В. А. Колывагин, Формальные группы и символ норменного вычета, *Изв. АН СССР. Сер. матем.*, 1979, том 43, выпуск 5, 1054–1120

СЕРИЯ
МАТЕМАТИЧЕСКАЯ
Том 43, № 5, 1979

УДК 519.4

В. А. КОЛЫВАГИН

ФОРМАЛЬНЫЕ ГРУППЫ И СИМВОЛ НОРМЕННОГО ВЫЧЕТА

Введение

Пусть L — конечное расширение $\mathbf{Q}_p$, L^{ab} — максимальное абелево расширение L, G_L^{ab} — группа Галуа L^{ab} над L. Согласно теории полей классов, существует каноническое непрерывное вложение $\theta_L : L^* \to G_L^{ab}$, называемое символом норменного вычета или отображением взаимности, образ которого плотен в G_L^{ab}.

Далее, существует следующий способ построения абелевых расширений. Пусть F — формальный (в данной работе «формальный закон» всегда означает «одномерный формальный закон») C-модульный закон конечной высоты, определенный над A. Здесь A — кольцо целых чисел K — конечного расширения $\mathbf{Q}_p$, C — кольцо целых чисел S — подполя K, содержащего $\mathbf{Q}_p$. То, что F — формальный C-модульный закон, означает, что F — формальный групповой закон и имеется вложение C в $\mathrm{End}_{\mathrm{on}\,A}(F)$ — кольцо эндоморфизмов F над A такое, что $c\mapsto[c]_F\equiv\equiv cX (\mathrm{mod\,deg} 2)$. Пусть M — алгебраическое расширение K, μ_M — максимальный идеал кольца целых чисел M. Пусть $E(\mu_M)$ — C-модуль точек F в μ_M. Пусть π — униформизирующая C, $f^{(n)}=[\pi^n]_F$. Из конечности высоты F (условия, что не все коэффициенты $[\pi]_F$ делятся на униформизирующую A) следует, что гомоморфизм $f^{(n)} : E(\mu_{\overline{K}})\to E(\mu_{\overline{K}})$ — изогения ($\overline{K}$ — алгебраическое замыкание K), т. е. $f^{(n)}$ сюръективен и имеет конечное ядро. Обозначим это ядро через $\varkappa_n$. Пусть $K_n=K(\varkappa_n)$ — это конечное расширение Галуа поля K. Предположим теперь, что L — конечное расширение K_n. Пусть $x\in E(\mu_L)$. Так как $f^{(n)}$ — изогения, то уравнение $f^{(n)}(X)=x$ разрешимо в $E(\mu_{\overline{K}})$. Пусть z — какой-нибудь корень. Очевидно, что все остальные имеют вид $z\oplus v$, где v пробегает $\varkappa_n$, а $\oplus$ — сложение в формальной группе. В частности, $N=L(z)$ — нормальное расширение L. Пусть $g\in\mathrm{Gal}(N/L)$. Отображение $g\mapsto g(z)\ominus z$ определяет вложение $\mathrm{Gal}(N/L)$ в $\varkappa_n$. В частности, N — абелево расширение над L.

Конечно, N является аналогом радикальных расширений из теории Куммера. Именно, пусть $F=F_m=X+Y+XY$ — мультипликативный закон, $K=\mathbf{Q}_p$, $C=\mathbf{Z}_p$. Тогда отображение $x\mapsto 1+x$ определяет изоморфизм

$E(\mu_M)$ и V_M — группы главных единиц M. Тогда $[p^n]_F=(X+1)^{p^n}-1$ и на V_M ему соответствует эндоморфизм возведения в p^n-ю степень. $\varkappa_n$ соответствует ζ_n — группа корней p^n-ой степени из 1, а расширение $N=L(z)$, где $f^{(n)}(z)=x$, совпадает с радикальным расширением $L(\sqrt[p^n]{1+x})$.

Определим теперь каноническое спаривание $L^*\otimes E(\mu_L)\to\varkappa_n$ следующим образом: $(a, x)_{L,n}=g(z)\ominus z$, где $g=\theta_L(a)$, $f^{(n)}(z)=x$. Если $F=F_m$, $\pi=p$, то спаривание соответствует классическому символу Гильберта $L^*\otimes V_L\to\zeta_n$ (спаривание $L^*\otimes L^*\to\zeta_n$ определяется спариванием $L^*\otimes \otimes V_L\to\zeta_n$).

Возникает задача об отыскании явного вида спаривания $(,)_{L,n}$, которой посвящена эта работа.

Первые явные формулы, описывающие символ Гильберта для $n=1$, $L=\mathbf{Q}_p(\sqrt[p]{1})$, были получены Куммером еще в прошлом веке.

И. Р. Шафаревич получил явные формулы для символа Гильберта для произвольных n и $L\supset\mathbf{Q}_p(\sqrt[p^n]{1})$. Именно, он связал с униформизирующей π_L поля L базис мультипликативной группы L и вычислил значения спаривания на образующих (см. ([5])). Недавно С. В. Востоков получил явное выражение для значения символа Гильберта $(a, b)_{L,n}$ в терминах степенных рядов, являющихся разложением a, b по π_L, некоторого степенного ряда, ассоциированного с π_L и образующей ζ_n, и отображения следа из максимального неразветвленного подрасширения L в $\mathbf{Q}_p$ (см. ([6])).

Далее, в ([8]) С. В. Востоков анонсировал аналогичный результат для спаривания, ассоциированного с формальной группой Любина — Тейта, определенной над кольцом целых чисел $\mathbf{Q}_p$.

Данная работа посвящена обобщению формул Артина — Хассе, Ивасавы и Уайлза. Эти формулы имеют однотипную структуру и приведены в порядке возрастания их общности.

В основном обобщение проводится по двум направлениям. Во-первых, мы расширяем класс формальных групп от мультипликативной у Артина, Хассе и Ивасавы и групп Любина — Тейта у Уайлза до произвольных (конечной высоты), во-вторых, мы рассматриваем произвольные поля определения спаривания: $(,)_{L,n}\forall L\supset K_n$. Формулы Артина — Хассе и Ивасавы касаются полей $\mathbf{Q}_p(\sqrt[p^n]{1})$, формулы Уайлза — K_n.

Остановимся несколько более подробно на полученных результатах и на соотношении их с результатами Артина — Хассе, Ивасавы и Уайлза.

Пусть l — логарифм F, т. е. формальный степенной ряд над K такой, что $l\equiv X(\mathrm{mod}\ \deg 2)$, $l(F(X, Y))=l(X)+l(Y)$. l индуцирует точную последовательность гомоморфизмов C-модулей:

$$0\to\varkappa\to E(\mu_{\overline{K}})\xrightarrow{l}\overline{K}\to 0,$$

где $\varkappa=E(\mu_{\overline{K}})_{\mathrm{tor}}=\bigcup_n\varkappa_n$.

Пусть h — высота относительно C эндоморфизма $[\pi]_F$: $\varkappa_n \simeq \left(\frac{C}{\pi^n C}\right)^h$ как C-модуль. Пусть $\varkappa = \varprojlim \varkappa_n$ — модуль Тейта. Тогда $\underset{\leftarrow}{\varkappa} \simeq C^h$. Выберем C-базис $\{e_i\}$ в $\underset{\leftarrow}{\varkappa}$. Пусть e_i^n — редукция e_i в $\varkappa_n$, так что $\{e_i^n\}$ — базис $\varkappa_n$. Если $L \supset K_n$, то под $(,)^i_{L,n}$ подразумеваем i-ю координату спаривания $(,)_{L,n}$.

Действие $G_K = \mathrm{Gal}(\bar{K}/K)$ на $\underset{\leftarrow}{\varkappa}$ определяет π-адическое представление $\delta: G_K \to GL_h(C)$.

Первые 6 параграфов посвящены общему случаю, § 7 — более детальному изучению формальных групп Любина — Тейта.

Основными результатами в общем случае являются следующие. Пусть M — конечное расширение K_t, $m \leqslant t$, причем t является достаточно большим по сравнению с m. Тогда существует дифференцирование $D^i_{M,m}: O_M \to W$, где W — некоторый подфактор M (являющийся O_M-модулем), над A такое, что

$$(a, x)^i_{M,m} = \mathrm{Tr}_{M/S}\left(\frac{D^i_{M,m}(a)}{a} l(x)\right) \quad \forall a \in M^*, \quad x \in E(\mu_M) | \nu(x) > \frac{1}{p-}. \tag{1}$$

Здесь

$$\frac{D^i_{M,m}(a)}{a} = k \frac{D^i_{M,m}(\pi_M)}{\pi_M} + \frac{D^i_{M,m}(u)}{u}$$

(π_M — униформизирующая M), если $a = \pi^k_M u$, $u \in U_M$, — логарифмическая производная, ассоциированная с $D^i_{M,m}$. $\nu: \bar{K}^* \to \mathbf{Q}$ — нормализованное нормирование: $\nu(p) = 1$.

$$(u, x)^i_{M,m} = \mathrm{Tr}_{M/S}(\log(u)(-D^i_{M,m}(x) l'(x))) \quad \forall u \in V_M | \nu(u-1) > \frac{1}{p-1}, \quad x \in E(\mu_M). \tag{2}$$

Здесь $\log: V_M \to M$ — обычный логарифм, $(-D^i_{M,m} l')$ — формальная логарифмическая производная, ассоциированная с дифференцированием $(-D^i_{M,m})$.

Отметим, что всякое дифференцирование $D: O_M \to W$ над A определяется по значению $w = D(\pi_M): D(r(\pi_M)) = r'(\pi_M) w$, где $r \in \tilde{A}[[X]]$, где $\tilde{A}$ — кольцо целых чисел максимального неразветвленного над K подрасширения M. Далее, такое отображение определяет дифференцирование $\Leftrightarrow D(M/K) w = 0$, где $D(M/K)$ — дифферента M над K.

Далее, показано, что $D^i_{M,m}$ могут быть нормированы по значениям инвариантов, связанных с представлением $\delta: G_K \to GL_h(C)$.

Из свойств спаривания и (1), (2) соответственно следует:

$$(N_{M/L}(b), x)^i_{L,n} = \mathrm{Tr}_{L/S}\left(\mathrm{Tr}_{M/L}\left(\frac{D^i_{M,m}(b)}{b}\right) l(x)\right) \quad \forall b \in M^*, \quad x \in E(\mu_L), \tag{3}$$

$$(u, N^F_{M/L}(y))^i_{L,n} = \mathrm{Tr}_{L/S}(\log(u)(-D^i_{M,m}(y) l'(y))) \quad \forall u \in V_L, \quad y \in E(\mu_M). \tag{4}$$

Здесь $M = L(\varkappa_t)$ для достаточно большого t, величина которого зависит от (F, f, L, n), $n \leqslant m \leqslant t$ также определяется по (F, f, L, n). $N^F_{M/L}$ — норма в формальной группе: $N^F_{M/L} = \bigoplus_\sigma x^\sigma$, где σ пробегает множество вложений M в $\overline{K}$ над L. В частности, (3) можно использовать для вычисления $(a, x)_{L,n}$ для $a \in L' = \bigcap_t N(L(\varkappa_t))$, где N — норма из $L(\varkappa_t)$ в L; аналогично, (4) — для вычисления $(u, x)_{L,n}$ для $x \in E'(\mu_L) = \bigcap_t N^F(E(\mu_t))$, где $\mu_t = \mu_M$ для $M = L(\varkappa_t)$.

Таким образом, в общем случае явные формулы получены по модулю значений инвариантов представлена G_K на модуле Тейта $\overleftarrow{\varkappa}$.

Остановимся теперь на случае формальных групп Любина—Тейта. В этом случае соответствующие инварианты могут быть явно вычислены с помощью теории формального умножения Любина—Тейта, так что дифференцирования строятся явно. Пусть $\Omega_A(O_{\overline{K}})$ обозначает модуль дифференциалов кольца целых чисел $\overline{K}$ над A. Дифференциалы $\omega_n = l'(e^n)\,de^n\,(h=1)$ порождают $\Omega_A(O_{\overline{K}})$ как $O_{\overline{K}}$-модуль. Определим дифференцирование $Q: O_{\overline{K}} \to \dfrac{\overline{K}}{\pi^{-\frac{1}{q-1}} O_{\overline{K}}}$, положив $Q(a) = b/\pi^n$, если $da = b\omega_n$ (определение корректно). Дифференцирования $D^i_{M,m}$ получаются из Q сужением и факторизацией.

Кроме того, явность ситуации позволяет уточнить условия на t, m в (3), (4). Соответствующие явные формулы содержатся в теоремах 7.15 и 7.18. Формула Уайлза получится, если в теореме 7.15 положить $L = K_n$, формула Ивасавы — $K = \mathbf{Q}_p$, $\pi = p$, $F = F_m$, $L = K_n$ (см. [3], [4]). Аналогично, теоремы 7.19 и 7.20 уточняют (1) и (2).

Далее, мы получаем формулу

$$(((-1)^{p-1}e^n_g), x)_{L,n} = \left[\mathrm{Tr}_{L/K}\left(\frac{l(x)}{\pi^n l'_g(e^n_g)\,e^n_g}\right)\right]_F (e^n) \quad \forall x \in E(\mu_L), \tag{5}$$

где g — формальный степенной ряд Любина — Тейта, являющийся унитарным многочленом степени q (q — число элементов в поле вычетов A) $\overset{\mathrm{def}}{\Leftrightarrow} g \in \Pi\Lambda_\pi$, $e^n_g = [1]_{f,g}(e^n)$, где $[1]_{f,g}$ — изоморфизм F и $F_g \equiv X (\mathrm{mod}\deg 2)$, l_g — логарифм F_g. При $K = \mathbf{Q}_p$, $\pi = p$, $f = (X+1)^p - 1$ ($F = F_m$), $g = f$ и $L = K_n$ (5) совпадает с формулой Артина — Хассе (см. [3]), а при $g = f$, $L = K_n$ — с аналогичной формулой, полученной Уайлзом в [4]. Кроме того, формула типа (5) получена нами и при $g \in \Pi\Lambda_\xi$ для некоторых $\xi \neq \pi$. В частности, это позволяет дополнить теоремы 7.15 и 7.19 в случае L = нормальное слабо и вполне разветвленное расширение I_jK_n, где I_j — неразветвленное расширение K степени j (см. теоремы 7.29 и 7.30, а также конец пункта 7.4.2). Соответствующая формула Артина — Хассе (см. [3]) получается, если в теореме 7.30 положить $K = \mathbf{Q}_p$, $\pi = p$, $f = (X+1)^p - 1$ ($F = F_m$), $j = 1$, $r = n = 1$; формула Ивасавы (см. [3]) — $K = \mathbf{Q}_p$, $\pi = p$, $f = (X+1)^p - 1$, $j = 1$, $r = n$; формула Уайлза — $j = 1$, $r = n = 1$. Кроме того, Уайлз доказывает аналогичную теорему для $j = 1$, $r = n$, но с более жесткими условиями на x (см. [4]).

Наконец, третья формула Артина — Хассе содержится в предложении 7.31 ($\pi=p$, $f=(X+1)^p-1$).

Отметим, что данная работа была написана независимо от работ ([3]), ([4]).

Формулировку первоначальных результатов автора по этой проблематике, близких к результатам ([4]), можно найти в ([7]).

Теперь несколько слов об обозначениях. Леммы, предложения, теоремы и т. д. имеют единую нумерацию в пределах каждого параграфа. Мы часто используем для обозначения формул и свойств наименования типа $S1$, $SP2$ и т. д. Если при ссылке желательно уточнить местонахождение формулы (свойства), мы добавляем к ее наименованию через двоеточие номер пункта, в котором она сформулирована: $S1:3.1$, $SP2:3.3$ и т. д. Иногда мы используем знак ■ — знак окончания доказательства. Если A — кольцо, то A^* — группа единиц A.

§ 1. Формальные групповые законы

1.1. Формальные степенные ряды. Пусть A — коммутативное кольцо с единицей, $A_n=A[[X_1, \ldots, X_n]]$ — кольцо формальных степенных рядов над A от переменных $X_1, \ldots, X_n$.

Ряд $f(X)=a_0+a_1X+\cdots\in A_1^*\Leftrightarrow a_0\in A^*$. Действительно, $(a_0+a_1X+\cdots)(b_0+b_1X+\cdots)=1\Leftrightarrow a_0b_0=1$, $\sum_{i=0}^{m} a_ib_{m-i}=0$ при $m\geqslant 1$. Если $a_0b_0=1$, то b_m при $m\geqslant 1$ последовательно определяются по формуле $b_m=-b_0\sum_{i=1}^{m} a_ib_{m-i}$.

Пусть B — коммутативное кольцо, μ — идеал B такой, что $\bigcap_{j=1}^{\infty}\mu^j=0$. Функция $\rho(x, y)=2^{-t}$, где $t=\max\{j\,|\,x-y\in\mu^j\}$, превращает B в метрическое пространство. Назовем пару (B, μ) полной, если B полно относительно μ-метрики. Пусть (B, μ) полна. Если $f(X_1, \ldots, X_n)\in B[[X_1, \ldots, X_n]]$, $x_1, \ldots, x_n\in\mu$, то определена подстановка $x_1, \ldots, x_n$ в f: $f(x_1, \ldots, x_n)\in B$ — соответствующий предел.

Примеры. B — коммутативное кольцо, $\mu=0$. Метрика дискретна, поэтому B полно. $f(0, \ldots, 0)$ — это просто свободный член ряда. Далее, в качестве полной пары (B, μ) можно взять $(A_m, \mu)=\{g\in A_m\,|\,g(0, \ldots, 0)=0\}$. В частности, если f — ряд от n переменных над A_m, $g_i\in A_m$, $g_i(0, \ldots, 0)=0$, то определен ряд $f(g_1, \ldots, g_n)\in A_m$ — это формальная подстановка рядов g_i в f.

Пусть $f\in A_1$, $f=a_0+a_1X+\ldots$. Положим $c(f)=a_1$. Очевидно, если $g\in A_1$, $g(0)=0$, то $c(f(g))=c(f)c(g)$.

Пусть $f\in A_1$, $f(0)=0$. Ряд $g\in A_1$ такой, что $g(0)=0$, $f(g)=g(f)=X$, существует $\Leftrightarrow c(f)\in A^*$. Так как $c(X)=1$, $c(f(g))=c(f)c(g)$, то необходимость очевидна. Если $c(f)\in A^*$, то ряд g такой, что $g(0)=0$, $f(g)=X$, однозначно строится с помощью последовательных приближений по модулю степеней X. Очевидно, $c(g)\in A^*$. Пусть $r\in A_1$ — такой, что $r(0)=0$,

$g(r)=X$. Тогда $g(f)=g(f(g(r)))=g(f(g)(r))=g(r)=X$ (подстановка ассоциативна). Значит, g — искомый ряд. Ряд g будем обозначать через f^{-1}.

1.2. Категория формальных групповых законов над A. Формальным групповым законом над A называется формальный степенной ряд $F(X, Y)$ над A от двух переменных, удовлетворяющий условиям:

$F1$. $F(X, 0)=X$; $F(0, Y)=Y$.

$F2$. $F(F(X, Y), Z)=F(X, F(Y, Z))$.

Из $F1$ следует, что $F(0, 0)=0$, поэтому подстановки в $F2$ определены (см. пункт 1.1.).

Из $F1$, $F2$ выводится, что существует единственный ряд $i(X)\in A_1$ такой, что $i(0)=0$, $F(X, i(X))=F(i(X), X)=0$. F называется коммутативным, если $F(X, Y)=F(Y, X)$. Как мы покажем ниже, если $\operatorname{char}(A)=0$, то коммутативность следует из $F1$, $F2$.

Примеры. Аддитивный закон: $F_a=X+Y$. Мультипликативный закон: $F_m=X+Y+XY$.

Пусть F, G — формальные групповые законы над A. Гомоморфизмом (над A) F в G называется ряд $f\in A_1$ такой, что $f(0)=0$ и

$H1$. $f(F(X, Y))=G(f(X), f(Y))$.

Очевидно, формальные групповые законы с гомоморфизмами образуют категорию, если в качестве композиции гомоморфизмов взять подстановку рядов. Будем обозначать эту категорию через $\Phi(A)$.

Пусть F, $G\in\Phi(A)$. Через $\operatorname{Hom}(F, G)$ обозначим множество гомоморфизмов F в G. Если G коммутативен, то $\operatorname{Hom}(F, G)$ имеет структуру абелевой группы. Если F коммутативен, то $\operatorname{End}(F)=\operatorname{Hom}(F, F)$ имеет структуру кольца. Имеем отображение (см. пункт 1.1) $c:\operatorname{Hom}(F, G)\to A$. Если G коммутативен, то c — гомоморфизм абелевых групп, если F коммутативен, то $c:\operatorname{End}(F)\to A$ — гомоморфизм колец.

Как обычно, гомоморфизм $f: F\to G$ называется изоморфизмом, если существует гомоморфизм $g: G\to F$ такой, что $f(g)=g(f)=X$. Из пункта 1.1 следует, что f — изоморфизм $\Leftrightarrow c(f)\in A^*$. Действительно, если $f(g)=g(f)=X$, то $g(G(X, Y))=g(G(f(g), f(g)))=g(f(F(g, g)))=$ $=F(g(X), g(Y))$.

Предложение 1.1. *Пусть* F, $G\in\Phi(A)$. *Если* $\operatorname{char}(A)=0$, *то* $c:\operatorname{Hom}(F, G)\to A$ — *вложение. Если* $\operatorname{char}(A)=p$ — *простое число, то* $f\in\operatorname{Hom}(F, G)$, $f\neq 0$, *имеет вид*: $f=t(X^{p^h})$, *где* $c(t)\neq 0$, h — *неотрицательное целое число.*

Доказательство. Пусть $f\in\operatorname{Hom}(F, G)$, $f\neq 0$. Дифференцируя $H1$ по X, имеем:

$$f'(F(X, Y))\,F_X(X, Y)=G_X(f(X), f(Y))\,f'(X).$$

Очевидно, $c(f)=f'(0)$. Из $F1$ следует, что $r(0)=1$, где $r(X)=F_X(0, X)$. Согласно пункту 1.1, $r\in A_1^*$. Поэтому, подставляя в полученное выше равенство $X=0$, $Y=X$, имеем:

$$f'(X)=c(f)\,\frac{G_X(0, f(X))}{F_X(0, X)}\,. \tag{1}$$

Таким образом, из $c(f)=0$ следует, что $f'(X)=0$. Если $\mathrm{char}(A)=0$, то это эквивалентно ($f(0)=0$) тому, что $f=0$. Если $\mathrm{char}(A)=p$, то это эквивалентно тому, что $f=f_1(X^p)$, где $f_1 \in A_1$, $f_1(0)=0$. Если мы покажем, что f_1 является гомоморфизмом формальных групповых законов над A, то все будет доказано. Пусть $\tilde{F}$ — ряд, полученный из F возведением коэффициентов в p-ю степень. Так как $a \mapsto a^p$ — эндоморфизм кольца A, то $\tilde{F} \in \Phi(A)$. Имеем:

$$f_1(\tilde{F}(X^p, Y^p)) = f_1(F^p) = f(F) = G(f, f) = G(f_1(X^p), f_1(Y^p)).$$

Отсюда, очевидно, следует: $f_1(\tilde{F}(X, Y)) = G(f_1(X), f_1(Y))$, т. е. $f_1 \in \mathrm{Hom}(\tilde{F}, G)$. ∎

Пусть $\mathrm{char}(A)=p$, $F, G \in \Phi(A)$, $f \in \mathrm{Hom}(F, G)$. Если $f \neq 0$, то число h из предложения 1.1 назовем высотой гомоморфизма f. Если $f=0$, то считаем высоту f бесконечной.

Пусть $F \in \Phi(A)$, F коммутативен. Имеется естественный гомоморфизм $\mathbf{Z} \to \mathrm{End}(F): n \mapsto [n]_F \overset{\text{def}}{—}$ это сумма в $\mathrm{End}(F)$ n экземпляров $f=X \in \mathrm{End}(F)$. Индукцией из $F1$, $F2$ получаем, что $[n]_F \equiv nX \pmod{\deg 2}$. Если $\mathrm{char}(A)=p$, то, очевидно, высота $[p]_F \geqslant 1$.

Пусть $\mathrm{char}(A)=0$, $F \in \Phi(A)$, F коммутативен. Согласно предложению 1.1, $\mathrm{End}(F)$ вкладывается в A: $\mathrm{End}(F) \simeq c(\mathrm{End}(F))$ — подкольцо A. Если $a \in c(\mathrm{End}(F))$, то $[a]_F \overset{\text{def}}{=} c^{-1}(a)$. Пусть C — подкольцо A. F называется формальным C-модульным законом над A, если $C \subset c(\mathrm{End}(F))$. В частности, F — всегда $\mathbf{Z}$-модульный закон. Из предложения 1.1 следует, что если F, G — C-модульные законы, $f \in \mathrm{Hom}(F, G)$, то f — гомоморфизм C-модульных законов: $f([a]_F) = [a]_G(f)$ $\forall a \in C$.

1.3. Логарифмы формального группового закона. Пусть $\mathrm{char}(A)=0$, $\bar{A}$ — локализация A по системе $\{1, 2, \ldots\}$. Считаем, что $A \subset \bar{A}$. По определению, $1, 2, \ldots \in \bar{A}^*$.

Если $t \in \tilde{A}_1$, то через $\int\limits_0^X t(X)\,dX$ обозначаем ряд $r \in \tilde{A}_1$ такой, что

$$r(0)=0,\ r'(X)=t(X),\ \text{т. е. если } t=\sum_{i=0}^{\infty} a_i X^i, \text{ то } r=\sum_{i=1}^{\infty} \frac{a_i}{i} X^i.$$

Логарифмом закона $F \in \Phi(A)$ называем гомоморфизм над $\bar{A}$ F в F_a, т. е. всякий ряд $l \in \bar{A}_1$ такой, что $l(0)=0$, $l(F(X, Y)) = l(X) + l(Y)$. Очевидно, логарифмы образуют $\bar{A}$-модуль: $\mathrm{Hom}_{\mathrm{on}\,\bar{A}}(F, F_a)$.

Предложение 1.2. *$\bar{A}$-модуль логарифмов закона F изоморфен $\bar{A}$. Изоморфизм и обратный к нему задаются отображениями*:

$$l \to c(l), \quad a \to a\int\limits_0^X \frac{dX}{F_X(0, X)}.$$

Доказательство. $\int\limits_0^X \frac{dX}{F_X(0, X)}$ будем обозначать через l_F (главный логарифм). Заметим, что $c(l_F)=1$. Предположим, что мы доказали, что l_F — логарифм. Пусть l — логарифм. Тогда $l_1=c(l)l_F-l$ — логарифм, причем $c(l_1)=0$. Согласно предложению 1.1, $l_1=0$, следовательно, $l=$ $=c(l)l_F$. Остается доказать, что l_F — логарифм. Запишем аксиому ассоциативности для $F: F(Z, F(X, Y))=F(F(Z, X), Y)$. Дифференцируя по Z, имеем:

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

Подставляя $Z=0$, получаем:

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

или

$$\frac{F_X(X, Y)}{F_X(0, F(X, Y))} = \frac{1}{F_X(0, X)}.$$

Далее,

$$\frac{d}{dX}(l_F(F(X, Y))) = l'_F(F(X, Y))\, F_X(X, Y) = \frac{F_X(X, Y)}{F_X(0, F(X, Y))} =$$
$$= \frac{1}{F_X(0, X)} = \frac{d}{dX} l_F(X).$$

Значит, $l_F(F(X, Y))=l_F(X)+t(Y)$. Подставляя $X=0$, имеем: $t(Y)=$ $=l_F(Y)$. ■

Примеры. $l_a = X\ (F=F_a)$, $l_m = \int\limits_0^X \frac{dX}{1+X} = X - \frac{X^2}{2} + \frac{X^3}{3} - \ldots$ $(F=F_m)$.

Следствие 1.3. *Если* $\operatorname{char}(A)=0$, *то все* $F\in\Phi(A)$ *коммутативны.*

Доказательство. $F(X, Y) = l_F^{-1}(l_F(X)+l_F(Y))$. ■

Следствие 1.4. *Пусть* $\operatorname{char}(A)=0$, $F, G\in\Phi(A)$, $f\in\operatorname{Hom}(F, G)$. *Тогда* $l_G(f)=c(f)l_F$.

Доказательство. Очевидно, $l_G(f)$ — логарифм F, а $c(l_G(f))=$ $=c(f)$. ■

В дальнейшем, под логарифмом $F\in\Phi(A)$, $\operatorname{char}(A)=0$, подразумеваем главный логарифм l_F.

§ 2. Формальные групповые законы над дискретно нормированными p-адическими кольцами. Формальные группы и изогении

2.1. Лемма Вейерштрасса. Пусть B—локальное кольцо, μ—максимальный идеал B, причем $\bigcap\limits_{j=1}^{\infty} \mu^j = 0$, пара (B, μ) полная (см. пункт 1.1).

ЛЕММА 2.1. *Пусть* $f\in B_1$, $f=a_0+a_1X+\ldots$, *причем* $a_0, \ldots$ $\ldots, a_{n-1}\in\mu$, $n\geqslant 1$, $a_n\notin\mu$ (*т. е.* a_n — *единица в* B). *Тогда существуют единственные полином* $c_0+c_1X+\ldots+X^n$ *и ряд* $b_0+b_1X+\ldots$ *над* B *такие, что* b_0 — *единица и*

$$f=(c_0+c_1X+\ldots+X^n)(b_0+b_1X+\ldots).$$

Доказательство. Имеем систему уравнений

$$\begin{gathered} c_0b_0 = a_0, \\ c_0b_1 + c_1b_0 = a_1, \\ \cdots\cdots\cdots \\ c_0b_{n-1} + \cdots + c_{n-1}b_0 = a_{n-1}, \\ c_0b_n + \cdots + b_0 = a_n, \\ c_0b_{n+1} + \cdots + b_1 = a_{n+1}, \\ \cdots\cdots\cdots\cdots\cdots \end{gathered}$$

Предположим, что мы доказали, что система имеет единственное решение c_t^i, b_k^i по модулю μ^i, $i = 1, 2, \ldots$, при условии, что b_0^i — класс единицы. Тогда, очевидно, система имеет единственное решение, причем $c_t = \lim c_t^i$, $b_k = \lim b_k^i$. Из первых n уравнений следует, что $c_t^1 = 0$ (b_0^1 — класс единицы, $a_0, \ldots, a_{n-1} \in \mu$). Поэтому b_k^1 = класс a_{n+k} из последующих уравнений. Остается заметить, что c_t^{i+1}, b_k^{i+1} однозначно определяются по c_t^i, b_k^i: так как $a_0, \ldots, a_{n-1} \in \mu$, то для определения c_t^{i+1} из первых n уравнений достаточно знать значения b_k^i, так как $c_t^{i+1} \equiv 0 \pmod{\mu}$, то b_k^{i+1} определяются по b_k^i, c_t^{i+1} из последующих уравнений. ■

2.2. Формальные группы (модули). Пусть B—A-алгебра вида $A \xrightarrow{\sigma} B$, где B — коммутативное кольцо с единицей, σ — гомоморфизм колец. Пусть μ — идеал B, $\bigcap_{j=1}^{\infty} \mu^j = 0$, пара (B, μ) — полная.

Если $F \in \Phi(A)$, то через $E_F(\mu)$ обозначаем μ со структурой топологической группы, индуцированной операциями σF, σi. Очевидно, (B, σ, μ) задает функтор из $\Phi(A)$ в категорию топологических групп.

Соответственно, если F—C-модульный закон, то $E_F(\mu)$ является C-модулем.

Примеры. $B = A_1$, $\mu = \{f \mid f(0) = 0\}$. $E_F(\mu)$ в этом случае называется группой кривых закона F. Далее, смотрите следующий пункт.

2.3. Формальные группы $E_F(\mu_M)$, изогении, модули $\varkappa_{f,n}$, $\varkappa_f$, $\overleftarrow{\varkappa_f}$. Пусть K — полное относительно дискретного нормирования поле характеристики 0, поле вычетов которого имеет характеристику p — простое число. $A = O_K$ — кольцо целых чисел K, μ_K — максимальный идеал A. Очевидно, $p \in \mu_K$, $p \neq 0$. Поэтому можно считать, что $K \supset \mathbf{Q}_p$, $A \supset \mathbf{Z}_p$.

Пусть $F \in \Phi(A)$, $f \in \mathrm{End}(F)$. Согласно (1) § 1, f' делится на $c(f)$ в A_1. Пусть c_n — фундаментальная последовательность элементов из $c(\mathrm{End}(F))$. Тогда $[c_n]_F$ — фундаментальная последовательность рядов из A_1 относительно покоэффициентной сходимости (т. е. $\forall i$ i-е коэффициенты $[c_n]_F$ образуют фундаментальную последовательность). Очевидно, $[c]_F = \lim [c_n]_F \in \mathrm{End}(F)$, где $c = \lim c_n$. Таким образом, $c(\mathrm{End}(F))$ замкнуто. В частности, $\mathbf{Z}_p \subset c(\mathrm{End}(F))$.

