Math-Net.Ru

Общероссийский математический портал

Л. В. Кузьмин, Об одном свойстве ℓ -адических логарифмов единиц локальных неабелевых полей, *Изв. РАН. Сер. матем.*, 2006, том 70, выпуск 5, 97–122

DOI: <https://doi.org/10.4213/im707>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.135.184

26 апреля 2023 г., 02:36:48

УДК 519.4

Л. В. Кузьмин

Об одном свойстве ℓ -адических логарифмов единиц локальных неабелевых полей

Продолжено изучение конечных абелевых групп $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$, определенных в работе [7] и характеризующих билинейную форму $U(K_n) \times U(K_n) \rightarrow \mathbb{Q}_\ell$, $(x, y) \rightarrow \text{Sp}_{K_n/\mathbb{Q}_\ell}(\log x \cdot \log y)$, где K_n – промежуточное подполе кругового $\mathbb{Z}_\ell$ -расширения K_∞/K , K – конечное расширение $\mathbb{Q}_\ell$, $U(K_n)$ – группа единиц поля K_n и $\log$ – ℓ -адический логарифм. Доказано, что для $\ell \geq 3$ и неабелева K всегда $\mathcal{A}_n^{(p)} \neq 0$ и $\mathcal{B}_n^{(p)} \neq 0$, за исключением случая, когда $\ell = 3$ и неабелево K является квадратичным расширением некоторого кругового поля. Исследован и этот исключительный случай.

Библиография: 8 наименований.

§ 1. Введение

Пусть ℓ – фиксированное простое число и K – конечное расширение поля рациональных ℓ -адических чисел $\mathbb{Q}_\ell$. Предположим, что K содержит первообразный корень из единицы ζ_0 степени ℓ при $\ell \neq 2$ (степени 4 при $\ell = 2$). Пусть $K_\infty := \bigcup_{n=0}^\infty K_n$ – круговое $\mathbb{Z}_\ell$ -расширение поля K , где $K_n = K(\zeta_n)$ и ζ_n – первообразный корень из единицы степени ℓ^m , $m = n + 1$ при $\ell \neq 2$ ($m = n + 2$ при $\ell = 2$).

Если $U(K_n)$ – группа единиц поля K_n , то ℓ -адический логарифм определяет для любого n естественный гомоморфизм

$$\log: U(K_n) \rightarrow K_n, \quad (1.1)$$

ядро которого совпадает с группой всех корней из единицы $\mu(K_n)$ поля K_n . Возникает задача об описании образа $\log U(K_n)$ как подгруппы (или как подмодуля Галуа) в аддитивной группе K_n . В частности, встает вопрос о том, как связаны группа $\log U(K_n)$ и двойственная группа

$$U(K_n)^\perp := \{x \in K_n \mid \text{Sp}_{K_n/\mathbb{Q}_\ell}(x \cdot \log y) \in \mathbb{Z}_\ell \text{ для всех } y \in U(K_n)\}. \quad (1.2)$$

Первые глубокие результаты в этом направлении были получены К. Ивасавой [1], который в случае $K = \mathbb{Q}_\ell(\zeta_0)$ получил характеристику групп $U(K_n)^\perp$. Автор в [2] обобщил результаты Ивасава на случай произвольных круговых локальных полей и исследовал строение набора билинейных форм

$$U(K_n) \times U(K_n) \rightarrow \mathbb{Q}_\ell, \quad (x, y) \rightarrow \text{Sp}_{K_n/\mathbb{Q}_\ell}(\log x \cdot \log y), \quad x, y \in U(K_n), \quad (1.3)$$

где $n = 0, 1, \dots$. В этой же работе были получены некоторые следствия, относящиеся к задаче о ℓ -адическом регуляторе. Другие приложения были рассмотрены в работах [3] и [4].

Работа выполнена при поддержке РФФИ (проект № 04-01-00082).

© Л. В. Кузьмин, 2006

Локальный результат, который лежит в основе всех этих приложений, был впервые получен в [2], но его наиболее простая формулировка и наиболее естественное доказательство были даны в [5]. В работе [7, теорема 1.2] было получено его простое обобщение, которое мы ниже сформулируем, но для этого необходимо дать одно определение.

Через $V(K_n)$ обозначим $\mathbb{Z}_\ell$ -подмодуль Галуа в $(U(K_n)/\mu(K_n)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, порожденный группой $U(K_n)/\mu(K_n)$ и примарным элементом $w_n \in \overline{K}_n$, где $\overline{K}_n$ – алгебраическое замыкание K_n , т.е. таким элементом, что $w_n^{\ell^m} \in U(K_n)$ и $K_n(w_n)/K_n$ – неразветвленное расширение степени ℓ^m , где ℓ^m – порядок ℓ -компоненты $\mu_\ell(K_n)$ группы $\mu(K_n)$. Таким образом,

$$V(K_n)/(U(K_n)/\mu(K_n)) \cong \mu_\ell(K_n).$$

Если понятно, какое основное поле K рассматривается, мы будем вместо $V(K_n)$ записывать просто V_n .

Заметим, что отображение (1.1) однозначно продолжается по линейности до отображения

$$\log: V(K_n) \hookrightarrow K_n.$$

Пусть $V_n^\perp$ – двойственная к V_n группа, определенная, как в (1.2).

ТЕОРЕМА А [7, теорема 1.2]. *Пусть K – круговое расширение поля $\mathbb{Q}_\ell$ такое, что $\zeta_0 \in K$ и $K(\zeta_1)/K$ разветвлено. Тогда для любого $p \geq 0$ и любого $n > p$ справедливо равенство*

$$(\gamma_p - 1)\Phi_n(\log V_n) = \text{Ker } \text{Sp}_{K_n/K_p}(V_n^\perp), \quad (1.4)$$

где γ_p – некоторая образующая группы Галуа $G(K_n/K_p)$,

$$\Phi_n = \ell^{-m-1} \sum_{i=0}^{n-1} \mathcal{F}_n^{(i)} \in \mathbb{Q}_\ell[G(K_n/K_0)], \quad (1.5)$$

$\mathcal{F}_n(i) = \ell \text{Sp}_{K_n/K_{n-i}} - \text{Sp}_{K_n/K_{n-i-1}}$ и Sp_{K_n/K_j} – след из поля K_n в K_j для $j \leq n$.

Возникает вопрос: в какой мере теорема А остается справедливой, если взять в качестве K произвольное конечное расширение поля $\mathbb{Q}_\ell$, содержащее ζ_0 ? Прежде всего заметим, что для произвольного K равенство (1.4) имеет смысл рассматривать только для p , больших некоторого p_0 , хотя бы уже потому, что для малых значений p поля K_p могут совпадать с K . В частности, вместо элемента Φ_n , который в общем случае может быть не определен, следует рассматривать элемент

$$\Phi_n(p) := \sum_{i=0}^{n-p-1} \mathcal{F}_n(i).$$

Очевидно, что для любого p_0 такого, что $0 \leq p_0 < p$, выполняется равенство

$$(\gamma_p - 1)\Phi_n(p_0) = (\gamma_p - 1)\Phi_n(p).$$

В работе [7, §2] для заданных поля K и индекса p были определены две последовательности конечных абелевых ℓ -групп $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$, $n = p+1, p+2, \dots$, характеризующих меру невыполнения равенства (1.4). Именно, полагая

$$\mathcal{M}_n^{(p)} := (\gamma_p - 1)\Phi_n(p)(\log V_n) \cap \text{Ker } \text{Sp}_{K_n/K_p}(V_n^\perp),$$

мы определяем группы

$$\mathcal{A}_n^{(p)} = (\gamma_p - 1)\Phi_n(p)(\log V_n)/\mathcal{M}_n^{(p)}, \quad \mathcal{B}_n^{(p)} = \text{Ker Sp}_{K_n/K_p}(V_n^\perp)/\mathcal{M}_n^{(p)}. \quad (1.6)$$

Если будет нужно явно указать поле K , мы будем вместо $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$ записывать $\mathcal{A}^{(p)}(K_n)$ и $\mathcal{B}^{(p)}(K_n)$ соответственно. В терминах этих групп теорема А утверждает, что для кругового поля K мы имеем $\mathcal{A}_n^{(p)} = \mathcal{B}_n^{(p)} = 0$ при всех $n > p \geq 0$.

