С. В. Востоков, Явная форма закона взаимности, *Изв. АН СССР. Сер. матем.*, 1978, том 42, выпуск 6, 1288–1321

СЕРИЯ
МАТЕМАТИЧЕСКАЯ
Том 42, № 6, 1978

УДК 519.48

С. В. ВОСТОКОВ

ЯВНАЯ ФОРМА ЗАКОНА ВЗАИМНОСТИ

Введение

1. Классический 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. X. Хассе свел эту задачу с помощью формулы (см. ([2]), стр. 58)

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1}=\prod_{\mathfrak{p}|n}\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)$$

к вопросу о нахождении явного выражения символа норменного вычета Гильберта $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)$ через числа α и β в локальном поле (конечном расширении поля p-адических чисел $\mathbf{Q}_p$).

Частные случаи в круговых расширениях поля $\mathbf{Q}_p$ были разобраны в работах ([1]), ([2]), ([4]). Основное достижение было сделано в работе ([5]), в которой был построен канонический базис мультипликативной группы локального поля и на базисных элементах задана конструкция, позволяющая вычислить символ Гильберта в конечное число шагов (см. § 6, п. 4).

В настоящей работе дается явная формула символа Гильберта через разложение заданных элементов α и β в ряды по локальной униформизирующей (см. § 6). При этом в § 2 строится спаривание в некоторой группе формальных рядов со значениями в кольце целых элементов $\mathfrak{o}$ подполя инерции поля k и доказываются свойства билинейности, кососимметричности и инвариантности этого спаривания (см. теорему 1, § 2, п. 4).

В § 3 вводится спаривание $\langle\alpha, \beta\rangle_\pi$ в мультипликативной группе локального поля с помощью спаривания, построенного в § 2, и проверяются свойства билинейности, кососимметричности и инвариантности этого спаривания, а также доказывается независимость его от способа разложения элементов α и β в ряды по простому элементу π поля k.

В § 5 вычисляется символ Гильберта для пары (π, ε), где ε — главная единица поля k. При этом в п. 1, § 5, доказывается существование однозначно заданного выбором простого элемента π и первообразного корня ζ степени p^n из единицы ряда $V(X)=v_1X^{-1}+v_2X^{-2}+\ldots$, с помощью которого можно, зная представление главной единицы ε в виде степенного ряда по простому элементу π, вычислить в явном виде символ Гильберта (π, ε) (см. предложение 7, § 5, п. 1). В следующих пунктах этого параграфа ряд $V(X)$ вычисляется в явном виде с помощью построенных в § 4 p^n-примарных элементов поля k, что дает нам формулу для символа Гильберта (π, ε) (см. теорему 3, § 1, п. 5).

В § 6 доказывается основной результат работы — общая формула символа норменного вычета Гильберта. При этом предлагается два варианта доказательства, первый из которых использует результаты §§ 2, 4, 5, т. е. свойства спаривания [A, B] и знание формулы для символа Гильберта (π, ε), а второй — результаты §§ 3, 4. Тем самым этот способ не использует теории полей классов, а опирается лишь на свойства спаривания $\langle\alpha, \beta\rangle_\pi$ (см. § 3), что, с одной стороны, дает чисто локальное определение символа Гильберта, а с другой — возможность вывести локальную теорию полей классов из свойств спаривания $\langle\alpha, \beta\rangle_\pi$ так же, как это было сделано, например, в ([6]) (см. § 7).

Во всей работе предполагается, что p — нечетное простое число.

2. Введем основные обозначения статьи.

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

e — абсолютный индекс ветвления поля k, $e_1 = \dfrac{e}{p-1}$,

π — простой элемент поля k,

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

ζ — первообразный корень степени p^n из 1, содержащийся в k,

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

T — подполе инерции в $k/\mathbf{Q}_p$,

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

Δ — автоморфизм Фробениуса в $T/\mathbf{Q}_p$,

tr — оператор следа в $T/\mathbf{Q}_p$,

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

Пусть корень ζ разложен в степенной ряд по простому элементу π с коэффициентами из $\mathfrak{o}$, т. е. $\zeta=1+c_1\pi+c_2\pi^2+\ldots$, тогда будем обозначать через $z(X)$ и $z_0(X)$ следующие ряды:

$$z_0(X) = c_1X + c_2X^2 + \ldots,$$

$$z(X) = 1 + z_0(X) = 1 + c_1X + c_2X^2 + \ldots .$$

Пусть $\varphi(X)=a_mX^m+a_{m+1}X^{m+1}+\ldots$ — произвольный формальный ряд с коэффициентами из $\mathfrak{o}$, тогда будем обозначать порядок этого ряда следующим образом: $\deg\varphi=m$.

Если $\varphi(X)$ и $\psi(X)$ — два формальных ряда с коэффициентами из $\mathfrak{o}$, то сравнение

$$\varphi(X)\equiv\psi(X) \mod \deg r$$

будет означать, что коэффициенты при степенях, меньших чем r, рядов φ и ψ равны между собой, а сравнение

$$\varphi(X) \equiv \psi(X) \bmod (p^n, \deg r)$$

будет означать, что эти же коэффициенты сравнимы по $\bmod p^n$.

Определим, наконец, действие автоморфизма Фробениуса Δ на формальный ряд $\varphi(X) = \sum\limits_r a_r X^r$ следующим образом:

$$\Delta\varphi = \varphi^\Delta = \sum_r a_r^\Delta X^{pr}.$$

§ 1. Функции l и E

Пусть $\mathfrak{o}_0[[X]]$ — аддитивная группа формальных степенных рядов без свободного члена с коэффициентами из кольца $\mathfrak{o}$, рассматриваемая как $\mathbf{Z}_p$-модуль. Пусть, далее, $1+\mathfrak{o}_0[[X]]$ — мультипликативная группа, рассматриваемая как мультипликативно записываемый $\mathbf{Z}_p$-модуль. Найдем функции, которые осуществляют изоморфизм между этими модулями.

1. Пусть $h(X)$ — степенной ряд с целыми коэффициентами из кольца $\mathfrak{o}$.

ЛЕММА 1. *Для любого $m \geqslant 1$ ряд $\dfrac{h^{pm} - h^{\Delta m}}{pm}$ имеет целые коэффициенты из кольца $\mathfrak{o}$.*

Доказательство. Утверждение леммы достаточно проверить для $m = p^r$. В этом же случае проверка происходит несложной индукцией по r. Лемма доказана.

Пусть $\varepsilon(X) \in 1+\mathfrak{o}_0[[X]]$. Определим функцию $l(\varepsilon)$ следующим образом:

$$l(\varepsilon) = \left(1 - \frac{\Delta}{p}\right) \log \varepsilon(X).$$

ЛЕММА 2. *Функция $l(\varepsilon)$ является степенным рядом без свободного члена с целыми коэффициентами, т. е. $l(\varepsilon) \in \mathfrak{o}_0[[X]]$.*

Доказательство. Пусть $\varepsilon(X) = 1 + h(X)$, где $h(X) \in \mathfrak{o}_0[[X]]$. Тогда при нечетном p имеем:

$$l(\varepsilon) = \sum_{m=1}^{\infty} \frac{(-1)^{m-1} h^m}{m} - \frac{1}{p} \sum_{m=1}^{\infty} \frac{(-1)^{m-1} h^{\Delta m}}{m} =$$

$$= \sum_{(m,p)=1} \frac{(-1)^{m-1} h^m}{m} + \sum_{m=1}^{\infty} (-1)^{m-1} \frac{h^{pm} - h^{\Delta m}}{pm}$$

и утверждение леммы в этом случае следует из леммы 1. Аналогично проверяется случай $p=2$. Лемма доказана.

Следствие. *Функция $l(\varepsilon)$ определена на главных единицах локального поля k и имеет значения при этом в простом идеале $\mathfrak{p}$.*

Заметим, что из доказанной леммы и очевидного равенства

$$l(\varepsilon\eta)=l(\varepsilon)+l(\eta), \tag{1}$$

где ε, $\eta\in 1+\mathfrak{o}_0[[X]]$, следует, что функция l задает гомоморфизм из мультипликативного $\mathbf{Z}_p$-модуля $1+\mathfrak{o}_0[[X]]$ в аддитивный $\mathbf{Z}_p$-модуль $\mathfrak{o}_0[[X]]$.

2. Найдем теперь обратное отображение из $\mathfrak{o}_0[[X]]$ в $1+\mathfrak{o}_0[[X]]$. Рассмотрим для этого функцию Шафаревича

$$E(X)=\exp\sum_{r=0}^{\infty}\frac{X^{p^r}}{p^r}$$

(см. [1], [5]). Из равенства

$$E(X)=\prod_{(m,p)=1}(1-X^m)^{-\frac{\mu(m)}{m}} \tag{2}$$

(см. [5], (3)) следует, что функция $E(X)$ является степенным рядом с целыми коэффициентами и свободным членом 1.

Свяжем функции E с автоморфизмом Фробениуса Δ и определим их для любого ряда $\varphi(X)$ из $\mathfrak{o}_0[[X]]$ следующим образом:

$$E(\varphi(X))=\exp\sum_{r=0}^{\infty}\frac{\varphi^{\Delta^r}}{p^r}.$$

Иногда для удобства мы эти функции будем писать в виде

$$E(\varphi(X))=\exp\left(1+\frac{\Delta}{p}+\frac{\Delta^2}{p^2}+\dots\right)(\varphi). \tag{3}$$

Очевидно, что функция E мультипликативна, т. е. если $\varphi(X)$ и $\psi(X)\in\in\mathfrak{o}_0[[X]]$, то

$$E(\varphi+\psi)=E(\varphi)E(\psi). \tag{4}$$

ЛЕММА 3. *Функция $E(\varphi(X))$ является степенным рядом с целыми коэффициентами и свободным членом 1, т. е. $E(\varphi(X))\in 1+\mathfrak{o}_0[[X]]$.*

Доказательство. Пусть $\varphi(X)=\sum_{m\geqslant 1}a_mX^m$, $a_m\in\mathfrak{o}$. Тогда из (4) следует, что

$$E(\varphi(X))=\prod_{m\geqslant 1}E(a_mX^m)$$

и поэтому утверждение леммы достаточно проверить для функций $E(a_mX^m)$. Если при этом a_m принадлежит мультипликативной системе $\mathfrak{R}$, то наше утверждение следует из (2). В общем случае оно вытекает из мультипликативности функции E и разложения любого элемента из $\mathfrak{o}$ в сумму элементов из $\mathfrak{R}$. Лемма доказана.

Следствие. *Функция $E(\varphi(X))$ определена на простом идеале $\mathfrak{p}$ поля k и имеет значения при этом в группе главных единиц поля k.*

ЛЕММА 4. *Функции* $l(\varepsilon)$ *и* $E(\varphi)$ *являются взаимно обратными отображениями, т. е.*

$$E(l(\varepsilon))=\varepsilon(X),\quad l(E(\varphi))=\varphi(X).$$

Доказательство. Из определения функций E и l следует:

$$E(l(\varepsilon))=\exp\left(1+\frac{\Delta}{p}+\frac{\Delta^2}{p^2}+\ldots\right)\left(\left(1-\frac{\Delta}{p}\right)\log\varepsilon\right)=\exp\log\varepsilon=\varepsilon(X),$$

$$l(E(\varphi))=\left(1-\frac{\Delta}{p}\right)\log E(\varphi)=\left(1-\frac{\Delta}{p}\right)\log\left(\exp\left(1+\frac{\Delta}{p}+\frac{\Delta^2}{p^2}+\ldots\right)(\varphi)\right)=$$
$$=\left(1-\frac{\Delta}{p}\right)\left(1+\frac{\Delta}{p}+\frac{\Delta^2}{p^2}+\ldots\right)(\varphi)=\varphi(X).$$

Лемма доказана.

Из доказанных лемм вытекает следующее

Предложение 1. *Функции* l *и* E *являются взаимно обратными изоморфизмами между мультипликативным* $\mathbf{Z}_p$*-модулем* $1+\mathfrak{o}_0[[X]]$ *и аддитивным* $\mathbf{Z}_p$*-модулем* $\mathfrak{o}_0[[X]]$.

§ 2. Спаривание [A, B]

1. Рассмотрим мультипликативную группу G формальных рядов вида

$$G=\{X^m\theta\varepsilon(X);\ m\in\mathbf{Z},\ \theta\in\mathfrak{R},\ \varepsilon(X)\in 1+\mathfrak{o}_0[[X]]\}.$$

Пусть $\mathrm{A}(X)$ и $\mathrm{B}(X)$ — два формальных ряда из G и при этом $\mathrm{A}=X^a\theta\varepsilon(X)$, $\mathrm{B}=X^b\theta'\eta(X)$, где $\theta,\theta'\in\mathfrak{R}$, а $\varepsilon,\eta\in 1+\mathfrak{o}_0[[X]]$.

Введем в группе G спаривание со значениями в кольце $\mathfrak{o}$ следующим образом:

$$[\mathrm{A},\mathrm{B}]=\operatorname{res}_X\Phi(X)W(X),\tag{5}$$

где

$$\Phi(X)=l(\varepsilon)\frac{dl(\eta)}{dX}-l(\varepsilon)\mathrm{B}^{-1}\frac{d\mathrm{B}}{dX}+l(\eta)\mathrm{A}^{-1}\frac{d\mathrm{A}}{dX},$$

а ряд $W(X)$ — некоторый фиксированный формальный ряд с коэффициентами из $\mathfrak{o}$, имеющий, вообще говоря, члены отрицательных степеней, для которого

$$\frac{d}{dX}W(X)\equiv 0\bmod p^n.\tag{6}$$

Замечание 1. *Ряд* $\Phi(X)$, *согласно лемме* 2, § 1, п. 1, *является степенным рядом с целыми коэффициентами, т. е.* $\Phi(X)\in\mathfrak{o}[[X]]$.

Замечание 2. *Если* $\mathrm{A}=\theta\in\mathfrak{R}$, *то очевидно, что* $[\theta,\mathrm{B}]=0$.

