное расширение поля k_0,

$\mathfrak{p}$ — простой идеал кольца целых элементов поля k,

π — простой элемент поля k,

e — индекс ветвления расширения k/k_0,

F — степень инерции расширения $k_0/\mathbf{Q}_p$,

$q = p^f$ — порядок поля вычетов в поле k_0,

$$e_1 = \frac{e}{q-1}, \quad e_i = e_1/q^{i-1}, \quad i = 1, 2, \ldots,$$

T — подполе инерции в расширении k/k_0,

$\mathfrak{o}$ — кольцо целых элементов поля T,

Δ — автоморфизм Фробениуса в T/k_0,

tr — оператор следа в T/k_0,

$\mathfrak{R}$ — мультипликативная система представителей поля вычетов в поле k,

ν — показатель в поле k, т. е. $\nu(\alpha) = a$, если $\alpha = \pi^a \xi$, где ξ — некоторая единица.

Обозначим, далее, через $\mathfrak{o}\{X\}$ множество рядов с целыми коэффициентами вида

$$\varphi(X) = \sum_{i \in \mathbf{Z}} d_i X^i, \quad d_i \in \mathfrak{o},$$

обладающих следующим свойством: $d_i \to 0$, если $i \to -\infty$. Множество $\mathfrak{o}\{X\}$ образует кольцо, которое содержит, очевидно, в качестве подкольца кольцо формальных степенных рядов с коэффициентами из $\mathfrak{o}$.

Если $\varphi(X) = d_m X^m + d_{m+1} X^{m+1} + \ldots$ — некоторый ряд Лорана из кольца $\mathfrak{o}\{X\}$, то его порядок m будем обозначать $\deg \varphi$.

Далее, если φ и ψ — два ряда из $\mathfrak{o}\{X\}$, то сравнение

$$\varphi \equiv \psi \bmod \deg s$$

будет означать равенство коэффициентов рядов φ и ψ при степенях, меньших s, а сравнение

$$\varphi \equiv \psi \bmod (\pi_0^r, \deg s)$$

будет означать, что эти же коэффициенты сравнимы между собой по $\bmod \pi_0^r$.

Определим, наконец, действие автоморфизма Фробениуса Δ на ряд $\varphi = \sum d_i X^i$ из кольца $\mathfrak{o}\{X\}$ следующим образом.

$$\Delta\varphi = \varphi^\Delta = \sum d_i^\Delta X^{qi}.$$

3. Пусть $F(X, Y)$ — однопараметрическая коммутативная формальная группа, определенная над кольцом целых элементов $\mathfrak{o}_0$ локального поля k_0 (см. [6]). Предположим, далее, что кольцо $\mathfrak{o}_0$ входит в кольцо эндоморфизмов формальной группы F, т. е. для любого элемента a из $\mathfrak{o}_0$ найдется ряд $[a](X)$ с целыми коэффициентами такой, что $[a] \circ F = F \circ [a]$ (таким образом, формальная группа $F(X, Y)$ является формальным $\mathfrak{o}_0$-модулем).

Если мы в максимальном идеале $\mathfrak{p}$ поля k (некоторого расширения поля k_0) будем складывать элементы и умножать их на элементы из кольца $\mathfrak{o}_0$ следующим образом:

$$\alpha \underset{F}{+} \beta = F(\alpha, \beta), \quad \alpha, \beta \in \mathfrak{p},$$

$$a\alpha = [a](\alpha), \quad a \in \mathfrak{o}_0, \quad \alpha \in \mathfrak{p},$$

то получим группу точек $F(\mathfrak{p})$ формального модуля F со структурой $\mathfrak{o}_0$-модуля.

Напомним, что если $\lambda(X)$ — логарифм формальной группы F, то формальный групповой закон $F(X, Y)$ можно представить в виде

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

(см. [6]) и если $[a](X)$ — эндоморфизм, задаваемый целым элементом a из кольца $\mathfrak{o}_0$, то

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

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

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

Тогда над кольцом $\mathfrak{o}_0$ существует единственная формальная группа F высоты 1 (называемая группой Любина — Тэйта) такая, что ряд $f(X)$ является ее эндоморфизмом (см. (4)). В дальнейшем мы этот эндоморфизм будем обозначать $[\pi_0]$ и, таким образом, по определению

$$[\pi_0](X) = \pi_0 X + X^q + \pi_0 \sum_{i=2}^{\infty} a_i X^i, \quad a_i \in \mathfrak{o}_0. \tag{3}$$

Мы будем говорить, далее, что формальная группа F принадлежит классу $\mathcal{F}_{\pi_0}$.

Как было доказано в (4), если f_1 и f_2 — два ряда из множества $\mathcal{F}_{\pi_0}$, то соответствующие им формальные группы Любина — Тэйта F_1 и F_2 изоморфны над $\mathfrak{o}_0$, т. е. существует степенной ряд $\varphi(X) \equiv X \bmod \deg 2$ с коэффициентами из $\mathfrak{o}_0$ такой, что

$$\varphi(F_1(X, Y)) = F_2(\varphi(X), \varphi(Y)), \tag{4}$$

причем этот ряд единственный.

4. Пусть, как и в п. 3, F — формальная группа Любина — Тэйта с эндоморфизмом $[\pi_0]$. В дальнейшем мы будем предполагать, что поле k содержит все корни изогении $[\pi_0^n]$ и ξ — фиксированный первообразный корень этой изогении, т. е.

$$[\pi_0^n](\xi) = 0, \quad [\pi_0^{n-1}](\xi) \neq 0.$$

Определим теперь обобщенный символ Гильберта на группе точек $F(\mathfrak{p})$, как это было сделано в (6), а именно, зададим спаривание между мультипликативной группой $k^\times$ и группой точек $F(\mathfrak{p})$ со значениями в корнях изогении $[\pi_0^n]$:

$$(\alpha, \beta)_F = \rho^{\sigma_\alpha} \underset{F}{\sim} \rho, \quad \alpha \in k^\times, \quad \beta \in F(\mathfrak{p}),$$

где σ_α — автоморфизм группы Галуа, соответствующий элементу α в силу локальной теории полей классов, а ρ — элемент алгебраического замыкания поля k, получающийся делением точки β на изогению $[\pi_0^n]$, т. е. $[\pi_0^n](\rho) = \beta$.

Очевидно, что это определение не зависит от выбора элемента ρ. Далее, нетрудно видеть, что обобщенный символ Гильберта $(\alpha, \beta)_F$ обладает, как и обычный символ Гильберта, следующими свойствами:

1) билинейность:

$$(\alpha_1\alpha_2, \beta)_F = (\alpha_1, \beta)_F \underset{F}{+} (\alpha_2, \beta)_F,$$

$$(\alpha, \beta_1 \underset{F}{+} \beta_2)_F = (\alpha, \beta_1)_F \underset{F}{+} (\alpha, \beta_2)_F,$$

2) норменность по первому аргументу, т. е. $(\alpha, \beta)_F = 0 \Leftrightarrow \alpha$ — мультипликативная норма из $k(\rho)$, где $[\pi_0^n](\rho) = \beta$.

Отметим еще одно свойство обобщенного символа Гильберта. Пусть F_1 и F_2 — две изоморфные формальные группы Любина — Тэйта и

$\varphi(X)$ — степенной ряд, задающий изоморфизм между ними (см. (4), п. 3). Тогда имеет место равенство

$$(\alpha, \beta)_{F_2} = \varphi((\alpha, \varphi^{-1}(\beta))_{F_1}). \tag{5}$$

§ 1. Несколько лемм

В этом параграфе мы проверим несколько утверждений относительно логарифма формальной группы F, а также корней изогении $[\pi_0^n]$.

1. Пусть F — формальная группа Любина — Тэйта с логарифмом $\lambda(X) = X + c_2X^2 + c_3X^3 + \ldots$, $c_i \in k_0$. Проверим справедливость следующих неравенств:

$$v(c_m) \geqslant -(m-1)e, \quad m \geqslant 2. \tag{6}$$

Действительно из равенства $\lambda([\pi_0](X)) = \pi_0\lambda(X)$ (см. (2), введение, п. 3) следует:

$$[\pi_0](X) + c_2([\pi_0](X))^2 + \ldots = \pi_0 X + \pi_0 c_2 X^2 + \ldots .$$

Приравняем коэффициенты при X^m в обеих частях последнего равенства. Тогда, учитывая определение эндоморфизма $[\pi_0]$ (см. (3), введение, п. 3), получим:

$$\pi_0 c_m = \pi_0^m c_m + \left(\sum_{i=2}^{m-1} c_i \alpha_i\right) + d_m,$$

где через α_i обозначен коэффициент при X^m в ряде $([\pi_0](X))^i$, а элемент d_m равен либо $\pi_0 a_m$, если $m \neq q$, либо $1 + \pi_0 a_q$, если $m = q$. Из последнего равенства следует:

$$c_m = \frac{d_m}{\pi_0 - \pi_0^m} + \sum_{i=2}^{m-1} \alpha_i \frac{c_i}{\pi_0 - \pi_0^m}.$$

Отсюда несложной индукцией получаем неравенства (6).

Изучим теперь область сходимости рядов $\lambda(X)$ и $\lambda^{-1}(X)$.

ЛЕММА 1.

а) *ряд* $\lambda(X)$ *сходится на идеале* $\mathfrak{p}$, *а ряд* $\lambda^{-1}(X)$ *сходится на идеале* $\mathfrak{p}^{e_1+1}$;

б) *ряды* $\lambda(X)$ *и* $\lambda^{-1}(X)$ *определяют взаимно обратные изоморфизмы между группой точек* $F(\mathfrak{p}^m)$ *и аддитивным* $\mathfrak{o}_0$*-модулем* $\mathfrak{p}^m$, *если* $m > e_1$;

в) *все корни изогении* $[\pi_0^n]$, *содержащиеся в группе точек* $F(\mathfrak{p})$, *являются корнями логарифма* $\lambda(X)$.

Доказательство. В классе изоморфных формальных групп Любина — Тэйта содержится формальная группа F_a с логарифмом Артина — Хассе

$$\lambda_a(X) = X + \frac{X^q}{\pi_0} + \frac{X^{q^2}}{\pi_0^2} + \ldots \tag{7}$$

(см. ([7])). Для рядов $\lambda_a(X)$ и $\lambda_a^{-1}(X)$ первые два утверждения леммы проверяются точно так же, как и в теореме 3, § 2, гл. IV ([6]).

Пусть, далее, $\varphi(X)$ — степенной ряд, задающий изоморфизм между F и F_a (см. (4), введение, п. 3). Тогда (см. лемму 3)

$$\lambda(X) = \lambda_a(\varphi^{-1}(X)), \quad \lambda^{-1}(X) = \lambda_a^{-1}(\varphi(X)),$$

поэтому сходимость ряда $\lambda(X)$ равносильна сходимости $\lambda_a(X)$, а сходимость $\lambda^{-1}(X)$ равносильна сходимости $\lambda_a^{-1}(X)$.

Последнее утверждение леммы проверяется точно так же, как и в теореме 3, § 2, гл. IV, ([6]). Лемма доказана.

ЛЕММА 2. *В классе изоморфных формальных групп Любина — Тэйта, соответствующих множеству $\mathcal{F}_{\pi_0}$ (см. введение, п. 3), найдется такая формальная группа F_0 с логарифмом λ_0, что для любого $n \geqslant 1$ коэффициенты ряда $g(X) = \lambda_a^{-1} \circ \lambda_0 \circ [\pi_0^n]_0$ при степенях, меньших q^n, делятся на π_0, а при степени q^n коэффициент равен* 1 *(здесь $[\pi_0]_0$ — эндоморфизм формальной группы F_0).*

Доказательство. Рассмотрим в кольце формальных степенных рядов с коэффициентами из поля k_0 следующее равенство:

$$\lambda(f(X)) = \pi_0 \lambda(X), \tag{8}$$

в котором $\lambda(X) \equiv X \bmod \deg 2$, $f(X) \equiv \pi_0 X \bmod \deg 2$. Нетрудно проверить, что этим равенством однозначно определяется ряд $f(X)$, если известен ряд $\lambda(X)$, и наоборот.

