Записки научных
семинаров ПОМИ
Том 338, 2006 г.

С. В. Востоков, А. Н. Зиновьев

АРИФМЕТИКА МОДУЛЯ КОРНЕЙ ИЗОГЕНИИ ФОРМАЛЬНОЙ ГРУППЫ В МАЛОМ ВЕТВЛЕНИИ

1°. Рассматриваем однопараметрическую формальную группу $F(x,y)$ конечной высоты h над кольцом целых $\mathfrak{O}_K$ локального поля K индекса ветвления e_0. Пусть $[p]_F(X) \in pX + \mathfrak{O}_K[\![X]\!]X^2$ – эндоморфизм умножения на p формальной группы F, и L – расширение поля K, содержащее все корни изогении $[p^n]_F(X)$. Считаем, что $e = e(L/\mathbb{Q}_p)$ – индекс ветвления поля L и $v = v_L$ – нормирование в поле L. Обозначим через π и Π простые элементы полей K и L соответственно. Наша цель – изучить $\mathbb{Z}_p$-модуль $\mathrm{Ker}[p^n]_F$, а также арифметику формального модуля, построенного на максимальном идеале $\mathfrak{M}_L$ поля L.

2°. Из определения высоты формальной группы следует, что

$$[p]_F(X) \equiv cX^{p^h} \bmod (\pi, \deg(p^h+1)), \quad c \in \mathfrak{O}_K^*.$$

Поэтому, используя подготовительную лемму Вейерштрасса, ряд $[p]_F(X)$ можно переписать в виде:

$$[p]_F(X) = \widetilde{[p]}_F(X) \cdot \varepsilon(X),$$

где $\varepsilon(X) \in 1 + X\mathfrak{O}_K[\![X]\!]$, а $\widetilde{[p]}_F(X)$ – многочлен степени p^h, точнее

$$\widetilde{[p]}_F(X) = pc_0X + \pi^{\alpha_1}c_1X^{p^{m_1}} + \dots + \pi^{\alpha_k}c_kX^p + c_hX^{p^h}, \qquad (1)$$

где $c_i := c_i(X)$, $0 \leqslant i \leqslant k$ – многочлены над $\mathfrak{O}_K$, степеней меньших $p^{m_{i+1}} - p^{m_i}$ соответственно, с обратимым свободным членом в $\mathfrak{O}_K$, а $c_h \in \mathfrak{O}_K^*$ (мы пишем $m_0 := 0$, $m_{k+1} := h$). Ясно, что все корни ряда $[p]_F(X)$ совпадают с корнями многочлена $\widetilde{[p]}_F(X)$.

Положим $\alpha_0 := e_0 \leqslant p$, $\alpha_{k+1} := 0$. Тогда имеем:

$$\alpha_{k+1} < \alpha_k < \alpha_{k-1} < \dots < \alpha_1 < \alpha_0.$$

Работа выполнена при поддержке грантов РФФИ 04-01-00082a и 06-01-00741a и гранта INTAS 05-1000008-8118I.

Пусть

$$h_i := m_i - m_{i-1}, \quad 1 \leqslant i \leqslant k+1, \quad q_i = p^{h_i}$$

(здесь $h_{k+1} = h - m_k$, $m_{k+1} = h$). Ясно, что

$$h_1 + h_2 + \dots + h_{k+1} = h.$$

Положим, далее,

$$e_*^{(i)} := \frac{e}{e_0}(\alpha_{i-1} - \alpha_i)/(p^{m_i} - p^{m_{i-1}}), \quad 1 \leqslant i \leqslant k+1.$$

Лемма 1. *Если $e_0 \leqslant p$, то*

$$e_*^{(1)} > e_*^{(2)} > \dots > e_*^{(k+1)}.$$

Доказательство. Ясно, что

$$e_*^{(i)} > e_*^{(i+1)} \Longleftarrow \frac{p^{m_{i+1}} - p^{m_i}}{p^{m_i} - p^{m_{i-1}}} > \frac{\alpha_i - \alpha_{i+1}}{\alpha_{i-1} - \alpha_i}.$$

Нетрудно видеть, далее, что левая часть больше $p-1$; с другой стороны, при условии $e_0 \leqslant p$, правая часть будет меньше $p-1$. $\Box$

Лемма 2. *Пусть z – ненулевой корень изогении $[p]_F(X)$ (а, значит, и многочлена $\widetilde{[p]}_F(X)$) в поле L. Тогда*

$$v(z) = e_*^{(i)}$$

при некотором $i : 1 \leqslant i \leqslant k+1$ (предполагаем, что $h \geqslant 2$ и $e_0 \leqslant p$).