Нашей ближайшей целью будет доказательство следующих свойств этого спаривания: билинейность, кососимметричность по $\bmod p^n$ и инвариантность по $\bmod p^n$.

2. Проверим в этом пункте билинейность и кососимметричность спаривания $[\mathrm{A},\mathrm{B}]$. Нетрудно видеть, что если $\mathrm{A}=X^a\theta\varepsilon(X)$, $\theta\in\mathfrak{R}$, $\varepsilon\in 1+\mathfrak{o}_0[[X]]$, то

$$\mathrm{A}^{-1}\frac{d\mathrm{A}}{dX}=aX^{-1}+\frac{d}{dX}\log\varepsilon.$$

Отсюда, из равенства (1), § 1, п. 1, и аддитивности производной следует билинейность нашего спаривания, т. е.

$$[\mathrm{A}_1\mathrm{A}_2, \mathrm{B}] = [\mathrm{A}_1, \mathrm{B}] + [\mathrm{A}_2, \mathrm{B}]; \quad [\mathrm{A}, \mathrm{B}_1\mathrm{B}_2] = [\mathrm{A}, \mathrm{B}_1] + [\mathrm{A}, \mathrm{B}_2].$$

Чтобы проверить кососимметричность по $\mathrm{mod}\, p^n$, заметим, что для нашего спаривания выполняется следующая

ЛЕММА 5. *Пусть ряд* $\Phi(X)$, *соответствующий элементам* A *и* B *в спаривании* (5), *является производной некоторого степенного ряда* $\varphi(X)$ *с целыми коэффициентами, т. е.* $\Phi(X) = \frac{d}{dX}\varphi(X)$, *где* $\varphi(X) \in \mathfrak{o}[[X]]$. *Тогда*

$$[\mathrm{A}, \mathrm{B}] \equiv 0 \bmod p^n.$$

Доказательство. Из условия леммы и сравнения (6) получим:

$$[\mathrm{A}, \mathrm{B}] = \mathrm{res}_X \left(\frac{d}{dX}\varphi\right) W \equiv \mathrm{res}_X \left(\frac{d}{dX}\varphi\right) W + \mathrm{res}_X \varphi \frac{d}{dX} W = \\ = \mathrm{res}_X \frac{d}{dX}(\varphi W) = 0 \bmod p^n.$$

Лемма доказана.

Из доказанной леммы немедленно следует кососимметричность по $\mathrm{mod}\, p^n$. Действительно,

$$[\mathrm{A}, \mathrm{B}] + [\mathrm{B}, \mathrm{A}] = \mathrm{res}_X \left(\frac{d}{dX} l(\varepsilon)\, l(\eta)\right) W \equiv 0 \bmod p^n.$$

3. Докажем теперь инвариантность спаривания [A, B] по $\mathrm{mod}\, p^n$ в случае, когда $\mathrm{A}=X$, $\mathrm{B}=\varepsilon(X) \in 1+\mathfrak{o}_0[[X]]$. В этом случае $\varepsilon(X)$ можно записать, согласно лемме 4, § 1, п. 2, в виде

$$\varepsilon(X) = E(l(\varepsilon)),$$

при этом $l(\varepsilon) \in \mathfrak{o}_0[[X]]$. Ввиду билинейности нашего спаривания и мультипликативности функции E (см. (4), § 1, п. 2), инвариантность достаточно проверить для следующей пары:

$$[X, E(\alpha X^m)], \quad \alpha \in \mathfrak{R}, \quad m \geqslant 1.$$

Пусть имеется следующая замена переменных:

$$X = g(Y) = Y\theta\psi(Y), \quad \theta \in \mathfrak{R}, \quad \psi(Y) \in 1 + \mathfrak{o}_0[[Y]].$$

Рассмотрим, как изменится ряд $E(\alpha X^m)$ при этой замене переменных. Так как функция E (см. (3), § 1, п. 2) существенным образом зависит от выбора переменной X, то мы будем обозначать входящий в ее определение автоморфизм Фробениуса для переменной X через Δ_1, а для переменной Y — через Δ_2, а функцию E для переменной X снабжать индексом E_X; таким образом,

$$E_X(\varphi) = \exp\left(1 + \frac{\Delta_1}{p} + \frac{\Delta_1^2}{p^2} + \dots\right)(\varphi(X)).$$

При этих обозначениях имеет место следующая формула замены переменных (см. также ([5]), формулу (46), стр. 136):

$$E_X(\alpha X^m)=E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S\right), \tag{7}$$

где $\alpha\in\mathfrak{R}$,

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

Действительно,

$$E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S\right)=\exp\left(1+\frac{\Delta_2}{p}+\frac{\Delta_2^2}{p^2}+\ldots\right)\left(1-\frac{\Delta_2}{p}\right)S\Big)=\exp S=$$
$$=\exp\left(\alpha g^m+\frac{(\alpha g^m)^p}{p}+\ldots\right)=\exp\left(\alpha X^m+\frac{\alpha^p X^{pm}}{p}+\ldots\right)=E_X(\alpha X^m)$$

и формула (7) доказана.

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

$$\left(1-\frac{\Delta_2}{p}\right)S=\alpha g^m+\sum_{r=1}^{\infty}\alpha^{p^r}\frac{g^{p^r m}-g^{p^{r-1}m\Delta_2}}{p^r} \tag{8}$$

и каждое слагаемое в сумме, стоящей справа, является рядом из $\mathfrak{o}_0[[X]]$ (см. лемму 1, § 1, п. 1).

Предложение 2. *Пусть $X=g(Y)$. Тогда при $p\neq 2$ имеет место сравнение*

$$[X, E_X(\alpha X^m)]\equiv\left[g(Y), E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S\right)\right]\bmod p^n.$$

Доказательство. Пусть

$$[X, E_X(\alpha X^m)]=\operatorname{res}_X\Phi(X)W(X),$$
$$\left[g(Y), E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S\right)\right]=\operatorname{res}_Y\Psi(Y)W(g(Y)).$$

Тогда по определению (5) ряд $\Phi(X)$ в первом равенстве имеет вид

$$\Phi(X)=\alpha X^{m-1}. \tag{9}$$

Подсчитаем теперь ряд $\Psi(Y)$ во втором равенстве:

$$\Psi(Y)=l(\psi)\frac{d}{dY}\left(1-\frac{\Delta_2}{p}\right)S-l(\psi)\frac{d}{dY}S+\left(1-\frac{\Delta_2}{p}\right)S\cdot g^{-1}\frac{dg}{dY}.$$

Представляя $\left(1-\frac{\Delta_2}{p}\right)S$ в виде (8), получим отсюда:

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

Из легко проверяемых равенств для произвольного ряда $\varphi \in \mathfrak{o}[[Y]]$ и $g(Y)=Y\theta\psi(Y)$:

$$\frac{d}{dY}\varphi^{\Delta_2}=pY^{p-1}\left(\frac{d\varphi}{dY}\right)^{\Delta_2},$$

$$g^{-1}\frac{dg}{dY}=\frac{dl(\psi)}{dY}+Y^{p-1}\left(g^{-1}\frac{dg}{dY}\right)^{\Delta_2} \tag{10}$$

следует:

$$\alpha^{p^r}\frac{d}{dY}\left(\frac{g^{p^r m}-g^{p^{r-1}m\Delta_2}}{p^{2r}m}-l(\psi)\frac{g^{p^{r-1}m\Delta_2}}{p^r}\right)=$$

$$=\alpha^{p^r}\frac{g^{p^r m}-g^{p^{r-1}m\Delta_2}}{p^r}\cdot g^{-1}\frac{dg}{dY}-l(\psi)\frac{d}{dY}\frac{(\alpha g^m)^{p^{r-1}\Delta_2}}{p^r}.$$

Поэтому окончательно получим:

$$\Psi(Y)=\alpha g^{m-1}\frac{dg}{dY}+\frac{d}{dY}\varphi(Y), \tag{11}$$

где

$$\varphi(Y)=\sum_{r=1}^{\infty}(\alpha g^m)^{p^{r-1}\Delta_2}S_r,$$

$$S_r=\frac{g^{p^r m-p^{r-1}m\Delta_2}-1}{p^{2r}m}-\frac{l(\psi)}{p^r}.$$

Проверим, что степенной ряд S_r имеет целые коэффициенты. Действительно, так как $g(Y)=Y\theta\psi(Y)$, то

$$g^{p^r m-p^{r-1}m\Delta_2}=\psi^{p^r m-p^{r-1}m\Delta_2}=\exp\log\psi^{p^r m\left(1-\frac{\Delta_2}{p}\right)}=\exp p^r ml(\psi),$$

откуда

$$S_r=\frac{\exp p^r ml(\psi)-1}{p^{2r}m}-\frac{l(\psi)}{p^r}=\sum_{i=2}^{\infty}\frac{p^{(i-2)r}m^{i-1}}{i!}l(\psi)^i.$$

Нетрудно видеть, что при $p\neq 2$ (вот место, где по существу используется нечетность простого числа p) ряд

$$\frac{p^{(i-2)r}m^{i-1}}{i!}l(\psi)^i\in\mathfrak{o}[[Y]],$$

так как $l(\psi)\in\mathfrak{o}[[Y]]$ (см. лемму 2, § 1, п. 1) и $p^{(i-2)r}m^{i-1}/i!\in\mathbf{Z}_p$, если $p\neq 2$. Таким образом, ряд $\varphi(Y)$ в формуле (11) является степенным рядом с целыми коэффициентами. Поэтому из (11), применяя лемму 5, п. 2, получим, учитывая еще (9):

$$\operatorname{res}_Y\Psi(Y)W(g(Y))=\operatorname{res}_Y\left(\alpha g^{m-1}\frac{dg}{dY}+\frac{d\varphi}{dY}\right)W(g(Y))\equiv$$

$$\equiv\operatorname{res}_Y\left(\alpha g^{m-1}\frac{dg}{dY}\right)W(g(Y))=\operatorname{res}_Y\Phi(g)W(g)\frac{dg}{dY}=\operatorname{res}_X\Phi(X)W(X)$$

и предложение доказано.

4. Проверим теперь инвариантность спаривания [A, B] в случае, когда $A=\varepsilon(X)$, $B=\eta(X)\in 1+\mathfrak{o}_0[[X]]$. Надо отметить, что эта часть не является необходимой нам в дальнейшем и приводится здесь в основном для полноты изложения. Так же как и в предыдущем пункте, используя представление $\varepsilon(X)$ и $\eta(X)$ в виде функций $E(l(\varepsilon))$ и $E(l(\eta))$, а также билинейность спаривания и мультипликативность функции E, легко видеть, что инвариантность в этом случае достаточно проверить для следующей пары:

$$[E(\alpha X^u),\ E(\beta X^v)],\qquad \alpha,\beta\in\mathfrak{R}.$$

Пусть, как и в п. 3, $X=g(Y)$, тогда (см. (7), п. 3)

$$E_X(\alpha X^u)=E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S_\varepsilon\right),\qquad S_\varepsilon=\sum_{r=0}^{\infty}\frac{(\alpha g^u)^{p^r}}{p^r},$$

$$E_X(\beta X^v)=E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S_\eta\right),\qquad S_\eta=\sum_{r=0}^{\infty}\frac{(\beta g^v)^{p^r}}{p^r}.$$

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

$$[E(\alpha X^u),\ E(\beta X^v)]\equiv\left[E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S_\varepsilon\right),\ E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S_\eta\right)\right]\bmod p^n.$$

Доказательство. Пусть

$$[E_X(\alpha X^u),\ E_X(\beta X^v)]=\operatorname{res}_X\Phi(X)\,W(X),$$

$$\left[E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S_\varepsilon\right),\ E_Y\left(\left(1-\frac{\Delta_2}{p}\right)S_\eta\right)\right]=\operatorname{res}_Y\Psi(Y)\,W(g(Y)).$$

Тогда по определению (5), п. 1, ряд $\Phi(X)$ в первом равенстве имеет вид

$$\Phi(X)=\alpha X^u\frac{d}{dX}\beta X^v-\alpha X^u\frac{d}{dX}\sum_{r=0}^{\infty}\frac{(\beta X^v)^{p^r}}{p^r}+\beta X^v\frac{d}{dX}\sum_{s=0}^{\infty}\frac{(\alpha X^u)^{p^s}}{p^s}.$$

Подсчитаем теперь ряд $\Psi(Y)$ во втором равенстве, пользуясь определением (5), п. 1:

$$\Psi(Y)=\Phi(g(Y))\frac{dg}{dY}+\sum_{r=1}^{\infty}\sigma_r+\sum_{r,s=1}^{\infty}\tau_{r,s},$$

где

$$\sigma_r=\alpha g^u\frac{d}{dY}\beta^{p^r}\frac{g^{p^rv}-g^{p^{r-1}v\Delta_2}}{p^r}+\beta^{p^r}\frac{g^{p^rv}-g^{p^{r-1}v\Delta_2}}{p^r}\frac{d}{dY}(\alpha g^u),$$

$$\tau_{r,s}=\beta^{p^r}\frac{g^{p^rv}-g^{p^{r-1}v\Delta_2}}{p^r}-\alpha^{p^s}\frac{g^{p^su}-g^{p^{s-1}u\Delta_2}}{p^s}\frac{d}{dY}\frac{(\beta g^v)^{p^{r-1}\Delta_2}}{p^r}.$$

Очевидно, что

$$\sigma_r=\frac{d}{dY}\left(\alpha\beta^{p^r}g^u\cdot\frac{g^{p^rv}-g^{p^{r-1}v\Delta_2}}{p^r}\right);$$

при этом ряд, стоящий под дифференциалом, является степенным рядом с целыми коэффициентами (см. лемму 1, § 1, п. 1) и мы можем записать:

$$\sum_{r=1}^{\infty} \sigma_r = \frac{d}{dY} \varphi_1(Y), \quad \varphi_1(Y) \in \mathfrak{o}[[Y]].$$

Далее, используя равенства (10), п. 3, нетрудно показать, что

$$\tau_{r,s} = \frac{d}{dY} ((\alpha g^u)^{p^{s-1}\Delta_2} (\beta g^v)^{p^{r-1}\Delta_2} \gamma_{r,s}),$$