Через $\overline{K}$ обозначаем фиксированное алгебраическое замыкание K, все алгебраические расширения K предполагаются содержащимися в $\overline{K}$.

Если L — конечное расширение K, то нормирование с K однозначно продолжается на L, и L полно. Если M — алгебраическое расширение K, то O_M, μ_M обозначают кольцо целых чисел M и его максимальный идеал.

Пусть $F \in \Phi(A)$, M — алгебраическое расширение K. Тогда через $E_F(\mu_M)$ обозначаем соответствующую формальную группу (см. п. 2.2. Точнее, $E_F(\mu_M) = \bigcup_{M \supset L \supset K \mid [L/K] < \infty} E_F(\mu_L)$). Все $E_F(\mu_M)$ — подгруппы $E_F(\mu_{\overline{K}})$.

Из того, что f' делится на $c(f)$, если $f \in \mathrm{End}(F)$, следует, что $E_F(\mu_M)$ — топологический $\mathbf{Z}_p$-модуль (M топологизируется множествами $\{x \mid \nu(x) > q, q \in \mathbf{Q}\}$, где $\nu: \overline{K}^* \to \mathbf{Q}$ — нормализированное нормирование: $\nu(p) = 1$).

Пусть $F, G \in \Phi(A)$, $f \in \mathrm{Hom}(F, G)$. f называется изогенией, если индуцированный им гомоморфизм $f: E_F(\mu_{\overline{K}}) \to E_G(\mu_{\overline{K}})$ сюръективен и имеет конечное ядро.

Обозначим через $\bar{f}$ редукцию f в $k[[X]]$, где k — поле вычетов K. Аналогично для F, G. Очевидно, $\overline{F}, \overline{G} \in \Phi(k)$, $\bar{f} \in \mathrm{Hom}(F, G)$. Назовем высотой f высоту $\bar{f}$ (см. пункт 1.2).

П р е д л о ж е н и е 2.2. $f \in \mathrm{Hom}(F, G)$ — *изогения* $\Longleftrightarrow$ *высота* f *конечна. В этом случае* $|\ker f| = p^h$, *где* h — *высота* f.

Д о к а з а т е л ь с т в о. Если $h = \infty$, то f делится на униформизирующую K, так что f заведомо несюръективен. Пусть $h < \infty$. Пусть $x \in \mu_L$, где L — конечное расширение K. Применим лемму 2.1 к $B = O_L$, ряду $-x + f$. Имеем:

$$-x + f = (c_0 + \cdots + X^{p^h})(b_0 + b_1 X + \cdots),$$

где b_0 — единица. Поэтому уравнение $f(X) = x$ (в $\mu_{\overline{K}}$) эквивалентно уравнению $c_0 + \cdots + X^{p^h} = 0$. Так как $c_0, \ldots, c_{p^h - 1} \in \mu_L$ (см. доказательство леммы 2.1), то всякий корень (в $\overline{K}$) уравнения принадлежит $\mu_{\overline{K}}$. Из (1) § 1 следует, что $f' = c(f)\, t$, где $t \in B_1^*$. Поэтому полином $P = c_0 + \cdots + X^{p^h}$ не имеет кратных корней: $f' = P(b_1 + \cdots) + P'(b_0 + b_1 X + \cdots)$. Значит, уравнение $f(X) = x$ имеет p^h корней в $\mu_{\overline{K}}$, что доказывает предложение. ∎

Пусть $F \in \Phi(A)$, $f \in \mathrm{End}(F)$, высота f конечна, $f^{(n)}$ — n-кратная композиция f. Обозначим через $\varkappa_{f,n}$ ядро $f^{(n)}: E_F(\mu_{\overline{K}}) \to E_F(\mu_{\overline{K}})$ — это конечная подгруппа в $E_F(\mu_{\overline{K}})$. $\varkappa_{f,n}$ образуют проективную систему групп относительно отображений $\varkappa_{f,n+1} \xrightarrow{f} \varkappa_{f,n}$. Через $\underleftarrow{\varkappa_f}$ обозначим $\varprojlim \varkappa_{f,n}$. $\varkappa_f \overset{\mathrm{def}}{=} \bigcup \varkappa_{f,n}$. $\varkappa_{f,n}$, $\varkappa_f$, $\underleftarrow{\varkappa_f}$ — $\mathbf{Z}_p$-модули.

Пусть K содержит S — конечное расширение $\mathbf{Q}_p$, π — униформизирующая в $C = O_S$, j — степень инерции S над $\mathbf{Q}_p$, т. е. $|k_S| = p^j$, где k_S — поле вычетов C.

Предположим, что $F \in \Phi(A)$ является C-модульным законом, причем $f = [\pi]_F$ имеет конечную высоту h_1. Очевидно, $\varkappa_{f,n}$, $\varkappa_f$, $\underleftarrow{\varkappa_f}$ являются C-модулями.

Предложение 2.3. *h_1 делится на $j: h_1 = jh$, и $\varkappa_{f,n} \simeq \left(\frac{C}{\pi^n C}\right)^h$, $\varkappa_f \simeq \simeq \left(\frac{S}{C}\right)^h$, $\underset{\leftarrow}{\varkappa_f} \simeq C^h$ как C-модули.*

Доказательство. $\varkappa_{f,1}$ является $k_S = \frac{C}{\pi C}$-модулем. Пусть h — размерность $\varkappa_{f,1}$ над k_S. Тогда, согласно предложению 2.2, $p^{h_1} = |\varkappa_{f,1}| = p^{jh}$. Значит, $h_1 = jh$. Пусть $\varkappa_{f,n} \simeq \sum_i \frac{C}{\pi^{d_i} C}$ — разложение в прямую сумму (конечного C-модуля). Из сюръективности f следует, что $d_i = n$; далее, так как $f^{(n-1)}(\varkappa_{f,n}) = \varkappa_{f,1}$, то число слагаемых равно h. Утверждения о проективном и индуктивном пределах очевидны. ■

2.4. Гомоморфизм $l_F: E_F(\mu_{\overline{K}}) \to \overline{K}$. Пусть $F \in \Phi(A)$, l_F—логарифм F. Как мы знаем, $l_F = X + \sum_{i=2}^{\infty} \frac{a_i}{i} X^i$, где $a_i \in A$. Через $\nu: \overline{K}^* \to \mathbf{Q}$ обозначаем нормализованное нормирование: $\nu(p) = 1$. Пусть $x \in \mu_{\overline{K}}$. Очевидно, $\nu\left(\frac{a_i x^i}{i}\right) = i\nu(x) - \nu(i) \to \infty$. Поэтому l_F сходится на всех элементах $\mu_{\overline{K}}$. Легко видеть, что из $l_F(F(X, Y)) = l_F(X) + l_F(Y)$, $l_F(f(X)) = c(f)\, l_F(X)$, где $f \in \operatorname{End}(F)$, следует, что $l_F: E_F(\mu_{\overline{K}}) \to \overline{K}$ — гомоморфизм $c(\operatorname{End}(F))$-модулей.

Обозначим через $\mu_{\overline{K},1}$ подмножество $\mu_{\overline{K}}$, состоящее из элементов x таких, что $\nu(x) > \frac{1}{p-1}$. Тогда $E_F(\mu_{\overline{K},1})$ — подгруппа $E_F(\mu_{\overline{K}})$, состоящая из элементов $x \in \mu_{\overline{K},1}$.

Предложение 2.4.1. *l_F является локальным изоморфизмом $E_F(\mu_{\overline{K}})$ и $\overline{K}$. Именно, l_F индуцирует изоморфизм $E_F(\mu_{\overline{K},1})$ на $\mu_{\overline{K},1}$, рассматриваемую как подгруппу аддитивной группы поля K. При этом l_F^{-1} сходится на $\mu_{\overline{K},1}$ и задает обратное отображение.*

2. Если $l_F = X + \sum_{i=2}^{\infty} b_i X^i$, $l_F^{-1} = X + \sum_{i=2}^{\infty} d_i X^i$, то $\nu(b_i x^i) > \frac{1}{p-1}$, $\nu(d_i x^i) > \frac{1}{p-1}$ при $\nu(x) > \frac{1}{p-1}$. Если $\nu(x) > \frac{1}{p-1}$, то $l_F(x) = x(1+\beta)$, $l_F^{-1}(x) = x(1+\gamma)$, где $\beta, \gamma \in \mu_{\overline{K}}$.

Доказательство. Пусть $\nu(x) > \frac{1}{p-1}$. Покажем, что $\nu\left(\frac{x^i}{i}\right) > \nu(x) > \frac{1}{p-1}$. Заметим, что $\nu(i) \leqslant \frac{i-1}{p-1}$, $i = 2, \ldots$. Действительно, можно считать, что $i = p^k$, но $k \leqslant \frac{p^k - 1}{p-1} = 1 + p + \cdots + p^{k-1}$. Поэтому из $\nu(x) > \frac{1}{p-1}$ следует, что $(i-1)\nu(x) > \frac{i-1}{p-1} \geqslant \nu(i) \Rightarrow i\nu(x) - \nu(i) > \nu(x)$. Из доказанного неравенства следуют утверждения о l_F из второй части предложения. Пусть $\nu(y) > \frac{1}{p-1}$, $z \in \mu_{\overline{K}}$ — такой элемент, что $\nu(z) > \frac{1}{p-1}$, $\nu(w) > 0$, где $w = \frac{y}{z}$ (ν сюръективно). Пусть $t(X) = \frac{l_F(zX)}{z}$. Тогда $t(X) \in O_L[[X]]$, где $L = K(z)$, и $c(t) = 1$. Из формальных соображений следует, что

$$t^{-1}(X) = \frac{l_F^{-1}(zX)}{z}.$$

Поэтому l_F^{-1} сходится на $y = zw$ и $l_F^{-1}(y) = zt^{-1}(w)$. При этом $l_F(l_F^{-1}(y)) = zt\left(\frac{l_F^{-1}(y)}{z}\right) = zw = y$. Кроме того, если $l_F^{-1} = X + \sum_{i=2}^{\infty} d_i X^i$, то $\nu(d_i y^i) \geqslant \nu(z) > \frac{1}{p-1}$. Наконец, если $\nu(x) > \frac{1}{p-1}$, то $x = l_F(l_F^{-1}(x)) = l_F^{-1}(x)(1+\beta)$ где $\beta \in \mu_{\overline{K}} \Rightarrow l_F^{-1}(x) = x(1+\gamma)$, $\gamma \in \mu_{\overline{K}}$. ■

Опишем теперь ядро и образ l_F. Предположим, что существует $f \in \mathrm{End}(F)$, $c(f) \in \mu_K$, $c(f) \neq 0$, такой, что высота f конечна.

Предложение 2.5. *Имеет место точная последовательность гомоморфизмов $c(\mathrm{End}(F))$-модулей:*

$$0 \to \varkappa_F \to E_F(\mu_{\overline{K}}) \xrightarrow{l_F} \overline{K} \to 0,$$

где $\varkappa_F = (E_F(\mu_{\overline{K}}))_{\mathrm{tor}}$, причем $\varkappa_F = \varkappa_f$.

Доказательство. То, что $\varkappa_F \in \ker l_F$, следует из того, что в $\overline{K}$ кручение тривиально. Обратно, если $l_F(x) = 0$, то при достаточно большом n $\nu(f^{(n)}(x)) > \frac{1}{p-1}$. Тогда из $l_F(f^{(n)}(x)) = c(f)^n l_F(x) = 0$ и предложения 2.4 следует, что $f^{(n)}(x) = 0$, Значит, $x \in \varkappa_f$. То, что $\varkappa_f \subset \varkappa_F$, следует из того, что высота $f^{(n)}$ конечна (см. предложение 2.2). Значит, $\ker l_F = \varkappa_f = \varkappa_F$. Пусть $y \in \overline{K}$. При достаточно большом n $\nu(c(f)^n(y)) > \frac{1}{p-1}$. Пусть $l_F(z) = c(f)^n y$, $f^{(n)}(w) = z$. Существование таких z и w следует из предложения 2.4 и из того, что $f^{(n)}$, имея конечную высоту, является, согласно предложению 2.2, изогенией. Тогда

$$c(f)^n l_F(w) = l_F(f^{(n)}(w)) = l_F(z) = c(f)^n y \Rightarrow l_F(w) = y.$$

Значит, l_F сюръективен. ■

§ 3. Каноническое спаривание

3.1. Сведения из теории полей классов. Если M/L — конечное расширение полей, то $N_{M/L}$ обозначает норму из M в L, если M/L — расширение Галуа, то через $G(M/L)$ обозначаем группу Галуа расширения.

Пусть L — конечное расширение $\mathbf{Q}_p$, L_{nr} — максимальное неразветвленное расширение L. Поле вычетов L_{nr} есть алгебраическое замыкание k_L — поля вычетов L, а естественный гомоморфизм $G(L_{nr}/L) \to G(\overline{k}_L/k_L)$

является изоморфизмом. Автоморфизму Фробениуса $\overline{k}_L$ над k_L: $a\mapsto a^j$, где $p^j=|k_L|$, соответствует автоморфизм в $G(L_{nr}/L)$, который также называется автоморфизмом Фробениуса. Обозначим его через Fr. Fr является топологической образующей $G(L_{nr}/L)$.

Через L^{ab} обозначаем максимальное абелево расширение L. $L^{ab}\supset L_{nr}$ и имеется точная последовательность

$$1\to I_{L^{ab}}\to G_L^{ab}\to G(L_{nr}/L)\to 1,$$

где $I_{L^{ab}}$ — подгруппа инерции в $G_L^{ab}=G(L^{ab}/L)$.

Существует непрерывный гомоморфизм $\theta_L: L^*\to G_L^{ab}$, называемый символом норменного вычета или отображением взаимности, обладающий следующими свойствами:

*S*1. $\theta_L(a)$ *на* L_{nr} *равен* $\mathrm{Fr}^{\nu_L(a)}$, *где* $\nu_L: L^*\to\mathbf{Z}$ — *сюръективное нормирование.*

*S*2. *Пусть* U_L — *группа единиц* O_L. θ_L *отображает* U_L *изоморфно на* $I_{L^{ab}}$.

*S*3. *Если* M/L — *конечное абелево расширение, то* θ_L *индуцирует точную последовательность*:

$$1\to N_{M/L}(M^*)\to L^*\xrightarrow{\theta_L} G(M/L)\to 1.$$

Далее, функториальные свойства символа:

*S*4. *Пусть* M/L — *конечное расширение. Тогда коммутативна диаграмма*

$$\begin{array}{ccc} M^* & \xrightarrow{\theta_M} & G_N^{ab} \\ \downarrow{\scriptstyle N_{M/L}} & & \downarrow \\ L^* & \xrightarrow{\theta_L} & G_L^{ab} \end{array}$$

Гомоморфизм справа устроен следующим образом: $M^{ab}\supset ML^{ab}\supset L^{ab}$ и $g\in G_M^{ab}$ сужается на L^{ab}.

*S*5. *Пусть* M/L — *конечное расширение. Тогда коммутативна диаграмма*

$$\begin{array}{ccc} M^* & \xrightarrow{\theta_M} & G_M^{ab} \\ \uparrow{\scriptstyle \mathrm{incl}} & & \uparrow{\scriptstyle V} \\ L^* & \xrightarrow{\theta_L} & G_L^{ab} \end{array}$$

Здесь V — гомоморфизм переноса. Он устроен следующим образом. Пусть $N\supset M$, N — конечное расширение Галуа поля L с группой Галуа G. $H=G(N/M)$ — подгруппа в G. Определим сначала $V_N: \frac{G}{G'}\to\frac{H}{H'}$, где G', H' — коммутанты G, H. Этот гомоморфизм будет двойственным к гомоморфизму $\mathrm{Hom}(H, \mathbf{C}^*)\to\mathrm{Hom}(G, \mathbf{C}^*)$, устроенному следующим образом: $\chi\mapsto\frac{\det i_*\chi}{\det i_*1}$, где $i_*\chi$, i_*1 — индуцированные с H на G представления (χ задает одномерное комплексное представление H). Отображения V_N

будут согласованными при переходе к $N_1 \supset N$, их проективный предел будет искомым отображением $V: G_L^{ab} \to G_M^{ab}$.

S6. *Пусть* $\sigma: L \to \overline{\mathbf{Q}}_p$ — *некоторое вложение* L *в* $\overline{\mathbf{Q}}_p$. *Коммутативна диаграмма*

$$\begin{array}{ccc} L^{\sigma *} & \xrightarrow{\theta_{L^\sigma}} & G_{L^\sigma}^{ab} \\ \uparrow{\scriptstyle\sigma} & & \uparrow \\ L^* & \xrightarrow{\theta_L} & G_L^{ab} \end{array}$$

Правый гомоморфизм устроен следующим образом. Пусть σ_1 — какое-нибудь продолжение σ на $\overline{\mathbf{Q}}_p$. Пусть $h \in G_L^{ab}$, h_1 — какое-нибудь продолжение h на $\overline{\mathbf{Q}}_p$. Тогда образом h в $G_{L^\sigma}^{ab}$ будет сужение на $L^{\sigma ab}$ автоморфизма $\sigma_1 h_1 \sigma_1^{-1}$. Легко видеть, что $\sigma_1 h_1 \sigma_1^{-1}$ оставляет неподвижным L^σ, отображение определено корректно и является гомоморфизмом.

Определение символа норменного вычета и доказательства его свойств можно найти в ([2]).

3.2. Расширения полей и символы, ассоциированные с формальным групповым законом. Пусть K — конечное расширение $\mathbf{Q}_p$, $A = O_k$, $F \in \Phi(A)$. Тогда $c(\mathrm{End}(F))$ открыто в своем поле частных. Отсюда легко видеть, что все $f \in \mathrm{End}(F)$ такие, что $c(f) \in \mu_K$, $c(f) \neq 0$, одновременно имеют конечную или бесконечную высоту. В первом случае будем говорить, что F имеет конечную высоту.

Пусть S — подполе K, π — униформизирующая $C = O_S$. Пусть F — формальный C-модульный закон над A конечной высоты. Положим $f = [\pi]_F$. Через $\varkappa_n$, $\varkappa$, $\underset{\leftarrow}{\varkappa}$ будем обозначать $\varkappa_{f,n}$, $\varkappa_f$, $\underset{\leftarrow}{\varkappa}_f$. Через h обозначаем C-высоту f, т. е. ранг $\underset{\leftarrow}{\varkappa}$ как C-модуля (см. предложение 2.3).

Зафиксируем C-базис $\{e_i\}$, $i = 1, 2, \ldots, h$, C-модуля $\underset{\leftarrow}{\varkappa}$, так что $\underset{\leftarrow}{\varkappa} = \sum_i Ce_i$. e_i^n будет обозначать редукцию e_i в $\varkappa_n$, e_i^n образуют $\frac{C}{\pi^n C}$-базис $\varkappa_n : \varkappa_n = \sum_i \frac{C}{\pi^n C} e_i^n$. Если $v \in \underset{\leftarrow}{\varkappa}\,(\varkappa_n)$, то через v^i обозначаем i-ю координату v, так что $v = \sum_i v^i e_i$. Через (v^i) обозначаем столбец координат v.

3.2.1. Поля, порожденные кручением. Символ δ. Обозначим через K_n поле $K(\varkappa_n)$. Очевидно, K_n — расширение Галуа поля K. $K_\infty = K(\varkappa)$. Пусть G_K обозначает $G(\overline{K}/K)$. Действие G_K на $\underset{\leftarrow}{\varkappa}$ определяет непрерывное представление $\delta: G_K \to GL_h(C)$ — группу матриц над C размера h на h с определителем в C^*. Именно,

$$((g(v))^i) = \delta(g)(v^i), \text{ где } v \in \underset{\leftarrow}{\varkappa},\ g \in G_k.$$

Очевидно, $\ker \delta = G(\overline{K}/K_\infty)$, и δ индуцирует вложение $G(K_\infty/K)$ в $GL_h(C)$. Далее, редукция δ в $GL_h\left(\frac{C}{\pi^n C}\right)$, ее мы обозначаем через δ_n, есть аналогичное представление G_k на $\varkappa_n$, оно индуцирует вложение $G(K_n/K)$ в $GL_h\left(\frac{C}{\pi^n C}\right)$.

Если M — алгебраическое расширение K, то через M_n, M_∞ обозначаем $M(\varkappa_n)$, $M(\varkappa)$. G_M является подгруппой G_K, и под $\delta: G_M \to GL_h(C)$ подразумевается сужение δ на G_M. Аналогично для δ_n.

Заметим, что M_{2n} абелево над M_n. Действительно, $\delta_{2n}(G(M_{2n}/M_n))$ принадлежит подгруппе $GL_h\left(\frac{C}{\pi^{2n}C}\right)$, состоящей из матриц $\equiv E(\operatorname{mod}\pi^n)$, где E — единичная матрица. Такая подгруппа, очевидно, коммутативна.

3.2.2. Радикальные расширения, спаривание $(,)_{L,n}$. L в дальнейшем всегда обозначает конечное расширение K. Если M — алгебраическое расширение K, то при фиксированном F будем писать $E(\mu_M)$ вместо $E_F(\mu_M)$.

Пусть $L\supset K_n$, что эквивалентно $E(\mu_L)\supset\varkappa_n$. Пусть $x\in E(\mu_L)$. Рассмотрим уравнение $f^{(n)}(X)=x$ в $E(\mu_{\overline{K}})$. Поскольку $f^{(n)}$ — изогения, то оно всегда разрешимо. Через $\oplus$, $\ominus$ будем обозначать сложение и вычитание в формальной группе: $y\oplus w=F(y, w)$, $y\ominus w=F(y, i(w))$. Если z, z_1 — решения уравнения, то $f^{(n)}(z\ominus z_1)=f^{(n)}(z)\ominus f^{(n)}(z_1)=x\ominus x=0$, так что $z\ominus z_1\in\varkappa_n$. Обратно, если z — решение, $v\in\varkappa_n$, то и $z\oplus v$ — решение. Значит, если z — решение, то все остальные имеют вид $z\oplus v$, где v пробегают $\varkappa_n$. Так как $g\in G_L$ переставляет корни $f^{(n)}(X)=x$, то $L(z)$ нормально над L. Более того, $L(z)$ — абелево над L. Действительно, пусть g_1, $g_2\in G(L(z)/L)$. Тогда $g_1(z)=z\oplus v_1$, $g_2(z)=z\oplus v_2 \Rightarrow (g_1g_2)(z)=(z\oplus v_1)\oplus v_2=(z\oplus v_2)\oplus v_1=(g_2g_1)(z)$. Отображение $g\mapsto\tau_x(g)=g(z)\ominus z$ является вложением $G(L(z)/L)$ в $\varkappa_n$, которое, очевидно, не зависит от выбора z.

Имеем спаривание

$$L^*\otimes E(\mu_L)\to\varkappa_n: (a, x)_{L,n}=\tau_x(\theta_L(a)).$$

Очевидно, оно билинейно, C-линейно справа, ядро справа есть $f^{(n)}(E(\mu_L))$.

3.3. Свойства спаривания $(,)_{L,n}$. Пусть $L\supset K_n$, $(,)_{L,n}$ — определенное в 3.2.2 спаривание. Спаривание обладает следующими свойствами:

$SP1$. $(,)_{L,n}$ *билинейно и C-линейно справа. Ядро справа есть* $f^{(n)}(E(\mu_L))$.

Из $S3$ (см. п. 3.1) следует

$SP2$. $(a, x)_{L,n}=0 \Leftrightarrow a$ *является нормой из* $L(z)$, *где* $f^{(n)}(z)=x$.

$SP3$. *Пусть M — конечное расширение L, $x\in E(\mu_L)$, $b\in M^*$. Тогда* $(b, x)_{M,n}=(N_{M/L}(b), x)_{L,n}$.

Это следует из $S4$ и определения спаривания.

$SP4$. *Пусть M — конечное расширение L, $a\in L^*$, $y\in E(\mu_M)$. Тогда* $(a, y)_{M,n}=(a, N^F_{M/L}(y))_{L,n}$, *где* $N^F_{M/L}(y)=\bigoplus\limits_\sigma y^\sigma$, *суммирование по вложениям M в $\overline{K}$ над L.*

Доказательство. Пусть $f^{(n)}(z)=y$, $N\supset M(z)$ — расширение Галуа над L. $G=G(N/L)$, $H=G(N/M)$. Пусть $G=\bigcup Hc_i$ — разложение G на правые классы смежности по H. Тогда c_i^{-1} будут представителями левых классов смежности G по H. Пусть $\chi : H \to \mathbf{C}^*$ — характер. Пользуясь явной конструкцией индуцированного модуля и индуцированного представления (см. ([1]), глава 18), можно показать, что

$$\frac{\det i_* \chi}{\det i_* 1}(g) = \prod_{c_i g c_j^{-1} \in H} \chi(c_i g c_j^{-1}).$$

Пусть r_k — некоторый $\mathbf{Z}_p$-базис $\varkappa_n$, $t_k \in \mathbf{N}$ — период r_k, т. е. $\varkappa_n = \sum_k \frac{\mathbf{Z}}{t_k \mathbf{Z}} r_k$. Определим $\chi_k : H \to \mathbf{C}^*$ следующим образом:

$$\chi_k(h) = \exp\left(\frac{2\pi i}{t_k} \alpha_k\right), \text{ где } (h, y)_{M,n} = \sum_k \alpha_k r_k.$$

Имеем:

$$\bigoplus_{c_i g c_j^{-1} = h \in H} (h, y)_{M,n} = g\left(\bigoplus_j c_j^{-1}(z)\right) \ominus \left(\bigoplus_j c_j^{-1}(z)\right).$$

Действительно, пусть $g c_j^{-1} = c_i^{-1} h$. Тогда

$$(g c_j^{-1})(z) = (c_i^{-1} h)(z) = c_i^{-1}((h, y)_{M,n} \oplus z) = (h, y)_{M,n} \oplus c_i^{-1}(z).$$

Остается заметить, что когда c_j различны, то и c_i различны, так как иначе $hc_j = hc_s$, но c_j и c_s — представители различных правых классов смежности G по H. Так что когда c_j пробегают всю систему представителей, то c_i, однозначно определяемые по c_j условием $c_i g c_j^{-1} \in H$, также пробегают всю систему представителей.

Но с другой стороны,

$$g\left(\bigoplus c_j^{-1}(z)\right) \ominus \left(\bigoplus c_j^{-1}(z)\right) = (g, N_{M/L}^F(y))_{L,n},$$

так как $f^{(n)}\left(\bigoplus c_j^{-1}(z)\right) = \bigoplus c_j^{-1}(y) = N_{M/L}^F(y)$. Вычисляя $\chi_k(\theta_M(a))$ с помощью $S5$, получим $SP4$.

$SP5$. *Пусть $\sigma : L \to \overline{K}$ — вложение L над K. Тогда*

$$(a^\sigma, x^\sigma)_{L^\sigma, n} = (a, x)_{L,n}^\sigma.$$

Это следует из $S6$ и определения спаривания.

$SP6$. *Пусть $L \supset \varkappa_m$, $n \leqslant m$. Тогда* $(a, x)_{L,n} = f^{(m-n)}((a, x)_{L,m}) = (a, f^{(m-n)}(x))_{L,m}$.

Доказательство непосредственно следует из определения.

Предположим, что $\tilde{F}$ — формальный C-модульный закон над A конечной высоты, изоморфный F. Достаточно, чтобы F был формальным законом над A, изоморфным F, тогда $\tilde{F}$ — автоматически C-модульный закон конечной высоты. Еще более конкретно, все такие законы имеют вид $\tilde{F} = t(F(t^{-1}(X), t^{-1}(Y)))$, где $t \in A_1$, $t(0) = 0$, $c(t) \in A^*$. При этом t является изоморфизмом F и $\tilde{F}$.

Итак, пусть $\tilde{F}$ — формальный C-модульный закон над A конечной высоты, изоморфный F. Пусть $t : F \to \tilde{F}$ — изоморфизм. Тогда $\tilde{f}^{(n)} = [\pi^n]_{\tilde{F}} =$

$=tf(t^{-1})$. Очевидно, K_n является инвариантом класса изоморфизма $F:\tilde{\varkappa}_n=t(\varkappa_n)$.

SP7. $\widetilde{(a, \tilde{x})_{L,n}} = t((a, t^{-1}(\tilde{x}))_{L,n}\ \forall a \in L^*,\ \ \tilde{x} \in E_{\tilde{F}}(\mu_L)$.

Доказательство непосредственно следует из определения спаривания.

3.4. Норменные ряды. Ряд $r \in A_1$ называется n-норменным (относительно F), если $r(0)=0$, $c(r) \in A^*$ и $\forall L \supset \varkappa_n$ имеет место

$r1$. $(r(x), x)_{L,n}=0\ \ \forall x \in E(\mu_L)\ ((0, x)_{L,n} \overset{\text{def}}{=} 0)$.

Свойство $r1$ мы будем записывать символически в виде $(r(X), X)_n = 0$. Из $SP7$ следует

$r2$. *Если* $t: F \to \tilde{F}$ — *изоморфизм, то* $\tilde{r} \in A_1$—*n-норменный относительно* $\tilde{F} \Leftrightarrow r=\tilde{r}(t)$ — *n-норменный относительно* F.

Покажем теперь, что n-норменные ряды существуют и укажем метод их построения. Пусть $g \in A_1$, $g(0)=0$, $c(g) \in A^*$.

Предложение 3.1. *Ряд* $s=\prod\limits_{v \in \varkappa_n} g(F(X, v))$ *принадлежит* A_1 *и имеет вид* $r_g(f^{(n)})$, *где* $r_g \in A_1$ (r_g *определяется однозначно, так как* $f^{(n)}$ *обратим в смысле композиции в* $K[[X]]$). *При этом* r_g—*n-норменный ряд и*

$$c(r_g) = \frac{\prod\limits_{v \in \varkappa_n, v \neq 0} g(v)}{\pi^n} c(g).$$

Доказательство. То, что $s \in A_1$, следует из того, что $s^\sigma = s$ $\forall \sigma \in G_K \left(\left(\sum a_i X^i\right)^\sigma \overset{\text{def}}{=} \sum a_i^\sigma X^i\right)$. Далее, $s(F(X, v)) = s(X)\ \ \forall v \in \varkappa_n$. Пусть $s_1 \in A_1$, $s_1(v)=0\ \forall v \in \varkappa_n$. Покажем, что s_1 делится на $f^{(n)}$. Пусть в соответствии с леммой 2.1 $s_1 = Ps_2$, где $s_2 \in A_1^*$, $P = X^{m_1} + \cdots$ — полином, $f^{(n)} = Qf_1$, где $f_1 \in A_1^*$, $Q = X^{m_2} + \cdots$ — полином. Так как $P(v)=0$, то P делится на $Q=\prod\limits_{v \in \varkappa_n}(X-v)$. Значит, s_1 делится на $f^{(n)}$. В частности, $s=f^{(n)}(a_0+a_1X+\ldots)$. Но из $s(F(X, v))=s(X)$ следует, что $a_1v+\ldots=0$ $\forall v \in \varkappa_n$. Значит, $a_1X+\ldots$ делится на $f^{(n)}$ и т. д. Итак, $s=r_g(f^{(n)})$. Очевидно, $r_g(0)=0$. Вычислим $s(r_g)$. Имеем:

$$\frac{s'(X)X}{s(X)} = \sum_{v \in \varkappa_n} \frac{g'(F(X, v))F_X(X, v)X}{g(F(X, v))}.$$

Отсюда следует:

$$\frac{s'(0)}{\prod\limits_{v \in \varkappa_n, v \neq 0} g(v)} = g'(0).$$

Далее,

$$r_g'(f^{(n)})f^{(n)\prime} = s' \Rightarrow r_g'(0) = \frac{s'(0)}{f^{(n)\prime}(0)} = \frac{s'(0)}{\pi^n} = \frac{c(g)\prod\limits_{v \in \varkappa_n, v \neq 0} g(v)}{\pi^n}.$$

Но $\prod\limits_{v\in\varkappa_n, v\neq 0} g(v)$ ассоциировано с $\prod\limits_{v\in\varkappa_n, v\neq 0} v$, что ассоциировано с π^n (следует из леммы 2.1). Значит, $c(r_g)\in A^*$. Остается доказать, что $(r_g(X), X)_n=0$. Пусть $L\supset\varkappa_n$, $x\in E(\mu_L)$, $f^{(n)}(z)=x$. Тогда $r_g(x)=\prod\limits_{v\in\varkappa_n} g(z\oplus v)=$ $=\prod\limits_i N_{L(z)/L}(g(z_i))$, где z_i — попарно несопряженные корни $f^{(n)}(X)=x$. Из $SP2$ следует, что $(r_g(x), x)_{L,n}=0$. ■

3.5. Специальное представление для спаривания $(,)_{L,n}$. Гомоморфизмы $\varphi^i_{L,n}$ и их свойства. Пусть $L\supset K_n$, $(,)_{L,n}$ — соответствующее спаривание. Через $(,)^i_{L,n}$ обозначим i-ю координату спаривания $(,)_{L,n}$. $(,)^i_{L,n}$ — спаривание со значениями в $\dfrac{C}{\pi^n C}$. Пусть $\varkappa_L=\varkappa\cap E(\mu_L)$. Через L^n будем обозначать аннулятор для $\varkappa_L$ — подгруппу в L^*, состоящую из элементов a таких, что $(a, v)_{L,n}=0$ $\forall v\in\varkappa_L$. Спаривание $(,)^i_{L,n}$ определяет гомоморфизм L^n в $\mathrm{Hom}_C\left(\dfrac{E(\mu_L)}{\varkappa_L}, \dfrac{C}{\pi^n C}\right)$.