При $h = 1$ имеем

$$v(z) = \frac{e}{p-1}. \tag{$*$}$$

Доказательство. Из вида многочлена $\widetilde{[p]}_F(X)$ (см. (1)) следует, что корень z этого уравнения должен удовлетворять условию

$$v(\pi^{\alpha_j} z^{p^{m_j}}) = v(\pi^{\alpha_i} z^{p^{m_i}}) \tag{2}$$

при некоторых $j < i$.

1) Пусть сперва $j = i-1$. Тогда из равенства (2) следует, что $v(z) = e_*^{(i)}$. Осталось проверить, что в остальных узлах нормирование больше, т.е., если $j \neq i-1, i$, то

$$v(\pi^{\alpha_j} z^{p^{m_j}}) > v(\pi^{\alpha_i} z^{p^{m_i}}) \tag{3}$$

при $v(z)=e_*^{(i)}$.

а) $j>i$. Тогда (3) равносильно

$$\frac{e}{e_0}\alpha_j+p^{m_j}e_*^{(i)}>\frac{e}{e_0}\alpha_i+p^{m_i}e_*^{(i)}\iff\frac{p^{m_j}-p^{m_i}}{p^{m_i}-p^{m_{i-1}}}>\frac{\alpha_i-\alpha_j}{\alpha_{i-1}-\alpha_i}.\qquad(4)$$

Левая часть, как нетрудно видеть, больше $p-1$, т.к. $m_j\geqslant m_i+1$. Для правой части имеем

$$\frac{\alpha_i-\alpha_j}{\alpha_{i-1}-\alpha_i}\leqslant\frac{e_0-1}{1}\leqslant p-1,\quad\text{если}\quad e_0\leqslant p.$$

Отсюда следует (4).

б) $j<i-1$. Тогда (3) равносильно неравенству

$$\frac{p^{m_i}-p^{m_j}}{p^{m_i}-p^{m_{i-1}}}<\frac{\alpha_j-\alpha_i}{\alpha_{i-1}-\alpha_i}$$

или, что то же самое

$$\frac{p^{m_{i-1}}-p^{m_j}}{p^{m_i}-p^{m_{i-1}}}<\frac{\alpha_j-\alpha_{i-1}}{\alpha_{i-1}-\alpha_i}.\qquad(5)$$

При этом

$$\frac{\alpha_j-\alpha_{i-1}}{\alpha_{i-1}-\alpha_i}\geqslant\frac{1}{e_0-1}\geqslant\frac{1}{p-1}.$$

С другой стороны

$$\frac{p^{m_{i-1}}-p^{m_j}}{p^{m_i}-p^{m_{i-1}}}<\frac{p^{m_{i-1}}-1}{p^{m_{i-1}+1}-p^{m_{i-1}}}=\frac{p^{m_{i-1}}-1}{p^{m_{i-1}}(p-1)}<\frac{1}{p-1},$$

и мы получили (5).

Итак, мы доказали, что если (2) выполнено для $j=i-1$, то все члены равенства $\widetilde{[p]}_F(z)=0$, кроме $\pi^{\alpha_{i-1}}c_{i-1}^{(0)}z^{p^{m_{i-1}}}$ и $\pi^{\alpha_i}c_i^{(0)}z^{p^{m_i}}$ имеют нормирования в L большие, чем $v(\pi^{\alpha_i}z^{p^{m_i}})$ (здесь $c_i^{(0)}:=c_i(0)$). Поэтому, $v(z)=e_*^{(i)}$ и при этом

$$v(c_j\pi^{\alpha_j}z^{p^{m_j}})>v(\pi^{\alpha_i}z^{p^{m_i}}),\quad j\neq i-1,i.\qquad(6)$$

2) Пусть (2) выполнено при некоторых $j<i-1$. Проверим, что тогда

$$v(\pi^{\alpha_{i-1}}z^{p^{m_{i-1}}})<v(\pi^{\alpha_i}z^{p^{m_i}}),\qquad(7)$$

если $h\geqslant 2$, $e_0\leqslant p$.