Предположим, что построенный по ряду $\lambda(X)$ с помощью равенства (8) ряд $f(X)$ принадлежит множеству $\mathcal{F}_{\pi_0}$. Тогда, согласно теории Любина — Тэйта (см. ([4])), существует единственная формальная группа F над кольцом $\mathfrak{o}_0$, эндоморфизмом которой будет ряд $f(X)$. С другой стороны, для формальной группы F существует единственный ряд $\lambda_F(X)$ (называемый логарифмом), задающий изоморфизм над k_0 формальной группы F в аддитивную формальную группу $X+Y$ (см. ([6])). В этом случае ряд λ_F тоже удовлетворяет равенству (3) (см. (2), введение, п. 3) и, значит, совпадает по вышесказанному с рядом $\lambda(X)$. Следовательно, мы доказали, что если ряд $f(X)$, построенный по заданному ряду $\lambda(X)$ с помощью (8), принадлежит множеству $\mathcal{F}_{\pi_0}$, то соответствующая ряду f формальная группа Любина — Тэйта F будет иметь своим логарифмом ряд $\lambda(X)$.

Возьмем теперь в качестве ряда $\lambda(X)$ следующий ряд:

$$\lambda(X) = X + \frac{c_1}{\pi_0} X^q + \frac{c_2}{\pi_0^2} X^{q^2} + \ldots, \quad c_i \in \mathfrak{o}_0, \tag{9}$$

где $c_i \equiv 1 \bmod \pi_0$. Несложно убедиться в том, что определяемый равенством (8) ряд $f(X)$ будет в таком случае принадлежать $\mathcal{F}_{\pi_0}$ и по только что доказанному ряд $f(X)$ будет эндоморфизмом некоторой формальной группы Любина — Тэйта F из класса $\mathcal{F}_{\pi_0}$, логарифмом которой будет заданный ряд (9).

Существование формальной группы F с логарифмом (9) можно было бы проверить и другим способом, а именно, так же как устанавливается

существование формальной группы F_a с логарифмом Артина — Хассе λ_a в работе ([7]).

Далее, непосредственно проверяется, что ряд λ_a^{-1}, обратный к логарифму Артина — Хассе λ_a (см. (7)) относительно подстановки, имеет вид

$$\lambda_a^{-1} = X + \frac{d_1}{\pi_0} X^q + \ldots + \frac{d_m}{\pi_0^m} X^{mq-m+1} + \ldots, \quad d_m \in \mathfrak{o}_0. \tag{10}$$

Поскольку формальная группа F с логарифмом (9) изоморфна формальной группе F_a с логарифмом λ_a (обе они принадлежат одному и тому же классу $\mathcal{F}_{\pi_0}$), то ряд $g = \lambda_a^{-1} \circ \lambda \circ [\pi_0^n]$ имеет целые коэффициенты (см. лемму 3, § 2, п. 1). Кроме того, из (2), введение, п. 3, следует, что ряд $g(X)$ можно переписать в виде $g = \lambda_a^{-1}(\pi_0^n \lambda(X))$.

Подберем теперь коэффициенты в логарифме (9) так, чтобы ряд $g(X)$ удовлетворял условию нашей леммы. Для этого подставим ряд $\pi_0^n \lambda(X)$ в ряд (10). Тогда коэффициент a_n при X^{q^n} в ряде g будет иметь вид

$$c_n + h(c_1, \ldots, c_{n-1}),$$

где

$$h = \sum_{m=1}^{1+q+\ldots+q^{n-1}} d_m \pi_0^{m(q-1)-m+1} \sum \frac{(mq-m+1)!}{\alpha_0! \ldots \alpha_{n-1}!} c_1^{\alpha_1} \ldots c_{n-1}^{\alpha_{n-1}} \pi_0^{(n-1)\alpha_0+\ldots+\alpha_{n-2}}$$

и суммирование во внутренней сумме происходит по всем неотрицательным наборам $\alpha_0, \ldots, \alpha_{n-1}$, удовлетворяющих условиям:

$$\alpha_0 + \ldots + \alpha_{n-1} = mq - m + 1, \quad \alpha_0 + \alpha_1 q + \ldots + \alpha_{n-1} q^{n-1} = q^n.$$

Пусть сперва $n = 1$. Тогда коэффициент a_1 равен $c_1 + \pi_0^{q-1} d_1$ и, значит, $a_1 = 1$, если $c_1 = 1 - \pi_0^{q-1} d_1$. Ясно при этом, что $c_1 \equiv 1 \bmod \pi_0$.

Пусть, далее, уже установлено существование целых $c_1, \ldots, c_{n-1}$, сравнимых с 1 по $\bmod \pi_0$, таких, что $a_1 = \ldots = a_{n-1} = 1$. Очевидно, что $h(c_1, \ldots, c_{n-1})$ делится на π_0. Поэтому, взяв c_n равным $1 - h(c_1, \ldots, c_{n-1})$, получим, что $c_n \equiv 1 \bmod \pi_0$ и при этом $a_n = 1$.

Рассматривая таким же образом коэффициенты при степенях, меньших q^n в ряде g, несложно проверить их делимость на π_0. Лемма доказана.

2. Пусть $[\pi_0]$ — эндоморфизм формальной группы F. Тогда для элемента, полученного применением эндоморфизма $[\pi_0]$ к $\alpha \in \mathfrak{p}$, легко проверяются следующие формулы:

$$[\pi_0](\alpha) \equiv \alpha^q \bmod \pi^{qi+1}, \text{ если } v(\alpha) = i < e_1, \tag{11а}$$

$$[\pi_0](\alpha) \equiv \pi_0 \alpha \bmod \pi^{i+e_1+1}, \text{ если } v(\alpha) = i > e_1, \tag{11б}$$

$$[\pi_0](\alpha) \equiv \pi_0 \alpha + \alpha^q \bmod \pi^{qe_1+1}, \text{ если } v(\alpha) = i = e_1. \tag{11в}$$

Из этих формул, в частности, следует, что если элемент α из $\mathfrak{o}_0$-модуля $F(\mathfrak{p})$ делится на π^{qe_1+1}, то он делится и на изогению $[\pi_0]$, т. е. $\alpha \equiv 0 \bmod \pi^{qe_1+1} \Rightarrow$ $\Rightarrow \alpha = [\pi_0](\rho)$, $\rho \in F(\mathfrak{p})$.

Далее, если $v(\alpha) \geqslant e_n$, то

$$v([\pi_0^n](\alpha)) \geqslant qe_1, \quad v(\pi_0^n \lambda(\alpha)) \geqslant qe_1. \tag{12}$$

Здесь первое неравенство следует непосредственно из формул (11а—в), а второе вытекает из него, если учесть еще равенство $\pi_0^n \lambda(\alpha) = \lambda([\pi_0^n](\alpha))$ и лемму 1, п. 1.

Пусть ξ — первообразный корень изогении $[\pi_0^n]$ (см. введение, п. 4). Тогда из формул (11а—в) несложно получить, что $v(\xi) = e_n$. Более того, из (11а) получаем сравнение $[\pi_0^{n-1}](\xi) \equiv \xi^{q^{n-1}} \bmod \pi^{e_1+1}$. Применяя теперь эндоморфизм $[\pi_0]$ и используя формулу (11в), получим:

$$\xi^{q^n} + \pi_0 \xi^{q^{n-1}} \equiv [\pi_0^n](\xi) = 0 \bmod \pi^{qe_1+1}. \tag{13}$$

Отметим, наконец, что все корни изогении $[\pi_0^n]$ образуют $\mathfrak{o}_0$-модуль с одной образующей.

3. Рассмотрим кольцо рядов $\mathfrak{o}\{X\}$ (см. введение, п. 2) и проверим, что ряд $f(X)$ из этого кольца обратим тогда и только тогда, когда обратим хотя один из его коэффициентов. Ряд, обратный к ряду $f(X)$ в кольце $\mathfrak{o}\{X\}$, будем обозначать в дальнейшем $1/f$.

Очевидно, что если ряд f обратим, то существует хоть один обратимый коэффициент. Пусть теперь ряд f имеет обратимые коэффициенты и степень m — наименьшая среди всех степеней с обратимыми коэффициентами (такая степень найдется, так как $a_i \to 0$, если $i \to -\infty$). Таким образом, ряд f можно записать в виде $f(X) = a_m X^m (1 + g(X))$, где a_m обратим в $\mathfrak{o}$, причем ряд g принадлежит кольцу $\mathfrak{o}\{X\}$, все его коэффициенты при отрицательных степенях делятся на π_0, а свободный член равен нулю. Тогда

$$1/f = (a_m X^m)^{-1}(1 - g + g^2 - g^3 + \ldots), \tag{14}$$

и чтобы существовал ряд $1/f$ в кольце $\mathfrak{o}\{X\}$, нам осталось проверить, что имеет смысл сумма $1 - g + g^2 - g^3 + \cdots$. Для этого достаточно доказать, что при достаточно большом s коэффициент при любой фиксированной степени X^r в ряде g^s делится на заданную степень π_0^t, т. е. стремится к нулю, если $s \to \infty$.

Ряд g по $\bmod \pi_0^t$ является рядом Лорана, т. е. имеет конечное число отрицательных степеней. Пусть по $\bmod \pi_0^t$ ряд g имеет вид

$$g(X) = d_0 X^{-u} + d_1 X^{-u+1} + \ldots + d_{u-1} X^{-1} + d_{u+1} X + \ldots,$$

при этом $d_0, d_1, \ldots, d_{u-1}$ делятся на π_0. Тогда коэффициент при X^r в ряде g^s будет равен

$$\sum \frac{s!}{\alpha_0! \alpha_1! \ldots} d_0^{\alpha_0} d_1^{\alpha_1} \ldots,$$

причем суммирование происходит по всем неотрицательным $\alpha_0, \alpha_1, \ldots$, удовлетворяющим условиям: $\alpha_0 + \alpha_1 + \cdots = s$, $-u\alpha_0 - (u-1)\alpha_1 - \cdots - \alpha_{u-1} +$

$+\alpha_{u+1}+2\alpha_{u+2}+\cdots=r$. Отсюда следует, что

$$(u+1)(\alpha_0+\alpha_1+\cdots+\alpha_{u-1})\geqslant s-r.$$

Последнее неравенство означает, что при фиксированном r коэффициент при X^r стремится к нулю, если $s\to\infty$, так как $d_0, d_1, \ldots, d_{u-1}$ делятся на π_0.

Таким образом, существование ряда $1/f$ при наших условиях доказано.

Отметим некоторые легко проверяемые свойства ряда $1/f$:

а) $f\equiv X^r \bmod \pi_0 \Leftrightarrow 1/f\equiv X^{-r} \bmod \pi_0$;

б) если ряды f и g обратимы в кольце $\mathfrak{o}\{X\}$, то

$$f\equiv g \bmod \pi_0^m \Leftrightarrow 1/f\equiv 1/g \bmod \pi_0^m;$$

в) если h обратим в $\mathfrak{o}\{X\}$ и f, g — произвольные ряды из $\mathfrak{o}\{X\}$, то

$$f\equiv g \bmod \pi_0^m \Leftrightarrow f/h\equiv g/h \bmod \pi_0^m;$$

г) если f обратим в $\mathfrak{o}\{X\}$, то

$$\frac{d}{dX}f\equiv 0 \bmod \pi_0^m \Leftrightarrow \frac{d}{dX}(1/f)\equiv 0 \bmod \pi_0^m.$$

4. Пусть $\xi=c_0\pi^{e_n}+c_1\pi^{e_n+1}+\ldots$ — некоторое разложение первообразного корня изогении $[\pi_0^n]$ в степенной ряд по простому элементу π с коэффициентами из кольца $\mathfrak{o}$, и пусть

$$z(X)=c_0X^{e_n}+c_1X^{e_n+1}+\ldots, \quad s_m(X)=[\pi_0^m](z). \tag{15}$$

При $m=n$ ряд $s_n(X)$ будем в дальнейшем обозначать просто через $s(X)$. В этом пункте мы проверим несколько сравнений относительно ряда $s_m(X)$.