где

$$\gamma_{r,s} = \frac{u}{p^r(p^s u + p^r v)} (g^{p^s u - p^{s-1} u \Delta_2} g^{p^r v - p^{r-1} v \Delta_2} - 1) - \frac{g^{p^s u - p^{s-1} u \Delta_2} - 1}{p^{r+s}}.$$

Проверим, что степенной ряд $\gamma_{r,s}(Y)$ имеет целые коэффициенты, т. е. $\gamma_{r,s} \in \mathfrak{o}[[Y]]$. Действительно, как и в предложении 2, имеем:

$$g^{p^s u + p^r v - p^{s-1} u \Delta_2 - p^{r-1} v \Delta_2} = \exp (p^s u + p^r v)\, l(\psi),$$
$$g^{p^s u - p^{s-1} u \Delta_2} = \exp p^s u l(\psi),$$

откуда получим:

$$\gamma_{r,s} = \frac{u}{p^r(p^s u + p^r v)} (\exp (p^s u + p^r v)\, l(\psi) - 1) - \frac{\exp p^s u l(\psi) - 1}{p^{r+s}} =$$
$$= \sum_{m=2}^{\infty} \frac{u(p^s u + p^r v)^{m-1} - p^{(m-1)s} u^m}{p^r m!} l(\psi)^m.$$

Нетрудно видеть, что при $p \neq 2$ число

$$\frac{u(p^s u + p^r v)^{m-1} - p^{(m-1)s} u^m}{p^r m!}$$

является p-целым, откуда следует, что $\gamma_{r,s} \in \mathfrak{o}[[Y]]$. Таким образом, мы можем записать:

$$\sum_{r,s} \tau_{r,s} = \frac{d}{dY} \varphi_2(Y), \text{ где } \varphi_2(Y) \in \mathfrak{o}[[Y]].$$

Используя лемму 5, п. 2, как и в предложении 2 получим:

$$\operatorname{res}_Y \Psi(Y)\, W(g(Y)) = \operatorname{res}_Y \left(\Phi(g) \frac{dg}{dY} + \frac{d\varphi_1}{dY} + \frac{d\varphi_2}{dY}\right) W(g) \equiv$$
$$\equiv \operatorname{res}_Y \Phi(g)\, W(g) \frac{dg}{dY} = \operatorname{res}_X \Phi(X)\, W(X),$$

и предложение доказано.

Сформулируем основной результат этого параграфа в виде следующей теоремы, вытекающей из результатов п. 2, предложений 2 и 3.

ТЕОРЕМА 1. *Спаривание* [A, B] *обладает свойством билинейности, кососимметричности по* mod p^n *и инвариантности по* mod p^n.

§ 3. Спаривание $\langle\alpha, \beta\rangle_\pi$

1. Построим с помощью спаривания [A, B] (см. § 2) спаривание в мультипликативной группе локального поля k со значениями в группе корней степени p^n из единицы. Пусть $\alpha=\pi^a\theta\varepsilon$, $\beta=\pi^b\theta'\eta$ — элементы локального поля k, при этом θ, θ' взяты из мультипликативной системы $\mathfrak{R}$, а ε, η — главные единицы. Пусть $\varepsilon=1+a_1\pi+a_2\pi^2+\ldots$ — некоторое разложение единицы ε в ряд по простому элементу π с коэффициентами из кольца $\mathfrak{o}$. Обозначим через $A(X)$ ряд $X^a\theta\varepsilon(X)$, где $\varepsilon(X)=1+a_1X+ +a_2X^2+\ldots$. Аналогичный смысл для элемента β имеют ряды $B(X)$ и $\eta(X)$. Пусть $z(X)$ — ряд, полученный из разложения корня ζ в степенной ряд по π (см. введение, п. 2). При этих обозначениях рассмотрим следующее спаривание:

$$\langle\alpha, \beta\rangle_\pi=\zeta^{\operatorname{tr}[A,B]}, \tag{12}$$

где [A, B] определено формулой (5), § 2, п. 1, в которой в качестве ряда $W(X)$ взят ряд $(z^{p^n}-1)^{-1}$.

Замечание 3. *Пусть $z(X)=z_0(X)+1$, тогда под рядом $(z^{p^n}-1)^{-1}$ понимается следующий ряд Лорана:*

$$(z^{p^n}-1)^{-1}=z_0^{-p^n}\left(1+\sum_{i=1}^{p^n-1}C_{p^n}^i z_0^{-i}\right)^{-1}. \tag{13}$$

Замечание 4. *Очевидно, что ряд $(z^{p^n}-1)^{-1}$ удовлетворяет условию* 6), § 2, п. 1.

Замечание 5. *Спаривание* (12) *зависит от выбора простого элемента π и от способа разложения элементов α и β в ряды по простому элементу π.*

Из доказанных в § 2 свойств спаривания [A, B] вытекает следующее

Предложение 4. *Спаривание $\langle\alpha, \beta\rangle_\pi$ билинейно, кососимметрично и инвариантно относительно выбора простого элемента π.*

2. Прежде чем доказывать независимость спаривания $\langle\alpha, \beta\rangle_\pi$ от способа разложения элементов α и β в ряды по π, проверим несколько утверждений. Рассмотрим следующие обозначения. Пусть

$$s_m(X)=z^{p^m}(X)-1, \quad u_m(X)=\frac{s_m(X)}{s_{m-1}(X)}.$$

Ряды $s_n(X)$ и $u_n(X)$ обозначаем в дальнейшем просто через s и u. Таким образом,

$$u(X)=\frac{s(X)}{s_{n-1}(X)}=1+z^{p^{n-1}}+z^{2p^{n-1}}+\ldots+z^{(p-1)p^{n-1}} \tag{14}$$

и, значит,

$$u(\pi)=1+\zeta^{p^{n-1}}+\ldots+\zeta^{(p-1)p^{n-1}}=0.$$

Заметим, что порядок ряда $z_0(X)=z(X)-1$, рассматриваемого по $\operatorname{mod} p$, равен $\frac{e}{p^{n-1}(p-1)}$, так как $z_0(\pi)=\zeta-1$. Отсюда и из (14) следует, в частности, что ряд $u(X)$ можно записать в виде

$$u(X) = p + pb_1X + \ldots + pb_{e-1}X^{e-1} + b_eX^e + b_{e+1}X^{e+1} + \ldots, \quad b_i \in \mathfrak{o};$$

при этом b_e — единица кольца $\mathfrak{o}$.

ЛЕММА 6. *Пусть* $\varphi(X)$ — *такой степенной ряд из* $\mathfrak{o}[[X]]$, *что* $\varphi(\pi) = 0$. *Тогда найдется ряд* $\psi(X) \in \mathfrak{o}[[X]]$ *такой, что*

$$\varphi(X) = u(X)\psi(X).$$

Доказательство. Из построения ряда $u(X)$ видно, что все его коэффициенты до степени $e-1$ включительно делятся на p, а коэффициент при X^e является единицей кольца $\mathfrak{o}$. Поэтому по подготовительной лемме Вейерштрасса найдется ряд $\varepsilon(X) \in 1 + \mathfrak{o}_0[[X]]$ такой, что $u_*(X) = u(X)\varepsilon(X)$ будет многочленом Эйзенштейна степени e.

Не нарушая общности, можно считать, что наибольший общий делитель всех коэффициентов ряда $\varphi(X)$ равен 1 (в противном случае его можно вынести из ряда $\varphi(X)$ в качестве целого множителя). Тогда для ряда $\varphi(X)$ найдется опять по подготовительной лемме Вейерштрасса ряд $\eta(X) \in 1 + \mathfrak{o}_0[[X]]$ такой, что $\varphi_*(X) = \varphi(X)\eta(X)$ будет многочленом. Ясно при этом, что $\varphi_*(\pi) = 0$.

Итак, мы получили два многочлена $\varphi_*(X)$ и $u_*(X)$, у которых есть общий корень π. При этом $u_*(X)$, будучи многочленом Эйзенштейна, является неприводимым многочленом без кратных корней. Отсюда следует, что $\varphi_*(X)$ делится без остатка на $u_*(X)$, т. е. $\varphi_*(X) = g(X)u_*(X)$, причем по лемме Гаусса многочлен g будет иметь целые коэффициенты. Из последнего равенства получаем:

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

где $\psi(X) = \varepsilon(X)g(X)\eta^{-1}(X) \in \mathfrak{o}[[X]]$. Лемма доказана.

Докажем теперь несколько равенств. Во-первых, нетрудно видеть, что имеет место следующее равенство:

$$u_{n+1}(X) = q(X)s(X) + p, \tag{15}$$

где

$$q(X) = (p-1) + (p-2)(z+1)^{p^n} + \ldots + 2(z+1)^{(p-3)p^n} + \\ + (z+1)^{(p-2)p^n} \in \mathfrak{o}[[X]].$$

Во-вторых, согласно лемме 1, § 1, п. 1,

$$s - s_{n-1}^{\Delta} = z^{p^n} - z^{p^{n-1}\Delta} \equiv 0 \bmod p^n,$$

откуда получаем:

$$s = s_{n-1}^{\Delta} + p^n h, \tag{16}$$

где $h \in \mathfrak{o}_0[[X]]$. Из (16) следует равенство $s^{-1} = s_{n-1}^{-\Delta}(1 - p^n h s^{-1})$, причем ряды s^{-1}, $s_{n-1}^{-\Delta}$ имеют целые коэффициенты из кольца $\mathfrak{o}$ (см. (13), п. 1). Поэтому отсюда получаем:

$$s_{n-1}^{-\Delta} = s^{-1} + p^n h s^{-2} + p^{2n} h^2 s^{-3} + \ldots . \tag{17}$$

Далее, по определению ряда $u(X)$ имеем:

$$s_{n-1}^{-\Delta}=u^{\Delta}s^{-\Delta}. \tag{18}$$

Докажем, наконец, для любого $r\geqslant 0$ сравнение

$$u^{p^r\Delta}\equiv u_{n+1}^{p^r}+p^{n+r}u_{n+1}^{p^r-1}z_0^{p^n(p-2)}h \bmod p^{n+r+1}, \tag{19}$$

где h взят из (16). Действительно, пусть сперва $r=0$, тогда из определения ряда s получим, что $s=(1+s_{n-1})^p-1$, и, следовательно,

$$u=\frac{s}{s_{n-1}}=p+C_p^2 s_{n-1}+\ldots+C_p^{p-1}s_{n-1}^{p-2}+s_{n-1}^{p-1}.$$

Тогда

$$u^{\Delta}-u_{n+1}=C_p^2(s_{n-1}^{\Delta}-s)+\ldots+C_p^{p-1}(s_{n-1}^{\Delta(p-2)}-s^{p-2})+(s_{n-1}^{\Delta(p-1)}-s^{p-1}). \tag{20}$$

Из (16) следует, что все члены в этом равенстве, кроме последнего, делятся на p^{n+1}. Последнюю разность, используя (16), можно записать в виде:

$$s_{n-1}^{\Delta(p-1)}-s^{(p-1)}=-C_{p-1}^1 s^{p-2}(p^n h)+C_{p-1}^2 s^{p-3}(p^n h)^2-\ldots+(p^n h)^{p-1}. \tag{21}$$

В правой части этого равенства все члены, начиная со второго, делятся на p^{n+1} при $p\neq 2$. Для первого слагаемого из определения ряда получаем:

$$s^{p-2}=((1+z_0)^{p^n}-1)^{p-2}\equiv -p^n z_0^{p^n(p-2)}h \bmod p^{n+1},$$

откуда

$$C_{p-1}^1 s^{p-2}p^n h\equiv -p^n z_0^{p^n(p-2)}h \bmod p^{n+1},$$

и тогда из (21) получим:

$$s_{n-1}^{\Delta(p-1)}-s^{p-1}\equiv p^n z_0^{p^n(p-2)}h \bmod p^{n+1}.$$

Последнее сравнение вместе с (20) дает нам требуемое сравнение (19) при $r=0$. В общем случае сравнение (19) доказывается несложной индукцией по r.

ЛЕММА 7. *Для любого $m\geqslant 1$ имеет место сравнение*

$$\frac{u^{m\Delta}}{pm}(1-p\Delta)(s^{-1})\equiv 0 \bmod (p^n, \deg 0). \tag{22}$$

Доказательство. Пусть сперва $m=p^r$. Из равенства (15) следует при $i\geqslant 1$, что

$$u_{n+1}^i s^{-1}\equiv p^i s^{-1} \bmod \deg 0,$$

так как для любого $j\geqslant 1$ ряд $(qs)^j s^{-1}$ будет степенным рядом. Отсюда и из (19) получаем:

$$\frac{u^{p^r\Delta}}{p^{r+1}}s^{-1}\equiv\left(\frac{u_{n+1}^{p^r}}{p^{r+1}}+p^{n-1}u_{n+1}^{p^r-1}z_0^{p^n(p-2)}h\right)s^{-1}\equiv$$

$$\equiv p^{p^r-r-1}s^{-1}+p^{n-1}u_{n+1}^{p^r-1}z_0^{p^n(p-2)}hs^{-1} \bmod (p^n, \deg 0). \tag{23}$$

Из (13), п. 1, получим $s^{-1} \equiv z_0^{-p^n} \bmod p$, откуда следует:

$$p^{n-1} z_0^{p^n(p-2)} h s^{-1} \equiv p^{n-1} z_0^{p^n(p-3)} h \bmod p^n. \tag{24}$$

Ряд $z_0^{p^n(p-3)}$ при $p \neq 2$ является степенным рядом с целыми коэффициентами, поэтому $z_0^{p^n(p-3)} h \equiv 0 \bmod \deg 0$. Отсюда и из (24) следует сравнение

$$p^{n-1} z_0^{p^n(p-2)} h s^{-1} \equiv 0 \bmod (p^n, \deg 0).$$

Тогда сравнение (23) примет вид:

$$\frac{u^{p^r \Delta}}{p^{r+1}} s^{-1} \equiv p^{p^r - r - 1} s^{-1} \bmod (p^n, \deg 0). \tag{25}$$

Если $r=0$, то из (18) и (17) следует сравнение

$$\frac{u^{p^r \Delta}}{p^r} s^{-\Delta} = u^{\Delta} s^{-\Delta} = s_{n-1}^{-\Delta} \equiv s^{-1} \bmod p^n.$$

Отсюда и из (25) получаем сравнение леммы в этом случае.