Действительно, в этом случае

$$v(z) = \frac{e}{e_0}(\alpha_j - \alpha_i)/(p^{m_i} - p^{m_j}).$$

Поэтому неравенство (7) равносильно

$$\frac{p^{m_i} - p^{m_{i-1}}}{p^{m_i} - p^{m_j}} > \frac{\alpha_{i-1} - \alpha_i}{\alpha_j - \alpha_i} = 1 - \frac{\alpha_j - \alpha_{i-1}}{\alpha_j - \alpha_i},$$

что равносильно неравенству

$$\frac{p^{m_{i-1} - p^{m_j}}}{p^{m_i} - p^{m_j}} < \frac{\alpha_j - \alpha_{i-1}}{\alpha_j - \alpha_i}.$$

Правая часть при этом всегда $\geqslant \frac{1}{e_0}$, т.к. $e_0 \geqslant \alpha_j > \alpha_{i-1} > \alpha_i \geqslant 0$. С другой стороны, левая часть $\leqslant \frac{p-1}{p^h-1}$, т.к. $0 \leqslant m_j < m_{i-1} < m_i \leqslant h$.

Но если $h \geqslant 2$ и $e_0 \leqslant p$, то

$$\frac{p-1}{p^h-1} < \frac{1}{e_0},$$

и неравенство (7) доказано.

Неравенство (7) означает, что уравнение $\widetilde{[p]}_F(X) = 0$ не может иметь корень со значением (2) при $j < i-1$. При $n = 1$ имеем $v(p) = v(z^{p-1})$, откуда следует $(*)$. Лемма доказана.

Следствие. *Если z – корень i-ой ступени изогении $[p]_F(X)$, т.е. $v(z) = e_*^{(i)}$, то все члены pc_0z, $\pi^{\alpha_1}c_1z^{p^h}, \ldots, c_hz^{p^h}$, кроме $\pi^{\alpha_{i-1}}c_{i-1}^{(0)}$ $z^{p^{m_{i-1}}}$ и $\pi^{\alpha_i}c_i^{(0)}z^{p^{m_i}}$ имеют порядки больше, чем $v(\pi^{\alpha_i}z^{p^{m_i}}) = \frac{e}{e_0}\alpha_i + p^{m_i}e_*^{(i)}$.*

Из лемм 1 и 2 вытекает

Лемма 3. *Пусть $e_0 \leqslant p$ и z, z' – корни изогении $[p]_F(X)$ порядков $e_*^{(i)}$ и $e_*^{(j)}$, $j < i$, соответственно. Тогда*

$$z +_F z' = F(z, z')$$

является корнем порядка $e_*^{(i)}$.

Доказательство. Ясно, что

$$z +_F z' \equiv z + z' \mod \Pi z, \quad \text{если} \quad i > j.$$

Поэтому $v(z +_F z') = e_*^{(i)}$, т.к. $e_*^{(i)} < e_*^{(j)}$. $\square$

Определение. 1) *Множество корней изогении $[p]_F(X)$ порядка $e_*^{(i)}$ назовем i-ой ступенью и обозначим $\mathfrak{Z}_i$.*

2) *Множество корней изогении $[p]_F(X)$ порядков $\geqslant e_*^{(i)}$ образует, согласно лемме 3, подмодуль в формальном модуле $F(\mathfrak{M}_L)$, который мы обозначим через $\mathfrak{Z}'_i$. (Положим $\mathfrak{Z}'_0 := (0)$).*

Лемма 4.

$$\#\mathfrak{Z}_i = q_i - 1, \#\mathfrak{Z}'_i = p^{m_i}. \tag{8}$$

Следствие. $\sum\limits_{i=1}^{k+1} \#\mathfrak{Z}_i = p^h - 1.$

Доказательство леммы. Докажем индукцией, что

$$\#\mathfrak{Z}_i \leqslant p^{m_i} - p^{m_{i-1}}, \#\mathfrak{Z}'_i \leqslant p^{m_i}. \tag{9}$$

1) $i = 1$. Если существует $z \in \zeta_1$, то он должен удовлетворять сравнению

$$p + c_1^{(0)} \pi^{\alpha_1} z^{p^m - 1} \equiv 0 \mod z\Pi, \quad c_1^{(0)} \in \mathfrak{O}_k^*,$$

которое имеет $p^{m_1} - 1$ решений, значит, существует не более $p^{m_1} - 1$ корней ступени $\mathfrak{Z}_1$, попарно несравнимых по $\mod z\Pi$. Если же существует другой корень z' из ступени $\mathfrak{Z}_1$, $z' \equiv z \bmod z\Pi$, то $z -_F z' \in \mathrm{Ker}[p]_F(X)$ и $v(z -_F z') = v(z - z') > e_*^{(1)}$.