Возникает вопрос о том, как устроены группы $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$ в случае, когда K – произвольное конечное расширение $\mathbb{Q}_\ell$, содержащее ζ_0 . Этот вопрос был частично рассмотрен в работах [6] и [7]. В частности, в [7] были построены первые примеры полей K с ненулевыми группами $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$.

В случае произвольного поля K основной результат о группах $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$ дает следующая теорема, являющаяся переформулировкой основной теоремы из [6].

ТЕОРЕМА В [7, теоремы 0.3 и 0.5]. Пусть K – произвольное конечное расширение поля $\mathbb{Q}_\ell$ и $\zeta_0 \in K$. Тогда существуют индекс p и неотрицательная константа c , зависящие только от K , такие, что для всех $n > p$

$$d(\mathcal{A}_n^{(p)}) = d(\mathcal{B}_n^{(p)}) \leq cn,$$

где $d(A)$ – минимальное число образующих конечной абелевой ℓ -группы A .

Этот результат позволил получить в [7] интересные приложения к слабой гипотезе о ℓ -адическом регуляторе (теоремы 6.3 и 6.4). В настоящей работе мы продолжим изучение групп $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$. Основным результатом является

ОСНОВНАЯ ТЕОРЕМА. Пусть K – конечное неабелево расширение поля $\mathbb{Q}_\ell$ и $\zeta_0 \in K$. Пусть $\ell \neq 2$, а в случае $\ell = 3$ пусть ни при каком n поле K_n не является квадратичным расширением своего максимального кругового подполя. Тогда существует индекс p , зависящий только от K , такой, что при всех $n > p$ выполнено $\mathcal{A}_n^{(p)} \neq 0$ и $\mathcal{B}_n^{(p)} \neq 0$.

Как будет объяснено далее, неравенства $\mathcal{A}_n^{(p)} \neq 0$ и $\mathcal{B}_n^{(p)} \neq 0$ для всех $n > p$ следуют из неравенств $\mathcal{A}_{p+1}^{(p)} \neq 0$ и $\mathcal{B}_{p+1}^{(p)} \neq 0$, которые доказываются в теореме 3.1 с эффективными оценками снизу на порядки групп $\mathcal{A}_{p+1}^{(p)}$ и $\mathcal{B}_{p+1}^{(p)}$, а в теореме 3.2 даны эффективные оценки снизу и на минимальное число образующих $d(\mathcal{A}_{p+1}^{(p)})$ и $d(\mathcal{B}_{p+1}^{(p)})$ этих групп. Как объясняется ниже, эти оценки справедливы и для $d(\mathcal{A}_n^{(p)})$, $d(\mathcal{B}_n^{(p)})$ при любом $n > p$.

Опишем план работы и перечислим другие полученные в ней результаты.

В § 2 мы напоминаем (предложение 2.1) определение параметров q , δ из [6], связанных с круговым $\mathbb{Z}_\ell$ -расширением K_∞/K , а также основные свойства согласованной системы локальных параметров $\{\lambda_n \in K_n\}$, $n \geq q$, построенной в [6]. Отметим, что параметр δ был впервые введен в [8]. Он определяется из условия $\mathcal{D}(K_n/k_n) = (\lambda_n^\delta)$ для всех $n \geq q$, где k_n – максимальное круговое подполе поля K_n и $\mathcal{D}(K_n/k_n)$ – дифферента расширения K_n/k_n .

Важной характеристикой расширения K_∞/K является набор элементов $\varepsilon_n := \lambda_n^\ell - \lambda_{n-1} \in K_n$. В предложении 2.2 мы вычисляем точное значение ℓ -адического показателя элемента ε_n , а в предложении 2.3 получаем начальные члены разложения элементов ε_n и $(\gamma_{n-1} - 1)\varepsilon_n$ по степеням λ_n . Заметим,

что из [6, теорема 5.1] следует, что для любого $n > q$ элемент ε_n можно получить подстановкой λ_n в некоторый универсальный ряд Лорана, но этот более глубокий результат здесь не будет использоваться.

В настоящей работе, как и в [6], мы используем логарифмы Артина–Хассе $\eta_n(\alpha, a)$, определенные, как в (2.14). Теорема 2.1 дает специальное представление для таких логарифмов, которое существенно используется в дальнейшем.

В § 3 доказывается основная теорема. Наша цель состоит в том, чтобы при заданных α, a, β, b , где α, β – целые элементы из максимального неразветвленного подполя поля K_{p+1} и a, b – некоторые натуральные числа, вычислить по модулю $\mathbb{Z}_\ell$ значение следа

$$\mathrm{Sp}_{K_{p+1}/\mathbb{Q}_\ell} [\eta_{p+1}(\alpha, a)(\gamma_p - 1)\Phi_{p+1}(p)\eta_{p+1}(\beta, b)]. \quad (1.7)$$

Вычисление упрощается тем, что в данном случае $(\gamma_p - 1)\Phi_{p+1}(p) = \ell^{-p-2}(\gamma_p - 1)$ при $\ell \neq 2$ и $(\gamma_p - 1)\Phi_{p+1}(p) = \ell^{-p-3}(\gamma_p - 1)$ при $\ell = 2$.

В предложениях 3.1 и 3.2 мы получаем некоторые сравнения, которые будут нужны для этого вычисления. Затем мы доказываем теорему 3.1, утверждающую, что $\mathcal{A}_{p+1}^{(p)} \neq 0$ и $\mathcal{B}_{p+1}^{(p)} \neq 0$, если $\ell > 3$ или $\ell = 3$ и $\delta \neq 1$ (условие $\delta = 1$ означает, что K_{p+1} – квадратичное разветвленное расширение своего максимального кругового подполя k_{p+1}). Более того, мы получаем эффективную оценку снизу для порядков рассматриваемых групп. Согласно [7, предложение 2.1] для любого $n > p + 1$ существуют эпиморфизмы $\mathcal{A}_n^{(p)} \rightarrow \mathcal{A}_{p+1}^{(p)}$, $\mathcal{B}_n^{(p)} \rightarrow \mathcal{B}_{p+1}^{(p)}$, поэтому из нашего результата следует также нетривиальность групп $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$ для всех $n > p$. Доказательство основано на том, что в случае, когда параметры a и b в (1.7) удовлетворяют условиям $al + b = (\ell - 1)(\delta + 1)$ и $b > \delta + 1$, величина (1.7) представляется в виде суммы слагаемых, из которых все, кроме, быть может, одного, принадлежат $\mathbb{Z}_\ell$. Наоборот, это последнее слагаемое при подходящем выборе α и β оказывается нецелым и, следовательно, таковым же является и все выражение (1.7).

В предложении 3.3 мы доказываем, что группы $\mathcal{A}_{p+1}^{(p)}$ и $\mathcal{B}_{p+1}^{(p)}$ аннулируются умножением на ℓ при $p > q$ ($p > q + 1$ при $\ell = 2$). Поскольку эти группы имеют одинаковые порядки [7, (2.3)], оценка снизу порядка группы $\mathcal{A}_{p+1}^{(p)}$ немедленно приводит к оценке снизу величины $d(\mathcal{A}_{p+1}^{(p)}) = d(\mathcal{B}_{p+1}^{(p)})$. Соответствующий результат формулируется в теореме 3.2. Наконец, из предложения 3.3 и результатов [7] следует, что для всех достаточно больших p и всех $n > p$ группы $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$ изоморфны (теорема 3.3). Наши рассуждения позволяют получить также оценку сверху минимального числа образующих групп $\mathcal{A}_{p+1}^{(p)}$ и $\mathcal{B}_{p+1}^{(p)}$ (теорема 3.4).