Если $r \geqslant 1$, то, во-первых, из (15) следует:

$$\frac{u_{n+1}^{p^r - 1}}{p^r} = p^{p^r - r - 1} + a_1 (qs) + a_2 (qs)^2 + \ldots + a_{p^r - 1} (qs)^{p^r - 1}, \tag{26}$$

где через a_i обозначено число $C^i_{p^r-1} p^{p^r - r - i - 1}$, а во-вторых, из (18), (17), (19) и (26) найдем:

$$\frac{u^{p^r \Delta}}{p^r} s^{-\Delta} = \frac{u^{(p^r-1)\Delta}}{p^r} u^{\Delta} s^{-\Delta} = \frac{u^{(p^r-1)\Delta}}{p^r} s_{n-1}^{-\Delta} =$$

$$= \frac{u^{(p^r-1)\Delta}}{p^r} \sum_{i=0}^{\infty} p^{ni} h^i s^{-i-1} \equiv \frac{u_{n+1}^{p^r-1}}{p^r} \sum_{i=0}^{\infty} p^{ni} h^i s^{-i-1} =$$

$$= (p^{p^r - r - 1} + a_1 (qs) + \ldots + a_{p^r-1} (qs)^{p^r-1}) (s^{-1} + p^n h s^{-2} + \ldots) \bmod p^n. \tag{27}$$

В этом сравнении имеем:

$$p^{p^r - r - 1} (s^{-1} + p^n h s^{-2} + \ldots) \equiv p^{p^r - r - 1} s^{-1} \bmod p^n. \tag{28а}$$

Далее, если $i \geqslant j$, то $(qs)^i h^{j-1} s^{-j} = q^i h^{j-1} s^{i-j}$ — степенной ряд, значит,

$$a_i (qs)^i (p^{(j-1)n} h^{j-1} s^{-j}) \equiv 0 \bmod \deg 0. \tag{28б}$$

Если же $1 \leqslant i < j$, то $p^r - r - i - 1 + (j-1)n \geqslant p^r - r - i - 1 + in = p^r - r - 2 + (i-1)(n-1) + n \geqslant n$ при $r \geqslant 1$, $p \neq 2$. Значит,

$$a_i (qs)^i (p^{(j-1)n} h^{j-1} s^{-j}) = C^j_{p^r-1} p^{p^r - r - i - 1 + (j-1)n} (qs)^i h^{j-1} s^{-j} \equiv 0 \bmod p^n, \tag{28в}$$

так как ряды q, s и h имеют целые коэффициенты.

Из сравнения (27), используя (28а—в), получим:

$$\frac{u^{p^r\Delta}}{p^r}\mathfrak{s}^{-\Delta} \equiv p^{p^r-r-1}\mathfrak{s}^{-1} \bmod (p^n, \deg 0).$$

Последнее сравнение вместе с (25) дает нам требуемое сравнение леммы при $m=p^r$, $r\geqslant 1$.

Пусть теперь $m=m'p^r$, где $(m', p)=1$. По только что доказанному имеем:

$$\frac{u^{p^r\Delta}}{p^{r+1}}(1-p\Delta)(\mathfrak{s}^{-1}) \equiv 0 \bmod (p^n, \deg 0). \tag{29}$$

Ряд $u^{(m'-1)p^r\Delta}/m'$ является степенным рядом с целыми коэффициентами, поэтому, умножая на него обе части сравнения (29), получим в общем случае сравнение леммы. Лемма полностью доказана.

3. Докажем теперь основной результат этого параграфа — независимость спаривания $\langle\alpha, \beta\rangle_\pi$ от способа разложения элементов α и β в ряды по π. Пусть главная единица ε двумя способами представлена в виде степенного ряда по простому элементу $\pi: \varepsilon=1+c_1\pi+c_2\pi^2+\ldots=$ $=1+d_1\pi+d_2\pi^2+\ldots$, где c_i, $d_j\in\mathfrak{o}$. Обозначим ряд $1+c_1X+\ldots$ через $\varepsilon_1(X)$, а ряд $1+d_1X+\ldots$ — через $\varepsilon_2(X)$. Пусть через $\langle\pi, \varepsilon\rangle^{(1)}$ обозначено спаривание (12), п. 1, полученное с помощью первого разложения единицы ε, а через $\langle\pi, \varepsilon\rangle^{(2)}$ — с помощью второго.

Предложение 5. *Спаривание* (12) *на паре* π, ε *не зависит от способа представления главной единицы* ε *в степенной ряд по* π, *т. е.* $\langle\pi, \varepsilon\rangle^{(1)}=\langle\pi, \varepsilon\rangle^{(2)}$.

Доказательство. Пусть $\eta(X)=\varepsilon_1(X)\varepsilon_2^{-1}(X)$. Чтобы доказать утверждение предложения, нам достаточно проверить в силу билинейности спаривания, что

$$\operatorname{tr}[X, \eta(X)] \equiv 0 \bmod p^n. \tag{30}$$

По определению (см. (5), § 2, п. 1) имеем:

$$[X, \eta(X)] = \operatorname{res}_X X^{-1}\mathfrak{s}^{-1}\left(1-\frac{\Delta}{p}\right)\log\eta(X). \tag{31}$$

Заметим, далее, что так как $\eta(\pi)=\varepsilon_1(\pi)\varepsilon_2^{-1}(\pi)=1$, то по лемме 6

$$\eta(X) = 1+u(X)\psi(X). \tag{31a}$$

Пусть теперь $\varphi(X)$ — произвольный ряд из $\mathfrak{o}_0[[X]]$, и пусть γ_0 — свободный член ряда $\frac{u^m\varphi}{m}\mathfrak{s}^{-1}$, а γ_1 — свободный член ряда $\frac{u^{m\Delta}}{pm}\varphi^\Delta\mathfrak{s}^{-1}$. Тогда из сравнения (22) леммы 7, умножая обе его части на φ^Δ, получим, в частности, сравнение

$$\gamma_0^\Delta \equiv \gamma_1 \bmod p^n,$$

откуда, во всяком случае, следует сравнение

$$\operatorname{tr}\gamma_0^\Delta \equiv \operatorname{tr}\gamma_1 \bmod p^n.$$

Но так так $\operatorname{tr}\gamma_0^\Delta=\operatorname{tr}\gamma_0$, то получим: $\operatorname{tr}(\gamma_0-\gamma_1)\equiv 0 \bmod p^n$. Последнее сравнение означает, что след свободного члена ряда $s^{-1}\left(1-\frac{\Delta}{p}\right)\left(\frac{u^m\varphi}{m}\right)$ делится на p^n, или, что то же самое,

$$\operatorname{tr}\operatorname{res}_X X^{-1}s^{-1}\left(1-\frac{\Delta}{p}\right)\left(\frac{u^m\varphi}{m}\right)\equiv 0 \bmod p^n.$$

Поэтому, полагая φ равным $(-1)^{m-1}\psi^m$, где ψ взят из (31а), получим:

$$\sum_{m=1}^{\infty}\operatorname{tr}\operatorname{res}_X X^{-1}s^{-1}\left(1-\frac{\Delta}{p}\right)\frac{u^m(-1)^{m-1}\psi^m}{m}\equiv 0 \bmod p^n.$$

Отсюда и из (31) следует (30). Предложение доказано.

Замечание 6. Несложно проверить независимость спаривания от способа разложения в ряд по π и в общем случае, но в дальнейшем нам это не потребуется.

§ 4. Примарные элементы

В этом параграфе строятся p^n-примарные элементы поля k, которые играют важную роль в задании символа Гильберта. Напомним, что элемент $\omega\in k$ называется p^n-примарным, если расширение $k(\sqrt[p^n]{\omega})/k$ неразветвлено. Впервые такие элементы были построены X. Хассе в работе ([3]), но в их конструкцию входят элементы, не принадлежащие основному полю k (см. ниже, лемма 8) и поэтому они не годятся для наших целей. В п. 3 примарные элементы будут получены иначе и они то и будут использоваться в дальнейшем.

1. Приведем в этом пункте построение примарного элемента Хассе, фактически не отличающееся от данного в работе ([3]), хотя вид этого элемента будет несколько иной.

Пусть $z(X)$ — степенной ряд, полученный из разложения корня ζ по π (см. введение, п. 2). Пусть, далее, $a\in\mathfrak{o}$ и A — элемент максимального неразветвленного расширения над T, который удовлетворяет равенству

$$\mathrm{A}^\Delta-\mathrm{A}=a \tag{32}$$

(продолжение автоморфизма Фробениуса Δ поля T на максимальное неразветвленное расширение обозначено здесь той же буквой Δ).

ЛЕММА 8. *Элемент* $H(a)=E(p^n\mathrm{A}^\Delta l(z))\,|_{X=\pi}$ *является* p^n*-примарным и при этом* $(\pi, H(a))=\zeta^{\operatorname{tr} a}$ (см. ([3]), стр. 183).

Доказательство. Пусть $\delta=\Delta^f$, где f — абсолютная степень инерции поля k. Из (32) следует, что $\mathrm{A}^{\Delta\delta}=\mathrm{A}^\Delta+\operatorname{tr} a$. Поэтому из мультипликативности функции E получаем:

$$E\,(\mathrm{A}^\Delta l\,(z))^{\delta-1}=E\,((\mathrm{A}^{\Delta\delta}-\mathrm{A}^\Delta)\,l\,(z))=E\,(l\,(z))^{\operatorname{tr} a}=z^{\operatorname{tr} a}$$

(мы использовали еще лемму 4, § 1, п. 2). Отсюда, с одной стороны,

$$H(a)^{\delta-1} = (E(p^n \mathrm{A}^\Delta l(z))|_{X=\pi})^{\delta-1} = z(\pi)^{p^n \operatorname{tr} a} = \zeta^{p^n \operatorname{tr} a} = 1,$$

значит, $H(a) \in k$. А с другой стороны,

$$\sqrt[p^n]{H(a)}^{\delta-1} = (E(\mathrm{A}^\Delta l(z))|_{X=\pi})^{\delta-1} = \zeta^{\operatorname{tr} a},$$

откуда следует $(\pi, H(a)) = \zeta^{\operatorname{tr} a}$. Лемма доказана.

2. Построим теперь иначе примарные элементы.

ЛЕММА 9. *Элемент* $\xi(a) = E(p^n a \log z)|_{X=\pi}$ *является* p^n-*примарным и* $(\pi, \xi(a)) = \zeta^{\operatorname{tr} a}$.

Доказательство. В максимальном неразветвленном над k расширении имеет место равенство

$$E(p^n \mathrm{A}^\Delta l(z)) = E(p^n a \log z) \exp p^n \mathrm{A} \log z. \tag{33}$$

Действительно, из определения функции E (см. (3), § 1, п. 2) получим:

$$E\left(p^n \left(1 - \frac{\Delta}{p}\right) \mathrm{A} \log z\right) = \exp p^n \mathrm{A} \log z.$$

С другой стороны, учитывая (32), имеем:

$$\left(1 - \frac{\Delta}{p}\right)(\mathrm{A} \log z) = \mathrm{A}^\Delta l(z) - a \log z.$$

Отсюда и из мультипликативности E следует (33).

Нетрудно видеть, что $\exp(p^n \mathrm{A} \log z(X))$ определен для любого элемента из идеала $\mathfrak{p}$ поля k, в частности, и для $X = \pi$. В этом случае мы получаем $\log(z(\pi)) = \log \zeta = 1$, значит, $\exp(p^n \mathrm{A} \log z(\pi)) = 1$, откуда

$$E(p^n \mathrm{A}^\Delta l(z))|_{X=\pi} = E(p^n a \log z)|_{X=\pi}.$$

Из этого равенства и леммы 8, п. 1, получаем наше утверждение.

Пусть теперь $\varphi(X)$ — степенной ряд без свободного члена с коэффициентами из $\mathfrak{o}$, т. е. $\varphi \in \mathfrak{o}_0[[X]]$, тогда ряд $\psi = (1 + \Delta + \Delta^2 + \ldots)(\varphi)$ тоже будет рядом из $\mathfrak{o}_0[[X]]$; при этом

$$\psi^\Delta - \psi = \varphi.$$

Отсюда, так же как в лемме 9, можно получить равенство

$$E(p^n \psi^\Delta l(z)) = E(p^n \varphi \log z) \exp(p^n \varphi \log z).$$

В этом равенстве, подставляя вместо X простой элемент π, получим:

$$\exp(p^n \varphi \log z(\pi)) = 1,$$

откуда следует равенство

$$E(p^n \psi^\Delta l(z))|_{X=\pi} = E(p^n \varphi \log z)|_{X=\pi}. \tag{34}$$

ЛЕММА 10. *Пусть* $\varphi(X)\in\mathfrak{o}_0[[X]]$, *тогда элемент*

$$E(p^n\varphi\log z)\big|_{X=\pi} \tag{35}$$

является p^n*-ой степенью; если при этом* $\deg\varphi\geqslant pe_1$, *то элемент* (35) *будет* p^{n+1}*-ой степенью в поле* k.

Доказательство. Ряд $\psi^\Delta(X)\in\mathfrak{o}_0[[X]]$, значит, в поле k имеет место равенство

$$E(p^n\psi^\Delta l(z))\big|_{X=\pi}=(E(\psi^\Delta l(z))\big|_{X=\pi})^{p^n}.$$

Отсюда и из (34) вытекает первое утверждение леммы. Если, далее, $\deg\varphi\geqslant pe_1$, то $\deg\psi^\Delta\geqslant pe_1$, значит, элемент $E(\psi^\Delta l(z)/p)$ будет однозначно определен на простом идеале $\mathfrak{p}$ поля k и поэтому

$$E(p^n\varphi\log z)\big|_{X=\pi}=\left(E\left(\frac{\psi^\Delta l(z)}{p}\right)\bigg|_{X=\pi}\right)^{p^{n+1}}.$$

Лемма доказана.