Значит, $z = z'$, т.к. любой ненулевой корень находится в какой-то ступени и $e_*^{(1)} > e_*^{(2)} > \cdots > e_*^{(k+1)}$. Итак, в $\mathfrak{Z}_1$ имеется не более $p^{m_1} - 1$ элементов. Отсюда $\mathfrak{Z}'_1 = \{0\} \cup \mathfrak{Z}_1$ имеет не более p^{m_1} элементов.

2) Индукционный переход. Пусть существует корень $z \in \mathfrak{Z}_i$. Тогда он удовлетворяет сравнению

$$\pi^{\alpha_{i-1}} c_{i-1}^{(0)} z^{p^{m_{i-1}}} + \pi^{\alpha_i} c_i^{(0)} z^{p^{m_i}} \equiv 0 \mod \pi^{\alpha_{i-1}} z^{p^{m_{i-1}}} \Pi$$

(здесь $c_i^{(0)} = c_i(0)$). Это сравнение равносильно

$$c_{i-1}^{(0)} + \pi^{\alpha_i - \alpha_{i-1}} c_i^{(0)} z^{p^{m_i} - p^{m_{i-1}}} \equiv 0 \mod \Pi. \tag{10}$$

Последнее сравнение имеет ровно $p^{m_i - m_{i-1}} - 1 = q_i - 1$ попарно несравнимых между собой решений, значит, существует не более $q_i - 1$ попарно несравнимых между собой по более высокому модулю корней i-ой ступени $\mathfrak{Z}_i$. Пусть это $z_1, z_2, \ldots, z_s$, $s \leqslant q_i - 1$ и

$z_i \not\equiv z_j \bmod z_1\Pi$. Пусть $z \in \mathfrak{Z}_i$ – еще какой-то корень, $z \neq z_1, \dots, z_s$. Тогда, например, $z \equiv z_1 \bmod z\Pi$. Поэтому, с одной стороны,

$$v(z -_F z_1^*) = v(z - z_1) > v(z_1) = e_*^{(i)},$$

а с другой: $z -_F z_1 \in \operatorname{Ker}[p]_F$, значит, $z -_F z_1 \in \mathfrak{Z}'_{i-1}$. По индукционному предположению, $\#\mathfrak{Z}'_{i-1} \leqslant p^{m_{i-1}}$. Поэтому для каждого $z_1, \dots, z_s$ имеется в $\mathfrak{Z}_i$ не более $p^{m_{i-1}}$ корней, а значит, всего корней в $\mathfrak{Z}_i$ не более $p^{m_{i-1}} s \leqslant m^{m_{i-1}}(p^{m_i - m_{i-1}} - 1) = p^{m_i} - p^{m_{i-1}}$, и мы проверили неравенства (9).

3) Докажем равенства

$$\#\mathfrak{Z}_i = p^{m_i} - p^{m_{i-1}}.$$

Пусть $x_i := \#\zeta_i$ и $z_1^{(i)}, \dots, z_{x_i}^{(i)}$ – все корни i-ой ступени $\mathfrak{Z}_i$. Из уравнения $[p]_F(X)/X = 0$ следует, что

$$p = \prod_{1 \leqslant i \leqslant k+1} \prod_{1 \leqslant j \leqslant x_i} z_j^{(i)}. \tag{11}$$

Отсюда, учитывая, что $v(z_j^{(i)}) = e_*^{(i)}$, получаем

$$x_1 e_*^{(1)} + x_2 e_*^{(2)} + \dots + x_{k+1} e_*^{(k+1)} = e. \tag{12}$$

Если предположить, что хоть один из x_i, например,

$$x_{i_0} < p^{m_{i_0}} - p^{m_{i_0} - 1},$$

то из последнего равенства и неравенства (9) имеем

$$e = \sum_{i=1}^{k+1} x_i e_*^{(i)} = \sum_{i=1}^{k+1} x_i \cdot \frac{e}{e_0} \cdot \frac{(\alpha_{i-1} - \alpha_i)}{p^{m_i} - p^{m_{i-1}}} < \sum_{i=1}^{k+1} \frac{e}{e_0}(\alpha_{i-1} - \alpha_i) = e,$$

что неверно. Лемма доказана.

Следствие. *Все поля* $\operatorname{Quot}(W(\mathbb{F}_{q_i}))$, $1 \leqslant i \leqslant k+1$, *содержатся в подполе инерции* T *поля* L*; при этом* $h_i | f$ *для любого* i, *где* $f = f(T/\mathbb{Q}_p)$ *– степень инерции поля* L.