Под l подразумеваем l_F — логарифм F. Обозначим через T_L образ $l: E(\mu_L)\to L$. Из предложений 2.4 и 2.5 следует, что T_L— C-подмодуль L максимального ранга (т. е. $T_L S=L$) и $l: \dfrac{E(\mu_L)}{\varkappa_L}\to T_L$ — изоморфизм C-модулей.

Определим спаривание $L\times L\to S$ следующим образом: $\langle y, w\rangle_L=$ $=\mathrm{Tr}_{L/S}(yw)$, где $\mathrm{Tr}_{L/S}$ — след из L в S. Очевидно, $\langle, \rangle_L$ отождествляет L с пространством характеров L в S (L — векторное пространство над S). Обозначим через R_L C-подмодуль L, состоящий из элементов $y\in L$ таких, что $\langle y, w\rangle_L\in C$ $\forall w\in T_L$. Элементы R_L естественно задают C-характеры T_L в C, причем вложение $R_L\to\mathrm{Hom}_C(T_L, C)$ — изоморфизм. Действительно, всякий C-характер $\chi: T_L\to C$ продолжается до характера L в S, который индуцируется некоторым элементом $y\in L$. Очевидно, $y\in R_L$. В частности, $\mathrm{Hom}_C\left(T_L, \dfrac{C}{\pi^n C}\right)$ отождествляется с $\dfrac{R_L}{\pi^n R_L}$.

Имеем цепочку гомоморфизмов:

$$L^n\xrightarrow{\alpha_i}\mathrm{Hom}_C\left(\frac{E(\mu_L)}{\varkappa_L}, \frac{C}{\pi^n C}\right)\cong\mathrm{Hom}_C\left(T_L, \frac{C}{\pi^n C}\right)\cong\frac{R_L}{\pi^n R_L},$$

где первый гомоморфизм задается так: $a\mapsto(a,)^i_{L,n}$.

Предложение 3.2. $\forall a\in L^n$ *существует единственный элемент* $\varphi^i_{L,n}(a)\in\dfrac{R_L}{\pi^n R_L}$ *такой, что*

$\varphi 1$. $(a, x)^i_{L,n}=\mathrm{Tr}_{L/S}(\varphi^i_{L,n}(a)\, l(x))$ $\forall x\in E(\mu_L)$. *При этом отображение* $\varphi^i_{L,n}: L^n\to\dfrac{R_L}{\pi^n R_L}$, *при котором* $a\mapsto\varphi^i_{L,n}(a)$, *является гомоморфизмом.*

Доказательство. $\varphi^i_{L,n}(a)$ — это значение на a композиции цепочки гомоморфизмов из предыдущего образца и только оно. ■

Далее в этом пункте мы опишем свойства $\varphi^i_{L,n}$, соответствующие свойствам SP.

$\varphi 2$. *Пусть M — конечное расширение L. Тогда $N_{M/L}(M^n)\subset L^n$, $\mathrm{Tr}_{M/L}(R_M)\subset R_L$ и диаграмма*

$$\begin{array}{ccc} M^n & \xrightarrow{\varphi^i_{M,n}} & \dfrac{R_M}{\pi^n R_M} \\ \downarrow{\scriptstyle N_{M/L}} & & \Big|{\scriptstyle \mathrm{Tr}_{M/L}} \\ L^n & \xrightarrow{\varphi^i_{L,n}} & \dfrac{R_L}{\pi^n R_L} \end{array}$$

коммутативна.

Доказательство. Очевидно $\varkappa_M\supset\varkappa_L$. Пусть $b\in M^n$, $x\in\varkappa_L$. Согласно $SP3$ $(N_{M/L}(b), x)_{L,n}=(b, x)_{M,n}=0$. Значит, $N_{M/L}(b)\in L^n$. Очевидно, $T_M\supset T_L$. Пусть $y\in R_M$, $w\in T_L$. Тогда $w\in T_M$. Значит, $\mathrm{Tr}_{M/S}(yw)\in C$ или $\mathrm{Tr}_{L/S}(\mathrm{Tr}_{M/L}(y)w)\in C$. Следовательно, $\mathrm{Tr}_{M/L}(y)\in R_L$. Пусть $b\in M^n$, $x\in E(\mu_L)$. Используя $SP3$ и $\varphi 1$, имеем

$$(N_{M/L}(b), x)^i_{L,n} = (b, x)^i_{M,n} = \mathrm{Tr}_{M/S}(\varphi^i_{M,n}(b)\, l(x)) =$$
$$= \mathrm{Tr}_{L/S}(\mathrm{Tr}_{M/L}(\varphi^i_{M,n}(b))\, l(x)).$$

Из предложения 3.2 тогда следует, что

$$\varphi^i_{L,n}(N_{M/L}(b)) = \mathrm{Tr}_{M/L}(\varphi^i_{M,n}(b)).$$

$\varphi 3$. *Пусть M — конечное расширение L. Тогда $L^{n'}\subset M^{n'}$, $R_L\subset R_M$ и диаграмма*

$$\begin{array}{ccc} M^{n'} & \xrightarrow{\varphi^i_{M,n}} & \dfrac{R_M}{\pi^n R_M} \\ \uparrow{\scriptstyle \mathrm{incl}} & & \uparrow \\ L^{n'} & \xrightarrow{\varphi^i_{L,n}} & \dfrac{R_L}{\pi^n R_L} \end{array}$$

коммутативна.

Здесь справа — гомоморфизм, индуцированный вложением R_L в R_M. Это свойство доказывается как $\varphi 2$ с использованием $SP4$ вместо $SP3$.

$\varphi 4$. *Пусть σ — вложение L в $\overline{K}$ над K. Тогда $(L^n)^\sigma=(L^\sigma)^n$, $R_{L^\sigma}=\sigma R_L$ и*

$$(\varphi^i_{L^\sigma,n}(a^\sigma)) = \delta_n(\sigma)\,\sigma\,(\varphi^i_{L,n}(a)).$$

Здесь слева и справа столбцы по i. Если $\sigma_1\in G_L$ — продолжение σ, то $\delta_n(\sigma_1)$ зависит лишь от σ, так как $L\supset K_n$. Так что можно писать $\delta_n(\sigma)$. $\varphi 4$ доказывается как $\varphi 2$ с использованием $SP5$, $\varphi 1$ и определения δ_n.

$\varphi 5$. *Пусть $L\supset K_m$, $m\geqslant n$. Тогда $L^m\subset L^n$ и при $a\in L^m$ $\varphi^i_{L,n}(a)$ есть редукция $\varphi^i_{L,m}(a)$ из $\dfrac{R_L}{\pi^m R_L}$ в $\dfrac{R_L}{\pi^n R_L}$.*

Это свойство очевидно следует из предложения 3.2 и $SP6$.

Наконец выясним, как меняется $\varphi^i_{L,n}$ при изоморфизме формальных законов. Пусть $t: F \to \tilde{F}$ — изоморфизм над A. Из следствия 1.4 следует, что $\tilde{l}=c(t)\,l(t^{-1})$. Далее, очевидно, что R_L, L^n — инварианты класса изоморфизма (для L^n это следует из $SP7$). Пусть $\tilde{e}_i$ — базис $\overleftarrow{\tilde{\varkappa}}$. Если $\tilde{e}_i=t(e_i)$, то будем называть t изоморфизмом пары (F, e_i) и пары $(\tilde{F}, \tilde{e}_i)$. Из предложения 3.2 и $SP7$ тогда следует

φ6. R_L, L^n — *инварианты класса изоморфизма. Если* $t: (F, e_i) \to (\tilde{F}, \tilde{e}_i)$ — *изоморфизм, то* $\tilde{\varphi}^i_{L,n}=c(t)^{-1}\varphi^i_{L,n}$.

§ 4. Гомоморфизмы $\psi^i_{L,n}$ и ρ^i_{Ln}

4.1. Гомоморфизмы $\psi^i_{L,n}$, их свойства. Напомним, что через $\mu_{\overline{K},1}$ мы обозначаем подмножество $\mu_{\overline{K}}$, состоящее из элементов x таких, что $\nu(x) > \frac{1}{p-1}$, где ν — нормализованное нормирование. Согласно предложению 2.4, l задает изоморфизм $E(\mu_{\overline{K},1})$ и $T_{\overline{K},1}$, где $T_{\overline{K},1}=\mu_{\overline{K},1}$ рассматриваемое как подгруппа аддитивной группы поля $\overline{K}$.

Пусть $L\supset K$. Тогда $\mu_{L,1}\overset{\text{def}}{=}\mu_L \cap \mu_{\overline{K},1}$. Очевидно, $\mu_L=\left\{y\in L \mid \nu_L(y) \geqslant \left[\frac{e(L)}{p-1}\right]+1\right\}$, где $e(L)$ — индекс ветвления L над $\mathbf{Q}_p$, ν_L — сюръективное нормирование L^* в $\mathbf{Z}$, $[\ ]$ — знак целой части числа. $T_{L,1}\overset{\text{def}}{=}T_{\overline{K},1}\cap L$ — C-подмодуль L. $E(\mu_{L,1})$ — подгруппа $E(\mu_L)$ и l индуцирует изоморфизм $E(\mu_{L,1})$ и $T_{L,1}$. Через $R_{L,1}$ мы будем обозначать C-подмодуль L, состоящий из элементов y таких, что $\langle y, w\rangle_L\in C$ $\forall w\in T_{L,1}$. Так как $T_{L,1}$ — C-подмодуль T_L, то R_L — C-подмодуль $R_{L,1}$. $R_{L,1}$ состоит из элементов y таких, что

$$\nu_L(y) \geqslant -\left(\left[\frac{e(L)}{p-1}\right]+1+\nu_L(D(L/S))\right),$$

где $D(L/S)$ — дифферента L над S.

Пусть $L\supset K_n$. Сужая правый аргумент спаривания $(,)^i_{L,n}$ на $E(\mu_{L,1})$ и рассуждая как при построении гомоморфизмов $\varphi^i_{L,n}$, имеем гомоморфизмы $\psi^i_{L,n}: L^* \to \frac{R_{L,1}}{\pi^n R_{L,1}}$ такие, что $\psi^i_{L,n}(a)$, где $a\in L^*$, однозначно определяются условием

ψ1. $(a, x)^i_{L,n}=\mathrm{Tr}_{L/S}(\psi^i_{L/n}(a)\,l(x))$ $\forall x\in E(\mu_{L,1})$.

Гомоморфизмы $\psi^i_{L,n}$ обладают свойствами, аналогичными свойствам $\varphi^i_{L,n}$, они доказываются совершенно аналогично. Не выписывая их специально, мы обозначим их через ψ2, ψ3 и т. д. Кроме того, $\varphi^i_{L,n}$ и $\psi^i_{L,n}$ связаны следующим образом, очевидно следующим из φ1 и ψ1:

φψ1. *Диаграмма*

$$\begin{tikzcd} L^n \arrow[r, "\varphi^i_{L,n}"] \arrow[dr, "\psi^i_{L,n}"'] & \dfrac{R_L}{\pi^n R_L} \arrow[d, dashed] \\ & \dfrac{R_{L,1}}{\pi^n R_{L,1}} \end{tikzcd}$$

коммутативна.

Правая стрелка индуцированна включением $R_L \subset R_{L,1}$.

4.2. Формула. Будем называть пару натуральных чисел (n, t) допустимой, если существует натуральное число k такое, что $t-n \geqslant k\alpha \geqslant n$, где α будет в дальнейшем всегда обозначать индекс ветвления S над $\mathbf{Q}_p$. Например, пара $(n, 2n+\alpha)$ допустима: в качестве k можно взять $k=\left[\dfrac{n+\alpha}{\alpha}\right]$.

Группа $E_{F_m}(\mu_L)$ канонически изоморфна группе главных единиц V_L поля L: $x \mapsto u = 1 + x$. Хорошей подгруппе $E_{F_m}(\mu_{L,1})$ при этом соответствует подгруппа $1+\mu_{L,1}$. Будем обозначать ее через $V_{L,1}$. Если $u \in V_L$, то $\log(u) \overset{\text{def}}{=} l_m(u-1)$. Соответственно, $\exp \overset{\text{def}}{=} 1 + l_m^{-1}$.

Предложение 4.1. *Пусть* $L \supset K_t$, (n, t) — *допустимая пара.* r — t-*норменный ряд. Тогда имеет место формула*

$$FO1. \quad (u,\ x)^i_{L,n} = \mathrm{Tr}_{L/S}\left(\log(u)\left(\frac{-\psi^i_{L,n}(r(x))\, r(x)\, l'(x)}{r'(x)}\right)\right)$$

$$\forall u \in V_{L,1}, \quad \forall x \in E(\mu_L) \quad (\psi^i_{L,n}(0) \overset{\text{def}}{=} 0).$$

Доказательство. Покажем, что достаточно доказать предложение, считая, что F таков, что X — t-норменный ряд относительно F. Действительно, положим $\widetilde{F} = r(F(r^{-1}(X),\ r^{-1}(X)))$, $\tilde{e}_i = r(e_i)$. Тогда $r:(F, e_i) \to (\widetilde{F}, \tilde{e}_i)$ — изоморфизм. Из $r2:3.4$ следует, что X—t-норменный ряд относительно $\widetilde{F}$. Считая, что для $\widetilde{F}$, $\tilde{r} = X$ предложение доказано, согласно $FO1$ и $SP7:3.3$ имеем:

$$(u,\ x)^i_{F,L,n} = (u,\ r(x))^i_{\widetilde{F},L,n} = \mathrm{Tr}_{L/S}(\log(u)\,(-\widetilde{\psi}^i_{L,n}(r(x))\, r(x)\, \widetilde{l}'(r(x)))) =$$

$$= \mathrm{Tr}_{L/S}\left(\log(u)\left(\frac{-\psi^i_{L,n}(r(x))\, r(x)\, l'(x)}{r'(x)}\right)\right),$$

так как $\widetilde{l}(r(X)) = c(r)\, l(X) \Rightarrow \widetilde{l}'(r(X)) = \dfrac{c(r)\, l'(X)}{r'(X)}$, а $\widetilde{\psi}^i_{L,n}(r(x)) = c(r)^{-1} \times \psi^i_{L,n}(r(x))$ согласно ψ6 — аналогу φ6.

Итак, считаем $r = X$. Пусть k — такое, что $t - n \geqslant \alpha k \geqslant n$, $\varepsilon = \dfrac{\pi^{k\alpha}}{p^k}$ — единица в C. Считая, что L фиксировано, будем опускать символ L в обозначениях. Пусть $u \in V_1$, $x \in E(\mu)$. Пользуясь билинейностью спаривания, имеем:

$$(u,\ x)_n = (u,\ x \ominus (x \times u^{p^k}))_n \oplus (u,\ x \times u^{p^k})_n, \tag{1}$$

где $\times$ — обычное умножение в L.

Преобразуем $(u, x \ominus (x \times u^{p^k}))_n$, пользуясь свойствами символа. Если $c \in C$, $v \in \varkappa_t$, то через cv обозначаем $[c]_F(v)$. Положим $m = n + \alpha k$, $y = x \times u^{p^k}$. Имеем: $(u, y)_n = \pi^{\alpha k}(u, y)_m = (\varepsilon p^k)(u, y)_m = \varepsilon(u^{p^k}, y)_m =$ (применили SP 6:3.3 и билинейность) $= \varepsilon\left(\frac{y}{x}, y\right)_m = \varepsilon(y, y)_m \oplus \varepsilon\left(\frac{1}{x}, y\right)_m = \varepsilon(x, \ominus y)_m =$ $= \varepsilon(x, x)_m \oplus \varepsilon(x, \ominus y)_m = \varepsilon(x, x \ominus y)_m$. Затем использовали: билинейность, то, что $(y, y)_m = 0$ (так как X — t-норменный ряд), снова билинейность, затем то, что $(x, x)_m = 0$, потом билинейность.

Итак,

$$(u, x \times u^{p^k})_n = \varepsilon(x, x \ominus (x \times u^{p^k}))_m. \tag{2}$$

Из предложения 2.4 следует, что

$$u^{p^k} = \exp(\log(u^{p^k})) = \exp(p^k \log(u)) = 1 + p^k \log(u) + p^{2k} w,$$

где $\nu(w) > \frac{1}{p-1}$ $\left(\nu(\log(u)) > \frac{1}{p-1}\right)$. Пусть $z = \log(u)$. Так как $x \ominus y \equiv$ $\equiv x \ominus x \equiv 0 \pmod{(u^{p^k} - 1)}$, то $\nu(x \ominus y) > \frac{1}{p-1}$. Имеем $l(x \ominus y) = l(x) -$ $- l(y)$. Согласно предложению 2.4, если $l = X + \sum_{i=2}^{\infty} b_i X^i$, $\nu(d) > \frac{1}{p-1}$, то $\nu(b_i d^i) > \frac{1}{p-1}$. Отсюда следует, что

$$l(y) = l(x + xp^k z + xp^{2k} w) = l(x) + l'(x)(xp^k z + xp^{2k} w) + p^{2k} w_1,$$

где $\nu(w_1) > \frac{1}{p-1}$, т. е.

$$l(y) = l(x) + l'(x) x p^k z + p^{2k} w_2,$$

где $\nu(w_2) > \frac{1}{p-1}$. Тогда

$$l(x \ominus y) = -l'(x) x p^k z - p^{2k} w_2.$$

Так как $\nu(z) > \frac{1}{p-1}$, π^n по условию делит p^k, $l'(x)$ — единица в O_L, то $x \ominus y$ — π^n-я степень в $E(\mu)$. Значит, из (1) и (2) следует, что

$$(u, x)_n = \varepsilon(x, x \ominus (x \times u^{p^k}))_m. \tag{3}$$

Так как $\nu(x \ominus y) > \frac{1}{p-1}$, то для вычисления правой части (3) можно воспользоваться гомоморфизмами ψ_m^i. Именно, согласно $\psi 1$,

$$\varepsilon(x, x \ominus y)_m^i = \varepsilon \operatorname{Tr}_{L/S}(\psi_m^i(x)\, l(x \ominus y)) = \varepsilon \operatorname{Tr}_{L/S}(\psi_m^i(x)(-l'(x) x p^k z - p^{2k} w_2)).$$

Поскольку $\psi_m^i(x) \in R_1$, $w_2 \in T_1$, π^m / p^{2k}, а $\operatorname{Tr}_{L/S}(R_1 T_1) \subset C$ по определению T_1, R_1, то эта величина равна

$$\varepsilon \operatorname{Tr}_{L/S}(\psi_m^i(x)(-l'(x) x p^k z)) = \pi^{\alpha k} \operatorname{Tr}_{L/S}(z(-\psi_m^i(x) x l'(x))).$$

Из (3) следует, что

$$(u, x)_n^i = \frac{1}{\pi^{m-n}} (\varepsilon(x, x \ominus y)_m^i).$$

Поэтому имеем окончательно:

$$(u, x)_n^i = \mathrm{Tr}_{L/S}(\log(u)(-\psi_n^i(x)\,x l'(x))).$$

При делении на $\pi^{m-n} = \pi^{\alpha k}$ полученное значение будет определено в $\frac{C}{\pi^n C}$, поэтому $\psi_m^i(x)$ можно заменить его редукцией $\psi_n^i(x)$ в $\frac{R_1}{\pi^n R_1}$ (согласно $\psi 5$ — аналогу $\varphi 5$: 3.3).■

4.3. Гомоморфизмы $\rho_{L,n}^i$. Связь $\psi_{L,n}^i$ и $\rho_{L,n}^i$.

Следствие 4.2. *Пусть $L \supset K_t$, (n, t) — допустимая пара. Тогда спаривание $V_{L,1} \otimes E(\mu_L) \to \varkappa_n$ C-линейно.*

Замечание. Структура C-модуля на $V_{L,1}$ вводится через изоморфизм $V_{L,1} \xrightarrow{\log} T_{L,1}$.

Доказательство. Достаточно поглядеть на $FO1$ (в доказательстве нуждается только C-линейность слева).

Применяя уже несколько раз используемую конструкцию, мы можем сконструировать гомоморфизмы $\rho_{L,n}^i : E(\mu_L) \to \frac{R_{L,1}}{\pi^n R_{L,1}}$ такие, что значение $\rho_{L,n}^i(x)$ однозначно определяется условием

$\rho 1$. $(u, x)_{L,n}^i = \mathrm{Tr}_{L/S}(\log(u)\,\rho_{L,n}^i(x))$ $\forall u \in V_{L,1}$.

Отметим только, что L должно содержать K_t, где t дополняет n до допустимой пары.

Предложение 4.3. *Пусть $L \supset K_t$, r — t-норменный ряд, (n, t) — допустимая пара. Тогда имеет место формула*

$$\psi\rho 1. \quad \frac{\psi_{L,n}^i(r(x))\,r(x)}{r'(x)} = -\frac{\rho_{L,n}^i(x)}{l'(x)} \quad \forall x \in \mu_L.$$

Доказательство следует из $FO1$ и определения $\rho_{L,n}^i$.

4.4. Следствия из формулы $\psi\rho 1$, отображения $D_{L,n}^i$. Пусть $L \supset K_n$. Определим $D_{L,n}^i : O_L \to \frac{R_{L,1}}{\pi^n R_{L,1}}$, где $\frac{R_{L,1}}{\pi^n R_{L,1}}$ рассматривается как O_L-модуль, следующим образом: $D_{L,n}^i(x) = \psi_{L,n}^i(x)\,x$. Очевидны свойства:

$D1$. $D_{L,n}^i(xy) = xD_{L,n}^i(y) + yD_{L,n}^i(x)$ $\forall x, y \in O_L$.

$D2$. $D_{L,n}^i(a^{p^k}) = 0$, *если* $\pi^n \mid p^k$.

Предложение 4.4. *Пусть $L \supset K_t$, (n, t) — допустимая пара, r — t-норменный ряд. Тогда*

$$D3. \quad \frac{D_{L,n}^i(r(x \oplus y))}{r'(x \oplus y)} = F_X(x, y)\frac{D_{L,n}^i(r(x))}{r'(x)} + F_Y(x, y)\frac{D_{L,n}^i(r(y))}{r'(y)}$$

$$\forall x, y \in \mu_L.$$

Доказательство. Имеем: $l(F(X, Y)) = l(X) + l(Y)$. Дифференцируя по X, Y, получаем:

$$l'(F(X, Y))\,F_X(X, Y) = l'(X), \quad l'(F(X, Y))\,F_Y(X, Y) = l'(Y).$$

Далее, согласно $\psi\rho 1$,

$$\frac{D^i_{L,n}(r(x\oplus y))}{r'(x\oplus y)}=-\frac{\rho^i_{L,n}(x\oplus y)}{l'(x\oplus y)}=-\frac{\rho^i_{L,n}(x)}{l'(x\oplus y)}-\frac{\rho^i_{L,n}(y)}{l'(x\oplus y)}=$$

$$=\left(\text{так как } \rho^i_{L,n} \text{ — гомоморфизм из } E(\mu_L) \text{ в } \frac{R_{L,1}}{\pi^n R_{L,1}}\right)=$$

$$=-\frac{F_X(x,y)\,\rho^i_{L,n}(x)}{l'(x)}-\frac{F_Y(x,y)\,\rho^i_{L,n}(y)}{l'(y)}=$$

$$=F_X(x,y)\,\frac{D^i_{L,n}(r(x))}{r'(x)}+F_Y(x,y)\,\frac{D^i_{L,n}(r(y))}{r'(y)} \quad \text{(снова применяем } \psi\rho 1). \blacksquare$$

Обозначим через H подмножество в $XA[[X]]$, где $XA[[X]]$ рассматривается как группа кривых закона F (см. пункт 2.2), состоящее из рядов η вида $\eta\in\overset{\infty}{\underset{i=1}{\oplus}}(\theta_i X^i)$. Здесь $\theta_i\in\Theta_L\bigcup 0$, где Θ_L — группа корней (q_L-1)-ой степени из 1 в L^*, $q_L=|k_L|$, k_L — поле вычетов L. Имеет место свойство

$D4$. *Пусть $L\supset K_t$, (n, t) — допустимая пара, r — t-норменный ряд. Пусть $\eta\in H$. Тогда*

$$\frac{D^i_{L,n}(r(\eta(x)))}{r'(\eta(x))}=\eta'(x)\,\frac{D^i_{L,n}(r(x))}{r'(x)} \qquad \forall\, x\in\mu_L.$$

Здесь η' — производная ряда: $\left(\sum a_i X^i\right)'=\sum a_i i X^{i-1}$.

Доказательство. Заметим, что $D^i_{L,n}(\theta)=0$, если $\theta\in\Theta_L\bigcup 0$. Это следует из $D2$: $\theta^{q_L^m}=\theta\ \forall\, m$. Тогда $D4$ формально выводится из $D1$, $D(\theta)=0$, $D3$ (очевидно, $D^i_{L,n}$ непрерывно).

ЛЕММА 4.5. *Пусть π_L — униформизирующая L. $\forall y\in\mu_L\ \exists!\ \eta\in H$ такой, что $y=\eta(\pi_L)$.*

Доказательство. Θ_L при редукции отображается биективно на k_L^*, так что $\Theta_L\bigcup 0$ образует полную систему представителей поля вычетов. θ_1 в представлении $y=\overset{\infty}{\underset{j=1}{\oplus}}(\theta_j\pi_L^j)$ определяется из условия $\frac{y}{\pi_L}\equiv\theta_1 \pmod{\pi_L}$. Так как $F(X, i(Y))\equiv X-Y \pmod{XY}$, то $x\ominus(\theta_1\pi_L)\equiv 0 \pmod{\pi_L^2}$. Пусть $\theta_1,\ldots,\theta_m$ таковы, что $y\ominus y_m\equiv 0 \pmod{\pi_L^{m+1}}$, где $y_m=\overset{m}{\underset{j=1}{\oplus}}(\theta_j\pi_L^j)$. Тогда θ_{m+1} определяется условием $\theta_{m+1}\equiv\frac{y\ominus y_m}{\pi_L^{m+1}} \pmod{\pi_L}$. Если $y_{m+1}=y_m\oplus\oplus(\theta_{m+1}\pi_L^{m+1})$, то $y\ominus y_{m+1}\equiv 0 \pmod{\pi_L^{m+2}}$ и т. д. Ряд η будем обозначать через η_y. Из $D4$ следует

$D5$. *В предположениях $D4$*

$$D^i_{L,n}(z)=r'(r^{-1}(z))\,\eta'_{r^{-1}(z)}(\pi_L)\,\frac{D^i_{L,n}(r(\pi_L))}{r'(\pi_L)} \qquad \forall\, z\in\mu_L.$$

Доказательство. Достаточно заметить, что $z=r(\eta_{r^{-1}(z)}(\pi_L))$. Тогда формула получится, если в $D4$ положить $x=\pi_L$, $\eta=\eta_{r^{-1}(z)}$.

Таким образом, $D5$ позволяет вычислить $D^i_{L,n}(z)$, $z \in \mu_L$, зная лишь значение $D^i_{L,n}$ на какой-нибудь униформизирующей $(r(\pi_L))$ поля L. Также может быть вычислено $D^i_{L,n}(u)$, где u—единица O_L. Именно, $r(\pi_L)\, D^i_{L,n}(u) = -\, uD^i_{L,n}(r(\pi_L)) + D^i_{L,n}(u \cdot r(\pi_L))$. Поскольку $ur(\pi_L)$, $r(\pi_L) \in \mu_L$, то соответствующие значения могут быть вычислены (по значению $D^i_{L,n}(r(\pi_L))$). Тогда $D^i_{L,n}(u)$ также будет вычислено, но по $\operatorname{mod} \frac{\pi^n}{\pi_L} R_{L,1}$.

По существу формулы $D1$ — $D5$ показывают, что $D^i_{L,n}$ ведут себя как дифференцирования над A. Конкретизации этого замечания и получению на этом пути дальнейшей информации о гомоморфизмах $\varphi^i_{L,n}$, $\psi^i_{L,n}$ и $\rho^i_{L,n}$ будут посвящены последующие усилия.

§ 5. p-адические дифференцирования и дифференциалы

5.1. Дифференцирования и дифференциалы. Пусть H — коммутативное кольцо с единицей, O — подкольцо H. Если W—H-модуль, то дифференцированием H в W над O называется отображение $D: H \to W$, удовлетворяющее следующим условиям:

$DI1$. $D(ab) = aD(b) + bD(a) \quad \forall a, b \in H$.

$DI2$. $D(a+b) = D(a) + D(b) \quad \forall a, b \in H$.

$DI3$. $D(a) = 0 \quad \forall a \in O$.

В частности, D — гомоморфизм O-модулей.

Рассмотрим категорию, объектами которой являются пары, состоящие из H-модуля W и дифференцирования $D: H \to W$ над O, их удобно обозначать в виде $H \xrightarrow{D} W$, а морфизм $H \xrightarrow{D_1} W_1$ в $H \xrightarrow{D_2} W_2$ — это гомоморфизм H-модулей $\beta: W_1 \to W_2$ такой, что коммутативна диаграмма

$$\begin{tikzcd} & W_1 \arrow[d, "\beta"] \\ H \arrow[ur, "D_1"] \arrow[r, "D_2"'] & W_2 \end{tikzcd}$$

Покажем, что в этой категории существует универсальный объект, приводя его стандартную конструкцию. Сопоставим каждому элементу $a \in H$ символ da (считаем, что для различных a символы da различны). Рассмотрим в H-модуле, состоящем из конечных линейных комбинаций da, подмодуль, порожденный элементами $d(ab) - adb - bda$, $d(a+b) - da - db$, где a, b пробегают H, а также da, где a пробегает O. Профакторизуем первый модуль по второму. Полученный модуль обозначим через $\Omega_O(H)$. Отображение $d: H \to \Omega_O(H)$ такое, что $d(a) =$ класс da, очевидно, является дифференцированием H в $\Omega_O(H)$ над O. $H \xrightarrow{d} \Omega_O(H)$ будет искомым универсальным объектом. В самом деле, если $H \xrightarrow{D} W$ — объект, то соответствующий гомоморфизм $\beta: \Omega_O(H) \to W$ строится так: гомоморфизм свободного модуля, при котором $da \mapsto D(a)$, тривиален на подмодуле, порожденном соотношениями, поэтому его можно пропустить через $\Omega_O(H)$. Так как $d(a)$ порождают $\Omega_O(H)$, то этот морфизм единствен.

Модуль $\Omega_O(H)$ называется модулем дифференциалов H над O, его элементы — дифференциальными формами, а элементы вида $d(a)$ — также дифференциалами. В дальнейшем будем писать иногда da вместо $d(a)$.

Пусть W—H-модуль. Через $D_O(H, W)$ обозначаем H-модуль дифференцирований H в W над O. Он естественным образом изоморфен $\mathrm{Hom}_H(\Omega_O(H), W)$. В соответствии с этим изоморфизмом имеем спаривание H-модулей $D_O(H, W)\otimes\Omega_O(H)\to W$, при котором $(D, da)=D(a)$.

Пусть H — подкольцо $\tilde{H}$. Тогда имеется естественный гомоморфизм $\Omega_O(H)\to\Omega_O(\tilde{H})$ такой, что $da\mapsto\tilde{d}a$.

5.2. Модули $\Omega_A(O_L)$, $D_A(O_L, W)$. Пусть K — конечное расширение $\mathbf{Q}_p$, $A=O_K$, L — конечное расширение K, $D(L/K)$ — дифферента L над K — целый идеал O_L.

Предложение 5.1.