3. В этом пункте мы получим из результатов предыдущих двух пунктов примарный элемент $\omega(a)$, который будет использован в дальнейшем. Обозначим ряд $z(X)^{p^n}-1$ через $s(X)$.

Предложение 6. *Элемент* $\omega(a)=E(a(z^{p^n}-1))\big|_{X=\pi}$, *где* $a\in\mathfrak{o}$, *является* p^n*-примарным и при этом*

$$(\pi,\omega(a))=\zeta^{\operatorname{tr}a}.$$

Доказательство. Из очевидного равенства $p^n\log z=\log(1+s)$ получаем:

$$E(p^na\log z)=E(as)\prod_{m=2}^{\infty}E\left(\frac{as^m}{m}\right)^{(-1)^{m-1}}.$$

Мы проверим сейчас, что для $m\geqslant2$ элемент $E\left(\frac{as^m}{m}\right)\Big|_{X=\pi}$ является p^n-ой степенью. Это дает нам, учитывая лемму 9, п. 2, утверждение нашего предложения.

По определению функции E имеем:

$$E\left(\frac{as^m}{m}\right)=\prod_{i=0}^{\infty}\exp\frac{(as^m)^{\Delta^i}}{mp^i}.$$

Нетрудно видеть, что $\exp(as^m/m)$ определен однозначно на простом идеале $\mathfrak{p}$ поля k. Поэтому из равенства $s(\pi)=\zeta^{p^n}-1=0$ будет следовать, что $\exp(as^m(\pi)/m)=1$ и поэтому элемент $E\left(\frac{as^m}{m}\right)\Big|_{X=\pi}$ будет p^n-ой степенью, если мы покажем, что для любого $i\geqslant1$, $m\geqslant2$ элемент

$$\varepsilon_i=\exp\frac{(as^m)^{\Delta^i}}{mp^i}\bigg|_{X=\pi}$$

является p^n-ой степенью.

Пусть $s_{n+1}(X)=z^{p^{n+1}}-1$. Ясно, что $s_{n+1}(\pi)=0$, поэтому из сравнения

$$s^{\Delta}(X)-s_{n+1}(X)=z^{p^n\Delta}-z^{p^{n+1}}\equiv 0 \bmod p^{n+1}$$

(см. лемму 1, § 1, п. 1) следует, что элемент $s^{\Delta}(\pi)$ делится на p^{n+1}, значит,

$$\nu(s^{m\Delta}(\pi))\geqslant m(n+1)e. \tag{36}$$

Применяя еще грубую оценку $\nu(m)\leqslant(m-1)e$, получаем тогда при $m\geqslant 2$:

$$\nu\left(\frac{a^{\Delta}s^{m\Delta}(\pi)}{mp^{n+1}}\right)\geqslant\nu(s^{m\Delta}(\pi))-\nu(m)-(n+1)e\geqslant(m-1)ne>e_1.$$

Следовательно, однозначно определен элемент

$$\exp\left(\frac{a^{\Delta}s^{m\Delta}}{mp^{n+1}}\right)\Bigg|_{X=\pi},$$

p^n-ая степень которого и будет давать ε_1.

Из (36) следует, во всяком случае, что $\nu(s^{m\Delta}(\pi))>e_1$, а тогда порядок элемента

$$c_i=\frac{\Delta^i(as^m(X))}{mp^i}\Bigg|_{X=\pi}$$

будет возрастающей функцией от i при фиксированном m. Действительно,

$$\nu(c_{i+1})-\nu(c_i)\geqslant(p^i-p^{i-1})\nu(s^{m\Delta}(\pi))-e>p^{i-1}(p-1)e_1-e=$$
$$=(p^{i-1}-1)e\geqslant 0.$$

Поэтому из доказанного выше следует, что однозначно определен элемент

$$\exp\frac{(as^m)^{\Delta^i}}{mp^{n+i}}\Bigg|_{X=\pi},$$

p^n-ая степень которого и будет давать ε_i, $i\geqslant 1$. Предложение доказано.

Точно таким же способом, используя при этом лемму 10, п. 2, проверяется следующая

ЛЕММА 11. *Пусть* $\varphi(X)\in\mathfrak{o}_0[[X]]$, *тогда элемент*

$$E(\varphi(X)(z^{p^n}-1))|_{X=\pi} \tag{37}$$

является p^n*-ой степенью; если при этом* $\deg\varphi\geqslant pe_1$, *то элемент* (37) *будет* p^{n+1}*-ой степенью в поле* k.

§ 5. Символ Гильберта (π, ε)

В этом параграфе мы займемся вычислением символа Гильберта для пары π, ε, где ε — некоторая главная единица локального поля k. Вначале мы установим существование ряда $V(X)=v_1X^{-1}+v_2X^{-2}+\dots$, однозначно задаваемого по $\operatorname{mod} p^n$ выбором простого элемента π и корня ζ, с помощью которого можно в явном виде вычислить символ Гильберта (π, ε) (см. ниже предложение 7). Затем найдем рекуррентные соотношения для ряда $V(X)$ (см. п. п. 3, 4) и, наконец, из этих соотношений получим формулу для ряда $V(X)$ (см. теорему 2, п. 5), что дает нам символ Гильберта (π, ε) (см. теорему 3, п. 5).

1. Докажем следующую лемму, с помощью которой и будет определяться ряд $V(X)$.

ЛЕММА 12. *Для каждого натурального m существует элемент v_m кольца $\mathfrak{o}$, обладающий следующими свойствами:*

а) *для всех β из $\mathfrak{o}$, если $m \leqslant pe_1$, и для всех β из $p^{-1}\mathfrak{o}$, если $m > pe_1$, имеет место равенство*

$$(\pi, E(\beta\pi^m)) = \zeta^{\operatorname{tr} \beta v_m}; \tag{38}$$

б) *равенство* (38) *определяет элемент v_m однозначно либо по* $\operatorname{mod} p^n$, *если $m \leqslant pe_1$, либо по* $\operatorname{mod} p^{n+1}$, *если $m > pe_1$*;

в) *если $(m, p) = 1$, то $v_m \equiv 0 \operatorname{mod} p^n$; если $m > pe_1$, то $v_m \equiv 0 \operatorname{mod} p$.*

Доказательство. Докажем сперва существование элемента v_m для $m \leqslant pe_1$, удовлетворяющего условию а). Возьмем в кольце $\mathfrak{o}$ два двойственных друг другу относительно оператора следа базиса над $\mathbf{Z}_p$. Пусть это будут $\alpha_1, \ldots, \alpha_f$ и $\alpha_1', \ldots, \alpha_f'$ (здесь f — абсолютная степень инерции поля k), тогда

$$\operatorname{tr} \alpha_i\alpha_j' = \delta_{ij}.$$

Пусть

$$(\pi, E(\alpha_i\pi^m)) = \zeta^{x_i}, \quad x_i \in \mathbf{Z}_p.$$

Рассмотрим элемент $v_m = \sum_{i=1}^{f} x_i\alpha_i'$. Тогда если $\beta = y_1\alpha_1 + \ldots + y_f\alpha_f$ — произвольный элемент из кольца $\mathfrak{o}$, $y_i \in \mathbf{Z}_p$, то, с одной стороны, из мультипликативности функции E будет следовать равенство

$$(\pi, E(\beta\pi^m)) = \zeta^{\gamma},$$

где $\gamma = x_1y_1 + x_2y_2 + \ldots + x_fy_f$, а с другой стороны, из двойственности базисов получаем:

$$\operatorname{tr} \beta v_m = \sum_{i,j} x_iy_j \operatorname{tr} \alpha_i\alpha_j' = \sum_{i=1}^{f} x_iy_i = \gamma,$$

и существование элемента v_m доказано.

Проверим теперь единственность найденного элемента по $\operatorname{mod} p^n$. Действительно, пусть w — другой элемент, удовлетворяющий нашему условию, тогда для всех $\beta \in \mathfrak{o}$ получим:

$$\operatorname{tr} \beta (v_m - w) \equiv 0 \operatorname{mod} p^n.$$

Отсюда и из невырожденности следа находим, что $v_m \equiv w \operatorname{mod} p^n$.

Пусть теперь $m > pe_1$. Тогда однозначно определен элемент $E(\beta\pi^m/p)$ при $\beta\in\mathfrak{o}$. Действительно, по определению

$$E\left(\frac{\beta\pi^m}{p}\right)=\prod_{i=0}^{\infty}\exp\left(\beta^{\Delta^i}\pi^{mp^i}/p^{i+1}\right),$$

при этом порядок элемента $\beta^{\Delta^i}\pi^{mp^i}/p^{i+1}$ не меньше чем $mp^i-(i+1)e$ и, значит, больше чем e_1. Поэтому для любого $i\geqslant 0$ однозначно определен элемент $\exp(\beta^{\Delta^i}\pi^{mp^i}/p^{i+1})$ (см. [7], стр. 323), а тем самым и $E(\beta\pi^m/p)$.

Точно так же как и выше, можно найти такой элемент $v'\in\mathfrak{o}$, однозначно определенный по $\operatorname{mod} p^n$, что для всех $\beta'\in\mathfrak{o}$ имеет место равенство

$$\left(\pi,\ E\left(\frac{\beta'\pi^m}{p}\right)\right)=\zeta^{\operatorname{tr}\beta'v'}.$$

Рассмотрим теперь элемент $v_m=pv'$, тогда для любого $\beta\in p^{-1}\mathfrak{o}$ имеем

$$(\pi,\ E(\beta\pi^m))=\left(\pi,\ E\left(\frac{\beta'\pi^m}{p}\right)\right)=\zeta^{\operatorname{tr}\beta'v'}=\zeta^{\operatorname{tr}\beta v_m},\tag{39}$$

где $\beta'=p\beta$, и существование элемента v_m в этом случае доказано.

Пусть теперь w — другой элемент, удовлетворяющий (39), тогда $\operatorname{tr}\beta(v_m-w)\equiv 0 \operatorname{mod} p^n$ при всех $\beta\in p^{-1}\mathfrak{o}$, откуда следует для всех $\beta'\in\mathfrak{o}$ сравнение

$$\operatorname{tr}\beta'(v_m-w)\equiv 0 \operatorname{mod} p^{n+1}.$$

Из невырожденности следа отсюда получаем, что $v_m\equiv w \operatorname{mod} p^{n+1}$. Заметим при этом, что v_m в нашем случае делится на p по построению. Нам осталось проверить, что $v_m\equiv 0 \operatorname{mod} p^n$, если $(m, p)=1$ (относительно этого утверждения см. также [5], стр. 128). Для $\theta\in\mathfrak{R}$ имеем следующее разложение (см. (2), § 1, п. 2):

$$E(\theta\pi^m)=\prod_{(i,p)=1}\left(1-(\theta\pi^m)^i\right)^{-\frac{\mu(i)}{i}}.$$

Далее, легко видеть, что если $\theta\in\mathfrak{R}$ и $(m, p)=(i, p)=1$, то

$$(\pi,\ 1-(\theta\pi^m)^i)=\left((\theta\pi^m)^i,\ 1-(\theta\pi^m)^i\right)^{\frac{1}{mi}}=1.$$

Из этих двух равенств и мультипликативности функции E получаем для всех $\beta\in\mathfrak{o}$:

$$(\pi,\ E(\beta\pi^m))=1.$$

Отсюда и из единственности элемента v_m по $\operatorname{mod} p^n$ следует сравнение $v_m\equiv 0 \operatorname{mod} p^n$, если $(m, p)=1$. Лемма доказана.

Рассмотрим ряд $V(X)=v_1X^{-1}+v_2X^{-2}+\ldots$, коэффициенты которого задаются леммой 12 (см. также [8], теорему 1). Тогда, согласно условию в) леммы, его можно представить в виде суммы двух рядов с целыми коэффициентами следующим образом:

$$V(X) = V_1(X) + pV_2(X),$$

где

$$V_1(X) = v_p X^{-p} + v_{2p} X^{-2p} + \ldots + v_{pe_1} X^{-pe_1},$$

$$V_2(X) = \frac{v_{pe_1+1}}{p} X^{-pe_1-1} + \frac{v_{pe_1+2}}{p} X^{-pe_1-2} + \ldots;$$

при этом, согласно условию б), коэффициенты рядов V_1 и V_2 заданы однозначно по $\operatorname{mod} p^n$.

Основная роль ряда $V(X)$ определяется следующим утверждением.

Предложение 7. *Пусть $\varepsilon(X)$ — ряд, полученный из разложения главной единицы ε поля k в ряд по простому элементу π и*

$$l(\varepsilon) = \left(1 - \frac{\Delta}{p}\right) \log \varepsilon(X).$$

Тогда $(\pi, \varepsilon) = \zeta^{\operatorname{tr} \gamma}$, *где* $\gamma = \operatorname{res}_X X^{-1} l(\varepsilon) V(X)$.

Доказательство. Согласно лемме 4, § 1, п. 2, имеем:

$$\varepsilon = E(l(\varepsilon))|_{X=\pi}.$$

Если теперь $l(\varepsilon) = a_1 X + a_2 X^2 + \ldots$, $a_i \in \mathfrak{o}$, то из мультипликативности функции E и определения ряда $V(X)$ получим:

$$(\pi, \varepsilon) = \prod_{m=1}^{\infty} (\pi, E(a_m \pi^m)) = \prod_m \zeta^{\operatorname{tr} a_m v_m} = \zeta^{\gamma},$$

где $\gamma = \sum_m a_m v_m$. Эта сумма $\sum_m a_m v_m$ и определяет $\operatorname{res}_X X^{-1} l(\varepsilon) V(X)$, что доказывает наше предложение (см. также предложение 1 из ([9])).

Замечание 7. *Результат предложения не зависит от способа разложения единицы ε в ряд по простому элементу π.*

Замечание 8. *Все коэффициенты ряда $V(X)$ достаточно в нашем предложении знать лишь по* $\operatorname{mod} p^n$.

Нашей основной задачей теперь будет вычисление ряда $V(X)$ по $\operatorname{mod} p^n$.