Доказательство. В каждой i-ой ступени ζ_i выберем попарно несравнимые между собой по $\bmod \Pi^{e_*^{(i)}+1}$ корни. Согласно сравнению (10) леммы 4, всего получим $q_i - 1$ корней. Фиксируем один из них z_1, тогда любой другой корень z будет удовлетворять сравнению

$$z \equiv \theta z_1 \mod z_1\Pi, \quad \text{где} \quad \theta \in \mathcal{R}^*_{q_i}.$$

Так как z и z_1 лежат в L, то и $\theta \in T$. При этом θ пробегает все элементы из $\mathcal{R}^*_{q_i}$, т.к. мы выбрали ровно $q_i - 1$ попарно несравнимых между собой корней. Значит, $\mathrm{Quot}(W(\mathbb{F}_{q_i})) \subset T$. Отсюда, в частности, следует, что $h_i | f$. $\square$

Выберем в системе представителей Тейхмюллера $\mathcal{R}^*_{a_i}$ элементы $\theta_1^{(i)} = 1$, $\theta_2^{(i)}, \ldots, \theta_{h_i}^{(i)}$, которые образуют базис $W(\mathbb{F}_{q_i})$ над $\mathbb{Z}_p$, и пусть $z_1^{(i)}, \ldots, z_{h_i}^{(i)}$ – такие корни из $\mathfrak{Z}_i$, что

$$z_j^{(i)}/z_1^{(i)} \equiv \theta_j^{(i)} \mod \Pi. \tag{13}$$

Лемма 5. *Элементы*

$$\{z_j^{(i)} \mid 1 \leqslant i \leqslant k+1; 1 \leqslant j \leqslant h_i\}$$

образуют базис $\mathrm{Ker}[p]_F$ *над* $\mathbb{Z}/p\mathbb{Z}$.

Доказательство. Пусть

$$\sum_{i=1}^{k+1}{}_{(F)} \quad \sum_{j=1}^{h_i}{}_{(F)} \quad [c_j^{(i)}]_F(z_j^{(i)}) = 0, \tag{14}$$

где $c_j^{(i)} \in \mathbb{Z}_p$. Рассмотрим это равенство по $\mod \Pi^{e_*^{(k+1)}+1}$. Ввиду лемм 1,2 получим

$$c_1^{(k+1)} z_1^{(k+1)} + \cdots + c_{h_{k+1}}^{(k+1)} z_{h_{k+1}}^{(k+1)} \equiv 0 \mod \Pi^{e_*^{(k+1)}+1}. \tag{15}$$

Из (13) следует тогда

$$(c_1^{(k+1)}\theta_1 + \cdots + |c_{h_{k+1}}^{(k+1)}\theta_{h_{k+1}})z_1 \equiv 0 \mod \Pi^{e_*^{(k+1)}} + 1,$$

откуда

$$c_1^{(k+1)}\theta_1 + \cdots + c_{h_{k+1}}^{(k+1)}\theta_{h_{k+1}} \equiv 0 \mod \Pi,$$

и значит,

$$c_1^{(k+1)} \equiv \cdots \equiv c_{h_{k+1}}^{(k+1)} \equiv 0 \mod \Pi,$$

т.к. $\theta_1, \ldots, \theta_{h_{k+1}}$ образуют базис $W(\mathbb{F}_{q_{k+1}})$ над $\mathbb{Z}_p$.

Далее рассматриваем равенство (14) по $\mod \Pi^{e_*^{(k)}+1}$ и получаем $c_1^{(k)} \equiv \cdots \equiv c_{h_k}^{(k)} \equiv 0 \bmod p$. Продолжая процесс, получим утверждение леммы.

Пусть $z^{(i)}$ – один из корней i-ой ступени $\mathfrak{Z}_i$ и $z^{(i)}(m)$ – какой-то корень уравнения

$$[p^{m-1}]_F(X) = z^{(i)},$$

т.е. $[p^m]_F(z^{(i)}(m)) = 0$, $[p^{m-1}]_F(z^{(i)}(m)) \neq 0$.

Лемма 6. *Имеет место равенство*

$$v(z^{(i)}(m)) = e_*^{(i)}/p^{(m-1)h}.$$

Доказательство. Индукция по m. При $m = 1$ равенство доказано в лемме 2.