Заметим, что в случаях $\ell = 2$ или $\ell = 3$ и $\delta = 1$ нет пар индексов a, b , удовлетворяющих указанным выше условиям, поэтому в этих случаях теорема 3.2 ничего не дает. Случай $\ell = 2$ мы надеемся рассмотреть в одной из последующих работ, а рассмотрению случая $\ell = 3$ посвящен следующий параграф.

В § 4 рассматривается случай $\ell = 3$, $\delta = 1$, который требует более тщательного анализа, так как теперь в (1.7) может быть несколько нецелых слагаемых, и мы хотим показать, что их сумма не может быть целой. Мы показываем, что в этом случае группы $\mathcal{A}_{p+1}^{(p)}$ и $\mathcal{B}_{p+1}^{(p)}$ могут быть как нулевыми, так и ненулевыми (теоремы 4.1 и 4.2) в зависимости от мощности поля вычетов поля K_{p+1} .

В заключение мы формулируем несколько открытых вопросов.

Все рассматриваемые поля предполагаются подполями некоторого фиксированного алгебраического замыкания $\overline{\mathbb{Q}}_\ell$ поля $\mathbb{Q}_\ell$. Через $\nu_\ell(\cdot)$ обозначается ℓ -адический показатель в $\overline{\mathbb{Q}}_\ell$, нормированный условием $\nu_\ell(\ell) = 1$. Если $\nu_\ell(x) = \nu_\ell(y)$, мы пишем иногда $x \sim y$. Запись $a \equiv b \pmod{c}$ означает, что $\nu_\ell(a - b) \geq \nu_\ell(c)$. Запись $a \equiv 0 \pmod{\mathbb{Z}_\ell}$ означает, что a – целый элемент.

§ 2. Вспомогательные результаты

Напомним сначала некоторые результаты из работы [6], которые потребуются нам в настоящей работе, дадим затем некоторое усиление этих результатов и докажем одно простое утверждение о логарифмах Артина–Хассе.

Везде в этом параграфе мы предполагаем, что K – фиксированное произвольное конечное расширение поля $\mathbb{Q}_\ell$, содержащее ζ_0 , и полагаем $K_n = K(\zeta_n)$, где ζ_n – первообразный корень из единицы степени ℓ^m ($m = n + 1$ при $\ell \neq 2$ и $m = n + 2$ при $\ell = 2$). Мы предполагаем, что корни ζ_n согласованы для различных n условием $\zeta_{n+1}^\ell = \zeta_n$.

Пусть $K_\infty = \bigcup_{n \geq 0} K_n$ – круговое $\mathbb{Z}_\ell$ -расширение поля K и H – максимальное неразветвленное подполе поля K_∞ . Тогда H – конечное расширение поля $\mathbb{Q}_\ell$, и для всех достаточно больших n поле K_n содержит круговое поле $k_n := H(\zeta_n)$. Следующее утверждение было доказано в [6, предложения 1.2 и 1.3].

ПРЕДЛОЖЕНИЕ 2.1. *Существуют целые неотрицательные числа q и δ , $\delta \not\equiv -1 \pmod{\ell}$, зависящие только от поля K , такие, что для любого $n \geq q$ расширение K_n/k_n чисто разветвлено и имеет некоторую степень e , не зависящую от n . Дифферента расширения K_n/k_n имеет вид*

$$\mathcal{D}(K_n/k_n) = (\lambda_n^\delta), \quad (2.1)$$

где λ_n – локальный параметр поля K_n , причем случай $\delta = 0$ возможен только тогда, когда $K_n = k_n$.

Абсолютная дифференда поля K_n имеет вид

$$\mathcal{D}(K_n) = \begin{cases} \ell^m \pi_0^{-1} \lambda_n^\delta & \text{при } \ell \neq 2, \\ 2^{m-1} \lambda_n^\delta & \text{при } \ell = 2, \end{cases} \quad (2.2)$$

где $\pi_0 = 1 - \zeta_0$.

Существует такая система локальных параметров $\lambda_n \in K_n$, что при любом $n \geq q$ выполняется сравнение

$$\lambda_{n+1}^\ell \equiv \lambda_n \pmod{\ell \lambda_n^{-\delta}}. \quad (2.3)$$

Если заданы индексы n, p такие, что $n > p \geq q$, то для дифференты расширения K_n/K_p справедлива формула

$$\mathcal{D}(K_n/K_p) = (\ell^{m-p} \lambda_n^\delta \lambda_p^{-\delta}). \quad (2.4)$$

Для $n > p \geq q$ пусть σ – некоторая образующая циклической группы Галуа $G(K_n/K_p)$ и $i_n(\sigma)$ определен как максимальный индекс i такой, что $\sigma(x) \equiv x \pmod{\lambda_n^i}$ для любого целого $x \in K_n$. Тогда

$$i_n(\sigma) = e \ell^{p+m-n} - \delta. \quad (2.5)$$

ЗАМЕЧАНИЕ. В работе [6, предложения 1.1 и 1.2] было показано, что в качестве q можно взять любой индекс такой, что расширение K_q/k_q чисто разветвлено и

$$\nu_\ell(\mathcal{D}(K_q/k_q)) < \frac{1}{2}, \quad (2.6)$$

где ν_ℓ – ℓ -адический показатель, нормированный условием $\nu_\ell(\ell) = 1$. Ниже, в качестве следствия из предложения 2.2 настоящей работы, будет показано, что в (2.6) строгое неравенство может быть заменено нестрогим.

Далее будут необходимы некоторые результаты об элементах $\varepsilon_n := \lambda_n^\ell - \lambda_{n-1}$. Для их формулировки и доказательства напомним, как строилась система униформизирующих элементов λ_n в [6]. В этой работе было доказано существование многочлена $F(X) = F(X, T) \in R[X]$, где $R = \mathcal{O}_H[[T]]$ – кольцо формальных степенных рядов одной переменной с коэффициентами из кольца целых $\mathcal{O}_H$ поля H , обладающего следующими свойствами:

(i) $F(X)$ – многочлен степени e со старшим коэффициентом 1, все остальные коэффициенты $F(X)$ делятся на T , причем свободный член не делится на T^2 ;

(ii) если $a_i(T)$ – коэффициент при X^i многочлена $F(X)$ и

$$a_i(T) = \sum_{j=j_0}^{\infty} a_{ij} T^j,$$

где $j_0 \geq 1$ и $a_{ij} \in \mathcal{O}_H$, то $\nu_\ell(a_{ij_0}) = 0$, т. е. a_{ij_0} – единица кольца $\mathcal{O}_H$;

(iii) пусть φ – автоморфизм Фробениуса поля H , действующий на R по правилу $\varphi(\sum_{i=0}^{\infty} c_i T^i) = \sum_{i=0}^{\infty} \varphi(c_i) T^i$, для целого n пусть $F^{(n)}(X, T)$ – многочлен, полученный из $F(X, T)$ действием φ^n на коэффициенты, и пусть $\pi_n = 1 - \zeta_n$ – стандартный униформизирующий элемент поля k_n ; тогда для любого $n \geq q$ в поле K_n существует униформизирующий элемент λ_n , удовлетворяющий равенству

$$F^{(-n)}(\lambda_n, \pi_n) = 0, \quad (2.7)$$

причем любое решение $\lambda_n \in K_n$ для $n > q$ индуцирует единственное решение $\lambda_{n-1} \in K_{n-1}$ уравнения $F^{(-n+1)}(X, \pi_{n-1}) = 0$, удовлетворяющее сравнению (2.3); в частности, если выбран некоторый униформизирующий элемент $\lambda_q \in K_q$, удовлетворяющий (2.7) для $n = q$, то однозначно определена последовательность $\lambda_q, \lambda_{q+1}, \dots, \lambda_n, \dots$, в которой каждый элемент удовлетворяет равенству (2.7) для соответствующего индекса и каждые два соседних члена удовлетворяют сравнению (2.3).