$\Omega 1$. $\Omega_A(O_L)\simeq\dfrac{O_L}{D(L/K)}$ *как O_L-модули. Если π_L — униформизирующая L, то $d\pi_L$ — образующая $\Omega_A(O_L)$.*

$\Omega 2$. *Пусть M — конечное расширение L. Гомоморфизм $\Omega_A(O_L)\to\to\Omega_A(O_M)$ — вложение.*

Доказательство. Предположим, что L неразветвлено над K. Пусть $a\in O_L$ таково, что $O_L=A[a]$. Пусть $P=X^n+\dots+b_n$ — неприводимый многочлен a над K. Тогда $P'(a)O_L=D(L/K)=O_L$, т. е. $P'(a)$ — единица. Имеем: $0=dP(a)=P'(a)da\Rightarrow da=0$. Значит, $\Omega_A(O_L)=0$.

Пусть теперь L произвольно. Пусть $\tilde{L}$ — максимальное неразветвленное над K подрасширение L. Если π_L— униформизирующая L, то $O_L==O_{\tilde{L}}[\pi_L]$. Если $P=X^n+\dots+b_n$— неприводимый многочлен π_L над $\tilde{L}$, то $P'(\pi_L)O_L=D(L/\tilde{L})=D(L/K)$. Отсюда очевидно, что $\Omega_A(O_L)$ порождается $d\pi_L$ и аннулируется $D(L/K)$. Рассмотрим отображение $D: O_L\to\dfrac{L}{O_L}$, устроенное следующим образом: $D(\pi_L)=\dfrac{1}{a}$, где $aO_L=D(L/K)$, $D(r(\pi_L))==r'(\pi_L)D(\pi_L)$, где $r\in O_{\tilde{L}}[X]$. Очевидно, отображение определено корректно и является дифференцированием O_L над A периода ровно $D(L/K)$. Поэтому $\Omega_A(O_L)=\dfrac{O_L}{D(L/K)}d\pi_L$.

Из $\Omega 1$ следует, что модуль Ω не меняется при замене K и L их неразветвленными расширениями. В частности, можно при изучении вопросов, связанных с Ω, предполагать, что L является вполне разветвленным расширением K.

Докажем $\Omega 2$. Считаем, что M/K вполне разветвлено. Пусть π_M— униформизирующая M, π_L— униформизирующая L.

$\pi_M, \dots, \pi_M^n$, где $n=[M/L]$, образуют базис μ_M над O_L. Пусть $\pi_L==b_1\pi_M^n+\dots+b_{n-1}\pi_M$. Если $P_1=b_1X^n+\dots+b_{n-1}X-\pi_L$, то $P_1(\pi_M)=0$. Значит, $P_1=b_1P$, где $P=X^n+\dots$—унитарный неприводимый многочлен π_M над L. Так как свободный член P_1— униформизирующая L, то b_1— единица O_L. Итак, $\exists P_2\in O_L[X]$ такой, что $\pi_L=P_2(\pi_M)$ и $P_2'(\pi_M)O_M=D(M/L)$. Значит, дифференциал $d\pi_L$ в $\Omega_A(O_M)$ равен $P_2'(\pi_M)d\pi_M$. Так как $D(M/K)=$

$=D(M/L)D(L/K)$, то период $d\pi_L$ в $\Omega_A(O_M)$ равен $D(L/K)$. Значит, $\Omega_A(O_L)\to\Omega_A(O_M)$ — вложение: согласно $\Omega 1$, период $d\pi_L$ в $\Omega_A(O_M)$ равен периоду $d\pi_L$ в $\Omega_A(O_L)$ ($\Omega_A(O_M)$ рассматривается при этом как O_L-модуль), а $d\pi_L$ является образующей $\Omega_A(O_L)$. ■

Следствие 5.2. *Пусть $L\supset K$ — конечное расширение, W—O_L-модуль, π_L— униформизирующая L. Если $D\in D_A(O_L, W)$, то $D(L/K)D(\pi_L)=0$ и отображение $D\mapsto D(\pi_L)$ задает изоморфизм $D_A(O_L, W)$ и $D(L/K)$-периодического подмодуля W. Обратное отображение устроено следующим образом: Пусть $w\in W$, $D(L/K)w=0$. Соответствующее дифференцирование имеет вид $D(r(\pi_L))=r'(\pi_L)w$, где $r\in O_{\tilde{L}}[X]$ ($\tilde{L}$ — максимальное неразветвленное над K подрасширение L). Кроме того, если $r\in O_{\tilde{L}}[[X]]$, то*

$$D(r(\pi_L))=r'(\pi_L)w.$$

Следствие 5.2 следует из $\Omega 1$, из того, что $D_A(O_L, W)\simeq\simeq\mathrm{Hom}_{O_L}(\Omega_A(O_L), W)$, и очевидной непрерывности $D\in D_A(O_L, W)$ (при дискретной топологии в W). ■

5.3. Дифферента поля K_m. K, A, F, e_i^m, K_m и т. д. обозначают то же самое, что в пункте 3.2 и далее. L обозначает конечное расширение K. $\nu:\overline{\mathbf{Q}}_p^*\to\mathbf{Q}$ — нормализованное нормирование.

В этом пункте нас будет интересовать величина дифференты L_m над L, а также величина подмодуля, порожденного в $\Omega_A(O_{K_m})$ дифференциалами de_i^m.

Предложение 5.3. *Существуют положительные константы $c_1, c_2\in\in\mathbf{R}$, зависящие от (F, π), такие, что*

*DIF*1. $\nu(D(L_m/L))\leqslant\frac{m}{\alpha}+\frac{\log_2(m)}{p-1}+c_2$, *где α — индекс ветвления S над $\mathbf{Q}_p$,*

$$\nu(D(K_m/K))\geqslant\frac{m}{\alpha}-c_1.$$

*DIF*2. *Пусть p_m обозначает период (образующая аннулирующего идеала) O_{K_m}-подмодуля в $\Omega_A(O_{K_m})$, порожденного de_i^m. Тогда $\nu(p_m)\geqslant\frac{m}{\alpha}-c_1$.*

Доказательство. Мы докажем предложение в несколько этапов. Сначала займемся оценками сверху.

Пусть M — конечное расширение $\mathbf{Q}_p$, N — конечное расширение Галуа поля M. Пусть Γ^v— группы ветвления N над M с верхней нумерацией ($v\in\mathbf{R}$, $v\geqslant-1$; см. ([2]), глава 1, § 9). Положим $\gamma(v)=|\Gamma^v|$. Согласно известной формуле (которая легко следует из определения Γ^v и предложения 9.4 § 9 главы 1 ([2])) имеем:

$$\nu(D(M/N))=\frac{1}{e(M)}\int_{-1}^{\infty}\left(1-\frac{1}{\gamma(v)}\right)dv, \tag{1}$$

где $e(M)$ — индекс ветвления M над $\mathbf{Q}_p$.

Предположим, что N абелево над M, $\theta:M^*\to G(N/M)$ — отображение взаимности. Согласно теории полей классов (см. теорему 4.1 § 4 главы 6 ([2])),

θ отображает $U_{M,v}$ на Γ^v, где $v \in \mathbf{N}$, $U_{M,v} = 1 + \pi_M^v O_M$, π_M — униформизирующая M. Предположим, что $G(N/M)$ p^k-периодична. Положим $\xi = \left[\frac{e(M)}{p-1}\right] + 1$. Тогда $U_{M,\xi+ke(M)}$ лежит в ядре $\theta : M^* \to G(N/M)$, так как

$$U_{M,\xi+ke(M)} = \exp(\log(U_{M,\xi+ke(M)})) = \exp(\pi_M^{\xi+ke(M)} O_M) = U_{M,\xi}^{p^k}$$

(см. предложение 2.4). Значит, пользуясь (1), имеем:

$$\nu(D(N/M)) \leqslant \frac{1+\xi}{e(M)} + k \leqslant \frac{1}{p-1} + \frac{2}{e(M)} + k. \tag{2}$$

Предположим, что $L \supset K_t$, пара (n, t) — допустимая (см. пункт 4.2). Пусть $x_1, \ldots, x_s \in E(\mu_L)$. Обозначим через $p(x_1, \ldots, x_s)$ период подмодуля, порожденного $\rho^i_{L,n}(x_j)$ в $\frac{R_{L,1}}{\pi^n R_{L,1}}$. Учитывая $\rho 1:4.3$ и рассуждая так же как при получении (2), имеем для $N = L(z_1, \ldots, z_s)$, $f^{(n)}(z_j) = x_j$ оценку

$$\nu(D(N/L)) \leqslant \frac{1}{p-1} + \frac{2}{e(M)} + \nu(p(x_1, \ldots, x_s)). \tag{3}$$

Пусть $m \geqslant 2\alpha$. Положим $\lambda(m) = \left[\frac{m}{2\alpha}\right]$. Тогда $\lambda(m) \geqslant 1$, $m - \lambda(m)\alpha \geqslant \lambda(m)\alpha$. Пусть $m_0 = m$, $\lambda_i = \lambda(m_i)$, $i = 0, 1, \ldots$, $m_{i+1} = m_i - \lambda_i\alpha$, $i = 0, \ldots$. Последовательность m_i обрывается на m_d, где d такое, что $m_d < 2\alpha$ $(m_{i+1} < m_i)$. Пусть $L \supset K$. Имеем башню полей $L_{m_0} \supset L_{m_1} \supset \ldots \supset L_{m_d} \supset L$. Применяя (2) к этажам башни ($G(L_{m_i}/L_{m_{i+1}})$ абелева и p^{λ_i}-периодична), имеем оценку:

$$\nu(D(L_m/L)) \leqslant \left(\lambda_0 + \frac{1}{p-1} + \frac{2}{e(m_1)}\right) + \ldots + \left(\lambda_{d-1} + \frac{1}{p-1} + \frac{2}{e(m_d)}\right) + \\ + \nu(D(L_{m_d}/L)),$$

где $e(m_i)$ — индекс ветвления L_{m_i} над $\mathbf{Q}_p$. Имеем:

$$e(m_i) \geqslant \frac{p^{m_i-1}(p-1)}{\nu(\pi)}.$$

Действительно, так как f' делится на π, то $f = \pi X + \varepsilon X^{p^j} + \pi X^2 f_1 + X^{p^j+1} f_2$, где $f_1, f_2 \in A[[X]]$, $j \geqslant 1$. Поэтому

$$f(e_1^1) = 0 \Rightarrow \nu(\pi e_1^1) = \nu((e_1^1)^{p^j}) \Rightarrow \nu(e_1^1) = \frac{\nu(\pi)}{p^j-1} \leqslant \frac{\nu(\pi)}{p-1}.$$

Далее, из $f(e_1^{n+1}) = e_1^n$ следует, что

$$p^j\nu(e_1^{n+1}) = \nu(e_1^n) \Rightarrow \nu(e_1^{n+1}) = \frac{\nu(e_1^n)}{p^j} \leqslant \frac{\nu(e_1^n)}{p} \leqslant \frac{\nu(\pi)}{p^n(p-1)}.$$

Так как L_{m_i} содержит $\varkappa_{m_i}$, то отсюда вытекает искомая оценка $\left(\frac{1}{e(m_i)} \leqslant \nu(x) \ \forall x \in L_{m_i} \mid \nu(x) > 0\right)$. Значит,

$$\frac{2}{e(m_1)} + \ldots + \frac{2}{e(m_d)} \leqslant \frac{2\nu(\pi)}{p-1}\left(1 + \frac{1}{p} + \ldots + \frac{1}{p^{d-1}}\right) \leqslant \frac{2\nu(\pi)p}{(p-1)^2}.$$

Оценим сверху число шагов от m_0 до m_d. $m_1 < m - \left(\frac{m}{2\alpha} - 1\right)\alpha = \frac{m}{2} + \alpha$. Итерируя, имеем $m_i < \frac{m}{2^i} + \alpha\left(1 + \frac{1}{2} + \ldots + \frac{1}{2^{i-1}}\right) < \frac{m}{2^i} + 2\alpha$. Значит, число шагов $d \leqslant i + 1$, где $\frac{m}{2^i} < 1$, т. е. $i > \log_2(m)$. В частности, $d \leqslant \leqslant \log_2(m) + 2$.

Так как $\lambda_0 + \ldots + \lambda_{d-1} = \frac{m - m_d}{\alpha}$, то получаем оценку

$$\nu(D(L_m/L)) \leqslant \frac{m}{\alpha} + \frac{\log_2(m)}{p-1} + c_3 + \nu(D(L_{2\alpha-1}/L)),$$

где $c_3 = \frac{2}{p-1} + \frac{2p\nu(\pi)}{(p-1)^2}$.

Покажем, что $\nu(D(L_{2\alpha-1}L)) \leqslant \nu(D(K_{2\alpha-1}/K))$. Действительно, пусть вообще N/M — расширение Галуа, L — расширение M (расширения предполагаются конечными). Тогда $T = NL$ — расширение Галуа поля L, причем $G(T/L)$ естественно вкладывается в $G(N/M)$. По определению, $\Gamma_i(T/L)$ состоит из автоморфизмов σ таких, что $\nu(\sigma(x) - x) \geqslant \frac{i+1}{e(T)} \forall x \in O_T$. Поэтому

$$\Gamma_i(T/L) \subset \Gamma_{\frac{(i+1)e(N)}{e(T)} - 1}(N/M).$$

Остается воспользоваться формулой

$$\nu(D(T/L)) = \frac{1}{e(T)} \sum_{i=0}^{\infty} (g_i - 1),$$

где $g_i = |\Gamma_i(T/L)|$, и аналогичной формулой для N/M (см. предложение 9.4, § 9, гл. I ([2])): $\Gamma_i(T/L) \subset \Gamma_0(N/M)$ при $i = 0, \ldots, \frac{e(T)}{e(N)} - 1$ и т. д. Из полученной выше оценки для $\nu(D(L_m/L))$ следует тогда оценка сверху в $DIF1$, причем в качестве c_2 можно взять

$$c_2 = \frac{2}{p-1} + \frac{2\nu(\pi)p}{(p-1)^2} + \nu(D(K_{2\alpha-1}/K)).$$

Займемся теперь оценками снизу. Прежде всего заметим следующее. Из $\Omega 1$, $\Omega 2$ следует, что период de_i^n в $\Omega_A(O_{K_{n+k}})$ по значению на нем ν равен периоду de_i^n в $\Omega_A(O_{K_n})$. Так как $e_i^n = f^{(k)}(e_i^{n+k})$, то $de_i^n = f^{(k)'}(e_i^{n+k}) \times \times de_i^{n+k}$. Но $f^{(k)'} = \pi^k(1 + a_1X + \ldots)$, $a_i \in A$ (см. (1) в § 1). Значит, если период de_i^n в $\Omega_A(O_{K_n}) \neq 1$ (т. е. $de_i^n \neq 0$), то период de_i^{n+k} в $\Omega_A(O_{K_{n+k}})$ равен $\pi^k \times$ (период de_i^n). Поэтому для того, чтобы доказать условие $DIF2$, из которого также очевидно следует оценка снизу в $DIF1$, достаточно показать, что при некотором n $de_i^n \neq 0$ хотя бы для одного i. Тогда в качестве c_1 можно взять $\frac{n}{\alpha}$. Действительно, $\nu(D(K_m/K) \geqslant \frac{m-n}{\alpha} = \frac{m}{\alpha} - \frac{n}{\alpha}$.

Пусть $L = K_t$, $\beta = (n, t)$ — допустимая пара. Обозначим через $p(\beta)$ период подмодуля, порожденного $\rho^i_{L,n}(E(\mu_L))$ (для всех i) в $\frac{R_{L,1}}{\pi^n R_{L,1}}$. Оценим снизу этот период. Пусть $x = \pi_L$ — униформизирующая L. Очевидно, $p(\beta)$ делится на $p(x)$ — период подмодуля, порожденного $\rho^i_{L,n}(x)$. Из леммы 2.1 следует, что уравнение $f^{(n)}(X) = x$ эквивалентно уравнению $P = 0$, где P — многочлен Эйзенштейна. Поэтому $D(N/L) = P'(z)\,O_N = f^{(n)\prime}(z)\,O_N = \pi^n O_N$, где $f^{(n)}(z) = x$, $N = L(z)$. Из (3) тогда следует, что $\nu(p(x)) \geqslant \frac{n}{\alpha} - \frac{2}{e(L)} - \frac{1}{p-1} \geqslant \frac{n}{\alpha} - \frac{1}{p-1} - 2$. Итак,

$$\nu(p(\beta)) \geqslant \frac{n}{\alpha} - \frac{1}{p-1} - 2. \tag{4}$$

ЛЕММА 5.4. *Пусть* $b \in \mu_{\overline{K}}$, $b \neq 0$. *Пусть* M — *конечное расширение* $\mathbf{Q}_p$, *порожденное* b *и коэффициентами* l — *логарифма* F. *Тогда* F *определен* (*что очевидно*) *над* O_M, *а подгруппа, порожденная в* $E(\mu_M)$ (*топологически*) *мультипликативными степенями* b, *содержит* $E(\mu^T_M)$ *для достаточно большого* $T \in \mathbf{N}$ (*т. е. открыта*).

Доказательство. Так как l является локальным изоморфизмом $E(\mu_M)$ и M, то достаточно доказать что элементы $l(b^j)$ порождают M над $\mathbf{Q}_p$. Предположим, что $\sigma: M \to \overline{\mathbf{Q}}_p$ — вложение такое, что $(l(b^j))^\sigma = l(b^j)$ $\forall j$.

Пусть $l = X + \sum\limits_{i=2}^{\infty} \frac{a_i}{i} X^i$, $a_i \in A$. Имеем:

$$\left(\frac{b^\sigma}{b}\right)^j - 1 = \sum_{i=2}^{\infty} \frac{a_i}{i} \frac{b^{\sigma j i}}{b^j} - \sum_{i=2}^{\infty} \frac{a_i}{i} b^{(i-1)j}.$$

Из предложения 2.4 следует, что $\left(\frac{b^\sigma}{b}\right)^j - 1$ делится в O_M на $\frac{b^j}{c^2}$, где $c \in O_M$ — любой элемент такой, что $\nu(c) > \frac{1}{p-1}$, $j \geqslant \frac{\nu(b)}{\nu(c)}$. Полагая $j = q^r$, где q — число элементов поля вычетов M, а r — достаточно большое число, видим, что $\frac{b^\sigma}{b} \equiv 1 \pmod{\mu_M}$. Пусть $u = \frac{b^\sigma}{b}$. Пусть d—такое, что $\nu(u^{p^d} - 1) > \frac{1}{p-1}$. Тогда $u^{p^d s} - 1$ ассоциировано с $\exp(s \log(u^{p^d})) - 1$, что ассоциировано с $s(u^{p^d} - 1)$ (см. предложение 2.4).

Сравнивая асимптотику при $s \to \infty$, $(s, p) = 1$ левой и правой части равенства $u^{p^d} - 1 = \frac{b^{p^d s}}{c^2} \varepsilon_s$, где $\varepsilon_s \in O_M$, видим, что $u^{p^d} = 1$. Взяв достаточно большое $j = sp^d + 1$, получим, что $u = 1$. Итак, $b^\sigma = b$. Рассуждая аналогично, видим, что $a_i^\sigma = a_i$. Так как b, a_i по условию порождают M, то $\sigma = id$. Значит, по теории Галуа, $l(b^j)$ порождают M. ∎

По-прежнему считаем, что $L = K_t$, $\beta = (n, t)$ — допустимая пара. Если мы заменим (F, e_i) на изоморфную пару $(\tilde{F}, \tilde{e}_i)$, то поля K_m не изменятся, периоды de_i^m будут совпадать с периодами $d\tilde{e}_i^m$. Если $r(X)$—t-норменный ряд для F, то ряд X будет t-норменным для $\tilde{F}=r(F(r^{-1}, r^{-1}))$ (следует из $r2:3.4$). Не меняя обозначений, будем считать, что X является t-норменным для F.

Так как $2n \leqslant t$, то $v \in \varkappa_n$ является π^n-ой степенью в $E(\mu_L)$. Тем более, $v \in \varkappa_1$ является π^n-ой степенью в $E(\mu_L)$. Положим $b = \prod\limits_{v \in \varkappa_1, v \neq 0} v$. Очевидно, $b \in \mu_K$, $b \neq 0$. Из $\psi\rho 1:4.3$ ($r = X$) следует, что $D^i_{L,n}(v) = 0$ $\forall v \in \varkappa_1$ (v—π^n-ая степень в $E(\mu_L)$). Из $D1:4.4$, $D3:4.4$ ($r = X$) следует, что $D^i_{L,n} = 0$ на подгруппе в $E(\mu_K)$, порожденной мультипликативными степенями b. Если M — подполе K, порожденное b и коэффициентами l, то, согласно лемме 5.4, $\exists\, T \in \mathbf{N}$ такое, что подгруппа, порожденная в $E(\mu_M)$ элементами b^i, содержит $E(\mu_M^T)$. Значит, $D^i_{L,n} = 0$ на μ_M^T.

Пусть Θ_L — группа корней $(q_L - 1)$-ой степени из 1 в L^*, где q_L — число элементов в поле вычетов L. Из $D2:4.4$ следует, что $D^i_{L,n}(\theta) = 0$ $\forall \theta \in \Theta_L$. Из $D1:4.4$ следует, что $D^i_{L,n}(\theta\mu_M^T) = 0$. Пусть $N = M(\Theta_L)$. Из леммы 4.5 следует, что подгруппа, порожденная $\theta\mu_M^T$ в $E(\mu_N)$, есть μ_N^T. Значит, $D^i_{L,n} = 0$ на μ_N^T.

Так же как при доказательстве леммы 4.5, доказываем, что aX^k, $k=1, 2, \ldots$, $a \in \mu_N^T$, порождают (топологически в группе кривых для F, см. пункт 2.2) $\mu_N^T X O_N[[X]]$. Аналогично доказательству $D4:4.4$ показываем, что для всякого ряда $\tau \in \mu_N^T X O_N[[X]]$ $D^i_{L,n}(\tau(x)) = \tau'(x) D^i_{L,n}(x)$, где $x \in \mu_L$.

Покажем, что $D^i_{L,n}\left(\operatorname{mod} \dfrac{\pi^n}{\pi_M^T \pi_L} R_{L,1}\right)$ являются дифференцированиями O_L в $\dfrac{R_{L,1}}{\frac{\pi^n}{\pi_M^T\pi_L} R_{L,1}}$ над O_N, где π_M, π_L — соответственно униформизирующие M и L. Пусть $\tau \in XO_N[[X]]$. Тогда

$$D^i_{L,n}((\pi_M^T\tau)(\pi_L)) = D^i_{L,n}(\pi_M^T)\,\tau(\pi_L) + \pi_M^T D^i_{L,n}(\tau(\pi_L)) = \pi_M^T D^i_{L,n}(\tau(\pi_L)),$$

так как $D^i_{L,n} = 0$ на $\pi_M^T O_N$ (применили также $D1:4.4$). Но

$$D^i_{L,n}((\pi_M^T\tau)(\pi_L)) = (\pi_M^T\tau)'(\pi_L)\, D^i_{L,n}(\pi_L) = \pi_M^T\tau'(\pi_L)\, D^i_{L,n}(\pi_L)$$

по доказанному выше. Значит,

$$D^i_{L,n}(\tau(\pi_L)) = \tau'(\pi_L)\, D^i_{L,n}(\pi_L) \left(\operatorname{mod} \frac{\pi^n}{\pi_M^T} R_{L,1}\right) \quad \forall \tau \in XO_N[[X]].$$

Всякий элемент из μ_L представляется в виде $\tau(\pi_L)$, где $\tau \in XO_N[[X]]$. Действительно, из леммы 4.5 для аддитивного закона следует, что всякий элемент $y \in \mu_L$ представляется (даже однозначно) в виде

$$y = \sum_{i=1}^{\infty} \theta_i \pi_L^i, \quad \theta_i \in \Theta_L \cup O.$$

Пусть $\gamma = \frac{\pi^n}{\pi_M^T \pi_L}$, и пусть $D^i : O_L \to \frac{R_{L,1}}{\gamma R_{L,1}}$ — редукция $D^i_{L,n}$. Свойство $DI1$: 5.1 для D^i следует из $D1:4.4$. Свойство $D^i_{L,n}(x+y) = D^i_{L,n}(x) + D^i_{L,n}(y)$ $(\mathrm{mod}\, \pi_L \gamma R_{L,1})$ при $x, y \in \mu_L$ следует из того, что

$$D^i_{L,n}(\tau(\pi_L)) = D^i_{L,n}(\pi_L)\,\tau'(\pi_L)\,(\mathrm{mod}\,\pi_L\gamma R_{L,1}) \quad \forall\, \tau \in XO_N[[X]],$$

а всякий элемент μ_L представим в виде $\tau(\pi_L)$: если $x = \tau_1(\pi_L)$, $y = \tau_2(\pi_L)$, то

$$x + y = (\tau_1 + \tau_2)(\pi_L) \Rightarrow D^i_{L,n}(x+y) = (\tau_1+\tau_2)'(\pi_L)\, D^i_{L,n}(\pi_L) =$$
$$= \tau_1'(\pi_L)\, D^i_{L,n}(\pi_L) + \tau_2'(\pi_L)\, D^i_{L,n}(\pi_L) = D^i_{L,n}(x) + D^i_{L,n}(y)\,(\mathrm{mod}\,\pi_L\gamma R_{L,1}).$$

Пусть $a, b \in O_L$. Тогда

$$D^i_{L,n}(\pi_L a + \pi_L b) = D^i_{L,n}(\pi_L a) + D^i_{L,n}(\pi_L b) =$$
$$= (a+b)\, D^i_{L,n}(\pi_L) + \pi_L (D^i_{L,n}(a) + D^i_{L,n}(b))\,(\mathrm{mod}\,\pi_L\gamma R_{L,1}).$$

Но $D^i_{L,n}(\pi_L a + \pi_L b)$ также равно $(a+b)\, D^i_{L,n}(\pi_L) + \pi_L D^i_{L,n}(a+b)$. Значит, $DI2:5.1$ для D^i также выполняется. Наконец, $\pi_L D^i_{L,n}(a) + a D^i_{L,n}(\pi_L) = D^i_{L,n}(\pi_L a) = a D^i_{L,n}(\pi_L)\,(\mathrm{mod}\,\pi_L\gamma R_{L,1})\ \forall\, a \in O_N$ ($\pi_L a = \tau(\pi_L)$, где $\tau = aX$)$\Rightarrow$ $\Rightarrow D^i = 0$ на O_N, т. е. $DI3:3.5$ выполнено для D^i.

Для $\tilde{p}$ — периода подмодуля, порожденного $D^i_{L,n}(O_L)$ в $\frac{R_{L,1}}{\gamma R_{L,1}}$ $\forall\, i$, из $\psi\rho\ 1:4.4$ и (4) следует оценка $\nu(\tilde{p}) \geqslant \frac{n}{\alpha} - c_4$, где $c_4 = \frac{1}{p-1} + 3 + \nu(\pi_M^T)$ $(\nu(\pi_L) \leqslant 1)$. Так как $D^i_{L,n}: O_L \to \frac{R_{L,1}}{\gamma R_{L,1}}$ — дифференцирования над O_N, то из следствия 5.2 следует

ЛЕММА 5.5. *Пусть* (n, t) — *допустимая пара. Тогда* $\nu(D(K_t/N)) = \nu(D(K_t/M)) \geqslant \frac{n}{\alpha} - c_4$ (N/M *неразветвлено*). ■

Пусть $\beta = (n, t)$ — допустимая пара. Обозначим через $p_1(\beta)$ период подмодуля, порожденного $\rho^i_{L,n}(e^t_j)$ в $\frac{R_{L,1}}{\pi^n R_{L,1}}$, где $L = K_t$. Из (3) следует, что

$$\nu(D(K_{t+n}/K_t)) \leqslant \nu(p_1(\beta)) + 2 + \frac{1}{p-1}. \tag{5}$$

Так как $D^i_{L,n}$ являются дифференцированиями $(\mathrm{mod}\,\gamma R_{L,1})$ над O_M, то для периода $\tilde{p}(\beta)$ подмодуля, порожденного de^t_j в $\Omega_{O_M}(O_L)$, имеем оценку

$$\nu(\tilde{p}(\beta)) \geqslant \nu(p_1(\beta)) - \nu(\pi_M^T) - 1 = \nu(p_1(\beta)) - c_7. \tag{6}$$

Пусть $t \geqslant 2\alpha$. Положим $n = \left[\frac{t}{2\alpha}\right]\alpha$. Пара (n, t) допустима, причем $n \geqslant \frac{t}{2} - \alpha$. Из леммы 5.5 следует, что

$$\nu(D(K_t/K)) \geqslant \frac{t}{2\alpha} - c_5, \tag{7}$$

где $c_5 = 1 + c_4 + \nu(D(K/M))$.

Из (5) следует, что

$$\nu(p_1(\beta)) \geqslant \nu(D(K_{\frac{3t}{2}-\alpha}/K_t)) - c_6, \tag{8}$$

где $c_6 = 2 + \frac{1}{p-1}$. Рассмотрим башню $K_{t_2} \supset K_{t_1} \supset K_t$, где $t_1 = \frac{3t}{2} - \alpha$, $t_2 = \frac{3t_1}{2} - \alpha = \frac{9}{4}t - \frac{5}{2}\alpha$, $\beta = (n, t)$, $\beta_1 = (n_1, t_1)$, где $n = \left[\frac{t}{2\alpha}\right]\alpha$, $n_1 = \left[\frac{t_1}{2\alpha}\right]\alpha$. Имеем:

$$\nu(\widetilde{p}(\beta_1)) + \nu(\widetilde{p}(\beta)) \geqslant \nu(p_1(\beta_1)) + \nu(p_1(\beta)) - 2c_7 \text{ (согласно (6))} \geqslant$$
$$\geqslant \nu(D(K_{t_2}/K_t)) - 2c_7 - 2c_6 \text{ (согласно (8))} \geqslant$$
$$\geqslant \nu(D(K_{t_2}/K)) - \nu(D(K_t/K)) - 2c_7 - 2c_6.$$

Используя оценку сверху для $\nu(D(K_t/K))$ в $DIF1$ и оценку снизу (7) для $\nu(D(K_{t_2}/K))$, продолжаем цепочку неравенств:

$$\geqslant \frac{t_2}{2\alpha} - c_5 - \frac{t}{\alpha} - \frac{\log_2(t)}{p-1} - 2c_7 - 2c_6 - c_2 = \frac{t}{8\alpha} - \frac{\log_2(t)}{p-1} - c_8,$$

где $c_8 = c_2 + c_5 + 2c_7 + 2c_6 + \frac{5}{2}$. Из $\Omega 1$, $\Omega 2$ следует, что естественное отображение $\Omega_{O_M}(O_L) \to \Omega_A(O_L)$ суть факторизация

$$\frac{O_L}{D(L/M)} d\pi_L \to \frac{O_L}{D(L/K)} d\pi_L.$$

Поэтому если для периода $p(a)$ элемента $\Omega_{O_M}(O_L)$ имеется оценка $\nu(p(a)) > c$, то для периода его образа $\bar{a}$ в $\Omega_A(O_L)$ будем иметь оценку $\nu(p(\bar{a})) > > c - \nu(D(K/M))$. Для достаточно большой константы c_1 из полученного выше неравенства для $\nu(\tilde{p}(\beta_1)) + \nu(\tilde{p}(\beta))$ следует, что

$$\max\{\nu(\tilde{p}(\beta_1)), \nu(\tilde{p}(\beta))\} > \nu(D(K/M)),$$

если $\frac{t_1}{\alpha} \geqslant c_1$. Значит, $\max\{\nu(p_{t_1}), \nu(p_t)\} = \nu(p_{t_1}) > 0$, где p_m — период подмодуля, порожденного de_i^m в $\Omega_A(O_{K_m})$.

Как было отмечено в начале доказательства оценок снизу, это (вместе с ранее доказанной оценкой сверху) доказывает предложение 5.3, причем в качестве константы в оценках снизу может быть взята описанная выше константа c_1. ■

Рассмотрим теперь специальный случай, когда π является униформизирующей поля K (т. е. K неразветвлено над S). В этом случае уравнение $\frac{f^{(n)}(X)}{f^{(n-1)}(X)} = 0$ эквивалентно (по лемме 2.1) уравнению $P_n(X) = 0$, где P_n — многочлен Эйзенштейна степени $q_S^{hn} - q_S^{h(n-1)}$, где q_S — число элементов поля вычетов S. Период de_i^n (порождающий $D(K(e_i^n)/K)$), равен

$$\left(\frac{f^{(n)}}{f^{(n-1)}}\right)'(e_i^n) = \frac{f^{(n)\prime}(e_i^n)}{f^{(n-1)}(e_i^n)}.$$

Так как $\nu(e_i^1) = \frac{1}{e(K)(q_S^h - 1)}$, где $e(K) = e(S)$ — абсолютный индекс ветвления, то имеет место

Предложение 5.6. *Предположим, что K неразветвлено над S, так что π — униформизирующая K. Тогда*

DIF3. $\nu(D(K_m/K)) \geqslant \frac{m}{\alpha} - \frac{1}{\alpha(q_S^h - 1)}$, *где* $\alpha = e(S)$, q_S — *число элементов в поле вычетов* S, h — O_S-*высота* f.