Из определения эндоморфизма $[\pi_0]$ (см. (3), введение, п. 3) следует сравнение

$$s_m(X)\equiv z^{q^m}(X) \bmod \pi_0. \tag{16}$$

Это сравнение, в частности, означает, что в кольце $\mathfrak{o}\{X\}$ можно рассматривать ряд $1/s_m$, для которого имеем:

$$1/s_m\equiv z^{-q^m}(X) \bmod \pi_0 \tag{17}$$

(см. а), п. 3). Далее, легко видеть, что $\frac{d}{dX}s_m\equiv 0 \bmod \pi_0^m$, а значит (см. г), п. 3),

$$\frac{d}{dX}(1/s_m)\equiv 0 \bmod \pi_0^m. \tag{18}$$

Пусть f и g — два степенных ряда из кольца $\mathfrak{o}[[X]]_0$. Тогда из определения эндоморфизма $[\pi_0]$ следует, что если $f\equiv g \bmod \pi_0^m$, то $[\pi_0](f)\equiv [\pi_0](g) \bmod \pi_0^{m+1}$. Отсюда, учитывая, что $z^q\equiv z^{\Delta} \bmod \pi_0$, можно несложной индукцией получить сравнение

$$s_m\equiv s_{m-1}^{\Delta} \bmod \pi_0^m, \tag{19}$$

и, значит (см. б), п. 3),

$$1/s_m \equiv (1/s_{m-1})^{\Delta} \bmod \pi_0^m. \tag{20}$$

Проверим, наконец, еще одно сравнение относительно ряда $s_m(X)$, а именно,

$$(s_{n-1}^{\Delta(q-1)} - s^{q-1})/s \equiv 0 \bmod (\pi_0^{n+1}, \deg 0). \tag{21}$$

Действительно, сравнение (19) можно записать в виде $s = s_{n-1}^{\Delta} + \pi_0^n h$, где $h(X)$ — некоторый степенной ряд. Тогда $s_{n-1}^{\Delta} = s - \pi_0^n h$. Возведя обе части последнего равенства в степень $q-1$ и воспользовавшись (16), получим:

$$s_{n-1}^{\Delta(q-1)} - s^{q-1} \equiv \pi_0^n z^{q^n(q-2)} h \bmod \pi_0^{n+1}.$$

Умножим обе части последнего равенства на ряд $1/s$ (см. в), п. 3) и используем при этом (17). Тогда в правой части получим ряд $\pi_0^n z^{q^n(q-3)} h$, который является при $q \geqslant 3$ степенным рядом, т. е. $\pi_0^n z^{q^n(q-3)} h \equiv 0 \bmod \deg 0$. Это дает нам (21).

Пусть через $u_m(X)$ обозначен ряд s/s_{m-1}. Тогда очевидно, что $u_m = \pi_0 + \pi_0 a_2 s_{m-1} + \pi_0 a_3 s_{m-1}^2 + \cdots$ (см. (3), введение, п. 3). Отсюда и из (19) для ряда $u = u_n$ вытекает сравнение

$$u^{\Delta} - u_{n+1} \equiv s_{n-1}^{\Delta(q-1)} - s^{q-1} \bmod \pi_0^{n+1}. \tag{22}$$

В дальнейшем нам будет удобно использовать разложение ряда $u = u_n$ в ряд по s_{n-1} в следующем виде:

$$u = \pi_0 + s_{n-1}(X)\rho(X), \tag{23}$$

где $\rho(X)$ — степенной ряд с целыми коэффициентами.

§ 2. Некоторые изоморфизмы

Пусть $\mathfrak{o}[[X]]_0$ — аддитивная группа формальных степенных рядов без свободного члена, рассматриваемая как $\mathfrak{o}_0$-модуль, и пусть $\mathscr{H}_F$ — $\mathfrak{o}_0$-модуль степенных рядов без свободного члена с коэффициентами из $\mathfrak{o}$, в котором сложение происходит по формальному групповому закону F, т. е.

$$\varphi(X) \underset{F}{+} \psi(X) = F(\varphi, \psi),$$

а действие операторов из кольца $\mathfrak{o}_0$ определено следующим образом:

$$a\varphi = [a](\varphi), \qquad a \in \mathfrak{o}_0.$$

В этом параграфе мы найдем для формального группового закона Любина — Тэйта F функции E_F и l_F, осуществляющие взаимно обратные изоморфизмы между аддитивным $\mathfrak{o}_0$-модулем $\mathfrak{o}[[X]]_0$ и $\mathfrak{o}_0$-модулем $\mathscr{H}_F$.

1. Пусть F_1 и F_2 — две формальные группы Любина — Тэйта из класса $\mathscr{F}_{\pi_0}$, и пусть λ_1, λ_2 — их логарифмы.

ЛЕММА 3. *Ряды* $\lambda_1^{-1}\circ\lambda_2$ *и* $\lambda_2^{-1}\circ\lambda_1$ *имеют целые коэффициенты из кольца* $\mathfrak{o}_0$ *и осуществляют изоморфизм между* F_1 *и* F_2, *т. е.* $\lambda_1^{-1}\circ\lambda_2 : F_2\to F_1$, $\lambda_2^{-1}\circ\lambda_1 : F_1\to F_2$ *и при этом* $\lambda_1^{-1}\circ\lambda_2 \equiv \lambda_2^{-1}\circ\lambda_1 \equiv X \bmod \deg 2$.

Доказательство. По условию формальные группы F_1 и F_2 принадлежат классу $\mathscr{F}_{\pi_0}$. Поэтому, в силу леммы 1, § 1, ([4]), существует единственный ряд $\varphi(X)$ с коэффициентами из кольца $\mathfrak{o}_0$, осуществляющий изоморфизм из F_1 в F_2. Далее, существует единственный ряд с коэффициентами из поля k_0, задающий изоморфизм из F_1 в F_2 над полем k_0 (см. ([6])). При этом нетрудно убедиться, что таким изоморфизмом является ряд $\lambda_2^{-1}\circ\lambda_1$ (см. (1), (4), введение, п. 3). Ряд $\varphi(X)$ тоже осуществляет этот изоморфизм, значит, $\varphi(X)=\lambda_2^{-1}\circ\lambda_1$, откуда следует, в частности, что ряд $\lambda_2^{-1}\circ\lambda_1$ имеет целые коэффициенты. Аналогично проверяется утверждение леммы относительно ряда $\lambda_1^{-1}\circ\lambda_2$. Лемма доказана.

2. В классе изоморфных между собой формальных групп Любина — Тэйта, соответствующих множеству степенных рядов $\mathscr{F}_{\pi_0}$ (см. введение, п. 3), существует формальная группа F_a, логарифмом которой является функция Артина — Хассе $\lambda_a(X)$ (см. (7), § 1, п. 1). Поэтому ряд $\lambda^{-1}\circ\lambda_a$, как было показано в п. 1, задает изоморфизм из F_a в данную формальную группу F с логарифмом λ. Таким образом, $\lambda^{-1}\circ\lambda_a$ имеет целые коэффициенты. Надо отметить, что ряд $\lambda^{-1}\circ\lambda_a$ является обобщением функции Шафаревича $E(X)=\exp\sum_{r\geqslant 0} X^{p^r}/p^r$ мультипликативного случая (см. ([3])). Тем самым $E(X)$ осуществляет изоморфизм из формальной группы Любина — Тэйта (над $\mathbf{Z}_p$) с логарифмом $X+X^p/p+X^{p^2}/p^2+\cdots$ в мультипликативную группу.

Свяжем теперь ряд $\lambda^{-1}\circ\lambda_a$ с автоморфизмом Фробениуса Δ и определим функцию $E_F(\varphi)$ для любого ряда $\varphi(X)$ из $\mathfrak{o}[[X]]_0$ следующим образом:

$$E_F(\varphi)=\lambda^{-1}\left(\sum_{r=0}^{\infty}\frac{\varphi^{\Delta^r}}{\pi_0^r}\right).$$

В дальнейшем мы эти функции будем использовать чаще всего в виде

$$E_F(\varphi)=\lambda^{-1}\left(\left(1+\frac{\Delta}{\pi_0}+\frac{\Delta^2}{\pi_0^2}+\ldots\right)(\varphi)\right). \tag{24}$$

Ряд $\lambda^{-1}\circ\lambda_a\circ\varphi$, вообще говоря, не совпадает с функцией $E_F(\varphi)$, но если $\theta\in\mathfrak{R}$, то

$$E_F(\theta X^m)=\lambda^{-1}(\lambda_a(\theta X^m)). \tag{25}$$

Отсюда, в частности, следует, что

$$E_F(\theta X^m)\equiv\theta X^m \bmod \deg 2m, \quad \theta\in\mathfrak{R}. \tag{26}$$

Далее, из определения функции E_F получаем, что для любых степенных рядов φ и ψ из кольца $\mathfrak{o}[[X]]_0$ имеет место равенство, называемое в даль-

нейшем формальной аддитивностью функции E_F:

$$E_F(\varphi+\psi)=E_F(\varphi)\underset{F}{+}E_F(\psi). \tag{27}$$

Кроме того, если $a\in\mathfrak{o}_0$, то

$$E_F(a\varphi)=[a]E_F(\varphi). \tag{28}$$

ЛЕММА 4. *Функция $E_F(\varphi)$ является степенным рядом с целыми коэффициентами без свободного члена и определена на простом идеале $\mathfrak{p}$ поля k.*

Доказательство. Первое утверждение леммы достаточно проверить, согласно (27), для ряда $\varphi=aX^m$, $a\in\mathfrak{o}$. В этом случае доказательство можно свести к функции $E_F(\theta X^m)$, если разложить элемент a в степенной ряд по π_0 с коэффициентами из $\mathfrak{R}$ и использовать (27), (28). Функция $E_F(\theta X^m)$, согласно (25) и лемме 3, является степенным рядом с целыми коэффициентами. Второе утверждение леммы является очевидным следствием первого.

3. Рассмотрим теперь ряд $\lambda_a^{-1}\circ\lambda$, задающий обратный изоморфизм из данной формальной группы F в формальную группу F_a с логарифмом Артина — Хассе $\lambda_a(X)$. Согласно лемме 3, п. 1, ряд $\lambda_a^{-1}\circ\lambda$ тоже будет степенным рядом с целыми коэффициентами без свободного члена.

Свяжем теперь, как и выше, ряд $\lambda_a^{-1}\circ\lambda$ с автоморфизмом Фробениуса Δ и определим функцию $l_F(\varphi)$ для любого ряда φ из $\mathfrak{o}[[X]]_0$ следующим образом:

$$l_F(\varphi)=\left(1-\frac{\Delta}{\pi_0}\right)(\lambda(\varphi))$$

(в мультипликативном случае см. ([11]), § 1). Полученная функция будет, очевидно, обратной к функции $E_F(\varphi)$, т. е.

$$l_F(E_F(\varphi))=\varphi,\quad E_F(l_F(\varphi))=\varphi, \tag{29}$$

и, кроме того, будет обладать следующими свойствами:

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

$$l_F(\varphi\underset{F}{+}\psi)=l_F(\varphi)+l_F(\psi),$$

$$l_F([a]\varphi)=al_F(\varphi),\quad a\in\mathfrak{o}_0.$$

Далее, так же как и для функции $E_F(\varphi)$ можно проверить, что $l_F(\varphi)$ является степенным рядом с целыми коэффициентами без свободного члена. Тем самым функция $l_F(\varphi)$ тоже определена на простом идеале $\mathfrak{p}$ поля k.

Замечание. Из результатов пунктов 2 и 3 следует, что функции E_F и l_F осуществляют взаимно обратные изоморфизмы между аддитивным $\mathfrak{o}_0$-модулем $\mathfrak{o}[[X]]_0$ и $\mathfrak{o}_0$-модулем $\mathscr{H}_F$.

4. Пусть $\varphi(X)$ — некоторый ряд из кольца $\mathfrak{o}[[X]]_0$. Если $\varphi=\pi_0^i\theta X^r$, где $\theta\in\mathfrak{R}$, то из (28), (26) и определения изогении $[\pi_0^i]$ следует для любого

$i \geqslant 0$ сравнение

$$E_F(\pi_0^i \theta X^r) \equiv \pi_0^i \theta X^r \bmod \deg(r+1).$$

Отсюда, раскладывая произвольный элемент a из кольца $\mathfrak{o}$ в ряд по простому элементу π_0 с коэффициентами из $\mathfrak{R}$ и используя формальную аддитивность функции E_F, получаем:

$$E_F(aX^r) \equiv aX^r \bmod \deg(r+1).$$

Из этого сравнения и формальной аддитивности функции E_F легко получается для произвольного ряда φ порядка r из кольца $\mathfrak{o}[[X]]_0$ сравнение

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

Аналогично проверяется, что

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

Из последних двух сравнений вытекает следующее утверждение.

ЛЕММА 5. *Пусть φ — ряд порядка r из кольца $\mathfrak{o}[[X]]_0$. Тогда для любого $a \in \mathfrak{o}$ имеет место сравнение*

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

Замечание. Сравнение леммы справедливо также и для любого элемента a из кольца целых пополнения максимального неразветвленного расширения поля T.