ПРЕДЛОЖЕНИЕ 2.2. Пусть $n > q$ и $\varepsilon_n = \lambda_n^\ell - \lambda_{n-1}$, где униформизирующие элементы λ_n и λ_{n-1} определены, как и выше. Тогда

$$\nu_\ell(\varepsilon_n) = \nu_\ell(\ell \pi_n \lambda_{n-1}^{-\delta}).$$

ДОКАЗАТЕЛЬСТВО. Прежде всего мы выведем из (2.7), что

$$\nu_\ell(F^{(-n+1)}(\lambda_n^\ell, \pi_{n-1})) = \nu_\ell(\ell \pi_n). \quad (2.8)$$

Можно представить элемент $0 = F^{(-n)}(\lambda_n, \pi_n)$ как сумму одночленов

$$\sum_{i=0}^e \sum_{j=0}^{\infty} a_{ij} \lambda_n^i \pi_n^j,$$

где коэффициенты $a_{ij} \in \mathcal{O}_H$ имеют тот же смысл, что и в (ii). При этом $a_{c0} = 1$, $a_{cj} = 0$ при $j > 0$, $a_{i0} = 0$ при $i < e$ и $a_{01} \neq 0$. Таким образом, $\sum_{j=0}^{\infty} a_{ij} \pi_n^j$ – коэффициент при X^i в $F^{(-n)}(X, \pi_n)$.

Возводя указанную выше сумму в ℓ -ю степень, получаем

$$0 = \sum c(i_1, \dots, i_\ell, j_1, \dots, j_\ell) a_{i_1 j_1} \cdots a_{i_\ell j_\ell} \lambda_n^{i_1 + \dots + i_\ell} \pi_n^{j_1 + \dots + j_\ell}, \quad (2.9)$$

где $i_k \in \{0, 1, \dots, e\}$ и $j_k \in \mathbb{Z}$, $j_k \geq 0$ для $k = 1, \dots, \ell$. Заметим, что коэффициент $c(i_1, \dots, i_\ell, j_1, \dots, j_\ell)$ делится на ℓ , за исключением случая, когда $i_1 = i_2 = \dots = i_\ell$ и $j_1 = j_2 = \dots = j_\ell$. В этом исключительном случае мы имеем $c(i_1, \dots, i_\ell, j_1, \dots, j_\ell) = 1$.

Если $c(i_1, \dots, i_\ell, j_1, \dots, j_\ell) \equiv 0 \pmod{\ell}$ и $a_{i_1 j_1} a_{i_2 j_2} \cdots a_{i_\ell j_\ell} \neq 0$, то не все индексы j_k равны нулю, так что соответствующий одночлен в (2.9) делится на $\ell \pi_n$. Если при этом не все индексы i_k равны нулю, то этот одночлен делится также на $\ell \pi_n \lambda_n$. Если все индексы i_k равны нулю, то этот одночлен делится даже на $\ell \pi_n^2$. Итак, мы имеем

$$0 \equiv \lambda_n^{e\ell} + \sum_{i=0}^{e-1} \sum_{j=1}^{\infty} a_{ij}^\ell \lambda_n^{i\ell} \pi_n^{j\ell} \pmod{\ell \pi_n \lambda_n}. \quad (2.10)$$

ЛЕММА 2.1. *Для любого $n \geq 1$ справедливо равенство $\nu_\ell(\pi_n^\ell - \pi_{n-1}) = \nu_\ell(\ell \pi_n)$. Более того, $\pi_n^\ell - \pi_{n-1} \equiv -\ell \pi_n \pmod{\ell \pi_n^2}$. В случае $n = 0$ и $\ell \neq 2$ мы имеем $\pi_0^\ell \equiv -\ell \pi_0 \pmod{\ell \pi_0^2}$.*

ДОКАЗАТЕЛЬСТВО. При $\ell = 2$ утверждение леммы проверяется непосредственно.

Пусть $\ell > 2$. Тогда

$$\pi_n^\ell = \pi_{n-1} + \sum_{i=1}^{\ell-1} \binom{\ell}{i} (-1)^i \zeta_n^i.$$

Учитывая, что $\sum_{i=1}^{\ell-1} \binom{\ell}{i} (-1)^i = 0$ и что $\binom{\ell}{i} \equiv 0 \pmod{\ell}$ при $1 \leq i \leq \ell - 1$, получаем

$$\pi_n^\ell - \pi_{n-1} = \sum_{i=1}^{\ell-1} \binom{\ell}{i} (-1)^i (\zeta_n^i - 1) \equiv 0 \pmod{\ell \pi_n}.$$

С другой стороны, $\zeta_n^i - 1 \equiv -i \pi_n \pmod{\pi_n^2}$, поэтому, учитывая, что $\binom{\ell}{i} \equiv \ell(-1)^{i-1}/i \pmod{\ell^2}$, получаем

$$\pi_n^\ell - \pi_{n-1} \equiv -\ell \pi_n \pmod{\ell \pi_n^2}.$$

Последнее утверждение леммы проверяется аналогично. Лемма доказана.

Учитывая, что $\varphi(a_{ij}) \equiv a_{ij}^\ell \pmod{\ell}$, где a_{ij} – коэффициенты из (2.10), и применяя лемму 2.1, мы получаем, что для любых i, j , где $0 \leq i < e$, $1 \leq j < \infty$, справедливо сравнение

$$a_{ij}^\ell \lambda_n^{i\ell} \pi_n^{j\ell} \equiv \varphi(a_{ij}) \lambda_n^{i\ell} \pi_{n-1}^j \pmod{\ell \pi_n}. \quad (2.11)$$

Таким образом, из (2.10) следует, что $F^{(-n+1)}(\lambda_n^\ell, \pi_{n-1}) \equiv 0 \pmod{\ell \pi_n}$.

Заметим, что при $i > 0$ сравнение (2.11) выполняется даже по модулю $\ell\pi_n\lambda_n$. Итак, чтобы доказать (2.8), достаточно проверить, что

$$\nu_\ell \left(\sum_{j=1}^{\infty} (a_{0j}^\ell \pi_n^{\ell j} - \varphi(a_{0j}) \pi_{n-1}^j) \right) = \nu_\ell(\ell\pi_n).$$

Согласно лемме 2.1 справедливо равенство $\pi_n^\ell - \pi_{n-1} = c\ell\pi_n$, где c – некоторая единица. С другой стороны, $\varphi(a_{0j}) = a_{0j}^\ell + \ell b_j$, где $b_j \in \mathcal{O}_H$. Таким образом,

$$\begin{aligned} a_{0j}^\ell \pi_n^{\ell j} - \varphi(a_{0j}) \pi_{n-1}^j &= a_{0j}^\ell (\pi_{n-1} + c\ell\pi_n)^j - (a_{0j}^\ell + \ell b_j) \pi_{n-1}^j \\ &\equiv \begin{cases} a_{01}^\ell c\ell\pi_n \pmod{\ell\pi_n^2} & \text{при } j = 1, \\ 0 \pmod{\ell\pi_n^2} & \text{при } j > 1. \end{cases} \end{aligned}$$