2. Установим несколько фактов, уточняющих свойства ряда $V(X)$.

ЛЕММА 13. *Пусть $\varphi(X) = \varphi_1(X) + \frac{\varphi_2(X)}{p}$, причем $\varphi_1, \varphi_2 \in \mathfrak{o}[[X]]$ и $\deg \varphi_2 \geqslant pe_1$. Тогда*

$$(\pi, E(X\varphi(X))|_{X=\pi}) = \zeta^{\operatorname{tr} \gamma},$$

где $\gamma = \operatorname{res}_X \varphi(X) V(X)$.

Доказательство. Из определения ряда $V(X)$, мультипликативности функции E и того, что $\deg \varphi_2 \geqslant pe_1$, так же как и в предложении 7, получаем:

$$\left(\pi, E\left(\frac{X\varphi_2(X)}{p}\right)\bigg|_{X=\pi}\right) = \zeta^{\operatorname{tr} \gamma_2},$$

где $\gamma_2 = \mathrm{res}_X\, \varphi_2(X)\, V_2(X)$. Очевидно, что $\mathrm{res}_X \frac{\varphi_2(X)}{p} V_1(X) = 0$, поэтому

$$\gamma_2 = \mathrm{res}_X \frac{\varphi_2(X)}{p} V_1(X) + \mathrm{res}_X\, \varphi_2(X)\, V_2(X) = \mathrm{res}_X \frac{\varphi_2(X)}{p} V(X).$$

Далее, из предложения 7 следует, что

$$(\pi,\ E(X\varphi_1(X))\,|_{X=\pi}) = \zeta^{\mathrm{tr}\,\gamma_1},$$

где $\gamma_1 = \mathrm{res}_X\, \varphi_1(X)\, V(X)$. Значит,

$$(\pi,\ E(X\varphi(X))\,|_{X=\pi}) = \zeta^{\mathrm{tr}\,\gamma},$$

где $\gamma = \gamma_1 + \gamma_2 = \mathrm{res}_X\, \varphi(X)\, V(X)$, и лемма доказана.

ЛЕММА 14. *Пусть, как и в предыдущей лемме,* $\varphi(X) = \varphi_1(X) + \frac{\varphi_2(X)}{p}$, $\varphi_1, \varphi_2 \in \mathfrak{o}[[X]]$, $\deg \varphi_2 \geqslant pe_1$. *Если элемент* $\varepsilon = E(\beta X\varphi(X))\,|_{X=\pi}$ *является* p^n*-ой степенью в поле* k *для всех* $\beta \in \mathfrak{o}$, *то*

$$\mathrm{res}_X\, \varphi(X)\, V(X) \equiv 0 \bmod p^n.$$

Доказательство. Так как единица ε является p^n-ой степенью, то $(\pi, \varepsilon) = 1$. С другой стороны, согласно лемме 13,

$$(\pi, \varepsilon) = \zeta^{\mathrm{tr}\,\beta\gamma},$$

где $\gamma = \mathrm{res}_X\, \varphi(X)\, V(X)$. Поэтому для всех $\beta \in \mathfrak{o}$ мы получаем сравнение

$$\mathrm{tr}\,\beta\gamma \equiv 0 \bmod p^n.$$

Отсюда и из невырожденности следа вытекает, что $\gamma = \mathrm{res}_X\, \varphi(X)\, V(X) \equiv 0 \bmod p^n$. Лемма доказана.

ЛЕММА 15. *Пусть* $\varphi(X) \in \mathfrak{o}[[X]]$ *и* $\deg \varphi \geqslant pe_1$. *Если элемент* $\varepsilon = E(\beta X\varphi(X))\,|_{X=\pi}$ *является* p^{n+1}*-ой степенью в поле* k *для всех* $\beta \in \mathfrak{o}$, *то*

$$\mathrm{res}_X\, \varphi(X)\, V(X) \equiv 0 \bmod p^{n+1}.$$

Доказательство. Так как $\deg \varphi \geqslant pe_1$, то однозначно определен элемент $\varepsilon' = E\left(\beta X \frac{\varphi(X)}{p}\right)\Big|_{X=\pi}$. Более того, из условия следует, что ε' является p^n-ой степенью в поле k, поэтому $(\pi, \varepsilon') = 1$. С другой стороны, согласно лемме 13,

$$(\pi, \varepsilon') = \zeta^{\mathrm{tr}\,\beta\gamma},$$

где $\gamma = \mathrm{res}_X \frac{\varphi(X)}{p} V(X)$. Поэтому, так же как и в лемме 14, получаем сравнение

$$\gamma = \mathrm{res}_X \frac{\varphi(X)}{p} V(X) \equiv 0 \bmod p^n,$$

откуда следует сравнение нашей леммы.

3. Найдем первое рекуррентное соотношение для ряда V. Прежде чем начать изложение, рассмотрим в кольце $\mathfrak{o}(X)$ всех формальных ря-

дов с коэффициентами из $\mathfrak{o}$ следующие обозначения. Пусть $h_1(X)$, $h_2(X)\in\mathfrak{o}(X)$. Тогда сравнение

$$h_1 \equiv h_2 \operatorname{mod}_* (p^r, \deg m)$$

будет означать, что сравнение

$$h_1 \equiv h_2 \operatorname{mod} (p^r, \deg m) \tag{40}$$

(см. введение, п. 2) выполняется лишь для степеней, делящихся на p, а сравнение

$$h_1 \equiv h_2 \operatorname{mod} ((p^r, \deg m); (p^s, \deg l))$$

будет обозначать сокращенную запись двух сравнений типа (40).

Из предложения 6, §4, п. 3, и предложения 7, п. 1, для всех $\beta\in\mathfrak{o}$ получаем сравнение

$$\operatorname{tr} \beta\gamma \equiv \operatorname{tr} \beta \operatorname{mod} p^n,$$

где $\gamma=\operatorname{res}_X X^{-1}s(X)\,V(X)$. Отсюда и из невырожденности следа получаем, что

$$\operatorname{res}_X X^{-1}s(X)\,V(X) \equiv 1 \operatorname{mod} p^n. \tag{41}$$

Далее, из леммы 11, §4, п. 3, и леммы 14, п. 2, получим, что для любого ряда $\varphi(X)\in\mathfrak{o}[[X]]$ имеет место сравнение

$$\operatorname{res}_X \varphi(X)\,s(X)\,V(X) \equiv 0 \operatorname{mod} p^n, \tag{42}$$

а если при этом $\deg\varphi\geqslant pe_1$, то из леммы 11, §4, п. 3, и леммы 15, п. 2, получим:

$$\operatorname{res}_X \varphi(X)\,s(X)\,V(X) \equiv 0 \operatorname{mod} p^{n+1}. \tag{43}$$

Воспользуемся произволом ряда $\varphi(X)$ и будем брать в качестве ряда $\varphi(X)$ степени $1, X, X^2, \ldots$ в (42) (в сравнении (43) степени $X^{pe_1}, X^{pe_1+1}, \ldots$). Тогда сравнения (42), (43) можно переписать в виде:

$$V(X)\,s(X) \equiv 0 \operatorname{mod} (p^n, \deg 0);\ (p^{n+1}, \deg(-pe_1)).$$

Объединяя последнее сравнение с (41), получаем первое рекуррентное соотношение для ряда $V(X)$:

$$V(X)\,s(X) \equiv 1 \operatorname{mod} (p^n, \deg 1);\ (p^{n+1}, \deg(-pe_1)),$$

означающее, что свободный член ряда Vs сравним с 1 по $\operatorname{mod} p^n$, все коэффициенты при отрицательных степенях делятся на p^n, а при степенях, меньших $(-pe_1)$, делятся на p^{n+1}.

4. Найдем теперь второе соотношение для ряда $V(X)$. Пусть, как и в §3, п. 2, ряд $z^{p^n}-1$ обозначен через $s(X)$, а ряд $s(X)/s_{n-1}(X)$ — через $u(X)$.

Предложение 8. *Для любого ряда* $\varphi(X)\in\mathfrak{o}_0[[X]]$ *и любого* $\beta\in\mathfrak{o}$ *имеет место равенство*

$$E\left(\left(1-\frac{\Delta}{p}\right)(\beta\varphi u)\right)\Big|_{X=\pi}=1.$$

Доказательство. Из определения функции E следует, что

$$E\left(\left(1-\frac{\Delta}{p}\right)(\beta\varphi u)\right)=\exp\beta\varphi(X)\,u(X).$$

Заметим при этом, что $\exp\beta\varphi u$ определен для всех элементов из идеала $\mathfrak{p}$, так как коэффициенты ряда $u(X)$ при степенях, меньших e, делятся на p (см. § 3, п. 2). Отсюда, учитывая, что $u(\pi)=0$, получаем:

$$E\left(\left(1-\frac{\Delta}{p}\right)(\beta\varphi u)\Big|_{X=\pi}=\exp\beta\varphi(\pi)\,u(\pi)=1.\right.$$

Предложение доказано.

Из доказанного предложения, используя лемму 14, п. 2, получаем сравнение

$$\operatorname{tr}\operatorname{res}_X X^{-1}V\left(1-\frac{\Delta}{p}\right)(\beta\varphi u)\equiv 0 \bmod p^n. \tag{44}$$

При этом мы действительно можем пользоваться леммой 14, так как в ряде $u(X)$, как сказано выше, все коэффициенты членов степеней, меньших e, делятся на p, значит, в ряде $\varphi^\Delta u^\Delta/p$ члены с нецелыми коэффициентами начинаются, по крайней мере, со степени pe, которая $\geqslant pe_1$; тем самым для ряда $\left(1-\frac{\Delta}{p}\right)(\varphi u)$ выполнены условия леммы 14.

ЛЕММА 16. *Пусть* γ_0, γ_1 — *такие элементы кольца* $\mathfrak{o}$, *что при всех* $\beta\in\mathfrak{o}$ *имеет место сравнение*

$$\operatorname{tr}(\beta\gamma_0+\beta^\Delta\gamma_1)\equiv 0 \bmod p^n,$$

тогда $\gamma_0^\Delta+\gamma_1\equiv 0 \bmod p^n$.

Доказательство. Из равенства $\operatorname{tr}\beta\gamma_0=\operatorname{tr}\beta^\Delta\gamma_0^\Delta$ получаем для всех $\beta\in\mathfrak{o}$:

$$\operatorname{tr}(\beta\gamma_0+\beta^\Delta\gamma_1)=\operatorname{tr}\beta^\Delta(\gamma_0^\Delta+\gamma_1).$$

Отсюда и из невырожденности следа вытекает утверждение леммы.

Сравнение (44) можно записать в виде

$$\operatorname{tr}\left(\beta\gamma_0-\beta^\Delta\frac{\gamma_1}{p}\right)\equiv 0 \bmod p^n,$$

где γ_0 — свободный член ряда $V\varphi u$, а γ_1 — свободный член ряда $V\varphi^\Delta u^\Delta$. Тогда из леммы 16 получим, что свободный член ряда

$$\varphi^\Delta u^\Delta V^\Delta-\frac{\varphi^\Delta u^\Delta}{p}V$$

делится на p^n. Воспользуемся произволом ряда $\varphi(X)$ и будем брать в качестве $\varphi(X)$ степени $X, X^2, \ldots$. Тогда последнее условие можно будет записать в виде следующего сравнения:

$$\frac{u^{\Delta}}{p}(1-p\Delta)(V) \equiv 0 \bmod_{*} (p^n, \deg 0)$$

(см. обозначения в п. 3).

5. В этом пункте мы проверим, что ряд $V(X)$, построенный в лемме 12, п. 1, сравним с рядом $s^{-1}(X)=(z^{p^n}-1)^{-1}$ по $\bmod p^n$ (относительно ряда s^{-1} см. (13), § 3, п. 1).

Рассмотрим систему сравнений

$$\begin{cases} s(X)\,Q(X) \equiv 1 \bmod (p^n, \deg 1);\ (p^{n+1}, \deg(-pe_1)), \\ \dfrac{u^{\Delta}(X)}{p}(1-p\Delta)(Q(X)) \equiv 0 \bmod_{*} (p^n, \deg 0), \end{cases} \tag{45}$$

где $Q(X)$ — некоторый формальный ряд из $\mathfrak{o}(X)$.

ЛЕММА 17. *К любому решению системы* (45) *можно добавлять или отбрасывать члены неотрицательных степеней.*

Доказательство. Пусть $h(X)$ — произвольный степенной ряд из $\mathfrak{o}[[X]]$. Тогда $\deg sh>0$, значит, $sh\equiv 0 \bmod \deg 1$ и тем более $sh\equiv 0 \bmod (p^n, \deg 1)$; $(p^{n+1}, \deg(-pe_1))$. Аналогично, $\deg (1-p\Delta)(h)\geqslant 0$, значит,

$$\frac{u^{\Delta}}{p}(1-p\Delta)(h) \equiv 0 \bmod \deg 0,$$

что дает нам второе сравнение системы. Лемма доказана.

Согласно доказанному в п. п. 3, 4, ряд $V(X)$, задаваемый леммой 12, п. 1, удовлетворяет системе (45). Далее, из леммы 7, § 3, п. 2, при $m=1$ следует, что и ряд $s^{-1}(X)$ удовлетворяет системе (45).