§ 3. Примарные элементы

В этом параграфе строятся π_0^n-примарные элементы поля k, играющие важную роль в задании символа Гильберта. Элемент ω группы точек $F(\mathfrak{p})$ называется π_0^n-примарным, если расширение поля k, полученное делением точки ω на изогению $[\pi^n]$, неразветвлено (в мультипликативном случае такие элементы были получены в [2] и [4]).

1. Построим π_0^n-примарные элементы в группе точек, являющиеся обобщением примарных элементов Хассе (см. [11], § 4, п. 1). Пусть $z(X)$ — степенной ряд, полученный из разложения корня ξ изогении $[\pi_0^n]$ по простому элементу π (см. (15), § 1, п. 4).

Пусть, далее, $a \in \mathfrak{o}$ и A — элемент кольца целых пополнения максимального неразветвленного над T расширения $\bar{T}$, который удовлетворяет равенству

$$\mathrm{A}^{\Delta} - \mathrm{A} = a \tag{30}$$

(продолжение автоморфизма Фробениуса Δ поля T на расширение $\bar{T}$ обозначено здесь той же буквой Δ).

ЛЕММА 6. *Элемент*

$$H(a) = E_F(\pi_0^n \mathrm{A}^{\Delta} l_F(z))\,|_{X=\pi}$$

является π_0^n-примарным и при этом $(\pi, H(a))_F = [\mathrm{tr}\, a](\xi)$.

Доказательство. Пусть Δ' — автоморфизм Фробениуса расширения $\bar{T}/T$. Из (30) следует $\mathrm{A}^{\Delta\Delta'} = \mathrm{A}^{\Delta} + \mathrm{tr}\, a$. Поэтому из формальной ад-

дитивности функции E_F получаем:

$$E_F(\mathrm{A}^{\Delta} l_F(z))^{\Delta'} = E_F((\mathrm{A}^{\Delta} + \mathrm{tr}\, a)\, l_F(z)) =$$
$$= E_F(\mathrm{A}^{\Delta} l_F(z)) \underset{F}{+} E_F((\mathrm{tr}\, a)\, l_F(z)) = E_F(\mathrm{A}^{\Delta} l_F(z)) \underset{F}{+} [\mathrm{tr}\, a]\, E_F(l_F(z)) =$$
$$= E_F(\mathrm{A}^{\Delta} l_F(z)) \underset{F}{+} [\mathrm{tr}\, a]\, z(X)$$

(в последнем равенстве мы использовали (29), § 2, п. 3). Отсюда, с одной стороны,

$$H(a)^{\Delta'} = H(a) \underset{F}{+} [\pi_0^n \mathrm{tr}\, a](z(\pi)) = H(a) \underset{F}{+} [\mathrm{tr}\, a]([\pi_0^n](\xi)) = H(a),$$

т. е. $H(a) \in T(\xi)$, а с другой стороны,

$$(E_F(\mathrm{A}^{\Delta} l_F(z))|_{X=\pi})^{\Delta'} = E_F(\mathrm{A}^{\Delta} l_F(z))|_{X=\pi} \underset{F}{+} [\mathrm{tr}\, a](\xi).$$

Отсюда, по определению обобщенного символа Гильберта (см. введение, п. 4), получим $(\pi, H(a)) = [\mathrm{tr}\, a](\xi)$ и лемма доказана.

Пусть корень изогении ξ двумя способами раскладывается в степенной ряд по простому элементу π с коэффициентами из $\mathfrak{o}$, т. е. $\xi = z_1(\pi) = z_2(\pi)$, и пусть $H_1(a)$ и $H_2(a)$ — π_0^n-примарные элементы, построенные в лемме 6 с помощью рядов $z_1(X)$ и $z_2(X)$ соответственно.

Следствие. *Примарные элементы $H_1(a)$ и $H_2(a)$ отличаются друг от друга на элемент, делящийся в группе точек $F(\mathfrak{p})$ на изогению $[\pi_0^n]$, т. е. $H_1(a) \underset{F}{\sim} H_2(a) = [\pi_0^n](\varepsilon)$, $\varepsilon \in F(\mathfrak{p})$.*

Доказательство. Пусть $\eta(X) = z_1(X) \underset{F}{\sim} z_2(X)$. Так как $\eta(\pi) = z_1(\pi) \underset{F}{\sim} z_2(\pi) = 0$, то, согласно лемме 6, § 3, работы ([11]), существует степенной ряд $\psi(X)$ с целыми коэффициентами такой, что $\eta(X) = \chi(X)\psi(X)$ (здесь $\chi(X)$ — произвольный неприводимый многочлен Эйзенштейна в расширении k/T, имеющий своим корнем простой элемент π). Так же как и в лемме 6, получаем равенство

$$E_F(\mathrm{A}^{\Delta} l_F(\chi\psi))^{\Delta'} = E_F(\mathrm{A}^{\Delta} l_F(\chi\psi)) \underset{F}{+} [\mathrm{tr}\, a](\chi\psi).$$

Отсюда, учитывая, что $\chi(\pi) = 0$, следует, что элемент $\varepsilon = E_F(\mathrm{A}^{\Delta} l_F(\chi\psi))|_{X=\pi}$ принадлежит группе точек $F(\mathfrak{p})$. Поэтому из определения $H_1(a)$ и $H_2(a)$ получаем:

$$H_1(a) \underset{F}{\sim} H_2(a) = E_F(\pi_0^n \mathrm{A}^{\Delta} l_F(z_1 \underset{F}{\sim} z_2))|_{X=\pi} = [\pi_0^n](\varepsilon),$$

и следствие доказано.

ЛЕММА 7. *Элемент*

$$P(a) = E_F(\pi_0^n a \lambda(z))|_{X=\pi}, \quad a \in \mathfrak{o},$$

совпадает с π_0^n-примарным элементом $H(a)$ и, значит, $(\pi, P(a))_F = [\mathrm{tr}\, a](\xi)$.

Доказательство. В максимальном неразветвленном над $T(\xi)$ расширении имеет место равенство

$$E_F(\pi_0^n A^\Delta l_F(z)) = E_F(\pi_0^n a\lambda(z)) \underset{F}{+} \lambda^{-1}(\pi_0^n A\lambda(z)). \tag{31}$$

Действительно, из определения функции E_F (см. (24), § 2, п. 2) получаем:

$$E_F\left(\pi_0^n\left(1-\frac{\Delta}{\pi_0}\right)A\lambda(z)\right) = \lambda^{-1}(\pi_0^n A\lambda(z)).$$

С другой стороны, учитывая (30), имеем:

$$\left(1-\frac{\Delta}{\pi_0}\right)A\lambda(z) = A^\Delta l_F(z) - a\lambda(z).$$

Отсюда и из формальной аддитивности функции E_F следует (31).

Далее, порядок элемента $z(\alpha)$ для любого α из $\mathfrak{p}$ не меньше чем e_n (см. (15), § 1, п. 4), значит, и порядок элемента $\pi_0^n\lambda(z(\alpha))$ не меньше чем qe_1 (см. (12), § 1, п. 2). Поэтому ряд $\lambda^{-1}(\pi_0^n A\lambda(z(X)))$ определен для любого элемента из идеала $\mathfrak{p}$ (см. лемму 1, § 1, п. 1), в частности, и для $X=\pi$. В этом случае мы получаем $\lambda(z(\pi))=\lambda(\xi)=0$. Значит, $\lambda^{-1}(\pi_0^n A\lambda(z(\pi)))=0$. Отсюда и из (31) следует, что $H(a)=P(a)$ и лемма доказана.

2. В этом пункте мы получим примарный элемент $\omega(a)$, который и будет использован в дальнейшем. Пусть, как и раньше, ряд $[\pi_0^n](z)$ обозначен через $s(X)$.

ЛЕММА 8. *Пусть* $\mu\geqslant 1$, *тогда*

$$v(s^{\Delta^\mu}(X)|_{X=\pi}) \geqslant e(1+\max(\mu, n)).$$

Доказательство. Из сравнения (19), § 1, п. 4, следует равенство

$$s^\Delta_{n+i-1} = s_{n+i} + \pi_0^{n+i} f_i, \quad i\geqslant 1,$$

причем порядок ряда $f_i(X)$ не меньше чем e_n, так как ряды s^Δ_{n+i-1} и s_{n+i} имеют порядки $\geqslant e_n$. Применим к обеим частям этого равенства оператор $\Delta^{\mu-i}$ и затем сложим полученные равенства для $i=1, 2, \ldots, \mu$. Тогда

$$s^{\Delta^\mu} = s_{n+\mu} + \pi_0^{n+\mu} f_\mu + \pi_0^{n+\mu-1} f^\Delta_{\mu-1} + \ldots + \pi_0^{n+1} f_1^{\Delta^{\mu-1}},$$

при этом $\deg f_i\geqslant e_n$. Если мы теперь в слагаемые правой части последнего равенства подставим вместо X простой элемент π и учтем, что $\deg f_i\geqslant e_n$, то получим неравенства:

$$v(\pi_0^{n+\mu-i} f^{\Delta^i}_{\mu-i}|_{X=\pi}) \geqslant (n+\mu-i)e + q^i e_n \geqslant e(1+\max(\mu, n)).$$

Отсюда следуют требуемые неравенства леммы, если заметим еще, что $s_{n+\mu}(\pi) = [\pi_0^{n+\mu}](\xi) = 0$.

Предложение 1. *Элемент*

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

где $a \in \mathfrak{o}$, *является* π_0^n*-примарным и при этом* $(\pi,\ \omega(a))_F = [\operatorname{tr} a](\xi)$.

Доказательство. Из (2) (введение, п. 3) для изогении $[\pi_0^n]$ следует, очевидно, равенство $\pi_0^n \lambda(z) = \lambda([\pi_0^n](z))$; отсюда получаем:

$$E_F(\pi_0^n a \lambda(z)) = E_F(as) \underset{F}{+} E_F(a\varphi), \tag{32}$$

где через $\varphi(X)$ обозначен ряд $\lambda(s) - s$. Проверим, что элемент $E_F(a\varphi)\,|_{X=\pi}$ делится на изогению $[\pi_0^n]$, т. е. найдется элемент ε из группы точек $F(\mathfrak{p})$ такой, что

$$E_F(a\varphi)\,|_{X=\pi} = [\pi_0^n](\varepsilon). \tag{33}$$

По определению функции E_F (см. § 2, п. 2) можно написать равенство

$$E_F(a\varphi) = \lambda^{-1}(a\varphi) \underset{F}{+} \sum_{\mu=1}^{\infty}{}_{(F)}\, \lambda^{-1}((a\varphi)^{\Delta^\mu}/\pi_0^\mu).$$

Поскольку элемент $\varphi(\alpha)$ для любого α из идеала $\mathfrak{p}$ имеет порядок, не меньший чем qe_1 (см. (12), § 1), то, значит, однозначно определен ряд $\lambda^{-1}(a\varphi)$ на идеале $\mathfrak{p}$ (см. лемму 1, § 1), в частности, и на элементе $X=\pi$. Но $s(\pi) = \lambda(s(\pi)) = 0$, значит,

$$\lambda^{-1}(a\varphi)\,|_{X=\pi} = 0. \tag{34}$$

Пусть $\lambda(X) = X + c_2X^2 + c_3X^3 + \cdots$, $c_i \in \mathfrak{o}_0$,— логарифм формальной группы F, тогда очевидно, что

$$\varphi(X) = \sum_{m\geqslant 2} c_m s^m.$$

Далее, элемент

$$x_{m,\mu} = (c_m s^{m\Delta^\mu}/\pi_0^{\mu+n})\,|_{X=\pi}$$

делится на π_0, если $m \geqslant 2$, $\mu \geqslant 1$. Действительно, если $m \geqslant 2$, то, используя (6) (§ 1, п. 1) и лемму 8, получим:

$$\begin{aligned} \nu(x_{m,\mu}) &\geqslant -(m-1)e + me(1 + \max(\mu, n)) - (\mu + n)e = \\ &= e + (m \cdot \max(\mu, n) - (\mu + n))e \geqslant e \end{aligned}$$

и мы проверили тем самым, что $x_{m,\mu} \equiv 0 \bmod \pi_0$. Это означает, что для любых $m \geqslant 2$, $\mu \geqslant 1$ однозначно определен элемент

$$\varepsilon_{m,\mu} = \lambda^{-1}(a^{\Delta^\mu} x_{m,\mu}), \quad a \in \mathfrak{o}$$

(см. лемму 1, § 1, п. 1). А тогда получим, что

$$\lambda^{-1}((a\varphi)^{\Delta^\mu}/\pi_0^\mu) = [\pi_0^n]\left(\sum_{m=2}^{\infty}{}_{(F)}\, \varepsilon_{m,\mu}\right).$$

Поэтому если мы применим к элементу $\varepsilon = \sum_{(F)} \varepsilon_{m,\mu}$ (здесь суммирование происходит по всем $m \geqslant 2$, $\mu \geqslant 1$) группы точек $F(\mathfrak{p})$ изогению $[\pi_0^n]$, то получим, учитывая (34), элемент $E_F(aq)\,|_{X=\pi}$, и равенство (33) доказано. Отсюда и из (32) получаем:

$$\omega(a) = P(a) \underset{F}{\frown} [\pi_0^n](\varepsilon), \tag{35}$$

что дает нам вместе с леммой 7 утверждение нашего предложения.