DIF4. $K(e_i^m)$ *вполне разветвлено над* K, e_i^m *является униформизирующей* $K(e_i^m)$ *и* ν *(период* de_i^m*)* $= \frac{m}{\alpha} - \frac{1}{\alpha(q_S^h - 1)}$. ■

§ 6. Явные формулы

6.1. Выражение $\varphi_{L,n}^i$ через $\psi_{M,m}^i$. В этом пункте мы покажем, как можно выразить гомоморфизмы $\varphi_{L,n}^i$ через $\psi_{M,m}^i$, где $M = L_t$ при достаточно большом t.

Итак, пусть $L \supset K_n$, $\varphi_{L,n}^i : L^n \to \frac{R_L}{\pi^n R_L}$ — соответствующие гомоморфизмы.

Предложение 6.1. *Пусть m таково, что* $\nu(f^{(m-n)}(x)) > \frac{1}{p-1}$ $\forall x \in E(\mu_L)$. *Пусть (m, t) — допустимая пара,* $M = L_t$. *Тогда* $N_{M/L}(M^*) \subset L^n$, $\mathrm{Tr}_{M/L}$ *задает гомоморфизм* $\frac{R_{M,1}}{\pi^m R_{M,1}}$ *в* $\frac{L}{\pi^n R_L}$ *и имеет место формула*

$\varphi\psi 2$. $\varphi_{L,n}^i(N_{M/L}(b)) = \mathrm{Tr}_{M/L}(\psi_{M,m}^i(b)) \quad \forall b \in M^*$.

Замечание. В частности, $\mathrm{Tr}_{M/L}(\psi_{M,m}^i(b)) \subset \frac{R_L}{\pi^n R_L}$.

Доказательство. Прежде всего заметим, что $\mathrm{Tr}_{M/L}(\pi^m R_{M,1}) \subset \pi^n R_L$. Действительно, согласно $\psi 2$ — аналогу $\varphi 2 : 3.5$, $\mathrm{Tr}_{M/L}(R_{M,1}) \subset R_{L,1}$. Из условия на m следует, что $\pi^{m-n} T_L \subset T_{L,1}$. Отсюда

$$\frac{1}{\pi^{m-n}} R_L \supset R_{L,1} \Rightarrow \pi^m R_{L,1} \subset \pi^n R_L.$$

Далее, имеем: $(N_{M/L}(b),\ x)_{L,n} = (b,\ x)_{M,n}$ (согласно $SP\,3:3.3$) $= (b,\ f^{(m-n)}(x))_{M,m}$ (согласно $SP\ 6:3.3$). Так как $\nu(f^{(m-n)}(x)) > \frac{1}{p-1}$, то, согласно $\psi\ 1:4.1$,

$$\begin{aligned}(b,\ f^{(m-n)}(x))_{M,m}^i &= \mathrm{Tr}_{M/S}(\psi_{M,m}^i(b)\, l(f^{(m-n)}(x))) = \\ &= \pi^{m-n}\, \mathrm{Tr}_{L/S}(\mathrm{Tr}_{M/L}(\psi_{M,m}^i(b))\, l(x)).\end{aligned}$$

Поскольку $\mathrm{Tr}_{M/L}(\psi_{M,m}^i(b)) \in \frac{L}{\pi^n R_L}$, выражение в скобках определено $(\mathrm{mod}\, \pi^n C)$ $(C = O_S)$. Чтобы получить $(N_{M/L}(b),\ x)_{L,n}^i$, мы должны разделить все на π^{m-n}. Остается $\mathrm{Tr}_{L/S}(\mathrm{Tr}_{M/L}(\psi_{M,m}^i(b))\, l(x))$. Для завершения доказательства требуется только учесть формулу-определение $\varphi 1 : 3.5$ (то, что

$\mathrm{Tr}_{M/L}(\psi^i_{M,m}(b)) \in \dfrac{R_L}{\pi^n R_L}$, следует из того, что левая часть равенства (т. е. $(N_{M/L}(b), x)^i_{L,n}$) принадлежит $\dfrac{C}{\pi^n C}$). ■

Предложение 6.2. *В качестве m в предложении* 6.1 *можно взять любое* $m > n + \alpha \log_p \left(\dfrac{e(L)}{p-1}\right) + \dfrac{\alpha}{p-1}$.

Доказательство. Пусть $k = m - n$. Так как $f^{(k)'}$ делится на π^k, то в слагаемом $a_i X^i$ ряда $f^{(k)}$ $\nu(a_i) + \nu(i) \geqslant \dfrac{k}{\alpha}$. Если $\nu(a_i) > \dfrac{1}{p-1}$, то все хорошо, если $\nu(a_i) \leqslant \dfrac{1}{p-1}$, то $\nu(i) \geqslant \dfrac{k}{\alpha} - \dfrac{1}{p-1}$. Но тогда

$$\nu(x^i) \geqslant \frac{p^{\frac{k}{\alpha} - \frac{1}{p-1}}}{e(L)} > \frac{1}{p-1} \quad \forall x \in \mu_L,$$

так как $\dfrac{k}{\alpha} - \dfrac{1}{p-1} > \log_p\left(\dfrac{e(L)}{p-1}\right)$. Значит,

$$\nu(f^{(k)}(x)) > \frac{1}{p-1} \quad \forall x \in \mu_L. \ ■$$

6.2. Выражение $\psi^i_{M,m}$ через дифференцирования. Пусть $M \supset K_t$, (m, t) — допустимая пара, $D^i_{M,m} : O_M \to \dfrac{R_{M,1}}{\pi^m R_{M,1}}$, $D^i_{M,m}(x) = \psi^i_{M,m}(x)x$. Предположим, что π^m делит $D(M/K)$. Пусть π_M — униформизирующая M. Согласно следствию 5.2, мы можем построить дифференцирования $D^i : O_M \to \dfrac{R_{M,1}}{\pi^m R_{M,1}}$ над A такие, что $D^i(\pi_M) = D^i_{M,m}(\pi_M)$. Именно, если $g \in \widetilde{A}[[X]]$, где $\widetilde{A}$ — кольцо целых чисел максимального неразветвленного над K подрасширения M, то $D^i(g(\pi_M)) = g'(\pi_M) D^i_{M,m}(\pi_m)$. Из $D5:4.4$ следует, что $D^i_{M,m}$ совпадает с D^i на μ_M. Из $D1:4.4$, $D1:5.1$ следует, что $D^i_{M,m}$ совпадает с D^i $\left(\mathrm{mod}\ \dfrac{\pi^m}{\pi_M} R_{M,1}\right)$: достаточно сравнить $D^i(\pi_M a)$ и $D^i_{M,m}(\pi_M a)$, где $a \in O_M$. Значит,

$$D^i_{M,m} : O_M \to \frac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$$

— дифференцирование над A. Из предложения 5.3 следует, что $\pi^m \mid D(M/K)$, если $\dfrac{t-m}{\alpha} \geqslant c_1$, где c_1 — константа из этого предложения. Итак, мы доказали

Предложение 6.3. *Пусть $M \supset K_t$, (m, t) — допустимая пара, причем такая, что $\pi^m | D(M/K)$, например, это так, если $\dfrac{t-m}{\alpha} \geqslant c_1$, где c_1 — кон-*

станта из предложения 5.3. *Тогда* $D^i_{M,m}: O_M \to \dfrac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$ $\left(\text{редукция } D^i_{M,m}\right.$ *в* $\left.\dfrac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}\right)$ — *дифференцирование над* A. ■

Покажем, как $\psi^i_{M,m}$ выражаются через дифференцирования

$$D^i_{M,m}: O_M \to \frac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$$

(при выполнении условий предложения 6.3). Очевидно,

$$\psi D1. \quad \begin{cases} \psi^i_{M,m}(\pi_M) = \dfrac{D^i_{M,m}(\pi_M)}{\pi_M} \left(\operatorname{mod} \dfrac{\pi^m}{\pi^2_M} R_{M,1}\right), \\ \psi^i_{M,m}(u) = \dfrac{D^i_{M,m}(u)}{u} \left(\operatorname{mod} \dfrac{\pi^m}{\pi_M} R_{M,1}\right), \text{ где } u \in U_M, \\ \psi^i_{M,m}(\pi^k_M u) = k\psi^i_{M,m}(\pi_M) + \psi^i_{M,m}(u) \quad (k \in \mathbf{Z}). \end{cases}$$

Очевидно, что $\psi^i_{M,m}$, определенные по $D^i_{M,m}$ таким образом, не зависят от выбора униформизирующей π_M.

$D^i_{M,m}: O_M \to \dfrac{R_{M,1}}{\pi^m R_{M,1}}$ были определены через $\psi^i_{M,m}$. Теперь, убедившись, что при определенных условиях $D^i_{M,m}$ являются дифференцированиями, мы хотим, воспользовавшись простотой классификации и конструкции дифференцирований, а также их хорошими функториальными свойствами, выразить $\psi^i_{M,m}$, а затем и $\varphi^i_{L,n}$, через $D^i_{M,m}$, построенные явно. Как мы знаем (см. предложение 5.1 и следствие 5.2), дифференцирование $D: O_M \to W$ над A определяется и явно строится по своему значению на π_M — униформизирующей M. Аналогично, если ω — дифференциальная форма такая, что подмодуль, порожденный ей в $\Omega_A(O_M)$, достаточно велик, то дифференцирование $D: O_M \to W$ над A определяется и строится с точностью до дифференцирований малого периода по (D, ω). В нашем случае естественно в качестве ω брать de^t_i, имея в виду то, что, согласно DIF 2: 5.3, периоды de^t_i в $\Omega_A(O_{K_t})$ достаточно велики. Присоединяя к полю $L \supset K_n$ достаточно много элементов $\varkappa: M = L_t$, где t достаточно велико, мы убедимся, что $D^i_{M,m}$ однозначно строятся по значениям $D^i_{M,k}(e^t_j)$, где $m \leqslant k \leqslant t$. Далее, $D^i_{M,k}(e^t_j)$ могут быть выражены через инварианты представления G_K на модуле Тейта $\delta: G_K \to GL_h(C)$. Возвращение в поле L будет обеспечено предложением 6.1: $\varphi^i_{L,n}(N_{M/L}(b))$ будет выражено через $\psi^i_{M,m}(b)$, построенное по $D^i_{M,m}$ с помощью $\psi D1$.

В случае формального группового закона Любина — Тейта значения инвариантов могут быть явно определены с помощью явного закона взаимности Любина — Тейта (см. теорему 7.2), так что в этом случае будут получены полностью явные формулы для $\varphi^i_{L,n}(N_{M/L}(\mathfrak{b}))$. Такова программа финальной части работы.

6.3. Значения $D(r(e^n_i))$. Построение дифференцирований. Пусть $M \supset K_t$, $\beta = (m, t)$ — допустимая пара. Если $a \in M^*$, то $\delta_{m+t}(\theta_M(a))$ (см. определение δ_n в пункте 3.3), где $\theta_M : M^* \to G^{ab}_M$ — отображение взаимности, $\equiv E\,(\mathrm{mod}\,\pi^t)$, так как элементам $G(M_{m+t}/M)$ соответствуют в $GL_h\left(\frac{C}{\pi^{m+t}C}\right)$ матрицы $\equiv E\,(\mathrm{mod}\,\pi^n)$. Поэтому имеем характеры (гомоморфизмы) $\chi_{M,\beta;i,j} : M^* \to \frac{C}{\pi^m C}$ такие, что

$\chi 1.$ $\quad \delta_{m+t}(\theta_M(a)) = E + \pi^t(\chi_{M,\beta;i,j}(a)) \in GL_h\left(\frac{C}{\pi^{m+t}C}\right).$

Для $M = K_t$ будем писать просто $\chi_{\beta;i,j}$. Из SP 3 : 3.3 следует

$\chi 2.$ $\quad \chi_{M,\beta;i,j}(a) = \chi_{\beta;i,j}(N_{M/K_t}(a))$.

Из определения спаривания $(\ ,\ )_{M,m}$ следует, что

$$((a, v)^i_{M,m}) = (\chi_{M,\beta;i,j}(a))(v^j),$$

где $v \in \varkappa_t$, (v^j) — столбец координат. В частности,

$\chi 3.$ $\quad (a, e^t_j)^i_{M,m} = \chi_{M,\beta;i,j}(a)$.

Согласно следствию 4.2, спаривание $V_{M,1} \otimes E(\mu_M) \to \varkappa_m$ C-линейно. Используя стандартное рассуждение (см. предложение 3.2 и его доказательство), видим, что $\chi_{M,\beta;i,j}$ однозначно определяют константы $c_{M,\beta;i,j} \in \frac{R_{M,1}}{\pi^m R_{M,1}}$ такие, что

$c\chi 1.$ $\quad \chi_{M,\beta;i,j}(u) = \mathrm{Tr}_{M/S}(\log(u)\, c_{M,\beta;i,j}) \quad \forall\, u \in V_{M,1}$.

Из $\chi 2$ следует, что $c_{M,\beta;i,j}$ есть образ $c_{\beta;i,j}$ при естественном отображении $\frac{R_{t,1}}{\pi^m R_{t,1}} \to \frac{R_{M,1}}{\pi^m R_{M,1}}$ ($R_{t,1} \subset R_{M,1}$ согласно $\psi 3$ — аналогу $\varphi 3 : 3.5$), где $R_{t,1} = R_{N,1}$ для $N = K_t$, а $c_{\beta;i,j} = c_{N,\beta;i,j}$. В дальнейшем, когда будет ясно, о каком поле M идет речь, под $\bar{c}_{\beta;i,j}$ мы подразумеваем образ $c_{\beta;i,j}$ в $\frac{R_{M,1}}{\pi^m R_{M,1}}$: $c_{M,\beta;i,j} = \bar{c}_{\beta;i,j}$. Из $\chi 3$, $c\chi 1$ и $\rho 1 : 4.3$ следует

$\rho c1.$ $\quad \rho^i_{M,m}(e^t_j) = \bar{c}_{\beta;i,j}$.

Из $SP7 : 3.3$ и $\rho 1 : 4.3$ следует, что если $g : (F, e_j) \to (\tilde{F}, \tilde{e}_j)$ — изоморфизм, то $\tilde{\rho}^i_{M,m}(g(x)) = \rho^i_{M,m}(x)$. Из $\rho c1$ тогда вытекает

$c1.$ *$c_{\beta;i,j}$ являются инвариантами класса изоморфизма (F, e_j).*

Из $\psi\rho 1 : 4.3$, $\rho c1$ следует

Предложение 6.4. *Пусть $M \supset K_t$, $\beta = (m, t)$ — допустимая пара. Если $r(X)$ — t-норменный ряд для F, то имеет место формула*

$Drel.$ $\quad \psi^i_{M,m}(r(e^t_j))\, r(e^t_j) = D^i_{M,m}(r(e^t_j)) = -r'(e^t_j)\,\frac{\bar{c}_{\beta;i,j}}{l'(e^t_j)}$. ■

Пусть $L \supset K$. По определению

$$R_{L,1} = \left\{ y \in L \mid \mathrm{Tr}_{L/S}(yw) \in C \quad \forall w \in L \mid \nu(w) > \frac{1}{p-1} \right\}.$$

Более явно

$$R_{L,1} = \left\{ y \in L \mid \nu_L(y) \geqslant -\nu_L(D(L/S)) - \left[\frac{e(L)}{p-1}\right] - 1 \right\},$$

где $\nu_L = \nu e(L)$ — сюръективное нормирование L^* в $\mathbf{Z}$: $\nu_L(\pi_L) = 1$, если π_L — униформизирующая L. В частности, $R_{L,1}$ — идеал (дробный) кольца O_L. Поскольку $\left[\frac{e(L)}{p-1}\right] = \frac{e(L)}{p-1} - \xi_L$, где $0 \leqslant \xi_L < 1$, то $R_{L,1} = \Big\{ y \in L \mid \nu(y) \geqslant$ $\geqslant -\nu(D(L/S)) - \frac{1}{p-1} - \frac{\zeta}{e(L)} \Big\}$, где $0 < \zeta_L \leqslant 1$. Отсюда очевидно, что идеал

$$R'_{L,1} = \left\{ y \in L \mid \nu(y) \geqslant -\nu(D(L/S)) - \frac{1}{p-1} \right\}$$

является O_L-подмодулем $R_{L,1}$, причем $\pi_L R_{L,1} \subset R'_{L,1}$. Вообще говоря, $R'_{L,1} \neq R_{L,1}$ и в этом случае, очевидно, $R'_{L,1} = \pi_L R_{L,1}$. Пусть $M \supset L$. Так как $D(M/S) = D(M/L) D(L/S)$, то $R'_{M,1} = (1/D(M/L)) R'_{L,1}$.

Пусть $\beta = (k, t)$ — допустимая пара. Напомним, что через $R_{t,1}$ мы обозначаем $R_{N,1}$, где $N = K_t$. Соответственно, $R'_{t,1} \overset{\mathrm{def}}{=} R'_{N,1}$. Предположим, что $\pi^k \mid D(K_t/K)$. Пусть π_t — униформизирующая K_t. Пусть $a_j \in O_{K_t}$ — такой элемент, что $de^t_j = a_j d\pi_t$. a_j определяется с точностью до слагаемого из $D(K_t/K) \supset \pi^k O_{K_t}$. Если π'_t — другая униформизирующая K_t, то $d\pi_t = \varepsilon d\pi'_t$, где ε — единица. Поэтому идеал $a_j R'_{t,1} + \frac{\pi^k}{\pi_t} R'_{t,1}$ зависит лишь от de^t_j.

По определению, $c_{\beta;i,j} \in \frac{R_{t,1}}{\pi^k R_{t,1}}$. Следующее предложение уточняет местонахождение $c_{\beta;i,j}$.

Предложение 6.5. *Пусть* $\beta = (k, t)$ — *допустимая пара, причем такая, что* $\pi^k \mid D(K_t/K)$, *например, это так, если* $\frac{t-k}{\alpha} \geqslant c_1$, *где* c_1 — *константа из предложения* 5.3. *Пусть* π_t — *униформизирующая* K_t, $a_j \in O_{K_t}$ — *такой элемент, что* $de^t_j = a_j d\pi_t$. *Тогда*

$$c2. \qquad c_{\beta;i,j} \in \frac{a_j R'_{t,1} + \frac{\pi^k}{\pi_t} R'_{t,1} + \pi^k R_{t,1}}{\pi^k R_{t,1}}.$$

Доказательство. Пусть $\lambda_{i,j}$ — представитель $c_{\beta;i,j}$ в $R_{t,1}$. Нужно показать, что $\lambda_{i,j} \in a_j R'_{t,1} + \frac{\pi^k}{\pi_t} R'_{t,1}$. Пусть $M \supset K_t$, π_M — униформизирующая M. Пусть $b \in O_M$ — такой элемент, что $d\pi_t = b d\pi_M$. Тогда $bO_M = D(M/K_t)$. Положим $\beta_j = b a_j \in O_M$. Тогда $de^t_j = \beta_j d\pi_M$. Согласно предложению 6.3,

$$D^i_{M,k} : O_M \to \frac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}}$$

являются дифференцированиями над A. Отсюда и из $Drel$ имеем:

$$D^i_{M,k}(r(e^t_j)) = -r'(e^t_j)\frac{\bar{c}_{\beta;i,j}}{l'(e^t_j)} \Rightarrow r'(e^t_j)\beta_j D^i_{M,k}(\pi_M) =$$

$$= -r'(e^t_j)\frac{\bar{c}_{\beta;i,j}}{l'(e^t_j)}\left(\operatorname{mod}\frac{\pi^k}{\pi_M}R_{M,1}\right).$$

Здесь $\bar{c}_{\beta;i,j}$ — образ $c_{\beta;i,j}$ в $\dfrac{R_{M,1}}{\pi^k R_{M,1}}$ $(R_{t,1}\subset R_{M,1})$. Отсюда следует, что $\lambda_{i,j}\in \in \beta_j R_{M,1}+\dfrac{\pi^k}{\pi_M}R_{M,1}$. Положим M=поле, полученное присоединением к K_t корня уравнения $X^n=\pi_t$, где $(n, p)=1$. $X^n-\pi_t$—многочлен Эйзенштейна, так что $e(M)=ne(K_t)$, $D(M/K_t)=\dfrac{\pi_t}{\pi_M}$. Значит,

$$\nu(\lambda_{t,j})\geqslant\min\left(\nu(\beta_j)-\nu(D(M/S))-\frac{1}{p-1}-\frac{\zeta_M}{ne(K_t)},\ \nu\left(\frac{\pi^k}{\pi_M}\right)-\nu(D(M/S))-\right.$$
$$\left.-\frac{1}{p-1}-\frac{\zeta_M}{ne(K_t)}\right).$$

Это эквивалентно тому, что

$$\nu(\lambda_{i,j})\geqslant\min\left(\nu(a_j)-\nu(D(K_t/S))-\frac{1}{p-1}-\frac{\zeta_M}{ne(K_t)},\right.$$
$$\left.\nu\left(\frac{\pi^k}{\pi_t}\right)-\nu(D(K_t/S))-\frac{1}{p-1}-\frac{\zeta_M}{ne(K_t)}\right).$$

Устремляя n к ∞, видим, что

$$\nu(\lambda_{t,j})\geqslant\min\left(\nu(a_j)-\nu(D(K_t/S))-\frac{1}{p-1},\right.$$
$$\left.\nu\left(\frac{\pi^k}{\pi_t}\right)-\nu\left(D(K_t/S)\right)-\frac{1}{p-1}\right),$$

а это эквивалентно тому, что $\lambda_{i,j}\in a_j R'_{t,1}+\dfrac{\pi^k}{\pi_t}R'_{t,1}$. ■

По-прежнему предполагаем, что $\pi^k | D(K_t/K)$. Покажем, что если $M\supset K_t$, то существуют дифференцирования

$$D^i: O_M\to\frac{R_{M,1}}{\dfrac{\pi^k}{\pi_M}R_{M,1}}$$

над A такие, что $D^i(e^t_1)=\eta_i=-\dfrac{c_{\beta;i,1}}{l'(e^t_1)}$. Это значит, что если $\beta_1\in O_M$—такой элемент, что $de^t_1=\beta_1\,d\pi_M$, то $\forall\, i$ должен существовать элемент $\gamma_i\in\dfrac{R_{M,1}}{\dfrac{\pi^k}{\pi_M}R_{M,1}}$ такой, что $\eta_i=\beta_i\gamma_i$: тогда положим $D^i(\pi_M)=\gamma_i$, $D^i(g(\pi_M))=g'(\pi_M)D^i\times$

$\times(\pi_M)$ $\forall g \in \widetilde{A}[[X]]$, где $\widetilde{A}$ — кольцо целых чисел максимального неразветвленного над K подрасширения M. Пусть $\lambda_{i,1}$ — представитель $c_{\beta;i,1}$ в $R_{t,1}$. Согласно предложению 6.5, $\lambda_{i,1} \in a_1 R'_{t,1} + \frac{\pi^k}{\pi_t} R'_{t,1}$, где $de_1^t = a_1\, d\pi_t$. Пусть $d\pi_t = b\, d\pi_M$. Положим $\beta_1 = a_1 b$. Имеем:

$$\frac{1}{b} R'_{t,1} = (1/D(M/K_t))\, R'_{t,1} = R'_{M,1} \subset R_{M,1},$$

$$\frac{\pi^k}{\pi_t} R_{t,1} \subset \frac{\pi^k}{\pi_M} \frac{D(M/K_t)}{\pi_t/\pi_M} R'_{M,1} \subset \frac{\pi^k}{\pi_M} R_{M,1},$$

так как $D(M/K_t)$ делится на $\frac{\pi_t}{\pi_M}$: $\nu_M(D(M/K_t)) \geqslant e(M/K_t) - 1$ (общее неравенство). Значит,

$$\eta_i = -\frac{1}{l'(e_1^t)} \lambda_{i,1} \in \beta_1 \frac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}},$$

что и требовалось показать.

Пусть $\gamma_i \in \dfrac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}}$ таково, что $\eta_i = \beta_1 \gamma_i$. Очевидно, γ_i определено $\left(\operatorname{mod} \frac{\pi^k}{\pi_M \beta_1} R_{M,1}\right)$. Пусть $m \leqslant k$. Тогда дифференцирование $D_1^i : O_M \to \dfrac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$ над A такое, что $D_1^i(\pi_M) = \bar{\gamma}_i$, где $\gamma_i \in \dfrac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}}$, $\beta_1\gamma_i = \eta_i$, определено однозначно, если $\pi^m \Big| \frac{\pi^k}{\beta_1}$. Очевидно, что при этом D_1^i совпадает с редукцией в $\dfrac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$ любого дифференцирования $D^i : O_M \to \dfrac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}}$ над A такого, что $D^i(e_1^t) = \eta_i$.

Мы можем без ограничения общности считать, что ν (период $de_1^t) \geqslant \frac{t}{\alpha} - c_1$ (см. начало доказательства оценок снизу в предложении 5.3). Условие $\pi^m \Big| \frac{\pi^k}{\beta_1}$ будет следовать тогда из условия $\frac{m}{\alpha} \leqslant \frac{k}{\alpha} - \nu(D(M/K)) + \frac{t}{\alpha} - c_1$.

Предложение 6.6. *Пусть $M \supset K_t$, $\beta = (k, t)$ — допустимая пара, причем такая, что $\frac{t-k}{\alpha} \geqslant c_1$, где c_1 — константа из предложения* 5.3. *Пусть $m \leqslant k$ таково, что*

$$\frac{m}{\alpha} + \nu(D(M/K)) + c_1 \leqslant \frac{k}{\alpha} + \frac{t}{\alpha}.$$

Тогда редукция $D^i_{M,m}: O_M \to \frac{R_{M,1}}{\pi^m R_{M,1}}$ *в* $\frac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$ *будет* (*согласно предложению* 6.3) *дифференцированием над* A, *которое определяется следующим образом. Существуют дифференцирования* $D^i: O_M \to \frac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}}$ *над* A *такие, что* $D^i(e_1^t) = -\frac{\bar c_{\beta:i,1}}{l'(e_1^t)}$, *их редукции в* $\frac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$ *определены однозначно и совпадают с*

$$D^i_{M,m}: O_M \to \frac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}.$$

Более явно, если π_M — *униформизирующая* M, $de_1^t = \beta_1 d\pi_{M_-}$, *то* $\gamma_i \in \frac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}}$ *такие, что* $\beta_1\gamma_i = -\frac{\bar c_{\beta:i,1}}{l'(e_1^t)}$ *существуют и определены однозначно* $\left(\mathrm{mod}\ \frac{\pi^m}{\pi_M} R_{M,1}\right)$. *Тогда* $D^i_{M,m}(\pi_M) = \bar\gamma_i$, $D^i_{M,m}(g(\pi_M)) = g'(\pi_M)\bar\gamma_i$, *где* $g \in \widetilde{A}[[X]]$, $\widetilde{A}$ —*кольцо целых чисел максимального неразветвленного над* K *подрасширения* M ($\bar\gamma_i$ — *редукция* γ_i).

Доказательство. Учитывая рассуждения перед формулировкой предложения, достаточно заметить только, что $D^i_{M,m}: O_M \to \frac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$ есть редукция (см. ψ5 — аналог ψ5 : 3.5) $D^i_{M,k}: O_M \to \frac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}}$, которое, согласно предложению 6.3, есть дифференцирование над A, причем отсюда и из $Dre1$ следует, что $D^i_{M,k}(e_1^t) = -\frac{\bar c_{\beta:i,1}}{l'(e_1^t)}$. ■

6.4. Описание $\varphi^i_{L,n}$ в терминах дифференцирований и норменного отображения из L_t в L. Используя результаты предыдущих трех пунктов этого параграфа, мы вычислим $\varphi^i_{L,n}$ на норменной подгруппе, соответствующей расширению L_t/L при достаточно большом t, в терминах норменного отображения $N: L_t^* \to L^*$ и дифференцирований O_{L_t} над A.

В частности, если L' обозначает пересечение норменных подгрупп $N(L_r^*)$, $r = 1, 2, \ldots$, то $\varphi^i_{L,n}$ будет вычислено на L'. По теории полей классов $\frac{L^*}{L'} \simeq G(L_\infty \cap L^{ab}/L)$.

ТЕОРЕМА 6.7. *Пусть* $L \supset K_n$, $\varphi^i_{L,n} : L^n \to \dfrac{R_L}{\pi^n R_L}$ — *соответствующие гомоморфизмы. Пусть* $m = n + 2 + \left[\alpha \log_p \left(\dfrac{e(L)}{p-1}\right) + \dfrac{\alpha}{p-1}\right]$, *где* $e(L)$ — *индекс ветвления* L *над* $\mathbf{Q}_p$, α — *индекс ветвления* S *над* $\mathbf{Q}_p$. *Пусть* k *столь велико, что*

$$\frac{t}{\alpha} + \frac{k}{\alpha} \geqslant \frac{m}{\alpha} + c_1 + \nu(D(M/K)), \quad \frac{k}{\alpha} + 1 \geqslant c_1,$$

где $t = 2k + \alpha$, $M = L_t$. *Например, это так при* $\dfrac{k}{\alpha} \geqslant \dfrac{m}{\alpha} + \dfrac{\log_2(2k+\alpha)}{p-1} + c_1 + c_2 + \nu(D(L/K))$ (c_1, c_2 — *константы из предложения* 5.3). *Тогда* M, t, k, m *удовлетворяют предложению* 6.6. *Пусть*

$$D^i_{M,m} : O_M \to \frac{R_{M,1}}{\dfrac{\pi^m}{\pi_M} R_{M,1}}$$

— *дифференцирования над* A, *построенные как в предложении* 6.6,

$$\psi^i_{M,m} : M^* \to \frac{R_{M,1}}{\dfrac{\pi^m}{\pi^2_M} R_{M,1}}$$

— *логарифмические производные, построенные по* $D^i_{M,m}$ *как в* $\psi D1$: 6.2. *Тогда* $N_{M/L}(M^*) \subset L^n$ *и имеет место формула*

$\varphi\psi 3$. $\quad \varphi^i_{L,n}(N_{M/L}(b)) = \mathrm{Tr}_{M/L}(\psi^i_{M,m}(b))$ $\left(\textit{определено в } \dfrac{R_L}{\pi^n R_L}\right)$ $\forall\, b \in M^*$.

Доказательство. Очевидно, $(k, 2k+\alpha)$ — допустимая пара. Оценим сверху $\nu(D(M/K))$. Из башни $L_t \supset L \supset K$ и оценки сверху в $DIF1$: 5.3 вытекает, что

$$\nu(D(M/K)) \leqslant \frac{t}{\alpha} + \frac{\log_2 t}{p-1} + c_2 + \nu(D(L/K)),$$

откуда следует пример в теореме. Так как из условия на k следует, что $\dfrac{t-k}{\alpha} = \dfrac{k}{\alpha} + 1 \geqslant c_1$, то M, t, k, m удовлетворяют условиям предложения 6.6. Остается последовательно применить предложения 6.1, 6.2, 6.3, ψD 1 : 6.2 и предложение 6.6. Следует только добавить, что условие на m обеспечивает включение $\mathrm{Tr}_{M/L}\left(\dfrac{\pi^m}{\pi^2_M} R_{M,1}\right) \subset \pi^n R_L$: так как

$$m - 1 \geqslant n + \alpha \log_p \left(\frac{e(L)}{p-1}\right) + \frac{\alpha}{p-1},$$

то

$$\mathrm{Tr}_{M/L}\left(\pi^{m-1} \frac{\pi}{\pi^2_M} R_{M,1}\right) \subset \mathrm{Tr}_{M/L}(\pi^{m-1} R_{M,1}) \subset \pi^n R_L$$

согласно предложениям 6.1 и 6.2 ($\pi^2_M \mid \pi$, так как $\pi^k \mid D(M/K) \Rightarrow e(M/K) > 1$). Поэтому в формуле $\varphi\psi 2$ из предложения 6.1, примененной в условиях теоремы, мы можем заменить $\psi^i_{M,m}: M^* \to \dfrac{R_{M,1}}{\pi^m R_{M,1}}$ на его редукцию в $\dfrac{R_{M,1}}{\dfrac{\pi^m}{\pi_M^2} R_{M,1}}$. ■

Замечание. Как следует из доказательства оценки сверху в $DIF1: 5.3$, в качестве c_2 можно взять

$$c_2 = \frac{2}{p-1} + \frac{2\nu(\pi)\,p}{(p-1)^2} + \nu(D(K_{2\alpha-1}/K)).$$

Следствие 6.8. *Если π — униформизирующая K, то в теореме 6.7 в качестве константы c_1 можно взять*

$$c_1 = \frac{1}{\alpha(q_S^h - 1)},$$

где q_S — число элементов поля вычетов S, h — C-высота f.