Это доказывает равенство (2.8), которое, в свою очередь, означает, что λ_n^ℓ является решением сравнения $F^{(-n+1)}(X, \pi_{n-1}) \equiv 0 \pmod{\ell\pi_n}$. Применяя теперь лемму Гензеля так, как это было сделано в [6, доказательство предложения 1.2], мы получаем, что λ_n^ℓ продолжается до решения λ_{n-1} уравнения $F^{(-n+1)}(X, \pi_{n-1}) = 0$, причем

$$\lambda_{n-1} = \lambda_n^\ell - F^{(-n+1)}(\lambda_n^\ell, \pi_{n-1})/G(\lambda_n^\ell, \pi_{n-1}) + \dots,$$

где $G(X, \pi_{n-1})$ – производная многочлена $F^{(-n+1)}(X, \pi_{n-1})$ и многоточием обозначены члены более высокого порядка. Легко видеть, что $\nu_\ell(G(\lambda_n^\ell, \pi_{n-1})) = \nu_\ell(G(\lambda_{n-1}, \pi_{n-1})) = \nu_\ell(\lambda_{n-1}^\delta)$, откуда, применяя (2.8), мы получаем утверждение предложения. Предложение доказано.

ПРЕДЛОЖЕНИЕ 2.3. Пусть γ_{n-1} – некоторая образующая группы Галуа $G(K_n/K_{n-1})$ и

$$\gamma_{n-1}(\lambda_n) = \begin{cases} \lambda_n + v\pi_0\lambda_n^{-\delta} & \text{при } \ell \neq 2, \\ \lambda_n + 2v\lambda_n^{-\delta} & \text{при } \ell = 2, \end{cases} \quad (2.12)$$

где $v \in K_n$ и $\nu_\ell(v) = 0$ (существование представления (2.12) следует из (2.5)). Тогда справедливы сравнения

$$(\gamma_{n-1} - 1)(\varepsilon_n) \equiv \begin{cases} v^\ell \pi_0^\ell \lambda_n^{-\ell\delta} + v\ell\pi_0\lambda_n^{\ell-1-\delta} \pmod{\ell\pi_0^2\lambda_n^{-2\delta}} & \text{при } \ell \neq 2, \\ 4v^2\lambda_n^{-2\delta} + 4v\lambda_n^{1-\delta} \pmod{8} & \text{при } \ell = 2. \end{cases}$$

Кроме того, имеет место сравнение

$$\varepsilon_n \equiv u\ell\lambda_n^{-\ell\delta+\delta+1} + z \pmod{\ell\lambda_n^{-\ell\delta+\delta+2}} \quad (2.13)$$

с некоторыми $u \in \mathcal{O}_H^\times$ и $z \in K_{n-1}$.

ДОКАЗАТЕЛЬСТВО. Пусть $\ell \neq 2$. Тогда из (2.12) следует, что

$$(\gamma_{n-1} - 1)\varepsilon_n = (\gamma_{n-1} - 1)\lambda_n^\ell = (\lambda_n + v\pi_0\lambda_n^{-\delta})^\ell - \lambda_n^\ell = v\ell\pi_0\lambda_n^{\ell-1-\delta} + \dots + v^\ell\pi_0^\ell\lambda_n^{-\ell\delta},$$

где все пропущенные члены в биномиальном разложении делятся на $\ell\pi_0^2\lambda_n^{-2\delta}$ (заметим, что из условия $n > q$ следует $\nu_\ell(\pi_0\lambda_n^{-\delta}) > 0$). Это доказывает первое утверждение предложения для случая $\ell > 2$. Для $\ell = 2$ это утверждение доказывается непосредственной проверкой.

Для доказательства второго утверждения в случае $\ell > 2$ представим элемент ε_n в виде $\varepsilon_n = u\ell\lambda_n^a + z + \dots$, где $z \in K_{n-1}$, $u \in \mathcal{O}_H^\times$ и a – максимальное целое число такое, что для некоторого $z \in K_{n-1}$ выполняется сравнение $\varepsilon_n - z \equiv 0 \pmod{\lambda_n^a}$. В частности, это означает, что $a \not\equiv 0 \pmod{\ell}$. Тогда из (2.12) следует, что

$$(\gamma_{n-1} - 1)\varepsilon_n = u\ell[(\lambda_n + v\pi_0\lambda_n^{-\delta})^a - \lambda_n^a + \dots] = u\ell av\pi_0\lambda_n^{a-\delta-1} + \dots,$$

где многоточием обозначены члены с более высоким ℓ -адическим показателем. Согласно уже доказанной части предложения элемент $(\gamma_{n-1} - 1)\varepsilon_n$ начинается с члена $v^\ell\pi_0^\ell\lambda_n^{-\ell\delta}$. Учитывая, что $\nu_\ell(\ell\pi_0) = \nu_\ell(\pi_0^\ell)$, мы получаем, что $a - \delta - 1 = -\ell\delta$, т.е. $a = -\ell\delta + \delta + 1$, что доказывает второе утверждение предложения в случае $\ell > 2$. Случай $\ell = 2$ разбирается аналогично. Заметим, что всегда $\delta \not\equiv -1 \pmod{\ell}$, что согласуется с условием $a \not\equiv 0 \pmod{\ell}$. Предложение доказано.

Применяя (2.12) к одночленам вида λ_n^a с произвольным целым a , мы получаем

СЛЕДСТВИЕ 2.1. Пусть индекс $n > q$ и параметр δ таковы, что выполнено $\nu_\ell(\pi_0\lambda_n^{-\delta-1}) > 0$ (например, это всегда имеет место при $n > q + 1$). Тогда для любого $x \in K_n$, $x \neq 0$, справедливо неравенство

$$\nu_\ell(\gamma_{n-1}(x) - x) \geq \begin{cases} \nu_\ell(x) + \nu_\ell(\pi_0\lambda_n^{-\delta-1}) & \text{при } \ell \neq 2, \\ \nu_2(x) + \nu_2(2\lambda_n^{-\delta-1}) & \text{при } \ell = 2. \end{cases}$$

Пусть n настолько велико, что $H \subset K_n$. Пусть $U(K_n)$ – группа единиц поля K_n и $\log U(K_n) \subset K_n$ – образ группы $U(K_n)$ относительно отображения ℓ -адического логарифма. Как известно, аддитивный $\mathbb{Z}_\ell$ -модуль $\log U(K_n)$ порождается логарифмами Артина–Хассе

$$\eta_n(a, \alpha) = \sum_{r=0}^{\infty} \ell^{-r} \varphi^r(\alpha) \lambda_n^{a\ell^r}, \quad (2.14)$$

где α принадлежит кольцу целых $\mathcal{O}_H$ поля H , φ – автоморфизм Фробениуса поля H и $a \in \mathbb{N}$. Мы всегда будем предполагать, что λ_n – локальный параметр из предложения 2.1.

ТЕОРЕМА 2.1. Пусть q и δ имеют тот же смысл, что и в предложении 2.1. Пусть, как и выше, $\varepsilon_n = \lambda_n^\ell - \lambda_{n-1}$, где $\lambda_n \in K_n$ и $\lambda_{n-1} \in K_{n-1}$ – локальные параметры из предложения 2.1. Тогда при $n > q + 1$ для любого логарифма Артина–Хассе справедлива формула

$$\eta_n(\alpha, a) = \alpha\lambda_n^a + \frac{a\varepsilon_n}{\ell} \sum_{r=1}^{\infty} \varphi^r(\alpha) \lambda_{n-1}^{a\ell^{r-1}-1} + \frac{1}{\ell} \eta_{n-1}(\varphi(\alpha), a) + A + B,$$

где при $\ell \geq 5$

$$A \equiv 0 \pmod{\ell\lambda_{n-1}^{a-2(\delta+1)}\pi_n^2}, \quad B = 0,$$

при $\ell = 3$

$$A \equiv 0 \pmod{\ell\lambda_{n-1}^{a-3(\delta+1)}\pi_n^3}, \quad B = 0,$$

а при $\ell = 2$

$$A \equiv 0 \pmod{\ell\lambda_{n-1}^{a-4(\delta+1)}\pi_n^4}, \quad B = \sum_r A_{r,2},$$

где $A_{r,2} = \frac{a(a\ell^{r-1}-1)}{4} \varepsilon_n^2 \varphi^r(\alpha) \lambda_{n-1}^{a\ell^{r-1}-2}$ и суммирование ведется по всем индексам $r \geq 1$ таким, что $a \cdot 2^{r-1} > 2$.