Замечание. Из равенства (35) и леммы 7 следует, что π_0^n-примарный элемент $\omega(a)$ отличается от π_0^n-примарного элемента $H(a)$ на элемент, делящийся на изогению $[\pi_0^n]$ в группе точек $F(\mathfrak{p})$. Поэтому примарный элемент $\omega(a)$, так же как и $H(a)$, согласно следствию из леммы 6, не зависит (с точностью до элемента, делящегося на изогению $[\pi_0^n]$ в группе точек $F(\mathfrak{p})$) от разложения корня изогении ξ в степенной ряд по простому элементу π с коэффициентами из $\mathfrak{o}$. Отметим, наконец, что разложение корня ξ может быть совершенно произвольным и не обязательно должно начинаться (как в (15), § 1, п. 4) с члена степени ϵ_τ.

§ 4. Арифметика группы точек

В этом параграфе будет построен канонический базис в группе точек $F(\mathfrak{p})$, который является обобщением канонического базиса Шафаревича группы главных единиц локального поля в мультипликативном случае (см. ([3]), § 1).

Мы не будем приводить подробных доказательств, так как в основном они проходят по той же схеме, что и в мультипликативном случае.

1. Проверим утверждение, являющееся аналогом теоремы Хензеля (см. ([12]), § 14). Оно дает нам условие, при котором некоторая система элементов группы точек $F(\mathfrak{p})$ будет системой образующих над кольцом $\mathfrak{o}_0$.

ЛЕММА 9. *Пусть для каждого i с условием: $i \not\equiv 0 \bmod q$, $1 \leqslant i < qe_1$, а также для $i = qe_1$ и для каждого $\theta \in \mathfrak{R}$ выбран элемент $\varepsilon_i(\theta)$ в группе точек $F(\mathfrak{p})$, удовлетворяющий условию: $\varepsilon_i(\theta) \equiv \theta\pi^i \bmod \pi^{i+1}$. Тогда любой элемент $\beta \in F(\mathfrak{p})$ можно представить в виде*

$$\beta = \sum_{i,r}{}_{(F)} [\pi_0^r](\varepsilon_i(\theta_{i,r})),$$

где r пробегает все целые неотрицательные числа.

Доказательство. Несложной индукцией можно проверить, что всякий элемент β из $F(\mathfrak{p})$ представим в виде

$$\beta = \sum_{i=1}^{\infty}{}_{(F)} \varepsilon_i(\theta_i), \tag{36}$$

где $\varepsilon_i(\theta_i)$ — элемент из $F(\mathfrak{p})$, удовлетворяющий сравнению

$$\varepsilon_i(\theta_i) \equiv \theta_i\pi^i \bmod \pi^{i+1}, \quad \theta_i \in \mathfrak{R}.$$

Далее действуем точно так же как и в мультипликативном случае (см. ([12]), § 14). А именно, будем заменять последовательно в (36) элементы $\varepsilon_i(\theta_i)$ для $i>qe_1$ на $[\pi_0]\varepsilon_{i-e_1}(\gamma^{-1}\theta_i)$ (здесь γ — первый коэффициент в разложении π_0 по простому элементу π), используя при этом формулу (11б). Затем элемент $\varepsilon_i(\theta_i)$ для $i=qh<qe_1$ будем заменять на $[\pi_0]\varepsilon_h(\theta_i^{q^{-1}})$, используя формулу (11а). Этот процесс приведет нас в конце концов к системе образующих, указанной в условии нашего предложения.

2. Докажем несколько сравнений относительно примарного элемента $H(a)$.

ЛЕММА 10. *Пусть* ξ — *фиксированный корень изогении* $[\pi_0^n]$. *Тогда*

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

Доказательство. Примарный элемент $H(a)$ получается применением изогении $[\pi_0^n]$ к элементу

$$E_F(\mathrm{A}^{\Delta} l_F(z))\,|_{X=\pi},$$

лежащему в пополнении максимального неразветвленного расширения поля k. Ряд $z(X)$ (см. § 1, п. 4) имеет обратимый первый коэффициент в кольце $\mathfrak{o}$ и при этом $z(\pi)=\xi$. Поэтому из леммы 5, § 2, п. 4, следует:

$$E_F(\mathrm{A}^{\Delta} l_F(z))\,|_{X=\pi} \equiv \mathrm{A}^{\Delta}\xi \bmod \pi^{e_n+1}.$$

Применяя теперь к этому элементу $n-1$ раз эндоморфизм $[\pi_0]$ и используя формулу (11а), § 1, п. 2, получим:

$$[\pi_0^{n-1}]E_F(\mathrm{A}^{\Delta} l_F(z))\,|_{X=\pi} \equiv (\mathrm{A}^{\Delta}\xi)^{q^{n-1}} \bmod \pi^{e_1+1}.$$

Если применить к получившемуся элементу снова эндоморфизм $[\pi_0]$, то придется пользоваться формулой (11в), § 1, п. 2. Тогда получим:

$$H(a) \equiv (\mathrm{A}^{\Delta}\xi)^{q^{n-1}}\pi_0 + (\mathrm{A}^{\Delta}\xi)^{q^n} \bmod \pi^{qe_1+1}.$$

Из этого сравнения, а также сравнений

$$\mathrm{A}^{\Delta q^n} - \mathrm{A}^{\Delta q^{n-1}} \equiv a^{q^n} \equiv a \bmod \pi_0$$

и (13), § 1, п. 2, вытекает сравнение нашей леммы.

ЛЕММА 11. *Если примарный элемент* $H(a)$ *делится на изогению* $[\pi_0]$ *в группе точек* $F(\mathfrak{p})$, *т. е.* $H(a)=[\pi_0](\rho)$, $\rho\in F(\mathfrak{p})$, *то* $\operatorname{tr} a\equiv 0 \bmod \pi$.

Доказательство. Из формул (11а—в), § 1, п. 2, следует, что порядок элемента ρ равен e_1. А тогда из равенства $H(a)=[\pi_0](\rho)$, формулы (11в), § 1, п. 2, и предыдущей леммы получаем сравнение

$$\rho\pi_0 + \rho^q \equiv a\xi^{q^n} \bmod \pi^{qe_1+1}.$$

Отсюда и из (13), § 1, п. 2, следует $\eta^q-\eta\equiv a \bmod \pi$, где $\eta=\rho/\xi^{q^{n-1}}$. Поэтому $a\equiv\eta^{\Delta}-\eta \bmod \pi$, так как $\eta^{\Delta}\equiv\eta^q \bmod \pi$. Значит, $\operatorname{tr} a\equiv 0 \bmod \pi$.

3. Рассмотрим теперь аналог канонического разложения Шафаревича для группы точек $F(\mathfrak{p})$.

Предложение 2. *Всякий элемент* β *из группы точек* $F(\mathfrak{p})$ *можно представить в виде*

$$\beta = H(b) \underset{F}{+} \sum_{i\,(F)} E_F(b_i\pi^i), \tag{37}$$

где b, $b_i \in \mathfrak{o}$, *а индекс* i *пробегает все значения между* 1 *и* qe_1, *не делящиеся на* q. *При этом элементы* $\operatorname{tr} b$, b_i *определены однозначно по* $\bmod \pi_0^n$.

Доказательство. К системе элементов $H(\theta)$, $E_F(\theta_i\pi^i)$, где θ, $\theta_i \in \mathfrak{R}$, можно применить лемму 9, согласно лемме 10 и сравнению (26), § 2. Тогда по лемме 9 всякий элемент β из $F(\mathfrak{p})$ представим в виде

$$\beta = \sum_{r\,(F)} ([\pi_0^r] H(\theta_r) \underset{F}{+} \sum_{i\,(F)} [\pi_0^r] E_F(\theta_{i,r}\pi^i)).$$

Отсюда, в силу формальной аддитивности функции E_F, получаем каноническое разложение (37).

Проверим единственность канонического разложения (37). Используя сравнения (11а—в), § 1, п. 2, и лемму 11, можно проверить так же как и в лемме 1, § 1, работы ([3]), следующее утверждение. Если

$$H(b) \underset{F}{+} \sum_{i\,(F)} E_F(b_i\pi^i) = 0, \tag{38}$$

то $\operatorname{tr} b \equiv 0 \bmod \pi_0$, $b_i \equiv 0 \bmod \pi_0$.

Отсюда, в точности как и в лемме 2, § 1, работы ([3]), доказывается, что в любом каноническом разложении корня изогении $[\pi_0]$

$$\xi_1 = H(\theta) \underset{F}{+} \sum_{i\,(F)} E_F(\theta_i\pi^i) \tag{39}$$

выполняются сравнения $\operatorname{tr} \theta \equiv 0 \bmod \pi_0^{n-1}$, $\theta_i \equiv 0 \bmod \pi_0^{n-1}$.

Пусть теперь

$$H(b) \underset{F}{+} \sum_{i\,(F)} E_F(b_i\pi^i) = 0,$$

тогда, согласно (38), элементы b_i делятся на π_0, т. е. $b_i = \pi_0 b_i'$, а для элемента b найдется $b' \in \mathfrak{o}$ такой, что $b \equiv \pi_0 b' \bmod \pi_0^n$. Следовательно,

$$H(b') \underset{F}{+} \sum_{i\,(F)} E_F(b_i'\pi^i) = \xi_1.$$

Здесь, согласно (39), имеем сравнения $\operatorname{tr} b' \equiv b_i' \equiv 0 \bmod \pi_0^{n-1}$, и единственность канонического разложения доказана.

Замечание. Примарный элемент $\omega(b)$, построенный в предложении 1, § 3, отличается от примарного элемента $H(b)$ на элемент, делящийся на изогению $[\pi_0^n]$. Поэтому мы можем в каноническом разложении (37) заменить примарный элемент $H(b)$ на $\omega(b)$. Далее, многочлен

$\sum_i b_i X^i$ в разложении (37) будем обозначать через $\omega_\beta(X)$. В дальнейшем мы будем использовать каноническое разложение в виде

$$\beta = \omega(b) \underset{F}{+} E_F(\omega_\beta)|_{X=\pi}. \tag{40}$$

§ 5. Вспомогательное спаривание

1. Рассмотрим мультипликативную группу $\mathcal{H}$ рядов вида

$$\mathcal{H} = \{X^m \theta \varepsilon(X),\ m \in \mathbf{Z},\ \theta \in \mathfrak{R}\},$$

где $\varepsilon(X)$ — степенной ряд с коэффициентами из $\mathfrak{R}$ и свободным членом 1. Пусть, далее, $\mathcal{H}_F$—$\mathfrak{o}_0$-модуль степенных рядов с коэффициентами из $\mathfrak{o}$, сложение в котором происходит по формальному закону F (см. начало § 2).