Нетрудно видеть, что коэффициенты ряда $s^{-1}(X)$, начиная с некоторого места, начинают делиться на сколь угодно большую степень числа p, в частности, на p^{n+1}. Коэффициенты ряда $V(X)$ тоже с некоторого места начинают делиться на p^{n+1}, а именно, с того номера m, для которого при всех $\beta\in\mathfrak{o}$ единица $E\left(\frac{\beta\pi^m}{p}\right)$ будет уже p^n-ой степенью (см. лемму 12, п. 1). Поэтому если мы рассмотрим ряд

$$R(X)=V(X)-s^{-1}(X)=\sum_i w_i X^{-i},$$

то найдется номер N такой, что $w_i\equiv 0 \bmod p^{n+1}$, если $i>N$. Далее, согласно лемме 17, можно считать, что $R(X)$ не имеет членов неотрицательных степеней, т. е.

$$R(X)\equiv w_1X^{-1}+w_2X^{-2}+\ldots+w_NX^{-N} \bmod p^{n+1}. \tag{46}$$

Из того, что $V(X)$ и $s^{-1}(X)$ удовлетворяют системе (45), следует, что $R(X)$ удовлетворяет системе

$$\begin{cases} s(X)\,R(X) \equiv 0 \bmod (p^n, \deg 1);\ (p^{n+1}, \deg(-pe_1)), \\ \dfrac{u^{\Delta}(X)}{p}(1-p\Delta)(R(X)) \equiv 0 \bmod_{*} (p^n, \deg 0). \end{cases} \tag{47}$$

Мы должны проверить теперь, что из (47) следует $R(X)\equiv 0 \bmod p^n$. Из сравнения

$$s(X)\equiv s_{n-1}^{\Delta}(X) \bmod p^n$$

следует, что все коэффициенты при степенях, взаимно простых с p, ряда $s(X)$, а значит, и ряда $s^{-1}(X)$ делятся на p^n. Далее, в лемме 12в) доказано, что $v_m\equiv 0 \bmod p^n$, если $(m, p)=1$. Отсюда следует, что и в ряде (46)

$$w_m\equiv 0 \bmod p^n, \quad (m, p)=1. \tag{48}$$

Далее, $s(X)\equiv z_0^{p^n} \bmod p$ (см. (13), § 3, п. 1) при этом порядок ряда z_0 равен $\dfrac{e}{p^{n-1}(p-1)}$, значит,

$$s(X)=pa_1X+\ldots+pa_{pe_1-1}X^{pe_1-1}+a_{pe_1}X^{pe_1}+a_{pe_1+1}X^{pe_1+1}+\ldots,$$

где a_{pe_1} — единица кольца $\mathfrak{o}$.

Если мы рассмотрим теперь в первом сравнении системы (47) коэффициенты при степенях $X^{-pe_1-1}, X^{-pe_1-2}, \ldots$, то получим следующую систему сравнений:

$$pa_1w_{i+1}+\ldots+pa_{pe_1-1}w_{i+pe_1-1}+a_{pe_1}w_{i+pe_1}+\ldots+a_{N-i}w_N\equiv 0 \bmod p^{n+1},$$
$$i=pe_1+1,\ pe_1+2,\ \ldots,\ N-pe_1.$$

Из этой системы можно однозначно по $\bmod p^{n+1}$ выразить коэффициенты $w_{2pe_1+1}, w_{2pe_1+2}, \ldots, w_N$ через $w_{pe_1+2}, \ldots, w_{2pe_1}$, а именно,

$$w_{2pe_1+i}\equiv \sum_{j=2}^{pe_1} p\alpha_{ij}w_{pe_1+j} \bmod p^{n+1}, \quad 1\leqslant i\leqslant N-2pe_1, \tag{49}$$

где α_{ij} однозначно определены по $\bmod p^n$.

Аналогично, рассмотрев коэффициенты при степенях $1, X^{-1}, \ldots, X^{-pe_1}$, получим следующую систему сравнений:

$$pa_1w_{i+1}+\ldots+pa_{pe_1-1}w_{i+pe_1-1}+a_{pe_1}w_{i+pe_1}+\ldots+a_{N-i}w_N\equiv 0 \bmod p^n,$$
$$i=0,\ 1,\ 2,\ \ldots,\ pe_1.$$

Из этой системы, подставив вместо w_{2pe_1+i} их выражения через w_{pe_1+j}, $1\leqslant j\leqslant pe_1$ (см. (49)), мы получим коэффициенты w_{pe_1+j}, выраженные через $w_1, w_2, \ldots, w_{pe_1}$, а именно,

$$w_{pe_1+j}\equiv \sum_{\rho=1}^{pe_1-1} p\beta_{j\rho}w_\rho \bmod p^n, \quad 0\leqslant j\leqslant pe_1, \tag{50}$$

где $\beta_{j\rho}$ однозначно определены по $\bmod p^{n-1}$. Наконец, подставив (50) в (49), получим:

$$w_{2pe_1+i}\equiv \sum_{\rho=1}^{pe_1-1} p^2\gamma_{i\rho}w_\rho \bmod p^{n+1}, \quad 1\leqslant i\leqslant N-2pe_1, \tag{51}$$

где $\gamma_{i\rho}$ однозначно определены по крайней мере по $\mathrm{mod}\, p^{n-1}$.

Прежде чем заняться вторым сравнением системы (47), сформулируем следующую несложную лемму.

ЛЕММА 18. *Система сравнений*

$$\sum_{j=1}^{m} c_{ij} x_j + p \sum_{j=1}^{m} d_{ij} x_j^{\Delta} \equiv 0 \bmod p^n, \qquad 1 \leqslant i \leqslant m,$$

имеет в кольце $\mathfrak{o}$ *единственное нулевое решение по* $\mathrm{mod}\, p^n$, *если* $\det (c_{ij})_{1 \leqslant i,\, j \leqslant m}$ *является единицей кольца* $\mathfrak{o}$.

Рассмотрим теперь второе сравнение системы (47). Согласно сделанному в § 3, п. 2, замечанию относительно ряда $u(X)$, мы можем ряд $u^{\Delta}(X)/p$ записать в виде

$$\frac{u^{\Delta}(X)}{p} = 1 + b_p X^p + \ldots + b_{pe-p} X^{pe-p} + \frac{b_{pe}}{p} X^{pe} + \frac{b_{pe+p}}{p} X^{pe+p} + \ldots,$$

где все коэффициенты b_i принадлежат кольцу $\mathfrak{o}$. Мы будем рассматривать коэффициенты при степенях $X^{-p}, X^{-2p}, \ldots, X^{-pe_1+p}$ во втором сравнении системы (47); коэффициент при X^{-p} в ряде $\frac{u^{\Delta}(X)}{p} R(X)$ имеет вид (см. (48))

$$w_p + b_p w_{2p} + \ldots + b_{pe_1-p} w_{pe_1} + \ldots + b_{pe-p} w_{pe} +$$
$$+ \frac{b_{pe}}{p} w_{pe+p} + \frac{b_{pe+p}}{p} w_{pe+2p} + \ldots .$$

Слагаемые $b_{pe_1-p} w_{pe_1}, b_{pe_1} w_{pe_1+p}, \ldots, b_{pe-p} w_{pe}$ можно с помощью (50) и (51) выразить в виде линейных комбинаций элементов $w_p, \ldots, w_{pe_1-p}$ с однозначно определенными по $\mathrm{mod}\, p^n$ коэффициентами, делящимися на p. Далее, если $p \neq 2$, то $pe + pi \geqslant pe + p > 2pe_1$, значит, элементы $\frac{b_{pe}}{p} w_{pe+p}, \frac{b_{pe+p}}{p} \times$ $\times\, w_{pe+2p}, \ldots$ выражаются через $w_p, w_{2p}, \ldots, w_{pe_1-p}$ с помощью формул (51) и поэтому они тоже будут линейными комбинациями элементов $w_p, w_{2p}, \ldots$ $\ldots, w_{pe_1-p}$ с однозначно определенными по $\mathrm{mod}\, p^n$ коэффициентами, делящимися на p. Отсюда следует, что коэффициент при X^{-p} в ряде $\frac{u^{\Delta}}{p} R$ можно представить в виде

$$c_{11} w_p + c_{12} w_{2p} + \ldots + c_{1,e_1-1} w_{pe_1-p};$$

при этом c_{11} — единица кольца $\mathfrak{o}$. Рассуждая точно так же, получим, что коэффициент при X^{-pi} в ряде $\frac{u^{\Delta}}{p} R$ представим по $\mathrm{mod}\, p^n$ в виде

$$pc_{i1} w_p + \ldots + pc_{i,i-1} w_{pi-p} + c_{ii} w_{pi} + \ldots + c_{i,e_1-1} w_{pe_1-p}, \qquad (52)$$

где c_{ii} — единица кольца $\mathfrak{o}$.

Рассматривая аналогично коэффициент при X^{-pi} в ряде $(-u^{\Delta}R^{\Delta})$, мы получим его в виде

$$p\sum_{j=1}^{e_1-1} d_{ij}w_{pj}^{\Delta}.$$

Поэтому из второго сравнения системы (47) получим следующую систему сравнений относительно $w_p, w_{2p}, \ldots, w_{pe_1-p}$:

$$pc_{i1}w_p + \ldots + pc_{ii-1}w_{pi-p} + c_{ii}w_{pi} + \ldots + c_{i,e_1-1}w_{pe_1-p} +$$
$$+p\sum_{j=1}^{e_1-1} d_{ij}w_{pj}^{\Delta} \equiv 0 \bmod p^n,$$
$$i = 1, 2, \ldots, e_1-1;$$

при этом $c_{11}, c_{22}, \ldots, c_{e_1-1,\, e_1-1}$ — единицы кольца $\mathfrak{o}$ (см. (52)). Тогда по лемме 18 мы получим: $w_{pj}\equiv 0 \bmod p^n$. Это означает (см. (50), (51)), что $R(X)\equiv 0 \bmod p^n$. Таким образом, нами получена следующая теорема.

ТЕОРЕМА 2. *Для ряда $V(X)$ при $p\neq 2$ имеет место сравнение*

$$V(X)\equiv (z^{p^n}-1)^{-1} \bmod p^n,$$

где ряд $z(X)$ получен из разложения корня ζ в степенной ряд по простому элементу π.

Из полученной теоремы и предложения 7, п. 1, при тех же обозначениях вытекает следующее утверждение.

ТЕОРЕМА 3. *Пусть $\varepsilon=1+a_1\pi+a_2\pi^2+\ldots$ — главная единица поля k и $l(\varepsilon)=\left(1-\frac{\Delta}{p}\right)\log\varepsilon(X)$. Тогда для символа Гильберта p^n-ой степени при $p\neq 2$ имеет место формула*

$$(\pi, \varepsilon) = \zeta^{\operatorname{tr}\gamma},$$

где $\gamma=\operatorname{res}_X X^{-1}l(\varepsilon)(z^{p^n}-1)^{-1}$.

§ 6. Закон взаимности

1. Приступим теперь к доказательству основного результата работы. Пусть $\alpha=\pi^a\theta\varepsilon$, $\beta=\pi^b\theta'\eta$ — элементы локального поля k, при этом θ, θ' взяты из мультипликативной системы представителей $\mathfrak{R}$, а ε, η — главные единицы. Пусть $\varepsilon=1+a_1\pi+a_2\pi^2+\ldots$ — разложение единицы ε в ряд по простому элементу π с коэффициентами из кольца $\mathfrak{o}$. Обозначим через $\mathrm{A}(X)$ ряд $X^a\theta\varepsilon(X)$, где $\varepsilon(X)=1+a_1X+a_2X^2+\ldots$, а через $l(\varepsilon)$ — функцию $\left(1-\frac{\Delta}{p}\right)\log\varepsilon(X)$ (см. § 1). Аналогичный смысл для элемента β имеют ряды $\mathrm{B}(X)$ и $l(\eta)$. Пусть, наконец, $z(X)$ — ряд, полученный из разложения корня ζ в степенной ряд по простому элементу π, т. е. $\zeta=z(\pi)$.

ТЕОРЕМА 4. *Для символа Гильберта p^n-ой степени элементов α и β при $p\neq 2$ имеет место формула*

$$(\alpha, \beta) = \zeta^{\operatorname{tr}\gamma},$$

где

$$\gamma = \operatorname{res}_X \left(l(\varepsilon) \frac{dl(\eta)}{dX} - l(\varepsilon)\, \mathrm{B}^{-1} \frac{d\mathrm{B}}{dX} + l(\eta)\, \mathrm{A}^{-1} \frac{d\mathrm{A}}{dX} \right) (z^{p^n} - 1)^{-1}$$

(относительно ряда $(z^{p^n} - 1)^{-1}$ см. замечание 3, § 3, п. 1).

Доказательство. Рассмотрим спаривание $\langle\alpha, \beta\rangle_\pi$ в мультипликативной группе $k^\times$ (см. (12), § 3, п. 1). Это спаривание является билинейным, кососимметричным и инвариантным (см. предложение 4, § 3, п. 1). Кроме того, согласно теореме 3, § 5, п. 5, наше спаривание совпадает с символом Гильберта на паре π, ε, т. е.

$$\langle\pi, \varepsilon\rangle_\pi = (\pi, \varepsilon). \tag{53}$$

Далее, наше спаривание совпадает с символом Гильберта на паре главных единиц ε, η. Действительно, пусть $\tau = \pi\varepsilon$, тогда

$$\langle\varepsilon, \eta\rangle_\pi = \langle\pi\varepsilon, \eta\rangle_\pi \langle\pi, \eta\rangle_\pi^{-1} = \langle\tau, \eta\rangle_\tau \langle\pi, \eta\rangle_\pi^{-1} = (\tau, \eta)(\pi, \eta)^{-1} = (\varepsilon, \eta). \tag{54}$$

Здесь первое равенство основано на билинейности спаривания, второе — на инвариантности, а третье — на свойстве (53). Поэтому в общем случае из (53), (54), билинейности и кососимметричности спаривания получаем:

$$\langle\alpha, \beta\rangle_\pi = \langle\pi, \eta\rangle_\pi^a \langle\pi, \varepsilon\rangle_\pi^{-b} \langle\varepsilon, \eta\rangle_\pi = (\pi, \eta)^a (\pi, \varepsilon)^{-b} (\varepsilon, \eta) = (\alpha, \beta).$$

Теорема доказана.

2. Другой вариант доказательства основной теоремы не использует знания формулы для символа Гильберта (π, ε), а опирается лишь на свойства спаривания $\langle\alpha, \beta\rangle_\pi$ (билинейность, кососимметричность, независимость и инвариантность) и канонический базис Шафаревича мультипликативной группы локального поля, о котором сейчас и пойдет речь, прежде чем приступить ко второму варианту доказательства.