ДОКАЗАТЕЛЬСТВО. Из равенства (2.14) и определения ε_n следует

$$\begin{aligned} \eta_n(\alpha, a) &= \alpha \lambda_n^a + \sum_{r=1}^{\infty} \ell^{-r} \varphi^r(\alpha) (\varepsilon_n + \lambda_{n-1})^{a\ell^{r-1}} \\ &= \alpha \lambda_n^a + \frac{a\varepsilon_n}{\ell} \sum_{r=1}^{\infty} \varphi^r(\alpha) \lambda_{n-1}^{a\ell^{r-1}-1} + \frac{1}{\ell} \eta_{n-1}(\varphi(\alpha), a) + \sum_{r=1}^{\infty} \sum_{i=2}^{a\ell^{r-1}-1} A_{r,i}, \end{aligned}$$

где

$$A_{r,i} = \ell^{-r} \varphi^r(\alpha) \binom{a\ell^{r-1}}{i} \lambda_{n-1}^{a\ell^{r-1}-i} \varepsilon_n^i.$$

Мы оценим $\nu_\ell(A_{r,i})$ в зависимости от значений индексов i и r . Предположим сначала, что $(i, \ell) = 1$. Тогда $\binom{a\ell^{r-1}}{i} \equiv 0 \pmod{\ell^{r-1}}$. Следовательно, $\nu_\ell(A_{r,i}) \geq \nu_\ell(\ell^{-1} \lambda_{n-1}^{a\ell^{r-1}} (\lambda_{n-1}^{-1} \varepsilon_n)^i)$. Согласно предложению 2.2 мы имеем $\nu_\ell(\varepsilon_n) = \nu_\ell(\ell \pi_n \lambda_{n-1}^{-\delta})$, поэтому

$$\nu_\ell(A_{r,i}) \geq \nu_\ell(\ell^{i-1} \lambda_{n-1}^{a\ell^{r-1}-i-\delta i} \pi_n^i) = \nu_\ell(\ell(\ell \lambda_{n-1}^{-\delta-1})^{i-2} \lambda_{n-1}^{a\ell^{r-1}} \lambda_{n-1}^{-2(\delta+1)} \pi_n^i).$$

Учитывая, что $n > q + 1$, мы получаем $\nu_\ell(\ell \lambda_{n-1}^{-\delta-1}) > 0$. Далее, $r \geq 1$, поэтому $a\ell^{r-1} \geq a$. Наконец, $i \geq 2$, следовательно, при $(i, \ell) = 1$ мы имеем

$$A_{r,i} \equiv 0 \pmod{\ell \lambda_{n-1}^{a-2(\delta+1)}}, \quad (2.15)$$

причем это сравнение справедливо при любом ℓ .

Предположим теперь, что $\ell \geq 3$ и $i \equiv 0 \pmod{\ell}$. Пусть $t = \nu_\ell(i)$. Тогда $\nu_\ell(\binom{a\ell^{r-1}}{i}) \geq \max\{0, r - t - 1\}$. Рассмотрим сначала случай $r - t - 1 < 0$, т.е. $r \leq t$. В этом случае $\max\{0, r - t - 1\} = 0$. Тогда из определения $A_{r,i}$ следует, что

$$\nu_\ell(A_{r,i}) \geq -r + \nu_\ell(\lambda_{n-1}^{a\ell^{r-1}}) + i\nu_\ell(\lambda_{n-1}^{-1} \varepsilon_n). \quad (2.16)$$

Можно переписать (2.16) в виде

$$\nu_\ell(A_{r,i}) \geq -r + \nu_\ell(\lambda_{n-1}^{a\ell^{r-1}-2(\delta+1)}) + 2\nu_\ell(\lambda_{n-1}^\delta \varepsilon_n) + (i-2)\nu_\ell(\lambda_{n-1}^{-1} \varepsilon_n). \quad (2.17)$$

Согласно предложению 2.2 мы имеем $\nu_\ell(\lambda_{n-1}^{-1} \varepsilon_n) \geq 1/2$ и $\nu_\ell(\lambda_{n-1}^\delta \varepsilon_n) \geq 1$. Поскольку $r \leq t$, $a\ell^{r-1} \geq a$ и $i \geq \ell^t$, из (2.17) получаем

$$\nu_\ell(A_{r,i}) \geq -t + \nu_\ell(\lambda_{n-1}^{a-2(\delta+1)}) + 2 + \frac{\ell^t - 2}{2} = -t + \frac{\ell^t}{2} + 1 + \nu_\ell(\lambda_{n-1}^{a-2(\delta+1)}).$$

Легко видеть, что $-t + \frac{\ell^t}{2} > 0$ при $\ell \geq 3$ и $t \geq 1$. Следовательно, в случае $\ell \geq 3$ и $r \leq t$ мы имеем

$$A_{r,i} \equiv 0 \pmod{\ell \lambda_{n-1}^{a-2(\delta+1)}}.$$

Рассмотрим теперь случай $r - t - 1 \geq 0$, т.е. $r > t$. В этом случае $\max\{0, r - t - 1\} = r - t - 1$, поэтому

$$\nu_\ell(A_{r,i}) \geq -t - 1 + \nu_\ell(\lambda_{n-1}^{a\ell^{r-1}}) + i\nu_\ell(\lambda_{n-1}^{-1} \varepsilon_n). \quad (2.18)$$

Снова можно переписать (2.18) в виде

$$\nu_\ell(A_{r,i}) \geq -t - 1 + \nu_\ell(\lambda_{n-1}^{a\ell^{r-1}-2(\delta+1)}) + 2\nu_\ell(\lambda_{n-1}^\delta \varepsilon_n) + (i-2)\nu_\ell(\lambda_{n-1}^{-1} \varepsilon_n). \quad (2.19)$$

Согласно предложению 2.2 $\nu_\ell(\lambda_{n-1}^\delta \varepsilon_n) > 1$. С другой стороны, $n-1 > q$, поэтому $\nu_\ell(\lambda_{n-2}^\delta) \leq 1/2$ и $\nu_\ell(\lambda_{n-1}^\delta) \leq 1/(2\ell)$. Следовательно, $\nu_\ell(\lambda_{n-1}^{-1} \varepsilon_n) > 1 - 1/\ell$. Таким образом, учитывая, что $i \geq \ell^t$, из (2.19) получаем

$$\nu_\ell(A_{r,i}) \geq -t - 1 + \nu_\ell(\lambda_{n-1}^{a\ell^{r-1}-2(\delta+1)}) + 2 + (\ell^t - 2) \left(1 - \frac{1}{\ell}\right) = \varphi(t) + \nu_\ell(\lambda_{n-1}^{a\ell^{r-1}-2(\delta+1)}),$$

где $\varphi(t) = -t - 1 + 2/\ell + \ell^t - \ell^{t-1}$. Если $\ell \geq 5$, то $\varphi(1) > 1$. С другой стороны, при $t \geq 1$ мы имеем $\varphi'(t) > 0$, т.е. $\varphi(t) > 1$ при любом $t \geq 1$. Следовательно, при $r > t$ и $\ell \geq 5$ мы имеем

$$A_{r,i} \equiv 0 \pmod{\ell \lambda_{n-1}^{a\ell^{r-1}-2(\delta+1)}},$$

что доказывает теорему в случае $\ell \geq 5$.