Определим спаривание группы $\mathcal{H}$ с $\mathfrak{o}_0$-модулем $\mathcal{H}_F$ со значениями в кольце $\mathfrak{o}$:

$$[\ ,\ ]_F : \mathcal{H} \times \mathcal{H}_F \to \mathfrak{o}.$$

Пусть $A(X) = X^a \theta \varepsilon(X)$ — ряд из $\mathcal{H}$, и пусть $\beta(X)$ — некоторый ряд из $\mathfrak{o}_0$-модуля $\mathcal{H}_F$. Тогда положим

$$[A,\ \beta]_F = \operatorname{res}_X \Phi(X)\, W^{\Delta}(X), \tag{41}$$

где

$$\Phi(X) = l_m(\varepsilon) \frac{dl_F(\beta)}{dX} - l_m(\varepsilon) \frac{d\lambda(\beta)}{dX} + l_F(\beta) A^{-1} \frac{dA}{dX};$$

при этом

$$l_m(\varepsilon) = \left(1 - \frac{\Delta}{q}\right) \log \varepsilon(X), \quad l_F(\beta) = \left(1 - \frac{\Delta}{\pi_0}\right) \lambda(\beta(X)),$$

а $W(X)$ — некоторый фиксированный ряд из кольца $\mathfrak{o}\{X\}$, производная которого делится на π_0^{n-1}, т. е.

$$\frac{d}{dX} W(X) \equiv 0 \bmod \pi_0^{n-1}. \tag{42}$$

2. В правой части равенства, определяющего ряд $\Phi(X)$ (см. (41)), не все слагаемые имеют целые коэффициенты. Все же имеет место следующее утверждение.

ЛЕММА 12. *Ряд $\Phi(X)$ в спаривании* (41) *является степенным рядом с целыми коэффициентами из кольца $\mathfrak{o}$.*

Доказательство. Последнее слагаемое в определении ряда $\Phi(X)$ имеет целые коэффициенты, так как $l_F(\eta) \in \mathfrak{o}[[X]]$ (см. § 2, п. 3). Далее,

$$l_m(\varepsilon) \frac{d}{dX} l_F(\beta) - l_m(\varepsilon) \frac{d}{dX} \lambda(\beta) = -\frac{l_m(\varepsilon)}{\pi_0} \frac{d}{dX} (\lambda(\beta))^{\Delta} =$$

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

Здесь предпоследнее равенство следует из легко проверяемой для любого степенного ряда $h(X)$ формулы

$$\frac{d}{dX}h^{\Delta} = qX^{q-1}\left(\frac{d}{dX}h\right)^{\Delta}. \tag{43}$$

Производная логарифма формальной группы F имеет целые коэффициенты (см. ([6])). Таким образом, для проверки утверждения леммы осталось доказать, что ряд $p^{f-1}l_m(\varepsilon)$ имеет целые коэффициенты. Из определения ряда $l_m(\varepsilon)$ получаем:

$$p^{f-1}l_m(\varepsilon) = (p^{f-1}+p^{f-2}\delta+\cdots+\delta^{f-1})\,l(\varepsilon),$$

где $l(\varepsilon) = (1-\frac{\delta}{p})\log\varepsilon$, $\Delta=\delta^f$ и δ — автоморфизм Фробениуса в подполе инерции расширения $k/\mathbf{Q}_p$. Функция $l(\varepsilon)$ является степенным рядом с целыми коэффициентами (см. ([11]), § 1, лемма 1). Поэтому и ряд $p^{f-1}l_m(\varepsilon)$ имеет целые коэффициенты. Лемма доказана.

Заметим также, что для нашего спаривания выполняется следующая

ЛЕММА 13. *Пусть $\varphi(X)$ — произвольный степенной ряд с коэффициентами из поля T такой, что ряд $p^{f-1}\varphi$ имеет целые коэффициенты. Тогда*

$$\operatorname{res}_X\left(\frac{d}{dX}\varphi\right)W^{\Delta} \equiv 0 \bmod \pi_0^n.$$

Доказательство. Из равенства (43), сравнения (42) для ряда W и условия леммы следует сравнение

$$\operatorname{res}_X\varphi\frac{d}{dX}W^{\Delta} = \operatorname{rex}_X(p^{f-1}\varphi)\,pX^{q-1}\left(\frac{d}{dX}W\right)^{\Delta} \equiv 0 \bmod \pi_0^n.$$

Далее,

$$\operatorname{res}_X\left(\frac{d}{dX}\varphi\right)W^{\Delta} + \operatorname{res}_X\varphi\left(\frac{d}{dX}W^{\Delta}\right) = \operatorname{res}_X\frac{d}{dX}(\varphi W^{\Delta}) = 0.$$

Отсюда и из предыдущего сравнения получаем требуемое сравнение леммы.

3. Отметим, что спаривание $[A, \beta]_F$ будет линейным по первому аргументу, так как логарифмическая производная $A^{-1}\frac{dA}{dX}$ и функция $l_m(\varepsilon)$ аддитивны. Кроме того, наше спаривание линейно и по второму аргументу, что следует из линейности функции l_F (см. § 2, п. 3) и аддитивности производной. Таким образом, спаривание $[A, \beta]_F$ билинейно, т. е.

$$[A_1A_2, \beta]_F = [A_1, \beta]_F + [A_2, \beta]_F,$$

$$[A, \beta_1+\beta_2]_F = [A, \beta_1]_F + [A, \beta_2]_F.$$

4. В этом пункте мы получим формулу замены переменных для функции E_F (в мультипликативном случае см. ([11]), § 2, п. 3, (7)), которая будет использована в следующем пункте для доказательства инвариантности спаривания $[A, \beta]_F$.

Пусть имеется следующая замена переменных:

$$X=g(Y)=Y\theta\psi(Y), \quad \theta\in\mathfrak{R}, \tag{44}$$

где степенной ряд $\psi(Y)$ с коэффициентами из $\mathfrak{R}$ и имеет свободный член 1. Рассмотрим, как изменится ряд $E_F(\alpha X^m)$, $\alpha\in\mathfrak{R}$, при этой замене переменных.

Функция E_F существенным образом зависит от выбора переменной X (см. (24), § 2, п. 2). Поэтому обозначим входящий в ее определение автоморфизм Фробениуса для переменной X через Δ_1, а для переменной Y — через Δ_2. При этом функцию E_F для переменной X снабдим индексом $E_{F,X}$. Таким образом, если $\varphi(X)$ — степенной ряд без свободного члена, то

$$E_{F,X}(\varphi)=\lambda^{-1}\left(\left(1+\frac{\Delta_1}{\pi_0}+\frac{\Delta_1^2}{\pi_0^2}+\ldots\right)(\varphi)\right).$$

При этих обозначениях имеет место следующая формула замены переменных:

$$E_{F,X}(\alpha X^m)=E_{F,Y}\left(\left(1-\frac{\Delta_2}{\pi_0}\right)(S)\right), \quad \alpha\in\mathfrak{R},$$

где

$$S=\sum_{r=0}^{\infty}\frac{(\alpha g^m)^{q^r}}{\pi_0^r}.$$

Действительно,

$$E_{F,Y}\left(\left(1-\frac{\Delta_2}{\pi_0}\right)S\right)=\lambda^{-1}\left(\left(1+\frac{\Delta_2}{\pi_0}+\frac{\Delta_2^2}{\pi_0^2}+\ldots\right)\left(1-\frac{\Delta_2}{\pi_0}\right)S\right)=\lambda^{-1}(S)=$$

$$=\lambda^{-1}\left(\alpha g^m+\frac{(\alpha g^m)^q}{\pi_0}+\ldots\right)=\lambda^{-1}\left(\alpha X^m+\frac{(\alpha X^m)^q}{\pi_0}+\ldots\right)=E_{F,X}(\alpha X^m),$$

и формула замены переменных доказана.

Заметим, что ряд $\left(1-\frac{\Delta_2}{\pi_0}\right)(S)$ имеет целые коэффициенты, так как

$$\left(1-\frac{\Delta_2}{\pi_0}\right)(S)=\alpha g^m+\sum_{r=1}^{\infty}\alpha^{q^r}\frac{g^{q^r m}-g^{q^{r-1}m\Delta_2}}{\pi_0^r} \tag{45}$$

и каждое слагаемое в правой части является степенным рядом с целыми коэффициентами (что легко проверить индукцией).

5. Проверим теперь инвариантность спаривания $[A, \beta]_F$ по $\bmod \pi_0^n$ относительно замены переменной в случае, когда $A=X$. Ряд $\beta(X)$ можно представить в виде $\beta(X)=E_F(l_F(\beta))$ (см. (29), § 2, п. 3). Поэтому ввиду билинейности спаривания и формальной аддитивности функции E_F инвариантность достаточно проверить для следующей пары X, $E_F(\alpha X^m)$, где $\alpha\in\mathfrak{R}$. Пусть, как и в п. 3, имеется следующая замена переменной: $X=g(Y)$ (см. (44)).

Предложение 3. *При $p\neq 2$ имеет место следующее сравнение:*

$$[X, E_{F,X}(\alpha X^m)]_F\equiv\left[g(Y), E_{F,Y}\left(\left(1-\frac{\Delta_2}{\pi_0}\right)(S)\right)\right]_F \bmod \pi_0^n.$$

Доказательство. Пусть

$$[X, E_{F,X}(\alpha X^m)]_F = \operatorname{res}_X \Phi(X)\, W^{\Delta}(X),$$
$$\left[g(Y), E_{F,Y}\left(\left(1-\frac{\Delta_2}{\pi_0}\right)(S)\right)\right]_F = \operatorname{res}_Y \Psi(Y)\, W^{\Delta}(g(Y)).$$

По определению (41) ряды $\Phi(X)$ и $\Psi(Y)$ имеют вид

$$\Phi(X) = \alpha X^{m-1},$$
$$\Psi(Y) = l_m(\psi)\frac{d}{dY}\left(1-\frac{\Delta_2}{\pi_0}\right)(S) - l_m(\psi)\frac{d}{dY}S + \left(1-\frac{\Delta_2}{\pi_0}\right)(S)\, g^{-1}\frac{dg}{dY}.$$

Учитывая (45), получим:

$$\Psi(Y) = \alpha g^{m-1}\frac{dg}{dY} +$$
$$+\sum_{r=1}^{\infty}\alpha^{q^r}\left(\frac{g^{q^r m} - g^{q^{r-1}m\Delta_2}}{\pi_0^r}\, g^{-1}\frac{dg}{dY} - l_m(\psi)\frac{d}{dY}\frac{g^{q^{r-1}m\Delta_2}}{\pi_0^r}\right).$$

Легко проверить следующую формулу:

$$g^{-1}\frac{dg}{dY} = \frac{d}{dY}l_m(\psi) + Y^{q-1}\left(g^{-1}\frac{dg}{dY}\right)^{\Delta_2}.$$

Отсюда и из равенства (43) следует:

$$\frac{d}{dY}\left(\frac{g^{q^r m} - g^{q^{r-1}m\Delta_2}}{q^r m\pi_0^r} - l_m(\psi)\frac{g^{q^{r-1}m\Delta_2}}{\pi_0^r}\right) =$$
$$= \frac{g^{q^r m} - g^{q^{r-1}m\Delta_2}}{\pi_0^r}\, g^{-1}\frac{dg}{dY} - l_m(\psi)\frac{d}{dY}\frac{g^{q^{r-1}m\Delta_2}}{\pi_0^r}.$$

Поэтому ряд $\Psi(Y)$ можно представить в виде

$$\Psi(Y) = \alpha g^{m-1}\frac{dg}{dY} + \frac{d}{dY}\left(\sum_{r=1}^{\infty}\varphi_r(Y)\right),$$

где

$$\varphi_r = (\alpha g^m)^{q^{r-1}\Delta_2} S_r, \quad S_r = \frac{g^{q^r m\left(1-\frac{\Delta_2}{q}\right)} - 1}{q^r m\pi_0^r} - \frac{l_m(\psi)}{\pi_0^r}.$$

Проверим теперь, что ряд φ_r удовлетворяет условию леммы 13, п. 2, т. е. $p^{f-1}\varphi_r \in \mathfrak{o}[[Y]]$. Действительно,

$$p^{f-1}S_r = p^{f-1}\left(\frac{\exp(q^r m l_m(\psi)) - 1}{q^r m\pi_0^r} - \frac{l_m(\psi)}{\pi_0^r}\right) = \sum_{i=2}^{\infty}\frac{\alpha_i}{i!}(p^{f-1}l_m(\psi))^i,$$

где $\alpha_i = (q^r m)^{i-1}/\pi_0^r\, p^{(f-1)(i-1)}$. Ряд $p^{f-1}l_m(\psi)$ имеет целые коэффициенты (см. доказательство леммы 12, п. 2). Далее, коэффициент α_i делится на p^{i-2}, что легко следует из условий $r \geqslant 1$, $i \geqslant 2$ и $q = p^f$. Поэтому при $p \neq 2$ элемент $\alpha_i/i!$ будет p-целым. Значит, ряд $p^{f-1}S_r$, а с ним и ряд $p^{f-1}\varphi_r$ будет иметь целые коэффициенты.