Пусть теперь

$$x := z^{(i)}(m+1)$$

– решение уравнения

$$[p]_F(X) = z^{(i)}(m), \tag{16}$$

т.е.

$$pc_0X + \pi^{\alpha_1}c_1X^{p^{m_1}} + \cdots + \pi^{\alpha_k}c_kX^{p^{m_k}} + c_hX^{p^h} = z^{(i)}(m).$$

Чтобы x стал корнем этого уравнения должно быть выполнено одно из равенств

$$v(z^{(i)}(m)) = v(\pi^{\alpha_j}x^{p^{m_j}}), \quad 0 \leqslant j \leqslant k+1 \tag{17}$$

$$v(\pi^{\alpha_{j-1}}x^{p^{m_{j-1}}}) = v(\pi^{\alpha_j}x^{p^{m_j}}) \tag{18}$$

(напомним, что $\alpha_0 = e_0$, $m_0 = 1$; $\alpha_{k+1} = 0$, $m_{k+1} = h$).

Равенства типа

$$v(\pi^{\alpha_j}x^{p^{m_j}}) = v(\pi^{\alpha_i}x^{p^{m_i}})$$

при $j \neq i-1,\ i+1$ невозможны, как это было показано в лемме 2.

Проверим сперва, что равенство (18) возможно только при $j = k+1$.

Пусть $0 \leqslant j \leqslant k$. Тогда по индукционному предположению имеем

$$v(z^{(i)}(m)) = e_*^{(i)}/p^{(m-1)h},$$

$$v(\pi^{\alpha_j}x^{p^{m_j}}) = \frac{e}{e_0}\alpha_j + p^{m_j}(v(x)).$$

Ясно, что $v(x) \geqslant 1$. Но

$$\begin{aligned} e_*^{(i)}/p^{(m-1)h} &= \frac{e}{e_0}\frac{\alpha_{i-1}-\alpha_i}{p^{m_i}-p^{m_{i-1}}}\cdot\frac{1}{p^{(m-1)h}} \\ &\leqslant \frac{e}{e_0}\cdot\frac{e_0-1}{p-1}\cdot\frac{1}{p^{(m-1)h}} \leqslant \frac{e}{e_0}\cdot\frac{p-2}{p-1} \leqslant \frac{e}{e_0}, \end{aligned} \tag{19}$$

т.к. $e_0 \leqslant p$ и $m \geqslant 1$.

С другой стороны,

$$\frac{e}{e_0}\alpha_j + p^{m_j}v(x) \geqslant \frac{e}{e_0} + 1 > \frac{e}{e_0},$$

т.к. при $j \leqslant k$ имеем $\alpha_j \geqslant 1$. Последнее неравенство вместе с (19) противоречит равенству (17) при $j \leqslant k$.

Проверим теперь невозможность равенств (18). Из (18) следует, что $v(x) = e_*^{(j)}$ (см. определение $e_*^{(j)}$).

Докажем, что

$$v(z^{(i)}(m)) < v(\pi^{\alpha_j}x^{p^{m_j}}). \tag{20}$$

Действительно, $v(z^{(i)}(m)) \leqslant \frac{e}{e_0}$ (см. (19)), с другой стороны,

$$\begin{aligned} v(\pi^{\alpha_j}x^{p^{m_j}}) &= \frac{e}{e_0}\left(\alpha_j + p^{m_j}\frac{\alpha_{j-1}-\alpha_j}{p^{m_j}-p^{m_{j-1}}}\right) \\ &= \frac{e}{e_0}\left(\alpha_{j-1} + \frac{p^{m_{j-1}}(\alpha_{j-1}-\alpha_j)}{p^{m_j}-p^{m_{j-1}}}\right) > \frac{e}{e_0} \end{aligned}$$

для всех $1 \leqslant j \leqslant k+1$. Тем самым, мы получили неравенство (20), что доказывает невозможность равенств (18). Итак, единственная возможность для корня x:

$$v(z^{(i)}(m)) = v(x^{p^h}),$$

откуда $v(x) = e_*^{(i)}/p^{mh}$. $\square$

Пусть $z_j^{(i)}$, $1 \leqslant i \leqslant k+1$, $1 \leqslant j \leqslant h_i$ – базис модуля $\mathrm{Ker}[p]_F$ из леммы 5 и при этом

$$z_j^{(i)}/z_1^{(i)} \equiv \theta_j^{(i)} \mod \Pi, \quad \theta_j^{(i)} \in \mathcal{R}_{q_i}^*$$

(см. (13)). Пусть $z_j^{(i)}(N)$ – фиксированные корни уравнений

$$[p^{N-1}]_F(X) = z_j^{(i)}$$

Теорема 1. *Элементы*

$$\{z_j^{(i)}(N), \quad 1 \leqslant i \leqslant k+1; \quad 1 \leqslant j \leqslant h_i\}$$

образуют базис модуля $\operatorname{Ker}[p^N]_F$ *над* $\mathbb{Z}/p^N\mathbb{Z}$.