При $\ell = 3$ осталось рассмотреть только случай $r > t > 0$. В этом случае, рассуждая, как и выше, мы получаем

$$\nu_\ell(A_{r,i}) \geq \nu_\ell(\lambda_{n-1}^{a\ell^{r-1}-3(\delta+1)}) + \varphi_1(t), \quad \varphi_1(t) = -t + 2\ell^{t-1}.$$

Имеем $\varphi_1(1) = 1$, $\varphi_1(2) = 4$ и $\varphi_1'(t) > 0$ при $t \geq 2$. Следовательно, $\varphi_1(t) \geq 1$ для любого натурального t , что доказывает теорему для $\ell = 3$.

Рассмотрим теперь случай $\ell = 2$. В этом случае $A = \sum_{r,i} A_{r,i}$, где суммирование проводится по всем наборам (r,i) таким, что $a2^{r-1} > i > 2$. Если i нечетно, то $A_{r,i}$ удовлетворяет сравнению (2.15). Пусть i четно, $t = \nu_2(i)$ и $r \leq t$. Тогда для $\nu_2(A_{r,i})$ справедливо неравенство (2.16), из которого следует

$$\nu_2(A_{r,i}) \geq -t + \nu_2(\lambda_{n-1}^{a\ell^{r-1}-4(\delta+1)}) + 4\nu_2(\lambda_{n-1}^\delta \varepsilon_n) + (i-4)\nu_2(\lambda_{n-1}^{-1} \varepsilon_n).$$

Как и в (2.17), мы имеем $i \geq \ell^t$, $\nu_2(\lambda_{n-1}^\delta \varepsilon_n) > 1$ и $\nu_2(\lambda_{n-1}^{-1} \varepsilon_n) \geq 1/2$. Следовательно,

$$\nu_2(A_{r,i}) \geq \nu_2(\lambda_{n-1}^{a\ell^{r-1}-4(\delta+1)}) + \varphi_2(t), \quad \varphi_2(t) = -t + 2 + 2^{t-1}.$$

Тогда $\varphi_2(1) = \varphi_2(2) = 2$ и $\varphi_2'(t) > 0$ при $t \geq 2$. Следовательно, $\varphi_2(t) > 1$ при любом натуральном t и

$$A_{r,i} \equiv 0 \pmod{\ell \lambda_{n-1}^{a-4(\delta+1)}}.$$

Осталось рассмотреть случай $\ell = 2$ и $r > t$. В этом случае, как и в (2.19), мы получаем

$$\nu_2(A_{r,i}) \geq -t - 1 + \nu_2(\lambda_{n-1}^{a\ell^{r-1}-4(\delta+1)}) + 4\nu_2(\lambda_{n-1}^\delta \varepsilon_n) + (i-4)(\lambda_{n-1}^{-1} \varepsilon_n).$$

Как и в случае $r \leq t$, отсюда получаем

$$\nu_2(A_{r,i}) \geq \nu_2(\lambda_{n-1}^{a-4(\delta+1)}) + \varphi_3(t), \quad \varphi_3(t) = -t + 1 + 2^{t-1}.$$

Снова мы видим, что $\varphi_3(1) = \varphi_3(2) = 1$ и $\varphi_3'(t) > 0$ при $t \geq 2$. Следовательно, $\varphi_3(t) \geq 1$ для любого натурального t , и в этом случае мы имеем

$$A_{r,i} \equiv 0 \pmod{\ell \lambda_{n-1}^{a-4(\delta+1)}}.$$

Теорема доказана полностью.

§ 3. Основная теорема

Фиксируем некоторый индекс $p > q$ и для некоторых $\alpha, \beta \in \mathcal{O}_H$ и натуральных a, b рассматриваем элемент

$$C = C(\alpha, a, \beta, b) := \text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}[\eta_{p+1}(\alpha, a)(\gamma_p - 1)\Phi_{p+1}(p)\eta_{p+1}(\beta, b)],$$

где, как и в (1.7), $\Phi_{p+1}(p) = \ell^{-m-1}\mathcal{F}_{p+1}^{(0)}$ и $m = m(p+1) = p+2$ при $\ell \neq 2$ ($m = m(p+1) = p+3$ при $\ell = 2$). Таким образом,

$$(\gamma_p - 1)\Phi_{p+1}(p) = \ell^{-m(p+1)}(\gamma_p - 1),$$

$$C(\alpha, a, \beta, b) = \text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}[\eta_{p+1}(\alpha, a)\ell^{-m(p+1)}(\gamma_p - 1)\eta_{p+1}(\beta, b)]. \quad (3.1)$$

В этом параграфе мы исследуем $C(\alpha, a, \beta, b) \bmod \mathbb{Z}_\ell$ как функцию от α, a, β, b при некоторых ограничениях, налагаемых на значения аргументов.

ПРЕДЛОЖЕНИЕ 3.1. Пусть $p > q$ при $\ell \neq 2$ и $p > q+1$ при $\ell = 2$. Пусть $b \geq \delta + 1$. Тогда при любом β

$$(\gamma_p - 1)\eta_{p+1}(\beta, b) \equiv \begin{cases} 0 \pmod{\pi_0 \lambda_{p+1}^{b-\delta-1}} & \text{при } \ell \neq 2, \\ 0 \pmod{2\lambda_{p+1}^{b-\delta-1}} & \text{при } \ell = 2. \end{cases}$$

Если $b > \delta + 1$, то справедливо сравнение

$$(\gamma_p - 1)\eta_{p+1}(\beta, b) \equiv \begin{cases} \beta b v \pi_0 \lambda_{p+1}^{b-\delta-1} \pmod{\pi_0 \lambda_{p+1}^{b-\delta}} & \text{при } \ell \neq 2, \\ 2\beta b v \lambda_{p+1}^{b-\delta-1} \pmod{2\lambda_{p+1}^{b-\delta}} & \text{при } \ell = 2, \end{cases}$$

где v имеет тот же смысл, что и в предложении 2.3. В частности, $v \in K_{p+1}$, $\nu_\ell(v) = 0$ и v не зависит от β и b .

ДОКАЗАТЕЛЬСТВО. Используя для $\eta_{p+1}(\beta, b)$ теорему 2.1, обозначая сумму $\sum_{r=1}^{\infty} \varphi^r(\beta) \lambda_p^{b\ell^{r-1}-1}$ через $S_p(\beta, b)$ и учитывая, что $S_p(\beta, b) \in K_p$, получаем

$$(\gamma_p - 1)\eta_{p+1}(\beta, b) = (\gamma_p - 1)\beta \lambda_{p+1}^b + b\ell^{-1}S_p(\beta, b)(\gamma_p - 1)\varepsilon_{p+1} + (\gamma_p - 1)A + (\gamma_p - 1)B,$$

причем случай $B \neq 0$ возможен только при $\ell = 2$.