Отсюда, используя лемму 13, получаем сравнение

$$\operatorname{res}_Y \Psi(Y) W^{\Delta}(g) = \operatorname{res}_Y \left(\alpha g^{m-1} \frac{dg}{dY} + \frac{d}{dY} \sum_{r=1}^{\infty} \varphi_r \right) W^{\Delta}(g) \equiv$$
$$\equiv \operatorname{res}_Y \left(\alpha g^{m-1} \frac{dg}{dY} \right) W^{\Delta}(g) = \operatorname{res}_Y \Phi(g) W^{\Delta}(g) \frac{dg}{dY} =$$
$$= \operatorname{res}_X \Phi(X) W^{\Delta}(X) \bmod \pi_0^n,$$

и предложение доказано.

§ 6. Спаривание $\langle \alpha, \beta \rangle_F$

1. Построим с помощью спаривания $[A, \beta]_F$ (см. § 5) спаривание между мультипликативной группой $k^\times$ локального поля k и группой точек $F(\mathfrak{p})$ со значениями в группе корней изогении $[\pi_0^n]$.

Пусть $\alpha = \pi^a \theta \varepsilon$ — элемент мультипликативной группы $k^\times$, причем $\theta \in \mathfrak{R}$, а ε — главная единица. Пусть $\varepsilon = 1 + a_1\pi + a_2\pi^2 + \cdots$ — некоторое разложение единицы ε в ряд по простому элементу π с коэффициентами из $\mathfrak{R}$. Обозначим через $A(X)$ ряд $X^a \theta \varepsilon(X)$, где $\varepsilon(X) = 1 + a_1 X + a_2 X^2 + \cdots$. Пусть, далее, элемент β взят из группы точек $F(\mathfrak{p})$ и $\beta = b_1\pi + b_2\pi^2 + \cdots$ — его разложение в ряд по π с коэффициентами из $\mathfrak{o}$. Обозначим через $\beta(X)$ ряд $b_1 X + b_2 X^2 + \cdots$. Наконец, ряд $z(X)$, как и во введении, получен из разложения корня ξ изогении $[\pi_0^n]$ в степенной ряд по π, т. е. $\xi = z(\pi)$.

Определим теперь спаривание $\langle\ ,\ \rangle_F$ следующим образом:

$$\langle \alpha, \beta \rangle_F = [\operatorname{tr} \gamma](\xi), \tag{46}$$

где $\gamma = [A, \beta]_F$, и в спаривании $[A, \beta]_F$ (см. (41), § 5) в качестве ряда W^Δ взят ряд $1/s$ (см. (15) и (14), § 1).

Замечание. Из сравнений (20), (18), § 1, п. 4, следует, что ряд $1/s$ удовлетворяет условию (42), § 5.

Из доказанных в § 5 свойств спаривания $[A, \beta]_F$ вытекает следующее утверждение.

Предложение 4. *Спаривание $\langle \alpha, \beta \rangle_F$ билинейно и является инвариантным относительно выбора простого элемента π, по крайней мере, для пары π, β, где $\pi \in k^\times$, $\beta \in F(\mathfrak{p})$.*

В определение спаривания $\langle \alpha, \beta \rangle_F$ входит еще, вообще говоря, и способ разложения элементов α, β в ряды по простому элементу π. Основной результат этого параграфа состоит в доказательстве независимости нашего спаривания от способа разложения в ряды по π.

2. Прежде чем приступить к доказательству независимости спаривания $\langle \alpha, \beta \rangle_F$, проверим следующую необходимую в дальнейшем лемму. Пусть, как и прежде, $\lambda(X) = X + c_2X^2 + c_3X^3 + \cdots$ — логарифм формальной группы F, через $u_m(X)$ обозначен ряд s_m/s_{m-1} и, наконец, $u(X) = u_n(X)$.

ЛЕММА 14. *Для любого $m \geqslant 1$ имеет место сравнение*

$$\frac{c_m}{\pi_0} u^{m\Delta} (1 - \pi_0 \Delta)(1/s) \equiv 0 \bmod (\pi_0^n, \deg 0). \tag{47}$$

Доказательство. Рассмотрим сперва второе слагаемое в левой части (47), т. е. ряд $c_m u^{m\Delta}/s^{\Delta}$. Тогда из равенств $u^{\Delta}/s^{\Delta} = 1/s^{\Delta}_{n-1}$ и $u^{\Delta} = \pi_0 + s^{\Delta}_{n-1}\rho^{\Delta}$ (см. (23), § 1, п. 4) получаем:

$$c_m u^{m\Delta}/s^{\Delta} = c_m u^{(m-1)\Delta}/s^{\Delta}_{n-1} = c_m \pi_0^{m-1}/s^{\Delta}_{n-1} + \sum_{i=1}^{m-1} \alpha_i s^{\Delta(i-1)}_{n-1}\rho^{\Delta i}, \tag{48}$$

где через α_i обозначен коэффициент $c_m \pi_0^{m-i} C^i_{m-1}$. Поскольку элемент $c_m\pi_0^{m-1}$ — целый (см. (6), § 1, п. 1), то в первом слагаемом можно заменить ряд $1/s^{\Delta}_{n-1}$ на сравнимый с ним по mod π_0^n ряд $1/s$ (см. (20), § 1, п. 4) и тогда получим:

$$c_m\pi_0^{m-1}/s^{\Delta}_{n-1} \equiv c_m\pi_0^{m-1}/s \bmod \pi_0^n.$$

Далее, во второй сумме правой части (48) каждое слагаемое является степенным рядом, так как ряды $s^{\Delta(i-1)}_{n-1}$, $\rho^{\Delta i}$ при $i \geqslant 1$ — степенные. Таким образом,

$$\sum_{i=1}^{m-1} \alpha_i s^{\Delta(i-1)}_{n-1}\rho^{\Delta i} \equiv 0 \bmod \deg 0.$$

Из последних двух сравнений вытекает:

$$c_m u^{m\Delta}/s^{\Delta} \equiv c_m\pi_0^{m-1}/s \bmod (\pi_0^n, \deg 0). \tag{49}$$

Займемся теперь первым слагаемым в левой части сравнения (47). Представим ряд $u^{\Delta}(X)$ в следующем виде:

$$u^{\Delta} = \pi_0 + s\varphi_0 + \pi_0^n\varphi_1 + \pi_0^{n+1}\varphi_2,$$

где

$$\varphi_0 = (u_{n+1} - \pi_0)/s, \quad \varphi_1 = (s^{\Delta(q-1)}_{n-1} - s^{q-1})/\pi_0^n,$$
$$\varphi_2 = (u^{\Delta} - u_{n+1} - \pi_0^n\varphi_1)/\pi_0^{n+1}.$$

Из определения ряда u_m (см. § 1, п. 4) и сравнений (19), (22), § 1, п. 4, следует, что ряды φ_0, φ_1, φ_2 являются степенными рядами с целыми коэффициентами. Таким образом, первое слагаемое в левой части (47) можно записать в виде:

$$\frac{c_m}{\pi_0} u^{m\Delta}/s = \frac{c_m}{\pi_0} \sum_{i=1}^{m} C^i_m s^{i-1}\varphi_0^i\psi^{m-i} + \frac{c_m}{\pi_0}\psi^m/s, \tag{50}$$

где $\psi = \pi_0 + \pi_0^n\varphi_1 + \pi_0^{n+1}\varphi_2$. Первая сумма в правой части равенства (50) является степенным рядом, так как s^{i-1}, φ_0^i, ψ^{m-i} — степенные ряды, значит,

$$\frac{c_m}{\pi_0} \sum_{i=1}^{m} C^i_m s^{i-1}\varphi_0^i\psi^{m-i} \equiv 0 \bmod \deg 0. \tag{51}$$

Далее,

$$\frac{c_m}{\pi_0}\psi^m/s = \frac{c_m}{\pi_0}(1/s) \sum_{\alpha+\beta+\gamma=m} \frac{m!}{\alpha!\,\beta!\,\gamma!} \pi_0^{\alpha+n\beta+(n+1)\gamma}\varphi_1^{\beta}\varphi_2^{\gamma}, \tag{52}$$

при этом каждое слагаемое в правой части, кроме $c_m\pi_0^{m-1}/s$ и $(mc_m\pi_0^{m+n-2}\varphi_1)/s$, будет делиться на π_0^n. Действительно, $v(c_m/\pi_0) \geqslant -me$ (см. (6), § 1, п. 1) и если $\beta \geqslant 2$ или $\gamma \geqslant 1$, то $\alpha+n\beta+(n+1)\gamma = m+(n-1)\beta+n\gamma \geqslant m+n$. Поэтому из (52) получаем сравнение:

$$\frac{c_m}{\pi_0}\psi^m/s \equiv c_m\pi_0^{m-1}/s + (mc_m\pi_0^{m+n-2}\varphi_1)/s \pmod{\pi_0^n}. \tag{53}$$

Коэффициент $mc_m\pi_0^{m+n-2}$ делится на π_0^{n-1}, так как $v(c_m) \geqslant -(m-1)e$. Поэтому из (21), § 1, п, 4, следует сравнение

$$(mc_m\pi_0^{m+n-2}\varphi_1)/s \equiv 0 \bmod (\pi_0^n, \deg 0).$$

А тогда (53) можно записать в виде

$$\frac{c_m}{\pi_0}\psi^m/s \equiv c_m\pi_0^{m-1}/s \bmod (\pi_0^n, \deg 0).$$

Отсюда, из (51) и (50) получаем:

$$\frac{c_m}{\pi_0}u^{m\Delta}/s \equiv c_m\pi_0^{m-1}/s \bmod (\pi_0^n, \deg 0).$$

Последнее сравнение вместе с (49) дает требуемое сравнение леммы.

3. Рассмотрим теперь доказательство независимости спаривания $\langle \pi, \beta\rangle_F$ от способа разложения элемента β в ряды по π. Если элемент β группы точек $F(\mathfrak{p})$ двумя способами представлен в виде степенного ряда по простому элементу π, то обозначим ряд, соответствующий первому разложению, через $\beta_1(X)$, а второму — через $\beta_2(X)$. Таким образом, $\beta = \beta_1(\pi) = \beta_2(\pi)$. Пусть через $\langle \pi, \beta\rangle_F^1$ обозначено спаривание (46), полученное с помощью первого разложения элемента β, а через $\langle \pi, \beta\rangle_F^2$ — с помощью второго. Пусть, наконец, $\eta(X) = \beta_1(X) \underset{F}{\sim} \beta_2(X)$.

Для доказательства независимости спаривания нам достаточно проверить, в силу его билинейности, что

$$\operatorname{tr}[X, \eta(X)]_F \equiv 0 \bmod \pi_0^n. \tag{54}$$

Точно так же как в предложении 5, § 3, работы ([11]), используя только при этом лемму 14 настоящего параграфа и рассматривая сравнения по $\bmod \pi_0^n$, доказывается следующее сравнение:

$$\operatorname{tr} \operatorname{res}_X (1/sX)\left(1-\frac{\Delta}{\pi_0}\right)(c_m u^m \varphi) \equiv 0 \bmod \pi_0^n, \tag{55}$$

где $\varphi(X)$ — произвольный степенной ряд с целыми коэффициентами из $\mathfrak{o}$ без свободного члена.

Так как $\eta(\pi) = \beta_1(\pi) \underset{F}{\sim} \beta_2(\pi) = 0$, то точно так же как в лемме 6, § 2, работы ([11]) доказывается, что существует степенной ряд $\psi(X)$ с коэффициентами из $\mathfrak{o}$ такой, что $\eta(X) = u(X)\psi(X)$ (относительно $u(X)$ см. § 1, п. 4). Поэтому если $\lambda(X) = X + c_2X^2 + c_3X^3 + \cdots$ — логарифм формальной группы F, то, полагая ряд φ в (55) равным $c_m\psi^m$ и суммируя срав-

нения (55) по m, получим:

$$\sum_{m=1}^{\infty} \operatorname{tr} \operatorname{res}_X (1/sX)\left(1-\frac{\Delta}{\pi_0}\right)(c_m u^m \psi^m) = \operatorname{tr} \operatorname{res}_X l_F(\eta)/sX \equiv 0 \bmod \pi_0^n,$$

что дает нам сравнение (54), и независимость спаривания для пары π, β доказана.