При этом

$$z_j^{(i)}(N)/z_1^{(i)}(N) \equiv \theta_j^{(i)p^{-(N-1)}} \mod \Pi \tag{21}$$

и элементы $\theta_1^{(i)p^{-(N-1)}} = 1,\ \theta_2^{(i)p^{-(N-1)}}, \dots, \theta_{h_i}^{(i)p^{-(N-1)}}$ *образуют базис* $W(\mathbb{F}_{q_i})$ *над* $\mathbb{Z}_p$.

Доказательство. 1) Индукцией по N докажем, что указанные выше элементы задают базис. Для $N=1$ это было проверено в лемме 5.

Пусть теперь

$$\sum_{1 \leqslant i \leqslant k+1} {}_{(F)} \sum_{1 \leqslant j \leqslant h_i} {}_{(F)}[c_j^{(i)}]_F(z_j^{(i)}(N)) = 0, \tag{22}$$

где $c_j^{(j)} \in \mathbb{Z}_p$. Тогда

$$0 = [p]_F(\sum_{i,j}{}_{(F)}[c_j^{(i)}]_F(z_j^{(i)}(N)) = \sum_{i,j}{}_{(F)}[c_j^{(i)}]_F z_j^{(i)}(N-1).$$

Откуда, по индукционному предположению, $c_j^{(i)} = p^{N-1}d_j^{(i)}$ при некоторых $d_j^{(i)} \in \mathbb{Z}_p$, и значит, равенство (22) переходит в

$$\sum_{i,j}{}_{(F)}[d_j^{(i)}]_F(z_j^{(i)}) = 0.$$

Отсюда, согласно лемме 5, $d_j^{(i)} \equiv 0 \mod p$.

2) Корень $z_j^{(i)}(N)$ является решением уравнения

$$z_j^{(i)} = [p^{N-1}]_F(X) = p^{N-1}d_1 + \dots + d_{p^{h(N-1)}}X^{p^{h(N-1)}},$$

где $d_i \in \mathfrak{O}_K[\![X]\!]^*$. При этом, при подстановке $X := z_j^{(i)}(N)$ все члены уравнения, кроме последнего, будут иметь нормирования бóльшие, чем $v(z_j^{(i)})$ (см. доказательство леммы 6). Поэтому

$$z_j^{(i)} \equiv d_{p^{h(N-1)}} z_j^{(i)}(N)^{p^{h(N-1)}} \mod z_j^{(i)}\Pi.$$

Откуда получаем

$$z_j^{(i)}(N)^{p^{h(N-1)}}/z_1^{(i)}(N)^{p^{h(N-1)}} \equiv z_j^{(i)}/z_1^{(i)} \equiv \theta_j^{(i)} \mod \Pi,$$

и мы имеем сравнение (21).

Теорема доказана.

Арифметика формального модуля

В этом пункте, используя результаты предыдущих параграфов, мы найдем образующие формального модуля над $\mathbb{Z}_p$. Итак, пусть локальное поле L содержит все корни изогении $[p]_F(X)$.

Пусть $\mathfrak{M}$ – максимальный идеал кольца целых поля L и $F(\mathfrak{M})$ формальный $\mathbb{Z}_p$-модуль на идеале $\mathfrak{M}$, таким образом, для α, $\beta \in F(\mathfrak{M})$ сложение задается формальным групповым законом F:

$$\alpha +_F \beta = F(\alpha, \beta),$$

$$a\alpha = [a]_F(\alpha) \quad \text{для} \quad a \in \mathbb{Z}_p,\ \alpha \in F(\mathfrak{M}).$$

Запишем изогению $[p]_F(X)$ в виде

$$[p]_F(X) = pc_0X + \pi^{\alpha_1}c_1X^{p^{m_1}} + \dots + \pi^{\alpha_k}c_kX^{p^{m_k}} + c_hX^{p^h},$$

где $c_i(X) \in \mathfrak{O}_K[\![X]\!]^*$, $c_0 \equiv 1 \bmod X$, $\alpha_0 := e_0 > \alpha_1 > \alpha_2 > \dots > \alpha_k > 0$; $0 = m_0 < m_1 < m_2 < \dots < m_k < m_{k+1} := h$, $e_*^{(i)} := \frac{e}{e_0}(\alpha_{i-1} - \alpha_i)/(p^{m_i} - p^{m_{i-1}})$, $e_*^{(1)} > e_*^{(2)} > \dots > e_*^{(k+1)} > 1$ (см. лемму 1).