Доказательство. Утверждение следствия вытекает из предложения 5.4: в качестве константы c_1 в оценках снизу в предложении 5.3 в этом случае можно взять $c_1 = \dfrac{1}{\alpha(q_S^h - 1)}$. ■

6.5. Аналог теоремы 6.7, получающийся переменой ролей мультипликативной и формальной групп в представлении для спаривания. Пусть $M \supset K_m$. Мы ввели гомоморфизмы $\varphi^i_{M,m}$, $\psi^i_{M,m}$, интерпретируя с помощью спаривания $(,)_{M,m}$ элементы мультипликативной группы как характеры формальной группы и используя гомоморфизм $l: E(\mu_M) \to M$. Можно, наоборот, интерпретировать элементы формальной группы как характеры мультипликативной группы и использовать гомоморфизм log: $V_M \to M$, где V_M — группа главных единиц.

Предположим, что $M \supset K_t$, причем (m, t) — допустимая пара. Очевидно, что построенные ранее гомоморфизмы $\rho^i_{M,m}$ играют при таком подходе роль $\psi^i_{M,m}$. Их свойства аналогичны свойствам $\psi^i_{M,m}$. Предположим, что $\pi^m \mid D(M/K)$. Пусть

$$D^i_{M,m}: O_M \to \frac{R_{M,1}}{\dfrac{\pi^m}{\pi_M} R_{M,1}}$$

— соответствующие дифференцирования (см. предложение 6.3). Тогда $\psi^i_{M,m}$ является мультипликативной логарифмической производной, ассоциированной с дифференцированием $D^i_{M,m}$ (см. $\psi D1$: 6.2), а $\rho^i_{M,m}$ является, что следует из $\psi\rho 1: 4.3$, формальной логарифмической производной, ассоциированной с $-D^i_{M,m}$:

$$\rho^i_{M,m}(x) = -D^i_{M,m}(x)\, l'(x) \quad \left(\operatorname{mod} \frac{\pi^m}{\pi_M} R_{M,1}\right).$$

Соответственно, можно построить гомоморфизмы, аналогичные $\varphi^i_{M,m}$ и обладающие аналогичными свойствами. Для краткости мы, не вводя для этих гомоморфизмов обозначений и не обсуждая их подробно, сразу сформулируем теорему — аналог теоремы 6.7, которая доказывается аналогично последней.

ТЕОРЕМА 6.9. *Пусть* $L \supset K_n$, *и пусть*

$$m = n + 1 + \alpha\left(1 + \left[\log_p\left(\frac{e(L)}{p-1}\right) + \frac{1}{p-1}\right]\right).$$

Пусть k *столь велико, что*

$$\frac{t}{\alpha} + \frac{k}{\alpha} \geqslant \frac{m}{\alpha} + c_1 + \nu(D(M/K)), \qquad \frac{k}{\alpha} + 1 \geqslant c_1,$$

где $t = 2k + \alpha$, $M = L_t$. *Например, это так при*

$$\frac{k}{\alpha} \geqslant \frac{m}{\alpha} + \frac{\log_2(2k+\alpha)}{p-1} + c_1 + c_2 + \nu(D(L/K)).$$

Тогда M, t, k, m *удовлетворяют предложению* 6.6.

Пусть

$$D^i_{M,m} : O_M \to \frac{R_{M,1}}{\dfrac{\pi^m}{\pi_M} R_{M,1}}$$

— *дифференцирования над* A, *построенные как в предложении* 6.6, *и пусть*

$$\rho^i_{M,m} : E(\mu_M) \to \frac{R_{M,1}}{\dfrac{\pi^m}{\pi_M} R_{M,1}}$$

— *формальные логарифмические производные, ассоциированные с дифференцированиями* $(-D^i_{M,m}) : \rho^i_{M,m}(x) = -D^i_{M,m}(x)\, l'(x)$. *Тогда* $\mathrm{Tr}_{M/L}$ *задает гомоморфизм* $\dfrac{R_{M,1}}{\dfrac{\pi^m}{\pi_M} R_{M,1}}$ *в* $\dfrac{L}{\pi^n J_L}$, *где*

$$J_L = \{y \in L \mid \mathrm{Tr}_{L/S}(yw) \in C \quad \forall\, w \in \log(V_L)\},$$

и имеют место формулы

$$(u, N^F_{M/L}(y))^i_{L,n} = \mathrm{Tr}_{L/S}(\log(u)\, \mathrm{Tr}_{M/L}(\rho^i_{M,m}(y))),$$

где $N^F_{M/L}$ — *норма в формальной группе*, $\forall\, u \in V_L$, $y \in E(\mu_M)$. ■

Дополнение к теоремам 6.7, 6.9. В качестве оценки для k можно также взять оценку

$$\frac{k}{\alpha} \geqslant \frac{m}{\alpha} + \frac{\log_2((2k+\alpha)\, r)}{p-1} + 2c_1 + 2c_2 + \nu(D(L/K_r)),$$

где r — максимальное такое, что $L \supset K_r$. Действительно, из башни $L_t \supset L \supset K_r \supset K$ следует, что

$$\nu(D(L_t/K) \leqslant \nu(D(L_t/L)) + \nu(D(L/K_r)) + \nu(D(K_r/K)).$$

Но

$$\nu(D(L_t/L)) \leqslant \nu(D(K_t/K_r)) \leqslant \frac{t}{\alpha} + \frac{\log_2(2k+\alpha)}{p-1} + c_2 + c_1 - \frac{r}{\alpha}$$

(см. $DIF1:5.3$, $DIF2:5.3$), а

$$\nu(D(K_r/K)) \leqslant \frac{r}{\alpha} + \frac{\log_2 r}{p-1} + c_2.$$

Значит,

$$\nu(D(L_t/K)) \leqslant \frac{t}{\alpha} + \frac{\log_2((2k+\alpha)r)}{p-1} + c_1 + 2c_2 + \nu(D(L/K_r)).$$

§ 7. Формальные группы Любина — Тейта

7.1. Теория формального умножения. Теория формального умножения принадлежит Любину и Тейту. Доказательства теорем, приведенных в этом пункте без доказательства, можно найти в ([2]) (глава 6, § 3).

7.1.1. Формальные A-модульные законы Любина — Тейта. Пусть K — конечное расширение $\mathbf{Q}_p$, $A=O_K$— кольцо целых чисел K, k— поле вычетов, $q=|k|$.

Пусть K_{nr}— максимальное неразветвленное расширение K, Fr — автоморфизм Фробениуса K_{nr} над K (см. пункт 3.1). Пусть $\hat{K}_{nr}$— пополнение K_{nr}, $\hat{A}_{nr}$— кольцо целых чисел $\hat{K}_{nr}$. Fr по непрерывности продолжается до автоморфизма $\hat{K}_{nr}$ над K — его мы также обозначаем через Fr. Пусть η — униформизирующая K. η остается униформизирующей и в $\hat{K}_{nr}$. Поле вычетов $\hat{K}_{nr}$— это $\bar{k}$ — алгебраическое замыкание k.

Покажем, что неподвижное подполе для Fr в $\hat{K}_{nr}$ есть K. Пусть $a\in\hat{K}_{nr}$, $\mathrm{Fr}(a)=a$. Умножая a на степень η, можно считать, что $a\in\hat{A}_{nr}$. Если $\bar{a}$ — вычет a в $\bar{k}$, то $\mathrm{Fr}(\bar{a})=\bar{a}$. Значит, $\bar{a}\in k$. Пусть $b_0\in A$, $\bar{b}_0=\bar{a}$. Тогда $a=b_0+\eta a_1$, где $a_1\in\hat{A}_{nr}$. Очевидно, $\mathrm{Fr}(a_1)=a_1$. Продолжая аналогично, получим ряд $\sum b_i\eta^i$, где $b_i\in A$, сходящийся к a. Но $\sum\limits_{i=0}^{\infty} b_i\eta^i\in A$. Значит, $a\in A$.

Пусть u — единица в $\hat{A}_{nr}$. Рассмотрим уравнение $\mathrm{Fr}(a)-ua=0$, $a\in\hat{A}_{nr}$. Если $x\in\bar{k}$, то $\mathrm{Fr}(x)-\bar{u}x=x^q-\bar{u}x$. Поэтому существует $b_0\in\hat{A}_{nr}$ такой, что $\mathrm{Fr}(b_0)-ub_0=a_1\eta$, причем $\bar{b}_0\neq 0$ ($\bar{u}\neq 0$). Аналогично, найдется $b_1\in\hat{A}_{nr}$ такой, что $\mathrm{Fr}(b_1)-ub_1=-a_1(\mathrm{mod}\,\eta)$. Тогда $\mathrm{Fr}(b_0+\eta b_1)-u(b_0+\eta b_1)=$ $=a_2\eta^2$. Продолжая таким образом, получим ряд $\Sigma b_i\eta^i$. Пусть $\varepsilon=\sum\limits_{i=0}^{\infty} b_i\eta^i$. Тогда $\mathrm{Fr}(\varepsilon)-u\varepsilon=0$, причем ε — единица. Очевидно, что при $u\equiv 1\,(\mathrm{mod}\,\eta^j)$ можно найти решение $\varepsilon\equiv 1\,(\mathrm{mod}\,\eta^j)$: можно положить $\beta_0=1$, $b_1=\ldots$ $\ldots=b_{j-1}=0$. Очевидно также, что $C_u=\{a\in\hat{A}_{nr}\,|\,\mathrm{Fr}(a)-ua=0\}$ — A-модуль. Если $a\in C_u$, то $\mathrm{Fr}\left(\frac{a}{\varepsilon}\right)=\frac{a}{\varepsilon}\Rightarrow a=\varepsilon b$, где $b\in A$. Итак, мы доказали

Предложение 7.1. *$C_u=A\varepsilon$, где ε — единица, причем $\varepsilon\equiv$ $\equiv 1\,(\mathrm{mod}(u-1))$.* ■

Следствие 7.2. *$C_1=A$.* ■

Пусть π — униформизирующая K. Обозначим через Λ_π подмножество $A[[X]]$, состоящее из рядов f таких, что

$\Lambda 1.$ $f(X)\equiv\pi X (\operatorname{mod} \deg 2)$.

$\Lambda 2.$ $f(X)\equiv X^q (\operatorname{mod} \pi)$.

Примеры: $f=\pi X+X^q$; $K=\mathbf{Q}_p$, $\pi=p$, $f=(X+1)^p-1$.

ТЕОРЕМА 7.3. 1. *Пусть $f\in\Lambda_\pi$. Формальный A-модульный закон F_f над A такой, что $[\pi]_{F_f}=f$, существует и единствен.*

2. *Пусть π, ξ — униформизирующие K, $\xi=\pi u$. Пусть $f\in\Lambda_\pi$, $g\in\Lambda_\xi$. Тогда*

$$c(\operatorname{Hom}_{on\hat{A}_{nr}}(F_f, F_g))\supset C_u. \blacksquare$$

Замечание. $\operatorname{Hom}_{on\hat{A}_{nr}}(F_f, F_g)$ обозначает множество гомоморфизмов F_f в F_g над $\hat{A}_{nr}$.

Следствие 7.4. *Если $\xi=\pi$, то $c(\operatorname{Hom}_{onA}(F_f, F_g))=A$.*

Доказательство. Пусть $t\in\operatorname{Hom}_{on\hat{A}_{nr}}(F_f, F_g)$, $c(t)\in A$. Тогда $c(t^{\mathrm{Fr}}\ominus t)=0\Rightarrow t^{\mathrm{Fr}}\ominus t=0$ (предложение 1.1)$\Rightarrow t^{\mathrm{Fr}}=t\Rightarrow t\in A[[X]]$. Здесь $\ominus$ — вычитание в $\operatorname{Hom}_{on\hat{A}_{nr}}(F_f, F_g)$. $\blacksquare$

Как мы знаем, всякий $t\in\operatorname{Hom}_{on\hat{A}_{nr}}(F_f, F_g)$ будет гомоморфизмом A-модульных законов (см. пункт 1.2). Если $a\in C_u$, то через $[a]_{f,g}$ будем обозначать гомоморфизм $c^{-1}(a)$. Если $f=g$, то $[a]_f\overset{\mathrm{def}}{=}[a]_{f,f}$. В частности, $[\pi]_f=f$.

Следствие 7.5. *F_f и F_g — законы, изоморфные над $\hat{A}_{nr}$. Если $\xi=\pi$, то F_f и F_g изоморфны над A.*

Доказательство. В качестве изоморфизма можно взять $[a]_{f,g}$, где a — единица.

7.1.2. Поля K_n, максимальное абелево расширение K и явный вид отображения взаимности $\theta_K: K^*\to G_K^{ab}$. Зафиксируем π — униформизирующую K. Пусть $f\in\Lambda_\pi$, F_f — соответствующий закон. (F_f, f) является примером пары, состоящей из формального C-модульного закона над A и $f=[\pi]_{F_f}$, где π — униформизирующая C, где $C=A$. Поэтому мы можем применять к (F_f, f) все определения, обозначения и утверждения для таких пар, введенные и полученные ранее в общем случае.

Очевидно, A-высота f равна 1, так как $q^h=p^{h_1}$, а $p^{h_1}=q$ из $\Lambda 2$. Здесь h_1 — высота f. Значит, согласно предложению 2.4, $\overleftarrow{\varkappa}=\overleftarrow{\varkappa}_f\simeq A$. Пусть e — образующая $\overleftarrow{\varkappa}$, e^n — редукция e в $\varkappa_n$: e^n — образующая $\varkappa_n\simeq\dfrac{A}{\pi^n A}$.

Как обычно, $K_n=K(\varkappa_n)$, $K_\infty=K(\overleftarrow{\varkappa})$. Поскольку при f, $g\in\Lambda_\pi$, $F_f\simeq F_g$, то K_n зависит лишь от π: $K_n=K_{\pi,n}$. K_∞ мы будем обозначать также через K_π.

Из предложения 5.4 следует, что K_n вполне разветвлено над K, e^n — униформизирующая K_n ($K_n=K(e^n)$) и $[K_n/K]=q^n-q^{n-1}$. Значит, вложение (см. пункт 3.3)

$$\delta_n: G(K_n/K)\to\left(\frac{A}{\pi^n A}\right)^*$$

— изоморфизм: $\left|\left(\frac{A}{\pi^n A}\right)^*\right| = q^n - q^{n-1}$. Соответственно $\delta: G(K_\pi/K) \to U_K = A^*$ — изоморфизм. Заметим также, что δ не зависит ни от выбора $f \in \Lambda_\pi$, ни от выбора образующей e в $\overleftarrow{\varkappa_f}$. Действительно, если $g \in \Lambda_\pi$, $\tilde{e}$ — образующая $\varkappa_g$, то $\tilde{e} = [a]_{f,g}(e)$ для некоторого $a \in A$. Пусть $\sigma \in G(K_\pi/K)$. Тогда

$$(\tilde{e})^\sigma = [a]_{f,g}([\delta(\sigma)]_f(e)) = [\delta(\sigma)]_g([a]_{f,g}(e)) = [\delta(\sigma)]_g(\tilde{e}).$$

Итак, $\delta: G(K_\pi/K) \to U_K$ — некоторый канонический изоморфизм. В частности, K_π абелево над K. Через $\theta_K: K^* \to G_K^{ab}$ мы обозначаем отображение взаимности (см. пункт 3.1).

ТЕОРЕМА 7.6. *Поля K_{nr} и K_π линейно разделены и $K^{ab} = K_{nr}K_\pi$:*

$$\begin{tikzcd}[column sep=small] & K^{ab} \arrow[dl, dash] \arrow[dr, dash] & \\ K_{nr} \arrow[dr, dash] & & K_\pi \arrow[dl, dash] \\ & K & \end{tikzcd}$$

При этом

$$\theta 1. \quad \begin{cases} \theta_K(\pi^m) = \mathrm{Fr}^m \text{ на } K_{nr},\ id \text{ на } K_\pi, \text{ где } m \in \mathbf{Z}, \\ \theta_K(u) = id \text{ на } K_{nr},\ \delta^{-1}(u^{-1}) \text{ на } K_\pi, \text{ где } u \in U_K \text{ — единицам } K. \blacksquare \end{cases}$$

Теорема 7.6 является обобщением классической теоремы о параметризации абелевых расширений $\mathbf{Q}_p$ круговыми расширениями и соответствующего явного вида отображения взаимности. Достаточно положить $K = \mathbf{Q}_p$, $\pi = p$, $f = (X+1)^p - 1$. Тогда $F_f = F_m$, $1 + \varkappa_n$ — группа корней p^n-ой степени из единицы.

7.2. Канонические дифференцирования.

7.2.1. $O_{\hat{N}}$-модули $\Omega_A(O_N)$, $D_A(O_N, W)$. Пусть N — алгебраическое расширение K. Конечные подрасширения над K в N образуют направленное множество относительно включения. Модули дифференциалов $\Omega_A(O_L)$ вместе с естественными отображениями образуют индуктивную систему. Имеется естественный гомоморфизм $\varinjlim \Omega_A(O_L) \to \Omega_A(O_N)$, индуцированный гомоморфизмами $\Omega_A(O_L) \to \Omega_A(O_N)$.

Предложение 7.7. *Отображения $\Omega_A(O_L) \to \Omega_A(O_N)$ — вложения, $\varinjlim \Omega_A(O_L) \to \Omega_A(O_N)$ — изоморфизм.*

Доказательство. Сюръективность $\varinjlim \Omega_A(O_L) \to \Omega_A(O_N)$ очевидна. Инъективность этого гомоморфизма будет следовать из того, что $\Omega_A(O_L) \to \Omega_A(O_N)$ — вложение. Покажем это. Если $\omega \in \Omega_A(O_L)$, $\omega = 0$ в $\Omega_A(O_N)$, то $\omega = 0$ в $\Omega_A(O_M)$, где M — некоторое конечное расширение L. Это следует из того, что в соотношении для ω (см. построение модуля. дифференциалов в пункте 5.1) участвует лишь конечное число символов вида cdb. Но тогда $\omega = 0$ согласно $\Omega 2: 5.2$. $\blacksquare$

Назовем расширение N сильно разветвленным, если $\forall \varepsilon > 0$ $\exists K \subset L_\varepsilon \subset N$ такое, что L_ε конечно над K, $\nu(D(L_\varepsilon/K)) > \frac{1}{\varepsilon}$.

Примеры: $N = K_\pi$, $N = \overline{K}$.

Предложение 7.8. *Пусть N сильно разветвлено. Тогда $\Omega_A(O_N)\simeq\frac{N}{O_N}$ как O_N-модуль.*

Доказательство. Выберем возрастающую башню $K\subset L^{(1)}\subset L^{(2)}\subset\ldots$ конечных расширений в N такую, что $\bigcup L^{(i)}=N$. Например, в качестве $L^{(i)}$ можно взять пересечение N с композитом всех расширений K степени i (как известно, их только конечное число). Выберем в каждом $L^{(i)}$ униформизирующую γ_i. Пусть $d\gamma_i=a_{i+1}d\gamma_{i+1}$, где $a_{i+1}\in O_{i+1}$ — кольцу целых чисел $L^{(i+1)}$. Пусть $b_1\in O_1$, $b_1O_1=D(L^{(1)}/K)$. Положим $b_{i+1}=a_{i+1}b_i$. Тогда $b_nO_n=D(L^{(n)}/K)$. Отождествим $\Omega_A(O_n)$ с $\frac{\frac{1}{b_n}O_n}{O_n}$, отобразив $d\gamma_n$ в $\frac{1}{b_n}$ (см. Ω 1 : 5.2). Очевидно, тогда отображение $\Omega_A(O_n)\to\Omega_A(O_{n+1})$ выглядит как естественное вложение $\frac{\frac{1}{b_n}O_n}{O_n}$ в $\frac{\frac{1}{b_{n+1}}O_{n+1}}{O_{n+1}}$, так что $\varinjlim\Omega_A(O_L)\simeq\simeq\varinjlim_n\Omega_A(O_n)\simeq\frac{N}{O_n}$. ■

Обозначим через $\hat N$ пополнение N, через $O_{\hat N}$ — кольцо целых чисел $\hat N$. Если $a\in O_N$, $a\neq 0$, то гомоморфизм $\frac{O_N}{aO_N}\to\frac{O_{\hat N}}{aO_{\hat N}}$, индуцированный вложением $O_N\to O_{\hat N}$, — изоморфизм, так что всякий a-периодический O_N-модуль посредством обратного изоморфизма является и $O_{\hat N}$-модулем.

Пусть W — O_N-модуль. Пусть $c\in O_N$, $b\in\mu_N$, $b\neq 0$. Обозначим через $W_{cb^{n-1}}$, $n\geqslant 1$, ядро умножения на cb^{n-1}. $W_{cb^{n-1}}$ образуют проективную систему модулей относительно умножения на b. Пусть $\overleftarrow{W}_{c,b}=\varprojlim W_{cb^{n-1}}$. Покомпонентное умножение на элементы $O_{\hat N}$ переводит проективные последовательности в проективные последовательности, так что $\overleftarrow{W}_{c,b}$ имеет структуру $O_{\hat N}$-модуля. $\mathrm{Hom}_{O_N}\left(\frac{N}{O_N},W\right)$ также обладает структурой $O_{\hat N}$-модуля: $(a\chi)(d)=\chi(ad)$.

Предложение 7.9. 1. *Пусть $N\supset K$, N сильно разветвлено. Пусть $b\in\mu_N$, $b\neq 0$, и пусть ω_n— последовательность дифференциальных форм в $\Omega_A(O_N)$ таких, что $b\omega_{n+1}=\omega_n$, $\omega_1\neq 0$. Пусть $p(\omega_1)$ порождает идеал, аннулирующий ω_1. Пусть W—O_N-модуль. Тогда ω_n порождают $\Omega_A(O_N)$ (как O_N-модуль) и отображение $D\mapsto\{(D,\omega_n)\}$ задает изоморфизм $O_{\hat N}$-модулей $D(O_N,W)$ и $\overleftarrow{W}_{p(\omega_1),b}$. Обратное отображение устроено так: если $\zeta=\{\zeta_n\}\in\in\overleftarrow{W}_{p(\omega_1)b}$, то $(\overleftarrow{D}_\zeta,a\omega_n)=a\zeta_n$.*

2. Пусть $I\supset N$. Тогда $\Omega_A(O_N)\to\Omega_A(O_I)$ — вложение, причем $O_I\Omega_A(O_N)=\Omega_A(O_I)$. Если W—O_I-модуль, то гомоморфизм сужения $D_A(O_I,W)\to D_A(O_N,W)$ — изоморфизм $O_{\hat I}$-модулей.

Доказательство. Отождествим $\Omega_A(O_N)$ с $\frac{N}{O_N}$. Пусть $\{\omega_n\}$ соответствует последовательность $\{a_n\}$. Поскольку a_n порождают (что очевидно) $\frac{N}{O_N}$, то отображение $\mathrm{Hom}_{O_N}\left(\frac{N}{O_N}, W\right) \to \underset{\leftarrow}{W}_{p(a_1),b}$ — вложение. Пусть $\xi = \{\xi_n\} \in \underset{\leftarrow}{W}_{p(a_1),b}$. Положим $\chi_\xi(ca_n) = c\xi_n$. Если $c_1a_n = c_2a_m$, то (считая без ограничения общности, что $m \leqslant n$) $a_m = b^{n-m}a_n$, так что

$$c_1a_n = c_2b^{n-m}a_n \Rightarrow c_1 \equiv c_2b^{n-m} \,(\mathrm{mod}\, p(a_1)\, b^{n-1}) \Rightarrow$$
$$\Rightarrow c_1\xi_n = c_2b^{n-m}\xi_n = c_2\xi_m.$$

Значит, $\chi \mapsto \{\chi(a_n)\}$ — изоморфизм. Далее, пусть $I \supset N$. То, что $\Omega_A(O_N) \to \Omega_A(O_I)$ — вложение, следует из предложения 7.7. Пусть при соответствующих отождествлениях оно выглядит как $\frac{N}{O_N} \xrightarrow{\tau} \frac{I}{O_I}$. Покажем, что $\nu(p(\tau(a_1))) = \nu(p(a_1))$. Если это не так, что $\nu(p(\tau(a_1))) < \nu(p(a_1))$. Поскольку $\nu(N)$ плотно в $\mathbf{Q}$, то $\exists c \in O_N$ такой, что $\nu(p(\tau(a_1))) < \nu(c) < \nu(p(a_1))$. Тогда $0 \neq \tau(ca_1) = c\tau(a_1) = 0$ — противоречие. Пусть $c = p(a_1)$. Пусть b_n, d_n — представители $a_n, \tau(a_n)$ в I. Тогда $b^{n+1}cb_{n+1} - b^ncb_n \in b^ncO_I$, $b^{n+1}cd_{n+1} - b^ncd_n \in b^ncO_I$.

Пусть $s_1 = \lim b^ncb_n$, $s_2 = \lim b^ncd_n$. Так как $s_1 \equiv cb^nb_n \,(\mathrm{mod}\, cb^nO_I)$, то $\frac{s_1}{cb^n} = a_n$. Аналогично, $\frac{s_2}{cb^n} = \tau(a_n)$. Так как $\nu(p(a_1)) = \nu(p(\tau(a_1)))$, то $u = \frac{s_1}{s_2}$ — единица. Очевидно, при отождествлении характеров из $\mathrm{Hom}_{O_N}\left(\frac{N}{O_N}, W\right)$, $\mathrm{Hom}_{O_I}\left(\frac{I}{O_I}, W\right)$ с элементами $\underset{\leftarrow}{W}_{c,b}$ гомоморфизм сужения выглядит как умножение на u, т. е. он — изоморфизм. ■

7.2.2. Модули $\Omega_A(O_{\overline{K}})$ и $D_A(O_{\overline{K}}, W_K)$. G_K обозначает $G(\overline{K}/K)$. $\Omega_A(O_{\overline{K}})$ наделяется естественной структурой G_K-модуля: $(b\,da)^g = b^g\,da^g$. Таким образом, $\Omega_A(O_{\overline{K}})$ — G_K-модуль. Если W — $O_{\overline{K}}$-модуль и одновременно G_K-модуль, то $D_A(O_{\overline{K}}, W)$ также имеет структуру G_K-модуля: $D^g(a) = g(D(g^{-1}(a)))$. Очевидно, $(D^g, \omega^g) = (D, \omega)^g$.

Пусть $\xi \in O_{\overline{K}}$, $\nu(\xi) = -\frac{1}{\alpha(q-1)}$ $(\alpha = e(K/\mathbf{Q}_p))$. Положим $W_K = \frac{\overline{K}}{\xi O_{\overline{K}}}$. Согласно предложению 7.9,

$$D_A(O_{\overline{K}}, W_K) \simeq \varprojlim \frac{\frac{1}{p^k}\xi O_{\overline{K}}}{\xi O_{\overline{K}}} \simeq O_{\hat{\overline{K}}}.$$

Пусть $U_{\hat{\overline{K}}}$ обозначает группу единиц $O_{\hat{\overline{K}}}$. Множество $O_{\hat{\overline{K}}}$-образующих $D_A(O_{\overline{K}}, W_K)$, очевидно, является главным однородным пространством над $U_{\hat{\overline{K}}}$ ($U_{\hat{\overline{K}}}$ рассматривается как G_K-модуль: автоморфизмы по непрерывности продолжаются на $\hat{\overline{K}}$). В частности, $D_A(O_{\hat{\overline{K}}}, W_K)$ соответствует некоторый элемент $v_K \in H^1(G_K, U_{\hat{\overline{K}}})$. В следующем пункте мы явно вычислим этот элемент

7.2.3. Канонические дифференцирования и их свойства. Пусть π — униформизирующая K, $f \in \Lambda_\pi$. Пусть π_1 — униформизирующая K_1. Очевидно, $\dfrac{\overline{K}}{\frac{1}{\pi_1} O_{\overline{K}}} = W_K\left(\nu(\pi_1) = \dfrac{1}{\alpha(q-1)}\right)$. Пусть e_f — образующая $\underset{\leftarrow}{\varkappa_f}$, e_f^n — редукция e_f в $\varkappa_{f,n}$. Положим $\omega_n = l_f'(e_f^n)\,de_f^n \in \Omega_A(O_\pi)$, где O_π — кольцо целых чисел K_π. Так как $l_f(f(X)) = \pi l_f(X)$, то $l_f'(f(X))f'(X) = \pi l_f'(X)$. Отсюда

$$\omega_n = l_f'(f(e_f^{n+1}))\,f'(e_f^{n+1})\,de_f^{n+1} = \pi\omega_{n+1}.$$

Напомним, что $\delta_\pi: G_K \to U_K$ — непрерывный гомоморфизм такой, что $(e_f)^g = [\delta_\pi(g)]_f(e_f)$. Из $l_f([u]_f(X)) = ul_f(X)$ следует, что $l_f'([u]_f(X))[u]_f'(X) = ul_f'(X)$. Отсюда

$$\omega_n^g = l_f'([\delta_\pi(g)]_f(e_f^n))\,[u]_f'(e_f^n)\,de_f^n = ul_f'(e_f^n)\,de_f^n,$$

где $u = \delta_\pi(g)$. Значит, $\omega_n^g = \delta_\pi(g)\,\omega_n$.

Рассмотрим дифференцирование $Q_{e_f}: O_\pi \to W_K$ над A, полагая $(Q_{e_f}, \omega_f) = \dfrac{1}{\pi^n}$ $\left(\text{см. предложение 7.9, } p(\omega_1) = \dfrac{\pi}{\pi_1}\right)$. Согласно предложению 7.9, это дифференцирование однозначно продолжается на $O_{\overline{K}}$. Именно, ω_n порождают $\Omega_A(O_{\overline{K}})$ как $O_{\overline{K}}$-модуль, если $a \in O_{\overline{K}}$, $da = b\omega_n$, то $Q_{e_f}(a) = b\dfrac{1}{\pi^n}$. Q_{e_f} является $O_{\hat{\overline{K}}}$-образующей $D_A(O_{\overline{K}}, W_K)$.

Предложение 7.10. $Q1$. $Q_{e_f}^g = \delta_\pi(g^{-1})\,Q_{e_f}$ $\forall\, g \in G_K$.

Доказательство. Имеем:

$$(Q_{e_f}^g, \omega_n) = (Q_{e_f}^g, \delta_\pi(g^{-1})\,\omega_n^g) = \delta_\pi(g^{-1})\,(Q_{e_f}, \omega_n)^g =$$
$$= \delta_\pi(g^{-1})\,(Q_{e_f}, \omega_n) = (\delta_\pi(g^{-1})\,Q_{e_f}, \omega_n). \blacksquare$$

Выясним, как изменится Q_{e_f} при изменении π и f. Пусть ξ — униформизирующая K, $\xi = \pi u$. Пусть $t \in \Lambda_\xi$, e_t — образующая $\underset{\leftarrow}{\varkappa_t}$. Пусть $\varepsilon \in C_u$, $[\varepsilon]_{f,t}$ — соответствующий изоморфизм F_f и F_t (см. предложение 7.1 и теорему 7.3).

Умножая ε на единицу из U_K, мы можем считать, что $e_t^n = [u^{-n}\varepsilon]_{f,t}(e_f^n)$ $([\xi]_t([u^{-(n+1)}\varepsilon]_{f,t}(e_f^{n+1})) = [u^{-n}\varepsilon]_{f,t}(e_f^n))$. Этим условием ε определяется однозначно. Так как $l_t([u^{-n}\varepsilon]_{f,t}) = u^{-n}\varepsilon l_f$, то $\omega_n = \dfrac{u^n}{\varepsilon} l_t'(e^n)\,de_t^n$.

Значит,

$$(Q_{e_t}, \omega_n) = \frac{u^n}{\varepsilon}\frac{1}{\xi^n} = \frac{1}{\varepsilon}\frac{1}{\pi^n} = \left(\frac{1}{\varepsilon} Q_{e_f}, \omega_n\right).$$

$Q2$. $Q_{e_t} = \dfrac{1}{\varepsilon} Q_{e_f}$.