Таким образом, учитывая еще предложение 4, п. 1, нами получена следующая

ТЕОРЕМА 1. *Спаривание* $\langle \alpha, \beta \rangle_F$ *между мультипликативной группой* $k^\times$ *и группой точек* $F(\mathfrak{p})$ *билинейно, является инвариантным относительно выбора простого элемента* π *и независимым от способа разложения элементов в ряды по* π, *по крайней мере, для пары* π, β, *где* $\pi \in k^\times$, $\beta \in F(\mathfrak{p})$.

Замечание. Можно доказать инвариантность и независимость спаривания для любых элементов $\alpha \in k^\times$, $\beta \in F(\mathfrak{p})$, но в дальнейшем нам это не потребуется.

§ 7. Явная форма обобщенного символа Гильберта

В этом параграфе мы изложим основной результат работы, а именно, найдем явную формулу для обобщенного символа Гильберта $(\alpha, \beta)_F$ на группе точек $F(\mathfrak{p})$ в случае, когда поле k_0 вполне разветвлено над $\mathbf{Q}_p$.

1. Проверим предварительно следующую лемму.

ЛЕММА 15. *Пусть* $c \in \mathfrak{o}$, *тогда*

$$(\pi, E_F(c\pi^i))_F = 0,$$

если i *взаимно просто с* p.

Доказательство. Из определения функции E_F получаем, что $E_F(\theta\pi^i) = \lambda^{-1}\lambda_a(\theta\pi^i)$, если $\theta \in \mathfrak{R}$ (см. (25), § 1, п. 2). Далее, ряд $\varphi(X) = \lambda^{-1}\lambda_0(X)$ осуществляет изоморфизм из формальной группы F_0 с логарифмом λ_0 (см. лемму 2 и 3) в формальную группу F с логарифмом λ. Поэтому

$$(\theta\pi^i, E_F(\theta\pi^i))_F = \varphi((\theta\pi^i, \lambda_0^{-1}\lambda\ (\theta\pi^i))_{F_0}) \tag{56}$$

(см. (5), введение, п. 4). Обозначим $\theta\pi^i$ через α и проверим, что $(\alpha, \lambda_0^{-1}\lambda_a(\alpha))_{F_0} = 0$. Для этого надо проверить согласно норменному свойству обобщенного символа Гильберта (см. введение, п. 4), что элемент α является мультипликативной нормой в расширении поля k, полученном делением точки $\lambda_0^{-1}\lambda_a(\alpha)$ на изогению $[\pi_0^n]_0$ формальной группы F_0. Таким образом, надо присоединить к полю k корни следующего ряда: $[\pi_0^n]_0(X) = \lambda_0^{-1}\lambda_a(\alpha)$, или, что то же самое, корни ряда $g(X) - \alpha$, где $g = \lambda_a^{-1} \circ \lambda_0 \circ [\pi_0^n]_0$. Ряд $g(X) - \alpha$ имеет, согласно лемме 2, § 1, п. 1, коэффициент, равный 1 при X^{q^n}, и все коэффициенты при степенях, меньших q^n, делятся на π. По подготовительной лемме Вейерштрасса найдется ряд $\varepsilon(X) \equiv 1 \bmod \deg 2$ с коэффициентами из кольца целых элементов локального поля k такой,

что ряд $f(X)=\varepsilon(X)(g(X)-\alpha)$ будет многочленом степени q^n. Ясно при этом, что многочлен $f(X)$ унитарен (т. е. старший коэффициент его равен 1) и имеет свободный член α. Кроме того, все корни ряда $g(X)-\alpha$ будут корнями многочлена $f(X)$, и наоборот. Из унитарности многочлена $f(X)$ следует, что элемент α является нормой в расширении поля k, полученном присоединением корней многочлена $f(X)$ (см., например, ([8]), лемма 4). Таким образом, $(\alpha, \lambda_0^{-1}\lambda_a(\alpha))_{F_0}=0$, а значит, и $(\theta\pi^i, E_F(\theta\pi^i))_F=0$ (см. (56)).

Отсюда, используя билинейность символа, взаимную простоту чисел i и p и вытекающее непосредственно из определения символа равенство $(\theta, \beta)_F=0$, $\theta\in\mathfrak{R}$, получаем:

$$(\pi, E_F(\theta\pi^i))_F=\left[\frac{1}{i}\right](\pi^i, E_F(\theta\pi^i))_F \underset{F}{+} (\theta, E_F(\theta\pi^i))_F=0.$$

В общем случае из этого равенства будет следовать результат леммы, если мы разложим элемент $c\in\mathfrak{o}$ в ряд по простому элементу π_0 с коэффициентами из $\mathfrak{R}$ и воспользуемся формальной аддитивностью функции E_F и билинейностью символа Гильберта. Лемма доказана.

Пусть $\alpha=\pi^a\theta\varepsilon$ — элемент локального поля k, причем $\theta\in\mathfrak{R}$, а ε — главная единица. Обозначим через $A(X)$ ряд $X^a\theta\varepsilon(X)$, где $\varepsilon(X)=1+d_1X+\cdots$ — ряд, соответствующий разложению единицы ε в степенной ряд по простому элементу π с коэффициентами из $\mathfrak{R}$, т. е. $\varepsilon(\pi)=\varepsilon$. Аналогично, ряд $\beta(X)$ соответствует разложению элемента β группы точек $F(\mathfrak{p})$ в степенной ряд по π с коэффициентами из $\mathfrak{o}$, т. е. $\beta(\pi)=\beta$. Наконец, $z(X)$, как и раньше,— ряд, соответствующий разложению корня ξ изогении $[\pi_0^n]$ в степенной ряд по π (см. (15), § 1, п. 4). Мы считаем, далее, что поле k_0, над кольцом целых элементов которого определена формальная группа F, вполне разветвлено над $\mathbf{Q}_p$. При этих условиях имеет место следующая

ТЕОРЕМА 2. *Для обобщенного символа Гильберта* $(\alpha, \beta)_F$, *где* $\alpha\in k^\times$, $\beta\in F(\mathfrak{p})$, *при* $p\neq 2$ *имеет место формула*

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

где

$$\gamma=\operatorname{res}_X\left(l_m(\varepsilon)\frac{d}{dX}l_F(\beta)-l_m(\varepsilon)\frac{d}{dX}\lambda(\beta)+l_F(\beta)A^{-1}\frac{dA}{dX}\right)\Big/[\pi_0^n](z)$$

(*относительно функций* l_m *и* l_F *см.* (41), § 5, п. 1, *а относительно ряда* $1/[\pi_0^n](z)$ *см.* (14), § 1, п. 3).

Доказательство. Рассмотрим спаривание $\langle\alpha, \beta\rangle_F$ и проверим, что оно совпадает с обобщенным символом Гильберта на паре π, β, где $\beta\in F(\mathfrak{p})$, т. е.

$$\langle\pi, \beta\rangle_F=(\pi, \beta)_F. \tag{57}$$

Из свойств независимости спаривания (см. теорема 1, § 6) следует, что мы можем использовать любое представление элемента β в виде степенного ряда по π. Возьмем поэтому представление элемента β в сте-

пенной ряд, соответствующее каноническому разложению (40), § 4, п. 3. Тогда, с одной стороны, для символа $(\pi, \beta)_F$ получим:

$$(\pi, \beta)_F = (\pi, E_F(w_\beta)|_{X=\pi})_F \underset{F}{+} (\pi, \omega(b))_F.$$

В нашем случае поле k_0 вполне разветвлено над $\mathbf{Q}_p$, значит, $q=p$ и поэтому в каноническом разложении (40), § 4, п. 3, все степени i взаимно просты с p. Таким образом, согласно лемме 15, имеем:

$$(\pi, E_F(w_\beta)|_{X=\pi})_F = \sum_{i\,(F)} (\pi, E_F(b_i\pi^i))_F = 0.$$

Кроме того, $(\pi, \omega(b))_F = [\mathrm{tr}\, b](\xi)$ (см. предложение 1, § 3), значит,

$$(\pi, \beta)_F = [\mathrm{tr}\, b](\xi). \tag{58}$$

С другой стороны, по определению спаривания имеем:

$$\langle \pi, E(w_\beta)|_{X=\pi}\rangle_F = [\mathrm{tr}\, \gamma](\xi),$$

где $\gamma = \mathrm{res}_X w_\beta/sX$. При этом из сравнения (19), § 1, п. 4, следует, что все коэффициенты ряда $1/s$ при степенях, не делящихся на $q=p$, делятся на π_0^n. Многочлен $w_\beta(X)$ вообще не имеет членов со степенями, делящимися на p. Это означает, что свободный член ряда w_β/s делится на π_0^n или, что то же самое, $\gamma = \mathrm{res}_X w_\beta/sX \equiv 0 \bmod \pi_0^n$. Отсюда получаем:

$$\langle \pi, E(w_\beta)|_{X=\pi}\rangle_F = 0.$$

Далее, по определению спаривания имеем:

$$\langle \pi, \omega(b)\rangle_F = \langle \pi, E(bs)|_{X=\pi}\rangle_F = [\mathrm{tr}\, \gamma'](\xi),$$

где $\gamma' = \mathrm{res}_X bs/sX = b$. Таким образом,

$$\langle \pi, \beta\rangle_F = [\mathrm{tr}\, b](\xi).$$

Последнее равенство вместе с (58) дает нам (57).

Проверим теперь, что наше спаривание совпадает с обобщенным символом Гильберта на паре ε, β, где ε — главная единица поля k, а $\beta \in F(\mathfrak{p})$. Пусть $\tau = \pi\varepsilon$, тогда

$$\begin{aligned}\langle \varepsilon, \beta\rangle_\pi = \langle \tau, \beta\rangle_\pi \mathbin{\widetilde{F}} \langle \pi, \beta\rangle_\pi = \langle \tau, \beta\rangle_\tau \mathbin{\widetilde{F}} \langle \pi, \beta\rangle_\pi = \\ = (\tau, \beta)_F \mathbin{\widetilde{F}} (\pi, \beta)_F = (\varepsilon, \beta)_F.\end{aligned} \tag{59}$$

Здесь первое равенство использует билинейность спаривания, второе — инвариантность, а третье — равенство (57) (мы обозначали, кроме того, спаривание $\langle \alpha, \beta\rangle_F$, построенное с помощью элемента π, через $\langle \alpha, \beta\rangle_\pi$, а с помощью τ — через $\langle \alpha, \beta\rangle_\tau$).

В общем случае из (57), (59) и билинейности спаривания получим:

$$\langle \alpha, \beta\rangle_F = [a]\langle \pi, \beta\rangle_F \underset{F}{+} \langle \varepsilon, \beta\rangle_F = [a](\pi, \beta)_F \underset{F}{+} (\varepsilon, \beta)_F = (\alpha, \beta)_F.$$

Теорема доказана.

Замечание. Если формальная группа F является мультипликативной, то формула для обобщенного символа Гильберта, найденная в теореме, в точности совпадает с формулой для обычного символа Гильберта (см. ([11]), теорема 4, § 5).

Поступило
3.I.1979

Литература

[1] **Hasse H.**, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II: Reziprozitätsgesetz, Jahresbericht der deutsche Math.—Ver., 6 (1930), 204.

[2] **Hasse H.**, Die Gruppe der p^n-primären Zahlen für einen Primteiler $\mathfrak{p}$ von p, J. reine u. angew. Math., 176 (1936), 174—183.

[3] **Шафаревич И. Р.**, Общий закон взаимосвязи, Матем. сб., 26 (68), № 1 (1950), 113—146.

[4] **Lubin J., Tate J.**, Formal complex multiplication in local fields, Ann. Math., 81 (1965), 380—387.

[5] **Iwasawa K.**, On explicit formulas för the norm residue symbol, J. Math. Soc. Japan, 20 (1968), 151—164.

[6] **Fröhlich A.**, Formal groups, Lect. Notes Math., 74 (1968), 140.

[7] **Cartier P.**, Groupes de Lubin — Tate généralisés, Invent. math., 35 (1976), 273—284.

[8] **Coates J., Wiles A.**, Explicit reciprocity laws, Soc. Math. France Astérisque, 41—42 (1977), 7—17.

[9] **Востоков С. В.**, Явная формула спаривания в формальных модулях, Докл. АН СССР, 241, № 2 (1978), 275—278.

[10] **Wiles A.**, Higher explicit reciprocity laws, Ann. Math., 167, № 2 (1978), 235—254.

[11] **Востоков С. В.**, Явная форма закона взаимности, Изв. АН СССР. Сер. матем., 42 (1978), 1287—1320.

[12] **Hasse H.**, Zahlentheorie, Berlin, 1963.