Из вида изогении $[p]_F(X)$ немедленно вытекают следующие равенства для элемента $\alpha \in F(\mathfrak{M})$.

$$[p]_F(\alpha) = \begin{cases} c_h^{(0)}\alpha^{p^h} + \dots, 1 \leqslant v(\alpha) < e_*^{(k+1)} \\ \pi^{\alpha_i}c_i^{(0)}\alpha^{p^{m_i}} + \dots,\ e_*^{(i+1)} < v(\alpha) < e_*^{(i)}, 1 \leqslant i \leqslant k \\ pc_0^{(0)}\alpha + \dots,\ e_*^{(1)} < v(\alpha) \\ \pi^{\alpha_{i-1}}c_{i-1}^{(0)}\alpha^{p^{m_{i-1}}} + \pi^{\alpha_i}c_i^{(0)}\alpha^{p^{m_i}} + \dots, \\ v(\alpha) = e_*^{(i)}, 1 \leqslant i \leqslant k+1 \end{cases}$$

(здесь $c_r^{(0)} := c_r(0)$, и v – нормирование в поле L). Точками обозначены члены более высокого порядка.

Используя эти равенства, мы получим образующие $\mathbb{Z}_p$-модуля $F(\mathfrak{M})$ так же, как в работе [4] для формальных модулей Любина–Тейта и в работе [5] для групп Хонда.

Пусть $\theta_1, \dots, \theta_f$ – базис кольца целых $\mathfrak{O}_T$ поля инерции T в L над $\mathbb{Z}_p$, состоящий из представителей системы Тейхлюллера $\mathcal{R}$. Пусть

$$\rho_i \equiv \pi^{\alpha_i} c_i^{(0)} \Pi^{-\frac{e}{e_0}\alpha_i} \mod \Pi, \ \rho_i \in \mathcal{R},$$

где Π – простой элемент поля L.

Тогда следующие элементы модуля $F(\mathfrak{M})$ будут системой образующих над $\mathbb{Z}_p$.

1) $x_{r,s} \equiv \theta_r \Pi^s \mod \Pi^{s+1}$, где $1 \leqslant s < e_*^{(k+1)}$, $p^h \nmid s$, $e_*^{(i+1)} < s < e_*^{(i)}$, $p^{m_i} e_*^{(i)} \nmid (s - \frac{e}{e_0}\alpha_i)$.

2) $y_{\theta_*}^{(i)} \equiv \theta_* \Pi^{e_*^{(i)}} \mod \Pi^{e_*^{(i)}+1}$, где θ_* пробегает все элементы из $\mathcal{R}$, которые удовлетворяют условию

$$\theta_* \not\equiv \rho_{i-1} + \rho_i \theta^{p^{m_i} - p^{m_{i-1}}} \mod \Pi$$

ни при каких $\theta \in \mathcal{R}$.

Литература

1. J. Lubin and J. Tate, *Formal complex multiplication in local fields.* — Ann. of Math. (2), **81**, No. 2 (1985), 380–387.
2. T. Honda, *On the theory of commutative formal groups.* — J. Math. Soc. Japan **22**, No. 2 (1970), 213–243.
3. E. de Shalit, *Relative Lubin-Tate groups.* — Proc. Amer. Math. Soc. **95**, No. 1 (1985), 1–4.
4. С. В. Востоков, *Норменное спаривание в формальных модулях.* — Изв. АН СССР, Сер. матем. **43**, Но. 4 (1979), 765–794.
5. О. В. Демченко, *Формальные группы Хонды: арифметика группы точек.* — Алгебра и анализ **12**, No. 1 (2000), 132–149.

Vostokov S. V., Zinoviev A. N. Arithmetic of the module of roots of the isogeny of a formal group in the case of small ramification.

In this paper for a one-dimensional formal group over the ring of integers of a local field in the case of small ramification, we study arithmetic of the module of roots of the isogeny as well as arithmetic of the formal module constructed on the maximal ideal of a local field containing all the roots of the isogeny.

С.-Петербургский государственный университет

С.-Петербургское отделение Математического института им. В. А. Стеклова РАН

E-mail: zinoviev@pdmi.ras.ru

Поступило 1 декабря 2006 г.