Заметим, что характеры δ_π и δ_ξ, рассматриваемые как коциклы из G_K в $U_{\hat{\overline{K}}}$, задают один и тот же класс когомологий в $H^1(G_K, U_{\hat{\overline{K}}})$. Действительно, так как

$$([u^{-n}\varepsilon]_{f,t}(e_f^n))^g = [u^{-n}\varepsilon^g]_{f,t}([\delta_\pi(g)]_f(e_f^n)) = \left[\delta_\pi(g)\frac{\varepsilon^g}{\varepsilon}\right]_t([u^{-n}\varepsilon]_{f,t}(e_f^n)),$$

то $\delta_\xi(g) = \dfrac{\varepsilon^g}{\varepsilon}\delta_\pi(g)$, но $g \mapsto \dfrac{\varepsilon^g}{\varepsilon}$ — непрерывная кограница. Из предложения 7.10 следует

Предложение 7.11. *Элемент $v_K \in H^1(G_K, U_{\hat{\overline{K}}})$, соответствующий $U_{\hat{\overline{K}}}$-однородному пространству $O_{\hat{\overline{K}}}$-образуюших $D_A(O_{\overline{K}}, W_K)$, задается непрерывным характером $g \mapsto \delta_\pi(g^{-1})$, класс когомологий которого не зависит от выбора π.* ■

Считая f, e_f фиксированными, будем писать Q вместо Q_{e_f}. Пусть M — конечное расщирение K_s. Определим дифференцирование над A

$$Q_{M,s} : Q_M \to \frac{P_M}{\frac{\pi^s}{\pi_1} P_M},$$

где $P_M = 1/(\pi_1 D(M/K))$ (дробный идеал O_M), следующим образом. Пусть π_M — униформизирующая M. Пусть $a \in O_M$, a', $b' \in O_M$ — такие, что $da = a'\,d\pi_M$, $\omega_s = l'_f(e_f^s)\,de_f^s = b'\,d\pi_M$. Тогда $Q_{M,s}(a) = \dfrac{a'}{b'\pi^s}$. То, что это отображение корректно определено, является дифференцированием над A и не зависит от выбора π_M, легко проверяется непосредственно из определения. Мы покажем это также следующим образом. $\dfrac{P_M}{\frac{\pi^s}{\pi_1}P_M}$ естественно вкладывается в $\dfrac{\overline{K}}{(1/(\pi_1 D(M/K_s)))\,O_{\overline{K}}}$ $\left(D(M/K) = D(M/K_s)\,D(K_s/K) = D(M/K_s)\,\dfrac{\pi^s}{\pi_1}\right)$ и образ $Q_{M,s}$ в $\dfrac{\overline{K}}{(1/(\pi_1 D(M/K_s)))\,O_{\overline{K}}}$ есть редукция из $\dfrac{\overline{K}}{\frac{1}{\pi_1}O_{\overline{K}}}$ в $\dfrac{\overline{K}}{(1/(\pi_1 D(M/K_s)))\,O_{\overline{K}}}$ дифференцирования Q, суженного на O_M. Действительно, пусть t достаточно велико, a', $b' \in O_M$, $c' \in O_{M_t}$ — такие, что $da = a'\,d\pi_M$, $\omega_s = b'\,d\pi_M$, $d\pi_M = c'\omega_t$ $(a \in O_M)$. Тогда $\pi^{t-s}\omega_t = \omega_s = b'c'\omega_t \Rightarrow$ $\Rightarrow \pi^{t-s} - b'c' \in \dfrac{\pi^t}{\pi_1}O_{\overline{K}}$. Значит,

$$Q(a) - \frac{a'}{\pi^s b'} = \frac{a'c'}{\pi^t} - \frac{a'}{\pi^s b'} = \frac{a'(c'b' - \pi^{t-s})}{\pi^t b'} \in$$

$$\in \frac{a'}{\pi_1 b'}O_{\overline{K}} \subset (1/(\pi_1 D(M/K_s)))\,O_{\overline{K}},$$

так как $b'O_M = D(M/K_s)$. ■

Предложение 7.12. *Пусть M — конечное расширение K, $M \cap K_\pi = K_s$. Пусть $N = M_{s+1}$. Тогда* $\delta_{s+1}(G(N/M)) = \dfrac{1+\pi^s A}{1+\pi^{s+1}A}$ $\left(\textit{под-группа } \left(\dfrac{A}{\pi^{s+1}A}\right)^*\right)$ *и* $\sum\limits_{g \in G(N/M)} (\delta_{s+1}(g) - 1)\, g$ *переводит* $\pi/D(N/M)$ *в* $\dfrac{\pi^{s+1}}{\pi_1} O_N$.

Доказательство. Из $S3:3.1$, $S4:3.1$ и теоремы 7.6 следует, что если L — конечное расширение K, то $\delta_m(G(L_m/L))$ есть образ в $\left(\dfrac{A}{\pi^m A}\right)^*$ проекции вдоль $\pi^{\mathbf{Z}}$ в U_K от $N_{L/K}(L^*)$. Отсюда следует утверждение о $G(N/M)$. Заметим также, что если r — максимальное такое, что $L \supset K_r$, то, вообще говоря, $L \cap K_\pi$ может строго содержать K_r, но $L_s \cap K_\pi = K_s$ для $s = r+1, \ldots$. Продолжим доказательство предложения. Поскольку поля M_m и символы δ_m зависят лишь от π, то можно считать, что f — такой, что $[\theta]_f = \theta X$, где $\theta^{q-1} = 1$. Например, таким свойством обладает $f = \pi X + X^q$, так как $f(\theta X) = \theta f(X)$, а условие коммутации с f однозначно определяет $[a]_f$ среди $g \in A[[X]]$ таких, что $g \equiv aX \pmod{\deg 2}$ (см. ([2]), глава 6, § 3, предложение 4.6). Очевидно, $O_N \supset O_M[e_f^{s+1}]$. Переходя к двойственным модулям относительно $\mathrm{Tr}_{N/M}$, имеем:

$$1/D(N/M) \subset \frac{1}{\pi} O_M[e_f^{s+1}] \Rightarrow \pi/D(N/M) \subset O_M[e_f^{s+1}].$$

Поэтому достаточно доказать, что $\sum\limits_{\theta^{q-1}=1} \theta\delta_{s+1}^{-1}(1+\theta\pi^s)$ переводит $(e_f^{s+1})^j$ в $\dfrac{\pi}{\pi_1} O_N$. Имеем:

$$\left(\sum_\theta \theta\delta_{s+1}^{-1}(1+\theta\pi^s)\right)(e_f^{s+1})^j = \sum_\theta \theta(F_f(e_f^{s+1}, \theta e_f^1))^j = \sum_\theta \sum_{i=1}^{\infty} a_i \theta^{i+1} (e_f^1)^i,$$

где $a_i \in O_N$. Остается учесть, что $\sum\limits_\theta \theta^{i+1} = 0$ при $i < q-2$, а при $i \geqslant q-2$ $(e_f^1)^i$ делится на $(e_f^1)^{q-2} \sim \dfrac{\pi}{\pi_1}$. ■

Пусть $M \supset K_s$. Обозначим через $QL_{M,s} : M^* \to \dfrac{\frac{1}{\pi_M} P_M}{\frac{\pi^s}{\pi_1 \pi_M} P_M}$ логарифмическую производную, ассоциированную с $Q_{M,s}$. Именно, $QL_{M,s}(u) = \dfrac{Q_{M,s}(u)}{u}$, если u — единица $\left(\text{так что } QL_{M,s} : U_M \to \dfrac{P_M}{\frac{\pi^s}{\pi_1} P_M}\right)$, $QL_{M,s}(\pi_M^k) = k\dfrac{Q_{M,s}(\pi_M)}{\pi_M}$.

Тривиально проверяется, что $QL_{M,s}$ не зависит от выбора π_M. $QL_{M,s}$ — это гомоморфизм из мультипликативной группы M в аддитивную группу O_M-модуля $\dfrac{\frac{1}{\pi_M} P_M}{\frac{\pi^s}{\pi_1 \pi_M} P_M}$.

Обозначим через $FQL_{M,s}: E(\mu_M) \to \dfrac{P_M}{\frac{\pi^s}{\pi_1} P_M}$ формальную логарифмическую производную: $FQL_{M,s}(x) = -Q_{M,s}(x)\, l'(x)$ (формальная группа, l относятся к F_f) $FQL_{M,s}$ является гомоморфизмом формальной группы $E(\mu_M)$ в аддитивную группу O_M-модуля $\dfrac{P_M}{\frac{\pi^s}{\pi_1} P_M}$. Это следует из равенств

$$l'(F(X, Y))\, F_X(X, Y) = l'(X), \quad l'(F, (X, Y))\, F_Y(X, Y) = l'(Y),$$

получающихся дифференцированием по X и Y равенства $l(F(X, Y)) = l(X) + l(Y)$, и из того, что $Q_{M,s}$ — дифференцирование над A.

Пусть $L \supset K$, r — максимальное число такое, что $L \supset K_r$. Обозначим сокращенно P_{L_s} через P_s, аналогичный смысл имеют обозначения Q_s, QL_s, FQL_s, $N_{t/s}$, $\mathrm{Tr}_{t/s}$ и т. д. Очевидно, $\mathrm{Tr}_{t/s}(P_t \subset P_s)$. Отсюда $\mathrm{Tr}_{t/s}\left(\frac{1}{\gamma_t} P_t\right) \subset \subset \frac{1}{\gamma_s} P_s$, где γ_m — униформизирующая L_m.

Предложение 7.13. *Имеют место коммутативные диаграммы*:

$$\begin{array}{ccc} L_t^* & \xrightarrow{QL_t} & \dfrac{\frac{1}{\gamma_t} P_t}{\frac{\pi^t}{\pi_1 \gamma_t} P_t} \\ \Big\downarrow N_{t/s} & & \Big\downarrow \mathrm{Tr}_{t/s} \\ L_s^* & \xrightarrow{QL_s} & \dfrac{\frac{1}{\gamma_s} P_s}{\frac{\pi^s}{\pi_1 \gamma_s} P_s} \end{array} \qquad \begin{array}{ccc} U_t & \xrightarrow{QL_t} & \dfrac{P_t}{\frac{\pi^t}{\pi_1} P_t} \\ \Big\downarrow N_{t/s} & & \Big\downarrow \mathrm{Tr}_{t/s} \\ U_s & \xrightarrow{QL_s} & \dfrac{P_s}{\frac{\pi^s}{\pi_1} P_s} \end{array}$$

$$\begin{array}{ccc} E(\mu_t) & \xrightarrow{FQL_t} & \dfrac{P_t}{\frac{\pi^t}{\pi_1} P_t} \\ \Big\downarrow N^F_{t/s} & & \Big\downarrow \mathrm{Tr}_{t/s} \\ E(\mu_s) & \xrightarrow{FQL_s} & \dfrac{P_s}{\frac{\pi^s}{\pi_1} P_s} \end{array}$$

где $N^F_{t/s}$ — формальная норма: $N^F_{t/s}(x) = \bigoplus_{g \in G_{t/s}} x^g$, при $s \geqslant r+1$, $t \geqslant s$. Кроме того, если $L \cap K_\pi = K_r$, то то же верно при $s \geqslant r$.

Доказательство. Достаточно рассмотреть случай $t = s+1$. Из $Q1$ и того, что Q_t есть редукция сужения Q на O_t, следует, что

$$QL_t\left(\prod_{g \in G_{t/s}} a^g\right) = \left(\sum \delta_t(g)\, g\right)(QL_t(a)) = \left(\sum g\right)(QL_t(a)) + $$
$$+ \left(\sum (\delta_t(g) - 1)\, g\right)(QL_t(a)).$$

Но $\sum (\delta_t(g)-1)g$ переводит $P_t=1/\pi_1 D(L_t/L_s)D(L_s/K)$ в $(\pi^{t-1}/(\pi_1^2\cdot \cdot D(L_s/K)))O_t=\frac{\pi^s}{\pi_1}P_sO_t$ согласно предложению 7.12 (см. также начало доказательства предложения 7.12). Значит,

$$QL_s(N_{t/s}(a))=QL_t(N_{t/s}(a))\left(\mathrm{mod}\,\frac{\pi^s}{\pi_1\gamma_s}P_s\right)=\mathrm{Tr}_{t/s}(QL_t(a)).$$

Для формальной логарифмической производной доказательство аналогично. ■

7.3. Явные формулы. Мы продолжаем считать фиксированной пару (F_f, e_f), состоящую из формального закона Любина — Тейта, соответствующего $f\in\Lambda_\pi$, и образующей e_f модуля Тейта $\varkappa_f$. Спаривание $\overleftarrow{(\ ,\ )}_{L,n}$ и ассоциированные с ним гомоморфизмы и инварианты будут относиться к (F_f, e_f).

7.3.1. Вычисление инвариантов c_β. Пусть $\beta=(m, t)$ — допустимая пара: $\exists n\in\mathbf{N}$ такое, что $t-m\geqslant n\alpha\geqslant m$, где α — индекс ветвления K над $\mathbf{Q}_p$.

Пусть π_t— униформизирующая K_t такая, что $N_{M/K}(\pi_t)=\pi$, где $M=K_t$. Существование такой π_t следует из $S3:3.1$, $\theta1:7.1$. Из $S4:3.1$ и $\theta1:7.1$ следует (см. $\chi1:6.3$), что

$$\chi_\beta(\pi_t^n u)=\frac{N_{M/K}(u^{-1})-1}{\pi^t}\quad(\mathrm{mod}\,\pi^m A)$$

Из $S3:3.1$, $\theta1:7.1$ следует, что $N_{M/K}(u^{-1})\equiv 1\,(\mathrm{mod}\,\pi^t))$, где u — единица.

Пусть $u\in V_M=1+\mu_M$. Пусть $N_{M/K}(u^{-1})=1+\pi^t a$, где $a\in A$. Тогда

$$\log(N_{M/K}(u^{-1}))=\pi^t a+\sum_{s=2}^{\infty}(-1)^{s-1}\frac{(\pi^t a)^s}{s}.$$

Покажем, что $\nu\left(\frac{\pi^{ts}}{s}\right)\geqslant\nu(\pi^{t+m})$ при $s\geqslant 2$. Нужно, чтобы $\frac{st}{\alpha}\geqslant\frac{m+t}{\alpha}+ +\nu(s)$. Можно считать, что $s=p^j$. Требуется доказать, что

$$\frac{p^j t}{\alpha}\geqslant\frac{m+t}{\alpha}+j\Leftrightarrow\frac{t}{\alpha}\geqslant\frac{m}{\alpha(p^j-1)}+\frac{j}{p^j-1}.$$

Так как

$$\frac{j}{p^j-1}=\frac{j}{(p-1)(1+p+\ldots+p^{j-1})}\leqslant 1,\qquad t\geqslant\alpha+m,$$

то это неравенство выполняется. Значит,

$$\chi LT1.\quad \chi_\beta(u)=\frac{\log(N_{M/K}(u^{-1}))}{\pi^t}=\mathrm{Tr}_{M/K}\left(\log(u)\cdot\left(-\frac{1}{\pi^t}\right)\right)\ (\mathrm{mod}\,\pi^m A)$$

$$\forall u\in V_M.$$

Из $\chi c1:6.3$. $\chi LT1$ следует

$$cLT1.\quad c_\beta=-\frac{1}{\pi^t}\,(\mathrm{mod}\,\pi^m R_{t,1}).$$

7.3.2. Уточнения теорем 6.7, 6.9 для закона Любина — Тейта. Пусть L — конечное расширение K_n. L будет фиксировано на протяжении этого пункта. Как обычно, $L_s = L(\varkappa_s)$. Пусть $M = L_s$. Тогда $Q_s = Q_{M,s}$, $QL_s = QL_{M,s}$, $FQL_s = FQL_{M,s}$, $P_s = P_M = 1/(\pi_1(D(M/K)))$, где π_1 — униформизирующая K_1. N_s, Tr_s будут обозначать соответственно $N_{M/K}$ и $\mathrm{Tr}_{M/K}$, $N_{t/s}$, $\mathrm{Tr}_{t/s}$—$N_{N/M}$, $\mathrm{Tr}_{N/M}$, где $N = L_t$, $t \geqslant s$. Далее $\mu_s = \mu_M$. Через L_s' мы обозначаем $\bigcap\limits_{t \geqslant s} N_{t/s}(L_s^*)$, аналогично, $U_s' = \bigcap\limits_{t \geqslant s} N_{t/s}(U_t) = U_s \bigcap L_s'$, где U_k — группа единиц L_k. $L' = L_1'$, $U_L' = U_1'$.

Предложение 7.14. $N_{t/s}(L_t') = L_s'$, $N_{t/s}(U_t') = U_s'$.

Доказательство. Из $S3:3.1$, $S4:3.1$, теоремы 7.6 следует, что $L_t' = \{a \in L_t^* \mid N_{L_t/K}(a) \in \pi^{\mathbf{Z}}\}$. Теперь утверждение очевидно. ■

Через γ_s обозначим униформизирующую L_s. $\varphi_{L,n}$: $L^n \to \dfrac{R_L}{\pi^n R_L}$ — гомоморфизм для (F_f, e_f); L — из предложения 3.2. Из $S3:3.1$, $S4:3.1$, теоремы 7.6 следует, что $L^n = \{a \in L^* \mid N_{L/K}(a) \in \pi^{\mathbf{Z}}(1 + \pi^{r+n}A)\}$, где $\varkappa_r = \varkappa_L = \varkappa \bigcap E(\mu_L)$.

ТЕОРЕМА 7.15. *Пусть r — максимальное число такое, что $L \supset K_r$. Пусть $s \geqslant n + r + \log_q(e(L/K_r))$, $s \geqslant 1 + n + r + \log_q(e(L/K_r))$ при $q = 2$, $n = 1$. Тогда Tr_s переводит $\dfrac{\pi^s}{\pi_1\gamma_s} P_s$ в $\pi^n R_L$, так что Tr_s индуцирует гомоморфизм $\dfrac{\frac{1}{\gamma_s} P_s}{\frac{\pi^s}{\pi_1\gamma_s} P_s}$ в $\dfrac{L}{\pi^n R_L}$. Справедлива формула*

$$\varphi LT1. \quad \varphi_{L,n}(N_s(b)) = \mathrm{Tr}_s(QL_s(b)) \;\; \forall\, b \in L_s'.$$

В частности, отображение $\mathrm{Tr}_s \circ QL_s \circ N_s^{-1}$ (на L') определено корректно, поэтому является гомоморфизмом из L' в $\dfrac{L}{\pi^n R_L}$ и $\varphi_{L,n} = \mathrm{Tr}_s \circ QL_s \circ N_s^{-1}$ на $L' \subset L^n$.

Дополнение к теореме. Как будет видно из доказательства, при $s \geqslant n + r + \log_q(e(L/K_r))$ $\mathrm{Tr}_s: \dfrac{\pi^s}{\pi_1} P_s \to \pi^n R_L$ и $\varphi_{L,n}(N_s(u)) = \mathrm{Tr}_s(QL_s(u))$ $\forall\, u \in U_s'$ $\left(\text{как мы знаем, } QL_s(u) \text{ определено в } \dfrac{P_s}{\frac{\pi^s}{\pi_1} P_s}\right)$. Соответственно, $\varphi_{L,n} = \mathrm{Tr}_s \circ QL_s \circ N_s^{-1}$ на U_L'.

Учитывая определение $\varphi_{L,n}$, из теоремы 7.15 получаем следующее утверждение.

ТЕОРЕМА 7.16. *В условиях теоремы 7.15 имеют место формулы:*

$$SPLT1. \quad (a,x)_{L,n} = [\mathrm{Tr}_{L/K}((\mathrm{Tr}_s \circ QL_s \circ N_s^{-1}(a))\, l_f(x)]_f(e_f^n)$$

$$\forall\, a \in L', \quad x \in E(\mu_L),$$

что эквивалентно

$SPLT2$. $(b, x)_{L_s,n} = [\mathrm{Tr}_{L_s/K}(QL_s(b)\, l_f(x))]_f(e_f^n)$

$$\forall\, b \in L_s', \quad x \in E(\mu_L).$$

Эквивалентность $SPLT1$ и $SPLT2$ следует из $SP3.3.3$.

Теорема 7.16 имеет дополнение, аналогичное дополнению к теореме 7.15.

Доказательство теоремы 7.15. Обозначим $R_{M,1}$ через $R_{t,1}$, где $M = L_t$, т. е.

$$R_{t,1} = 1/(D(L_t/K)\, \gamma_t^{\frac{e(M)}{p-1}+1}).$$

Так как π_1 делит $\gamma_t^{\frac{e(M)}{p-1}} \sim p^{\frac{1}{p-1}}$, то $\frac{1}{\gamma_t} P_t = 1/(\gamma_t \pi_1 D(L_t/K)) \subset R_{t,1}$. Значит, если $k < t$, то

$$\frac{\pi^t}{\pi_1\gamma_t} P_t \subset \frac{\pi^k}{\gamma_t} R_{t,1}.$$

Пусть D равно факторизации Q_t в $\dfrac{R_{t,1}}{\frac{\pi^k}{\gamma_t} R_{t,1}}$. Тогда D — дифференцирование над A, причем $D(e^t) = \dfrac{1}{\pi^t l'(e^t)}$. Пусть теперь t, k, m — такие, как в теореме 6.7. Пусть $\beta = (k, t)$ — допустимая пара. Согласно $cLT1$, $c_\beta = -\dfrac{1}{\pi^t}$. Так как $t = 2k + \alpha$, то $t > k$. Пусть $M = L_t$. Дифференцирование $D_{M,m}: O_M \to \dfrac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$, фигурирующее в теореме 6.7, совпадает с редукцией Q_t в $\dfrac{R_{M,1}}{\frac{\pi^m}{\pi_M} R_{M,1}}$. Действительно, если D — редукция Q_t в $\dfrac{R_{M,1}}{\frac{\pi^k}{\pi_M} R_{M,1}}$, то $D(e^t) = -\dfrac{\bar{c}_\beta}{l'(e^t)}$ и $D_{M,m}$ — редукция D согласно предложению 6.6. В частности, $\psi_{M,m}: M^* \to \dfrac{R_{M,1}}{\frac{\pi^m}{\pi_M^2} R_{M,1}}$ в теореме 6.7 можно заменить на $QL_t: M^* \to \dfrac{\frac{1}{\gamma_t} P_t}{\frac{\pi^t}{\pi_1\gamma_t} P_t}$, а на U_M — на $QL_t: U_M \to \dfrac{P_t}{\frac{\pi^t}{\pi_1} P_t}$. Теперь мы хотим воспользоваться коммутативной диаграммой из предложения 7.13 и спуститься как можно ниже к полю L. Именно, предположим, что s таково, что $\mathrm{Tr}_s\left(\frac{\pi^s}{\pi_1\gamma_s} P_s\right) \subset \pi^n R_L$. Пусть $a \in L'$, $b \in L_s'$ такой, что $N_s(b) = a$. Пусть $c \in L_t'$, $N_{t/s}(c) = b$. Тогда, согласно $\varphi\psi3: 6.4$ (с заменой $\psi_{M,m}$ на QL_t), $\varphi_{L,n}(a) = \mathrm{Tr}_t(QL_t(c))$ в

$\frac{L}{\pi^n R_L}\left(\mathrm{Tr}_t\colon \frac{\pi^t}{\pi_1\gamma_t} P_t \to \pi^n R_L\right)$. Но так как $\mathrm{Tr}_s\left(\frac{\pi^s}{\pi_1\gamma_s} P_s\right) \subset \pi^n R_L$, то $\mathrm{Tr}_t(QL_t(c)) = \mathrm{Tr}_s(\mathrm{Tr}_{t/s}(QL_t(c)))$. Но $\mathrm{Tr}_{t/s}(QL_t(c)) = QL_s(b)$ согласно предложению 7.13. Аналогично, верны формулы из дополнения к теореме 7.15, если $\mathrm{Tr}_s\left(\frac{\pi^s}{\pi_1} P_s\right) \subset \pi^n R_L$.

Итак, остается лишь выяснить, когда $\mathrm{Tr}_s\left(\frac{\pi^s}{\pi_1\gamma_s} P_s\right) \subset \pi^n R_L$.

Сначала мы уточним поведение $l_f\colon E(\mu_{\overline{K}}) \to \overline{K}$.

Предложение 7.17. *l_f изоморфно отображает подгруппу $E(\mu_{\overline{K}})$, состоящую из элементов $x \mid \nu_K(x) > \frac{1}{q-1}$ $(\nu_K = \alpha\nu)$, на аддитивную группу идеала $O_{\overline{K}}$, состоящего из элементов $y \mid \nu_K(y) > \frac{1}{q-1}$. При этом обратное отображение задается l_f^{-1}, сходящимся на $y \mid \nu_K(y) > \frac{1}{q-1}$. Кроме того, $\nu(l_f(x)) = \nu(x)$ при $\nu_K(x) > \frac{1}{q-1}$.*

Таким образом, предложение 7.17 уточняет предложение 2.4 для логарифмов формальных законов Любина — Тейта.

Доказательство. Предположим, что мы доказали, что $l_f(\varpi X)$ делится на ϖ в $O_K[[X]]$ при $\nu_K(\varpi) > \frac{1}{q-1}$. Тогда, рассуждая как при доказательстве предложения 2.4, мы покажем, что l_f^{-1} сходится на y при $\nu_K(y) > \frac{1}{q-1}$ и задает отображение в $\left\{x \mid \nu_K(x) > \frac{1}{q-1}\right\}$, обратное к l_f. Так как $\nu_K(\varpi) > \frac{1}{q-1}$, то $f(\varpi X)$ делится ровно на $\pi\varpi$. Итерируя, получим, что $f^{(n)}(\varpi X)$ делится ровно на $\pi^n\varpi$. Пусть n столь велико, что $\nu(\pi^n\varpi) > \frac{1}{p-1}$. Из доказательства предложения 2.4 тогда следует, что $\pi^n l_f(\varpi X) = l_f(f^{(n)}(\varpi X))$ делится на $\pi^n\varpi \Rightarrow l_f(\varpi X)$ делится на ϖ. Аналогично, так как $\nu(f^{(n)}(\varpi)) = \nu(\pi^n\varpi)$, то $\nu(l_f(\varpi)) = \nu(\varpi)$ (точнее, $l_f(\varpi) = \varpi(1+\gamma)$, где $\gamma \in \mu_{\overline{K}}$). ■

В частности, если M — конечное расширение K, то l_f отображает изоморфно $E\left(\mu_M^{\left[\frac{e(M/K)}{q-1}\right]+1}\right)$ на $\mu_M^{\left[\frac{e(M/K)}{q-1}\right]+1}$, а обратный изоморфизм задается l_f^{-1}.

Пусть $x \in E(\mu_L)$. Тогда $f(x) \equiv x^q \pmod{\pi x}$. Пусть

$$s' \geqslant \log_q\left(\frac{e(L/K)}{q-1}\right) + 1 = r + \log_q(e(L/K_r)).$$

Тогда $\nu_K(f^{(s'-1)}(x)) \geqslant \frac{1}{q-1}$. Значит, $f^{(s')}(x)$ делится на $\pi\pi_1$. Учитывая предложение 7.17, видим, что $\frac{\pi^{s'-1}}{\pi_1} T_L \subset O_L$, где $T_L = l_f(E(\mu_L))$.

Значит,

$$T_L \subset \frac{\pi_1}{\pi^{s'-1}} O_L \Rightarrow \frac{\pi^{s'-1}}{\pi_1} (1/D(L/K)) \subset R_L.$$

Tr_s переводит $\frac{\pi^s}{\pi_1} P_s = \pi^s/(\pi_1^2 D(L/K)\, D(L_s/L))$ в $\frac{\pi^s}{\pi_1^2}/D(L/K) \subset \frac{\pi^{s-s'+1}}{\pi_1} R_L$. Поэтому если $s \geqslant n+s'$, то Tr_s переводит $\frac{\pi^s}{\pi_1} P_s$ в $\pi^n R_L$. Далее, Tr_s переводит $\frac{\pi^s}{\pi_1 \gamma_s} P_s \subset \frac{\pi^s}{\pi_1 \pi_L} P_s$ в $\frac{\pi^{s-s'+1}}{\pi_1 \pi_L} R_L$. Поэтому если $q \neq 2$ или $n \neq 1 \Leftrightarrow$ $\Leftrightarrow \pi_1 \pi_L | \pi$, то при $s \geqslant n+s'$ Tr_s переводит $\frac{\pi^s}{\pi_1 \gamma_s} P_s$ в $\pi^n R_L$. Если $q=2$, $n=1$, то, увеличив s на 1, также будем иметь нужное включение. Теорема доказана. ■

Обозначим через $E'(\mu_k) \bigcap_{t \geqslant k} N_{t/K}^F(E(\mu_t))$ — это подгруппа $E(\mu_k)$ $(N_{t/K}^F(x) = \bigoplus_{g \in G_{t/K}} x^g)$.

Аналогично доказательству теоремы 7.15, с использованием теоремы 6.9 вместо теоремы 6.7 и соответствующей коммутативной диаграммы из предложения 7.13, доказывается

ТЕОРЕМА 7.18. *Пусть r — максимальное число такое, что $L \supset K_r$. Пусть $s \geqslant \alpha \log_p \left(\frac{e(L/\mathbf{Q}_p)}{p-1}\right)$ при $q > p$ (тогда $\pi_1^2 \mid p^{\frac{1}{p-1}}$), $s \geqslant 1 + \alpha \log_p \left(\frac{e(L/\mathbf{Q}_p)}{p-1}\right)$ при $q = p$ (α — индекс ветвления K над $\mathbf{Q}_p$). Тогда Tr_s переводит $\frac{\pi^s}{\pi_1} P_s$ в $\pi^n J_L$, где $J_L = \{y \in L \mid \mathrm{Tr}_{L/K}(yw) \in A \ \ \forall w \in \log(1+\mu_L)\}$, так что Tr_s индуцирует гомоморфизм $\dfrac{P_s}{\frac{\pi^s}{\pi_1} P_s}$ в $\dfrac{L}{\pi^n J_L}$. При этом справедлива формула*

SPLT3. $(u, N_s^F(y))_{L,n} = [\mathrm{Tr}_{L/K}(\log(u) \times \mathrm{Tr}_s(FQL_s(y)))]_f(e_f^n) \quad \forall u \in V_L$, $y \in E'(\mu_s)$.

SPLT3 эквивалентна

SPLT4. $(u, y)_{L_s,n} = [\mathrm{Tr}_{L_s/K}(\log(u)\, FQL_s(y))]_f(e_f^n) \ \forall u \in V_L, \ y \in E'(\mu_s)$. ■

Предположим, что $L \cap K_\pi = K_r$. Согласно предложению 7.13 и теореме 7.15, $\varphi_{L,n}$ совпадает с $QL_r : U_L \to \dfrac{P_L}{\frac{\pi^r}{\pi_1} P_L}$ на U_L' по mod $\frac{\pi^r}{\pi_1} P_L$ и совпадает с $QL_r : L^* \to \dfrac{\frac{1}{\pi_L} P_L}{\frac{\pi^r}{\pi_1 \pi_L} P_L}$ на L' по mod $\frac{\pi^r}{\pi_1 \pi_L}$. Ортогональными модулями относительно спаривания $(y, w) \mapsto \mathrm{Tr}_{L/K}(yw) \pmod{\pi^n A}$ для $\frac{\pi^r}{\pi_1} P_L, \frac{\pi^r}{\pi_1 \pi_L} P_L$ являются соответственно модули $\frac{\pi_1^2}{\pi^{r-n}} O_L$ и $\frac{\pi_1^2 \pi_L}{\pi^{r-n}} O_L$.

Покажем, что $l_f(x) \in \frac{\pi_1^2}{\pi^{r-n}} O_L$ $\left(\in \frac{\pi_1^2\pi_L}{\pi^{r-n}} O_L\right)$ при $\nu_K(x) \geqslant \frac{2}{(q-1)q^{r-n}}$ $\left(\nu_K(x) \geqslant \frac{2}{(q-1)q^{r-n}} + \nu_K(\pi_L)\right)$. Из предложения 7.17 следует, что это вытекает из неравенства $\nu_K([\pi^{r-n}]_f(x)) \geqslant \frac{2}{q-1}$, которое при $r=n$ совпадает с условием. Пусть $r>n$. Тогда

$$\nu_K([\pi^{r-n}]_f(x)) \geqslant \min(q\nu_K(c),\ 1+\nu_K(c)),$$

где $c=[\pi^{r-n-1}]_f(x)$. Но

$$\nu_K(c) \geqslant \min(q^{r-n-1}\nu_K(x),\ 1+\nu_K(x)) = \frac{2}{(q-1)q}.$$

Значит,

$$\nu_K([\pi^{r-n}]_f(x)) \geqslant \min\left(\frac{2}{q-1},\ 1+\frac{2}{(q-1)q}\right) \geqslant \frac{2}{q-1}.$$

То, что $l_f(x) \in \frac{\pi_1^2\pi_L}{\pi^{r-n}}$ при $\nu_K(x) \geqslant \frac{2}{(q-1)q^{r-n}} + \nu_K(\pi_L)$, доказывается аналогично. Аналогично же (с заменой F_f на F_m) доказывается, что $\log(u) \in \frac{\pi_1^2}{\pi^{r-n}} O_L$ при $\nu(u-1) \geqslant \frac{2}{(p-1)p^t}$, $\nu(u-1) \geqslant \frac{1}{(p-1)p^t}$ при $q>p$ (тогда $\pi_1^2 \mid p^{\frac{1}{p-1}}$), где $\pi^{r-n} \mid p^t$.