В работе ([5]), § 1, был найден канонический базис в группе главных единиц локального поля k следующего вида:

$$\{E(c_i\pi^i), H(a)\}, \quad 1 \leqslant i < pe_1, \quad (i, p) = 1, \quad c_i, a \in \mathfrak{o},$$

где $H(a)$—p^n-примарная единица Хассе (см. § 4, п. 1). При этом любая главная единица ε представима в виде

$$\varepsilon = \prod_{\substack{1 \leqslant i < pe_1 \\ (i,p)=1}} E(c_i\pi^i)\, H(a_\varepsilon) \tag{55}$$

и разложение (55) единственно с точностью до p^n-ых степеней, т. е. ε—p^n-ая степень $\Longleftrightarrow c_i \equiv 0 \bmod p^n$, $\operatorname{tr} a_\varepsilon \equiv 0 \bmod p^n$. Заменим в этом базисе примарную единицу $H(a)$ на построенную в предложении 6, § 4, п. 3, примарную единицу $\omega(a)$, которая отличается от $H(a)$ на элемент p^n-ой степени. Обозначим ряд $\sum c_i X^i$, $1 \leqslant i < pe_1$, $(i, p)=1$, через $\varphi_\varepsilon(X)$. В дальнейшем мы будем использовать каноническое разложение в следующем виде:

$$\varepsilon = E(\varphi_\varepsilon)\,|_{X=\pi}\,\omega(a_\varepsilon). \tag{56}$$

3. Приступим теперь ко второму варианту доказательства основной теоремы, который не использует формулы для символа (π, ε) и теории полей классов.

Рассмотрим опять спаривание $\langle\alpha, \beta\rangle_\pi$ и проверим, что оно совпадает с символом Гильберта на паре π, ε, т. е.

$$\langle\pi, \varepsilon\rangle_\pi = (\pi, \varepsilon). \tag{57}$$

Из свойства независимости спаривания (см. предложение 5, § 3, п. 3) следует, что мы можем использовать любое представление главной единицы ε в виде степенного ряда по π. Возьмем поэтому каноническое разложение (56). Тогда, с одной стороны, для символа Гильберта получим:

$$(\pi, E(\varphi_\varepsilon(X))\,|_{X=\pi}) = \prod_i (\pi, E(c_i\pi^i)) = 1,$$

так как $(i, p)=1$ (см. лемму 5, § 5, п. 1) и, кроме того, $(\pi, \omega(a_\varepsilon)) = \zeta^{\operatorname{tr} a_\varepsilon}$ (см. предложение 5, § 3, п. 3). Таким образом,

$$(\pi, \varepsilon) = \zeta^{\operatorname{tr} a_\varepsilon}. \tag{58}$$

С другой стороны, по определению спаривания имеем:

$$\langle\pi, E(\varphi_\varepsilon)\,|_{X=\pi}\rangle_\pi = \zeta^{\operatorname{tr}\gamma},$$

где $\gamma = \operatorname{res}_X X^{-1}\varphi_\varepsilon \cdot s^{-1}$. При этом все коэффициенты ряда $s^{-1}(X)$ при степенях, взаимно простых с p, делятся на p^n (см., например, (16), § 3, п. 2). А многочлен $\varphi_\varepsilon(X)$ не имеет членов со степенями, делящимися на p. Это означает, что свободный член ряда $\varphi_\varepsilon \cdot s^{-1}$ делится на p^n, или, что то же самое, $\gamma = \operatorname{res}_X X^{-1}\varphi_\varepsilon s^{-1} \equiv 0 \bmod p^n$. Отсюда

$$\langle\pi, E(\varphi_\varepsilon)\,|_{X=\pi}\rangle_\pi = 1. \tag{59}$$

Далее, по определению спаривания, имеем:

$$\langle\pi, \omega(a_\varepsilon)\rangle_\pi = \langle\pi, E(a_\varepsilon\mathfrak{s})\,|_{X=\pi}\rangle_\pi = \zeta^{\operatorname{tr}\gamma'},$$

где $\gamma' = \operatorname{res}_X X^{-1}a_\varepsilon\mathfrak{s}(X)\,\mathfrak{s}^{-1}(X) = a_\varepsilon$, т. е. $\langle\pi, \omega(a_\varepsilon)\rangle_\pi = \zeta^{\operatorname{tr} a_\varepsilon}$, откуда получаем:

$$\langle\pi, \varepsilon\rangle_\pi = \zeta^{\operatorname{tr} a_\varepsilon}. \tag{60}$$

Это равенство вместе с (58) дает нам (57). Дальнейшее доказательство теоремы 3 проходит точно так же как и в п. 1.

4. Покажем теперь, что закон взаимности Шафаревича является следствием закона взаимности, полученного в теореме 4, п. 1. Изложим сперва основные результаты работы ([5]). В этой работе было введено спаривание $\delta_\pi(\alpha, \beta)$ в мультипликативной группе локального поля k со значениями в группе p^n-примарных элементов следующим образом:

$$\delta_\pi(\pi, \varepsilon) = H(a_\varepsilon), \tag{61}$$

где $H(a_\varepsilon)$ взят из (55), и

$$\delta_\pi(E(c\pi^i), E(d\pi^j)) = \delta_\pi(\pi, E(icd\pi^{i+j})), \tag{62}$$

если $(i, p) = 1$, $(j, p) = 1$. По мультипликативности спаривание δ_π распространяется на любую пару α, β.

В работе ([5]) были доказаны следующие свойства этого спаривания: билинейность, кососимметричность, невырожденность и инвариантность по $\operatorname{mod} p$ (инвариантность в общем случае доказана в ([6])). Наконец, в § 4 работы ([5]) было проверено, что характер от спаривания $\delta_\pi(\alpha, \beta)$ совпадает с символом Гильберта, т. е.

$$\chi(\delta_\pi(\alpha, \beta)) = (\alpha, \beta).$$

П р е д л о ж е н и е 9. *Спаривание $\langle\alpha, \beta\rangle_\pi$ совпадает с $\chi(\delta_\pi(\alpha, \beta))$.*

Д о к а з а т е л ь с т в о. Мы будем использовать независимость спаривания $\langle\alpha, \beta\rangle_\pi$ от разложения в ряды по π (см. § 3), а также вместо канонического разложения (55) каноническое разложение (56). В этом случае, с одной стороны (см. (61)),

$$\chi(\delta_\pi(\pi, \varepsilon)) = \chi(H(a_\varepsilon)) = \zeta^{\operatorname{tr} a_\varepsilon},$$

а с другой стороны (см. (60)), $\langle\pi, \varepsilon\rangle_\pi = \zeta^{\operatorname{tr} a_\varepsilon}$, откуда

$$\langle\pi, \varepsilon\rangle_\pi = \chi(\delta_\pi(\pi, \varepsilon)). \tag{63}$$

Проверим, что

$$\langle E(c\pi^i), E(d\pi^j)\rangle_\pi = \langle\pi, E(icd\pi^{i+j})\rangle_\pi, \quad (i, p) = (j, p) = 1. \tag{64}$$

Это равенство, учитывая (63), даст нам совпадение спаривания $\langle\alpha, \beta\rangle_\pi$ с характером от спаривания Шафаревича на паре $E(c\pi^i)$, $E(d\pi^j)$ (см. (62)). По определению (см. (12), § 3, п. 1) имеем:

$$\langle E(c\pi^i), E(d\pi^j)\rangle_\pi = \zeta^{\operatorname{tr}\gamma}, \quad \langle\pi, E(icd\pi^{i+j})\rangle_\pi = \zeta^{\operatorname{tr}\gamma'},$$

где

$$\gamma = \operatorname{res}_X\left(icdX^{i+j-1} + \sum_{r=1}^{\infty}\left(ic^{\Delta^r} dX^{p^r i+j-1} - jcd^{\Delta^r} X^{i+p^r j-1}\right)\right)s^{-1}(X),$$

$$\gamma' = \operatorname{res}_X(icdX^{i+j-1} \cdot s^{-1}(X)).$$

Поскольку все коэффициенты ряда $s^{-1}(X)$ при степенях, взаимно простых с p, делятся на p^n (см. (16), § 3, п. 2), то при $r \geqslant 1$ и $(i, p) = 1$,

$(j, p)=1$ получим:

$$\operatorname{res}_X ic^{\Delta^r} dX^{p^r i+j-1}\mathfrak{s}^{-1}(X) \equiv 0 \bmod p^n,$$

$$\operatorname{res}_X jcd^{\Delta^r} X^{i+p^r j-1}\mathfrak{s}^{-1}(X) \equiv 0 \bmod p^n.$$

Отсюда

$$\gamma \equiv \operatorname{res}_X icd\, X^{i+j-1}\mathfrak{s}^{-1}(X) = \gamma' \bmod p^n,$$

что и доказывает (64). Тем самым утверждение предложения проверено на базисных элементах мультипликативной группы, а из билинейности спаривания следует, что оно выполнено в общем случае. Предложение доказано.

§ 7. Теория полей классов

1. Проверим, что спаривание $\langle\alpha, \beta\rangle_\pi$, определенное, в § 3, п. 1, обладает норменным свойством, т. е. $\langle\alpha, \beta\rangle_\pi=1 \Longleftrightarrow \beta$ — норма в расширении $k(\sqrt[p^n]{\alpha})/k$. Доказательство этого факта проходит по той же схеме, что и доказательство норменного свойства символа Шафаревича (см. [6], теорема 1).

Пусть сперва $\alpha=\pi$, $\beta=\varepsilon$ и $\langle\pi, \varepsilon\rangle_\pi=1$. По свойству независимости спаривания (см. предложение 5, § 3, п. 3) мы можем использовать для ε каноническое разложение (56), § 6, п. 2. Так как при этом всегда $\langle\pi, E(\varphi_\varepsilon)\,|_{X=\pi}\rangle=1$ (см. (59), § 6, п. 2), то из равенства $\langle\pi, \varepsilon\rangle_\pi=1$ следует: $\langle\pi, \omega(a_\varepsilon)\rangle_\pi=1$. Последнее означает, что $\omega(a_\varepsilon)$—p^n-ая степень в k. С другой стороны, элемент $E(\varphi_\varepsilon)\,|_{X=\pi}$ является нормой в $k(\sqrt[p^n]{\pi})/k$ (см. [5], стр. 128). Отсюда следует, что ε будет нормой в $k(\sqrt[p^n]{\pi})/k$.

Пусть теперь $\langle\alpha, \beta\rangle_\pi=1$, $\nu(\alpha)\not\equiv 0 \bmod p$, тогда найдется целое число a такое, что элемент α^a с точностью до p^n-ых степеней будет равен некоторому простому элементу τ. Используя инвариантность спаривания, получаем:

$$\langle\alpha, \beta\rangle_\pi = 1 \Leftrightarrow \langle\alpha^a, \beta\rangle_\pi = 1 \Leftrightarrow \langle\tau, \beta\rangle_\pi = 1 \Leftrightarrow \langle\tau, \beta\rangle_\tau = 1.$$

Отсюда следует, по доказанному выше, что β есть норма в $k(\sqrt[p^n]{\tau})/k$, а значит, и в $k(\sqrt[p^n]{\alpha})/k$.

Действуя так же, как при доказательстве невырожденности символа Шафаревича $\delta_\pi(\alpha, \beta)$ (см. [5], стр. 129), нетрудно проверить, что для любого β найдется простой элемент τ такой, что $\langle\tau, \beta\rangle_\pi=1$.

Пусть, наконец, $\langle\alpha, \beta\rangle_\pi=1$, $\nu(\alpha)\equiv 0 \bmod p$. Найдем простой элемент τ такой, что $\langle\tau, \beta\rangle_\pi=1$. Тогда $\langle\alpha\tau, \beta\rangle_\pi=1$ и при этом $\nu(\alpha\tau)\not\equiv 0 \bmod p$, значит, по только что доказанному, элемент β будет нормой в $k(\sqrt[p^n]{\alpha\tau})/k$. Кроме того, β будет нормой и в $k(\sqrt[p^n]{\tau})/k$. так как $\langle\tau, \beta\rangle_\tau=\langle\tau, \beta\rangle_\pi=1$. Поэтому β будет нормой в $k(\sqrt[p^n]{\alpha})/k$. Норменное свойство спаривания $\langle\alpha, \beta\rangle_\pi$ доказано полностью.

2. Доказательство свойств спаривания $\langle\alpha, \beta\rangle_\pi$ не использует теории полей классов или свойств символа Гильберта. Это позволяет вывести локальную теорию полей классов из свойств спаривания. А именно, так же как в § 2 ([6]), можно проверить следующее утверждение, вытекающее из норменности спаривания $\langle\alpha, \beta\rangle_\pi$, полученного в п. 1.

Пусть H — подгруппа конечного индекса в $k^\times$, содержащая $k^{\times p^n}$, и H' — ортогональное дополнение группы H относительно скалярного произведения $\langle\alpha, \beta\rangle_\pi$. Тогда H' является подгруппой норм в расширении $k(\sqrt[p^n]{H})/k$. Отсюда можно получить все основные теоремы локальной теории полей классов.

Поступило
6.VI.1978

Литература

1 **Artin E., Hasse H.,** Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln, Abh. Mathem. Seminar, Hamburg, 6 (1928), 146—162.

2 **Hasse H.,** Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. II. Reziprozitätsgesetz, Leipzig — Berlin, 1930.

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

4 **Iwasawa K.,** On explizit formulas for the norm residue symbol, J. Math. Soc. Japan, 20 (1968), 151—164.

5 **Шафаревич И. Р.,** Общий закон взаимности. Матем. сб., 26 (68) (1950): 1, 113—146.

6 **Лапин А. И.,** Теория символа Шафаревича, Изв. АН СССР. Сер. матем., 17 (1953), 13—50.

7 **Боревич З. И., Шафаревич И. Р.,** Теория чисел, М., «Наука», 1972.

8 **Востоков С. В.,** Ортогональный базис локального поля, Изв. АН СССР. Сер. матем., 37 (1973), 1228—1240.

9 **Востоков С. В.,** Второй множитель в законе взаимности, Зап. научн. семинаров Ленингр. отд. Матем. ин-та АН СССР, 75 (1978), 59—66.