Итак, нами получена

ТЕОРЕМА 7.19. *Пусть* $L \cap K_\pi = K_r$. *Тогда*

*SPLT*5. $(u, x)_{L,n} = [\mathrm{Tr}_{L/K}(QL_r(u)\, l_f(x))]_f(e_f^n)$ $\forall u \in U_L'$, $\forall x \in E(\mu_L)$ *таких, что* $l_f(x) \in \frac{\pi_1^2}{\pi^{r-n}} O_L$. *В частности,* $\forall x \in E(\pi_{r-n+1}^2 O_L)$, *где* π_{r-n+1} — *униформизирующая* K_{r-n+1}. *Аналогично,*

*SPLT*6. $(a, x)_{L,n} = [\mathrm{Tr}_{L/K}(QL_r(a)\, l_f(x))]_f(e_f^n)$ $\forall a \in L'$, $\forall x \in E(\mu_L)$ *таких, что* $l_f(x) \in \frac{\pi_1^2\pi_L}{\pi^{r-n}}$. *В частности,* $\forall x \in E(\pi_{r-n+1}^2\pi_L O_L)$. ∎

Аналогично ($D_{M,m}$ из теоремы 6.9 при достаточно больших t есть редукция Q_t) получаем следующее утверждение.

ТЕОРЕМА 7.20. *Пусть* $L \cap K_\pi = K_r$. *Тогда*

*SPLT*7. $(u, x)_{L,n} = [\mathrm{Tr}_{L/K}(\log(u)\, FQL_r(x)]_f(e_f^n)$ $\forall x \in E'(\mu_L)$, $u \in V_L$, *таких, что* $\log(u) \in \frac{\pi_1^2}{\pi^{r-n}} O_L$. *В частности, при* $\nu(u-1) \geqslant \frac{2}{(p-1)p^t}$, $\nu(u-1) \geqslant \frac{1}{(p-1)p^t}$ *при* $q>p$, *где* $\pi^{r-n} \mid p^t$. ∎

7.4. Дополнение к пункту 7.3.

7.4.1. Норменные ряды и вычисление $\varphi_{g,L,n}((-1)^{p-1} e_g^n)$ для $g \in \Pi\Lambda_\xi$. Пусть ξ — униформизирующая K. Обозначим через $\Pi\Lambda_\xi$ подмножество Λ_ξ, состоящее из полиномов степени q с старшим коэффициентом $=1$.

Предложение 7.21. *Пусть* $g \in \Pi\Lambda_\xi$. *Тогда при* $m>0$

$N1. \quad \prod_{v \in \varkappa_{g,m}} F_g(X, v) = (-1)^{p-1} g^{(m)}(X).$

Доказательство. Сравнивая нули полиномов от Y, имеем:

$$\prod_{v \in \varkappa_{g,m}} (Y - F(X, v)) = g^{(m)}(Y) - g^{(m)}(X).$$

Значит,

$$\prod_{v \in \varkappa_{g,m}} F(X, v) = (-1)^{|\varkappa_{g,m}|-1} g^m(X),$$

но $|\varkappa_{g,m}| = q^m \equiv p \pmod 2$. ■

Из предложения 3.1 следует

Предложение 7.22. *Если* $g \in \Pi\Lambda_\xi$, *то* $(-1)^{p-1}X$—*t-норменный ряд для* F_g $\forall t$. ■

Из $r2:3.4$ следует

Предложение 7.23. *Пусть* $f \in \Lambda_\xi$, $g \in \Pi\Lambda_\xi$. *Пусть* $u \in U_K$. *Ряд* $(-1)^{p-1}[u]_{f,g}(X)$—*t-норменный для* F_f $\forall t$. ■

Подставляя в $N1$ $F(X, Y)$ вместо X $(F=F_g)$ и пользуясь ассоциативностью, имеем:

$$\prod_{v \in \varkappa_{g,m}} F(X, F(Y, v)) = (-1)^{p-1} g^{(m)}(F(X, Y)).$$

Беря логарифмическую производную по X, получаем:

$$\sum_{v \in \varkappa_{g,m}} \frac{F_X(X, F(Y, v))}{F(X, F(Y, v))} = \frac{g^{(m)\prime}(F(X, Y)) F_X(X, Y)}{g^{(m)}(F(X, Y))}.$$

Подставив $X=0$, $Y=e_g^{m+n}$, имеем:

$$\sum_{v \in \varkappa_{g,m}} \frac{F_X(0, F(e_g^{m+n}, v))}{F(e_g^{m+n}, v)} = \frac{g^{(m)\prime}(e_g^{m+n}) F_X(0, e_g^{m+n})}{e_g^n},$$

что эквивалентно

$TR1. \quad \sum_{v \in \varkappa_{g,m}} \frac{1}{\xi^{n+m} l_g'(F_g(e_g^{n+m}, v)) F_g(e_g^{n+m}, v)} = \frac{1}{\xi^n l_g'(e_g^n) e_g^n}$, так как $l' = \frac{1}{F_X(0,X)}$, $l(g^{(m)}) = \xi^m l \Rightarrow l'(g^{(m)}) g^{(m)\prime} = \xi^m l'$.

Предложение 7.24. *Пусть* $L \supset K_{\xi,n}$. *Пусть* $\varphi_{g,L,n} : L^{g,n} \to \frac{R_{g,L}}{\xi^n R_{g,L}}$ — *гомоморфизм, соответствующий* (F_g, e_g). *Тогда*

$\varphi LT2. \quad \varphi_{g,L,n}((-1)^{p-1} e_g^n) = \frac{1}{\xi^n l_g'(e_g^n) e_g^n} \pmod{\xi^n R_{g,L}}.$

Доказательство. Из φ $3:3.5$ следует, что достаточно рассмотреть случай $L = K_{\xi,n}$. Пусть s достаточно велико. Из $N1$ следует, что $N_s(e_g^s) =$

$=(-1)^{p-1}e_g^n$, где N_s — норма из L_s в L. По определению, $QL_{g,s}(e_g^s) = = \frac{1}{\xi^s l'_g(e_g^s)\,e_g^s}$. Остается применить формулу $\varphi LT1$ из теоремы 7.15 и $TR1$. ■

7.4.2. Вариация g. Фиксируем $f\in\Lambda_\pi$ и e_f — образующую $\varkappa_f$. $\varphi_{L,n}$, $Q_{L,n}$, $QL_{L,n}$, $FQL_{L,n}$, $E(\mu_L)$ и т. д. относятся к (F_f, e_f). Мы хотим, пользуясь связью $\varphi_{L,n}$ и $\varphi_{g,L,n}$, вычислить $\varphi_{L,n}$ на $(-1)^{p-1}e_g^n$, пользуясь формулой $\varphi LT2$. Во-первых, мы знаем, что если $g\in\Pi\Lambda_\pi$, $e_g=[1]_{f,g}(e_f)$, то $\varphi_{g,L,n}=\varphi_{L,n}$ (см. φ 6 : 3.5). Это определяет значение

$$\varphi_{L,n}((-1)^{p-1}e_g^n) = \frac{1}{\pi^n l'_g(e_g^n)\,e_g^n}.$$

Кроме того, можно еще варьировать униформизирующую π. Если $g\in\Lambda_\xi$, то значок g вверху или внизу (F_g, $\varphi_{g,M,n}$, $L^{g,n}$) будет обозначать, что соответствующий объект относится к F_g (к (F_g, e_g), если фиксирована e_g).

Будем обозначать через I_j неразветвленное расширение K степени j. Из теоремы 7.6 следует

Предложение 7.25. *$I_jK_{\xi,n}=I_jK_{\pi,n}\Leftrightarrow u^j\equiv 1\ (\mathrm{mod}\,\pi^n)$, где $u=\frac{\xi}{\pi}$.* ■

Положим $M=I_jK_{\pi,r}$. Пусть $\xi=\pi u$, $u^j\equiv 1\,(\mathrm{mod}\,\pi^r)$. Пусть $g\in\Lambda_\xi$. $\mathrm{Fr}_M=\mathrm{Fr}_K^j$ — автоморфизм Фробениуса M_{nr} над M. Пусть $\varepsilon\in C_u$ (см. лемму 7.1 и теорему 7.2) — единица. Тогда $\varepsilon^{\mathrm{Fr}_M}=u^j\varepsilon\equiv\varepsilon\,(\mathrm{mod}\,\pi^r)$. Из доказательства леммы 7.1 следует, что $\exists\tau_\varepsilon\in U_{I_j}$ такая, что $\varepsilon/\tau_\varepsilon\equiv 1\,(\mathrm{mod}\,\pi^r)$. При этом τ_ε, очевидно, определяется этим условием с точностью до множителя, являющегося единицей в I_j, сравнимой с $1\,(\mathrm{mod}\,\pi^r)$. Пусть T_M, $T_{g,M}$ обозначают соответственно $l(E(\mu_M))$, $l_g(E_g(\mu_M))$. Как мы знаем (см. предложение 7.17 и далее), $\pi_1\pi_M O_M\subset T_M\subset\frac{\pi_1}{\pi^{r-1}}O_M$. Поэтому A-подмодуль $\tau_\varepsilon T_M$ в M зависит лишь от $\tau_\varepsilon\,(\mathrm{mod}\,\pi^r)$, т. е. от ε, а поскольку ε определена с точностью до множителя в U_K, то в конечном счете — от g.

Предложение 7.26. *Отображение $x\mapsto[\varepsilon]_{f,g}(x)\ominus_g l_g^{-1}((\varepsilon-\tau_\varepsilon)\,l(x))= =y(x)$ задает изоморфизм $E(\mu_M)$ и $E_g(\mu_M)$. При этом $l_g(y)=\tau_\varepsilon l(x)$. В частности, $T_{g,M}=\tau_\varepsilon T_M$.*

Доказательство. Во-первых, $(\varepsilon-\tau_\varepsilon)\,l(x)\in\pi_1\pi O_{\hat{M}_{nr}}$, так как $(\varepsilon-\tau_\varepsilon)\equiv 0\,(\mathrm{mod}\,\pi^r)$. Таким образом, $l_g^{-1}((\varepsilon-\tau_\varepsilon)\,l(x))$ определено (см. предложение 7.17: в нем K можно расширить до $\hat{\hat{K}}$ — это не изменит доказательства). Покажем, что $y\in E(\mu_M)$, что эквивалентно тому, что $\mathrm{Fr}_M(y)=y$,

$$\mathrm{Fr}_M(y) = [\varepsilon u^j]_{f,g}(x)\ominus_g l_g^{-1}(\varepsilon u^j-\tau_\varepsilon)\,l(x)) =$$
$$= [\varepsilon u^j]_{f,g}(x)\ominus_g l_g^{-1}(\varepsilon(u^j-1)\,l(x))\ominus_g l_g^{-1}((\varepsilon-\tau_\varepsilon)\,l(x)) =$$
$$= [\varepsilon u^j]_{f,g}(x)\ominus_g[\varepsilon(u^j-1)]_{f,g}(x)\ominus_g l_g^{-1}((\varepsilon-\tau_\varepsilon)\,l(x)) = y,$$

так как из $l_g([\varepsilon(u^j-1)]_{f,g}(x)=\varepsilon(u^j-1)\,l(x)$ следует, что

$$l_g^{-1}(\varepsilon(u^j-1)\,l(x)) = [\varepsilon(u^j-1)]_{f,g}(x)$$
$$\left(\nu_K(\varepsilon(u^j-1)\,l(x)) > \frac{1}{q-1},\ \nu_K([\varepsilon(u^j-1)]_{f,g}) > \frac{1}{q-1},\right.$$

см. предложение 7.17 и далее). То, что $x \mapsto y$ — гомоморфизм и $l_g(y) = \tau_\varepsilon l(x)$, очевидно. Так как (что легко проверяется)

$$y \mapsto \left[\frac{1}{\varepsilon}\right]_{g,f} \ominus l^{-1}\left(\left(\frac{1}{\varepsilon} - \frac{1}{\tau_\varepsilon}\right) l_g(y)\right)$$

является обратным гомоморфизмом, то $x \mapsto y$ — изоморфизм. ■

Предложение 7.27. *Пусть* $\xi = \pi u$, $u^j \equiv 1 \pmod{\pi^{2n}}$, $g \in \Lambda_\xi$, $e_g^n = [u^{-n}\varepsilon]_{f,g}(e_f^n)$, τ_ε — *единица* I_j *такая, что* $\varepsilon/\tau_\varepsilon \equiv 1 \pmod{\pi^{2n}}$. *Пусть* $M = I_j K_{\pi,n}$. *Тогда* $M^{g,n} = M^n$, *умножение на* $\frac{1}{\tau_\varepsilon}$ *задает изоморфизм* $\frac{R_M}{\pi^n R_M}$ *на* $\frac{R_{g,M}}{\xi^n R_{g,M}}$ *и* $\varphi_{g,M,n} = \frac{1}{\tau_\varepsilon}\varphi_{M,n}$.

Доказательство. Пусть $x \in E(\mu_M)$, $y = y(x) \in E_g(\mu_M)$. Пусть $f^{(n)}(z) = x$. Так как $\varepsilon - \tau_\varepsilon \equiv 0 \pmod{\pi^{2n}}$, то $\frac{\varepsilon - \tau_\varepsilon}{\pi^n} l(x) \subset \pi\pi_1 O_{\hat{M}_{nr}}$. Поэтому l_g^{-1} сходится на $\frac{\varepsilon - \tau_\varepsilon}{\pi^n} l(x)$. Положим

$$w = w(z) = [\varepsilon]_{f,g}(z) \ominus_g l_g^{-1}\left(\frac{\varepsilon - \tau_\varepsilon}{\pi^n} l(x)\right).$$

Очевидно, $[\pi^n]_g(w) = y$. Значит, $g^{(n)}([u^{-n}]_g(w)) = y$. Следовательно, для $a \in M^*$

$$[u^{-n}]_g(w) \oplus_g (a, y)_{g,M,n} = [u^{-n}]_g\left([\varepsilon u^{j\nu_M(a)}]_{f,g}(z \oplus \zeta) \ominus_g l_g^{-1}\left(\frac{\varepsilon u^{j\nu_M(a)} - \tau_\varepsilon}{\pi^n} l(x)\right)\right),$$

где $\zeta = (a, x)_{M,n}$. Имеем:

$$l_g^{-1}\left(\frac{\varepsilon u^{j\nu_M(a)} - \tau_\varepsilon}{\pi^n} l(x)\right) = l_g^{-1}\left(\frac{\varepsilon(u^{j\nu_M(a)} - 1)}{\pi^n} l(x)\right) \oplus l_g^{-1}\left(\frac{\varepsilon - \tau_\varepsilon}{\pi^n} l(x)\right).$$

Так как $\varepsilon(u^{j\nu_M(a)} - 1) \equiv 0 \pmod{\pi^{2n}}$, то

$$\nu_K([\varepsilon(u^{j\nu_M(a)} - 1)]_{f,g}(z)) > \frac{1}{q-1}.$$

Поэтому

$$l_g^{-1}\left(\frac{\varepsilon(u^{j\nu_M(a)} - 1}{\pi^n} l(x)\right) = [\varepsilon(u^{j\nu_M(a)} - 1)]_{f,g}(z).$$

Учитывая, что $[u^{j\nu_M(a)}]_f(\zeta) = \zeta$, так как $u^j \equiv 1 \pmod{\pi^{2n}}$, $\zeta \in \varkappa_n$, имеем:

$$(a, y)_{g,M,n} = [u^{-n}\varepsilon]_{f,g}((a, x)_{M,n}).$$

Предложение 7.27 следует тогда из предложения 7.26 и определения φ (см. $\varphi 1:3.5$). ■

Предложение 7.28. *Пусть* $L \supset I_j K_{\pi,n}$. *Пусть* $\xi = \pi u$, *где* $u^j \equiv 1 \pmod{\pi^{2n}}$. *Пусть* $g \in \Pi\Lambda_\xi$, $e_g^n = [u^{-n}\varepsilon]_{f,g}(e_f^n)$, *где* $\varepsilon \in C_u$. *Пусть* τ_ε — *единица в* I_j *такая, что* $\varepsilon/\tau_\varepsilon \equiv 1 \pmod{\pi^{2n}}$. *Тогда*

$$\varphi LT3. \quad \varphi_{L,n}((-1)^{p-1} e_g^n) = \frac{\tau_\varepsilon}{\xi^n l_g'(e_g^n)\ e_g^n}.$$

Доказательство. Из $\varphi 3:3.5$ следует, что достаточно доказать формулу для $L=M=I_jK_{\pi,n}$. Но в этом случае она следует из $\varphi LT2$ и предложения 7.27. ■

Пусть $M = I_jK_{\pi,n}$. Мы имеем гомоморфизмы $QL_s : M_s^* \to \dfrac{\frac{1}{\gamma_s} P_s}{\frac{\pi^s}{\pi_1\gamma_s} P_s}$ — логарифмические производные. Здесь $P_s = P_{M_s}$, а $QL_s = QL_{N,s}$, где $N = M_s$. γ_s — униформизирующая M_s. Мы уточним сейчас QL_s до гомоморфизма $QL_s : M_s^* \to \dfrac{\frac{1}{\gamma_s} P_s}{\frac{\pi^s}{\pi_1} P_s}$. Во-первых, на единицах QL_s уже определено $\left(\mathrm{mod}\, \frac{\pi^s}{\pi_1} P_s\right)$. Положим

$$QL_s\left((e_f^s)^k u\right) = k\,\frac{1}{\pi^s l'(e_f^s)\, e_f^s} + QL_s(u).$$

Покажем, что при $e_g^s = [u^{-s}\varepsilon]_{f,g}(e_f^s)$, где $u^j \equiv 1 \pmod{\pi^s}$, $g \in \Lambda_{\pi u}$,

$$QL_s(e_g^s) = \frac{\tau_\varepsilon}{\xi^s l_g'(e_g^s)\, e_g^s} \qquad (\xi = \pi u).$$

Дифференцирование

$$Q_s : O_s \to \frac{P_s}{\frac{\pi^s}{\pi_1} P_s}$$

продолжается до дифференцирования

$$Q_s : \hat{O}_{s,nr} \to \frac{P_s\hat{O}_{s,nr}}{\frac{\pi^s}{\pi_1} P_s\hat{O}_{s,nr}},$$

где $\hat{O}_{s,nr}$ — кольцо целых чисел пополнения максимального неразветвленного расширения поля M_s: на $O_{s,nr}$ оно продолжается расширением кольца констант до $O_{I_{j,nr}}$, а затем по непрерывности. Пусть $[u^{-n}\varepsilon]_{f,g}(X) = t(X)$. Тогда

$$QL_s(e_g^s) = QL_s(e_f^s) + QL_s\left(\left(\frac{t(X)}{X}\right)(e_f^s)\right).$$

Имеем:

$$QL_s\left(\left(\frac{t(X)}{X}\right)(e_f^s)\right) = \left(\left(\frac{t'(e_f^s)}{e_f^s} - \frac{t(e_f^s)}{(e_f^s)^2}\right)\Big/\frac{t(e_f^s)}{e_f^s}\right)\frac{1}{\pi^s l'(e_f^s)} =$$

$$= \frac{t'(e_f^s)}{e_g^s l'(e_f^s)\, \pi^s} - QL_s(e_f^s).$$

Но

$$l_g([u^{-s}\varepsilon]_{f,g}) = u^{-s}\varepsilon l \Rightarrow l'_g([u^{-s}\varepsilon]_{f,g})\,[u^{-s}\varepsilon]'_{f,g} = u^{-s}\varepsilon l' \Rightarrow QL_s(e_g^s) =$$

$$= \frac{\varepsilon}{u^s\pi^s l'_g(e_g^s)\,e_g^s} = \frac{\varepsilon}{\xi^s l'_g(e_g^s)\,e_g^s} = \frac{\tau_\varepsilon}{\xi^s l'_g(e_g^s)\,e_g^s},$$

так как $\varepsilon - \tau_\varepsilon \equiv 0 \pmod{\pi^s}$.

ТЕОРЕМА 7.29. *Пусть* $M = I_j K_{\pi,n}$. $\mathrm{Tr}_{2n/n}$ *переводит* $\frac{\pi^{2n}}{\pi_1}P_{2n}$ *в* $\pi^n R_M$, *так что индуцирует гомоморфизм*

$$\mathrm{Tr}_{2n/n} : \frac{\frac{1}{\gamma_{2n}}P_{2n}}{\frac{\pi^{2n}}{\pi_1}P_{2n}} \to \frac{M}{\pi^n R_M}.$$

При этом справедлива формула

$\varphi LT4$. $\varphi_{M,n}(a) = \mathrm{Tr}_{2n/n}(QL_{2n}(b))$, *где* $N_{M/K}(a) \in \pi^{\mathbf{Z}}(U_K^j \cap (1+\pi^{2n}A))$, *а* b *таково (всегда существует), что* $N_{2n}(b) = a$. *В частности, при* $(j, p) = 1$ *или* $\nu\left(\frac{\pi^{2n}}{p^k}\right) > \frac{1}{p-1}$, *где* $p^k = (j, p^\infty)$, *формула справедлива* $\forall a \in M^n$ (*т. е. на всей области определения* $\varphi_{M,n}$).

Доказательство. Для $a \in U'_M$ — группе единиц с тривиальной нормой в K — $\varphi LT4$ следует из дополнения к теореме 7.15. Далее, если e_g^n — образующая $\varkappa_{g,n}$, где $g \in \Pi\Lambda_\xi$, $\left(\frac{\xi}{\pi}\right)^j \equiv 1 \pmod{\pi^{2n}}$, то $N_{M/K} \times ((-1)^{p-1}e_g^n) = \xi^j$. Действительно, если p нечетно, то $N_{M/K}(e_g^n) = ((-1)^{q^n-q^{n-1}}\xi)^j$, так как степень M над $K_{\xi,n}$ равна j, а неприводимый унитарный многочлен для $e_g^n \in K_{\xi,n}$ над K равен $\frac{g^{(n)}}{g^{(n-1)}}$: он имеет $q^n - q^{n-1}$ корней и свободный член ξ. Если $p = 2$, то, аналогично, $N_{M/K}(-e_g^n) = \xi^j$. Но мы вычислили $\varphi_{L,n}((-1)^{p-1}e_g^n)$ (см. $\varphi LT3$: 7.1), а из того, что $N_{2n/n}(e_g^{2n}) = (-1)^{p-1}e_g^n$, где $e_g^n = [u^{-n}\varepsilon]_{f,g}(e_f^n)$, $e_g^{2n} = [u^{-2n}\varepsilon]_{f,g}(e_f^{2n})$ (см. N1:7.4), $QL_{2n}(e_g^{2n}) = \frac{\tau_\varepsilon}{\xi^{2n}l'_g(e_g^{2n})\,e_g^{2n}}$ и TR 1:7.4 следует, что

$$\varphi_{L,n}((-1)^{p-1}e_g^n) = \mathrm{Tr}_{2n/n}(QL_{2n}(e_g^{2n}))$$

(неоднозначность $N_{2n/n}^{-1}$ несущественна — это следует из теоремы 7.15). Далее, M^n состоит из элементов $a \mid N_{M/K}(a) \in \pi^{\mathbf{Z}}(1+\pi^{2n}A)$. Очевидно, $U_K^j \cap (1+\pi^{2n}A) = 1+\pi^{2n}A$ при $(j, p) = 1$. Если $\nu\left(\frac{\pi^{2n}}{p^k}\right) > \frac{1}{p-1}$, то $U_K^j \cap (1+\pi^{2n}A) \supset (1+\pi^{2n}A) \cap W^{p^k}$, где $W = \left\{u \mid \nu(u-1) \geqslant \nu\left(\frac{\pi^{2n}}{p^k}\right)\right\}$. Но из предложения 2.4 следует, что

$$W^{p^k} = \left\{u \mid \nu(u-1) \geqslant \nu(p^k) + \nu\left(\frac{\pi^{2n}}{p^k}\right)\right\} = 1+\pi^{2n}A.$$

Это доказывает «В частности ...». ■

Пусть теперь $M = I_j K_{\pi,r}$. Пусть $\xi = \pi u$, $u^j \equiv 1 \pmod{\pi^r}$, $g \in \Lambda_\xi$. Пусть $x \in E(\pi^2_{r-n+1} O_M)$. Мы знаем, что $[\pi^{r-n}](x) \in \pi_1^2 O_M$. Пусть

$$y = [\varepsilon]_{f,g}(x) \ominus_g l_g^{-1}((\varepsilon - \tau_\varepsilon) l(x)),$$

и пусть $f^{(n)}(z) = x$. Тогда

$$[\xi^n]_g \left([u^{-n}]_g \left([\varepsilon]_{f,g}(z) \ominus_g l_g^{-1} \left(\frac{(\varepsilon - \tau_\varepsilon)}{\pi^n} l(x) \right) \right) \right) = y$$

$\left(\frac{\varepsilon - \tau_\varepsilon}{\pi^n} l(x) \subset \pi_1^2 O_{\widehat{M}_{nr}}\right.$, поэтому l_g^{-1} сходится на $\left.\frac{\varepsilon - \tau_\varepsilon}{\pi^n} l(x) \right)$. Пусть $a \in M^*$, $\zeta = (a, x)_{M,n}$. Тогда

$$(a, y)_{g,M,n} = [u^{-n}\varepsilon]_{f,g}(\zeta) \oplus_g [\varepsilon(u^{j\nu_M(a)} - 1)]_{f,g}(z) \ominus_g l_g^{-1} \left(\frac{\varepsilon(u^{j\nu_M(a)} - 1)}{\pi^n} l(x) \right).$$

Но

$$[\varepsilon(u^{j\nu_M(a)} - 1)]_{f,g}(z) = \left[\varepsilon \frac{u^{j\nu_M(a)} - 1}{\pi^r} \right]_{f,g} ([\pi^{r-n}]_f(x)) \in \pi_1^2 O_{\widehat{M}_{nr}}.$$

Значит,

$$[\varepsilon(u^{j\nu_M(a)} - 1)]_{f,g}(z) = l_g^{-1} \left(\frac{\varepsilon(u^{j\nu_M(a)} - 1)}{\pi^n} l(x) \right)$$

(так как l_g на обеих величинах принимает одинаковое значение). Итак,

$$(a, y)_{g,M,n} = [u^{-n}\varepsilon]_{f,g}((a, x)_{M,n}).$$

Пусть $e_g^r = [u^{-r}\varepsilon]_{f,g}(e_f^r)$. Из $\varphi LT2 : 7.4$ следует, что

$$((-1)^{p-1} e_g^r, y)_{g,M,n} = \left[\mathrm{Tr}_{M/K} \left(\frac{1}{\xi^r l_g'(e_g^r) e_g^r} l_g(y) \right) \right] (e_g^n) =$$

$$= \left[\mathrm{Tr}_{M/K} \left(\frac{\tau_\varepsilon}{l_g'(e_g^r) e_g^r \xi^r} l(x) \right) \right]_g (e_g^n) = [\mathrm{Tr}_{M/K}(QL_r((-1)^{p-1} e_g^r) l(x))]_g (e_g^n)$$

(QL_r — уточненная логарифмическая производная). Значит,

$$((-1)^{p-1} e_g^r, x)_{M,n} = [\mathrm{Tr}_{M,K}(QL_r((-1)^{p-1} e_g^r) l(x))]_f (e_f^n).$$

Из этой формулы и из теоремы 7.19 аналогично выводу теоремы 7.29 из формулы $\varphi LT3 : 7.4$ и теоремы 7.15 выводится

ТЕОРЕМА 7.30. *Пусть $M = I_j K_{\pi,r}$, $n \leqslant r$. Имеет место формула*:

$$SPLT8. \quad (a, x)_{M,n} = [\mathrm{Tr}_{M/K}(QL_r(a) l(x))]_f (e_f^n)$$

$$\forall a \in M^* \,|\, N_{M/K}(a) \in \pi^{\mathbb{Z}} (U_K^j \cap (1 + \pi^r A)), \quad x \in E(\pi^2_{r-n+1} O_M).$$

В частности, при $(j, p) = 1$ или $\nu\left(\frac{\pi^r}{p^k}\right) > \frac{1}{p-1}$, где $p^k = (j, p^\infty)$, формула верна $\forall a \in M^*$, $\forall x \in E(\pi^2_{r-n+1} O_M)$. ■

Покажем, как теоремы этого пункта обобщаются на случай нормального вполне и слабо разветвленного расширения L поля $M = I_j K_{\pi,n}$. Согласно общей теории (см. ([2]), гл. 1, § 8), $L = M(\sqrt[i]{\gamma_M})$, где γ_M — униформизирующая M, $i \mid q^j - 1$ (в частности L — абелево расширение M). При этом γ_M определена этим условием с точностью до единицы из $U_M^i = \Theta_j^i V_M$, где Θ_j — группа корней из 1 степени $q^j - 1$, $V_M = 1 + \mu_M$. Через $\sqrt[i]{\gamma_M}$ обозначается корень i-ой степени из γ_M (неоднозначность выбора для нас несущественна).

Покажем, что $\varphi_{L,n}(\sqrt[i]{\gamma_M}) = \frac{1}{i}\varphi_{M,n}(\gamma_M) \pmod{\pi^n R_L}$ $(R_M \subset R_L)$. Действительно, это следует из того, что $\varphi_{L,n}(\sqrt[i]{\gamma_M}) = \frac{1}{i}\varphi_{L,n}(\gamma_M)$ и $\varphi 3: 3.5$. Поэтому из $\varphi LT3: 7.4$ следует, что

$$\varphi_{L,n}(\sqrt[i]{\theta(-1)^{p-1} e_g^n}) = \frac{\tau_\varepsilon}{i\xi^n l_g'(e_g^n)\, e_g^n}.$$

Здесь θ — элемент Θ_j такой, что $\theta(-1)^{p-1} e_g^n$ — i-ая степень в L^*.

Далее, $M_s \cap L = M$. Поэтому $G(L_s/L)$ канонически изоморфна $G(M_s/M)$. Следовательно,

$$N_{L_s/L}\left(\sqrt[i]{\theta_1 e_g^s}\right) = \sqrt[i]{N_{M_s/M}(\theta_1 e_g^s)} = \sqrt[i]{\theta(-1)^{p-1} e_g^n}.$$

Очевидно, $N_{L,K}\left(\sqrt[i]{\theta(-1)^{p-1} e_g^n}\right) = \xi^j$. Логарифмическую производную

$$QL_s: L_s^* \to \frac{\frac{1}{\gamma_s} P_s}{\frac{\pi^s}{\pi_1 \gamma_s} P_s}$$

$(s \sim L_s$ в QL_s, γ_s, $P_s)$ уточним до гомоморфизма в $\dfrac{\frac{1}{\gamma_s} P_s}{\frac{\pi^s}{\pi_1} P_s}$, положив $QL_s(\sqrt[i]{\gamma_M}) = \frac{1}{i} QL_{M_s,s}(\gamma_M)$. Из всего этого для L следует теорема 7.29, в формулировке которой нужно M заменить на L, и теорема 7.30, в формулировке которой нужно заменить M на L.

Уточним формулу $\chi LT1: 7.3$ для случая $K = \mathbf{Q}_p$.

Предложение 7.31. *Пусть $L \supset K_n$. Имеет место формула*

$$\chi LT2. \quad (u, e_f^n)_{L,n} = \begin{cases} \mathrm{Tr}_{L/K}\left(\log(u)\left(-\frac{1}{\pi^n}\right)\right) & \text{при } p \neq 2, \\ \mathrm{Tr}_{L/K}\left(\log(u)\left(-\frac{1}{\pi^n(1-2^{n-1})}\right)\right) & \text{при } p = 2, \ n > 1. \end{cases}$$

Доказательство. Формула следует из теоремы 7.18, если учесть, что

$$N_{s/n}^F(e_f^s) = \begin{cases} e_f^s \text{ при } p \neq 2, \\ [2^{s-n} - 2^{s-1}]_f(e_f^s) \text{ при } p = 2. \end{cases}$$

Конечно, ее можно доказать также аналогично χLT 1 : 7.3 — нужно просто сравнить $\frac{\log(N_{L,K}(u^{-1}))}{\pi^n}$ и $\frac{N_{L,K}(u^{-1})-1}{\pi^n}$, учитывая, что $N_{L,K}(u^{-1}) = 1 + \pi^n a$. ■

Поступило
25.XII.1978

Литература

1 **Ленг С.,** Алгебра, М., «Мир», 1968.

2 Алгебраическая теория чисел (под редакцией Дж. Касселса и А. Фрелиха), М., «Мир», 1969.

3 **Iwasawa K.,** On explisit formulas for the norm residue sumbol, J. Math. Soc. Japan, 20, № 1—2 (1968), 151—164.

4 **Wiles A.,** Higher resiprosity lawers, Ann. Math., 107, № 2 (1978), 235—254.

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

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

7 **Колывагин В. А.,** Символ норменного вычета в локальных полях, Успехи матем. наук, № 6 (1978), 217—218.

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