Применяя (2.12), при любом $b \geq 1$ получаем

$$(\gamma_p - 1)\beta \lambda_{p+1}^b \equiv \begin{cases} \beta b v \pi_0 \lambda_{p+1}^{b-\delta-1} \pmod{\pi_0 \lambda_{p+1}^{b-\delta}} & \text{при } \ell \neq 2, \\ 2\beta b v \lambda_{p+1}^{b-\delta-1} \pmod{2\lambda_{p+1}^{b-\delta}} & \text{при } \ell = 2. \end{cases} \quad (3.2)$$

Для вычисления элемента $(\gamma_p - 1)\varepsilon_{p+1}$ мы применим предложение 2.3. Согласно последнему утверждению леммы 2.1 $\pi_0^\ell \equiv -\ell\pi_0 \pmod{\ell\pi_0^2}$, поэтому, учитывая, что $\lambda_{p+1}^\ell \equiv \lambda_p \pmod{\lambda_{p+1}^{\ell+1}}$, для любого $b \geq 1$ получаем

$$b\ell^{-1}S_p(\beta, b)(\gamma_p - 1)\varepsilon_{p+1} = \begin{cases} -b\varphi(\beta)v^\ell\pi_0\lambda_p^{b-\delta-1} + \dots & \text{при } \ell \neq 2, \\ 2b\varphi(\beta)v^2\lambda_p^{b-\delta-1} + \dots & \text{при } \ell = 2, \end{cases} \quad (3.3)$$

где многоточие обозначает члены с более высоким ℓ -адическим показателем. Таким образом, при $b > \delta + 1$ левая часть (3.3) сравнима с нулем по модулю

$\pi_0 \lambda_p^{b-\delta-1}$ (по модулю $2\lambda_p^{b-\delta-1}$ при $\ell = 2$) и, следовательно, по модулю $\pi_0 \lambda_{p+1}^{b-\delta}$ (по модулю $2\lambda_{p+1}^{b-\delta}$ при $\ell = 2$). Если $b = \delta + 1$, то $\nu_\ell(\lambda_p^{b-\delta-1}) = \nu_\ell(\lambda_{p+1}^{b-\delta-1}) = 0$.

Рассмотрим теперь член $(\gamma_p - 1)A$. Если $\ell \geq 5$, то согласно теореме 2.1 $A \equiv 0 \pmod{\ell \lambda_p^{b-2(\delta+1)}}$. Так как $\ell \lambda_p^{b-2(\delta+1)} = \lambda_p^{b-\delta} \ell \lambda_p^{-\delta-2}$, $p > q$ и $\delta \geq 1$, мы получаем, что

$$\nu_\ell(\lambda_p^{\delta+2}) \leq \nu_\ell(\lambda_p^{3\delta}) \leq \frac{1}{\ell} \nu_\ell(\lambda_q^{3\delta}) \leq \frac{3}{2\ell}.$$

Поскольку $\nu_\ell(\pi_0) = 1/(\ell - 1) < 1 - 3/(2\ell)$, мы имеем

$$A \equiv 0 \pmod{\pi_0 \lambda_p^{b-\delta}}. \quad (3.4)$$

Если $\ell = 3$, то согласно теореме 2.1 $A \equiv 0 \pmod{\ell \lambda_p^{b-3(\delta+1)} \pi_{p+1}^3}$. В этом случае $\pi_{p+1}^3 \sim \pi_p$ и $\nu_\ell(\pi_p) \geq \nu_\ell(\lambda_p^2)$, поэтому

$$\nu_\ell(\ell \lambda_p^{b-3(\delta+1)} \pi_{p+1}^3) \geq 1 + \nu_\ell(\lambda_p^{b-\delta}) - \nu_\ell(\lambda_p^{2\delta+1}). \quad (3.5)$$

Пусть $\delta \geq 2$. Тогда $\nu_\ell(\lambda_p^{2\delta}) = \frac{1}{3} \nu_\ell(\lambda_{p-1}^{2\delta}) \leq \frac{1}{3} \nu_\ell(\lambda_q^{2\delta}) \leq \frac{1}{3}$. Поскольку $2\delta \geq 4$, мы имеем $\nu_\ell(\lambda_p) \leq 1/12$, т. е. $\nu_\ell(\lambda_p^{2\delta+1}) \leq 5/12 < 1/2$. Учитывая, что $\nu_\ell(\pi_0) = 1/2$, мы получаем из (3.5), что

$$\nu_\ell(\ell \lambda_p^{b-3(\delta+1)} \pi_{p+1}^3) \geq \nu_\ell(\pi_0) + \nu_\ell(\lambda_p^{b-\delta}),$$

т. е. для A выполняется сравнение (3.4).

Предположим теперь, что $\delta = 1$. Тогда в (3.5) мы имеем $\nu_\ell(\lambda_p^{2\delta+1}) = \nu_\ell(\lambda_{p-1}) \leq \nu_\ell(\lambda_q^\delta) \leq 1/2$, откуда для A снова следует сравнение (3.4). Этим предложение доказано для $\ell \geq 3$.

Наконец, пусть $\ell = 2$. Согласно теореме 2.1 $A \equiv 0 \pmod{2\lambda_p^{b-4(\delta+1)} \pi_{p+1}^4}$. Применяя следствие из предложения 2.3, мы получаем, что $(\gamma_p - 1)A \equiv 0 \pmod{4\lambda_p^{b-4(\delta+1)} \pi_{p+1}^4}$. Учитывая, что $\pi_{p+1}^4 \sim \pi_p^2$ и индекс ветвления K_p над k_p не меньше 2, мы получаем $\nu_\ell(\lambda_p^{-4} \pi_{p+1}^4) \geq 0$. Условие $p > q + 1$ означает, что $\nu_\ell(\lambda_p^{4\delta}) = \nu_\ell(\lambda_{p-2}^\delta) \leq \nu_\ell(\lambda_q^\delta) \leq 1/2$. Следовательно,

$$(\gamma_p - 1)A \equiv 0 \pmod{2\lambda_p^b}. \quad (3.6)$$

Согласно определению слагаемого B в теореме 2.1, для того чтобы оценить $(\gamma_p - 1)B$, достаточно оценить $(\gamma_p - 1)A_{r,2}$ для любого $r \geq 1$ такого, что $b2^{r-1} > 2$, где

$$A_{r,2} = \frac{b(b2^{r-1} - 1)}{4} \varepsilon_{p+1}^2 \varphi^r(\beta) \lambda_p^{b2^{r-1}-2}.$$

Очевидно, что

$$(\gamma_p - 1)A_{r,2} = \frac{b(b2^{r-1} - 1)}{4} \varphi^r(\beta) \lambda_p^{b2^{r-1}-2} (\gamma_p - 1) \varepsilon_{p+1}^2.$$

Согласно предложению 2.3 $\gamma_p(\varepsilon_{p+1}) = \varepsilon_{p+1} + 4v^2 \lambda_{p+1}^{-2\delta} + \dots$, где $\nu_2(v) = 0$ и многогоочием обозначены члены с более высоким 2-адическим показателем. Тогда $(\gamma_p - 1)\varepsilon_{p+1}^2 \equiv 0 \pmod{8\varepsilon_{p+1}\lambda_{p+1}^{-2\delta}}$. Поскольку $\lambda_{p+1}^{2\delta} \sim \lambda_p^\delta$ и $\varepsilon_{p+1} \equiv 0 \pmod{2\lambda_p^{-\delta}}$, мы получаем $\varepsilon_{p+1}\lambda_{p+1}^{-2\delta} \equiv 0 \pmod{2\lambda_p^{-2\delta}}$. В частности, это означает, что $\nu_\ell(\varepsilon_{p+1}\lambda_{p+1}^{-2\delta}) > 0$ и $(\gamma_p - 1)\varepsilon_{p+1}^2 \equiv 0 \pmod{8}$.

Учитывая, что δ четно при $\ell = 2$, т. е. $\delta \geq 2$, и, следовательно, $b2^{r-1} - 2 \geq b - \delta$, мы получаем для любого r сравнение $(\gamma_p - 1)A_{r,2} \equiv 0 \pmod{2\lambda_p^{b-\delta}}$. Следовательно,

$$(\gamma_p - 1)B \equiv 0 \pmod{2\lambda_p^{b-\delta}}, \quad (3.7)$$

что завершает доказательство предложения.

СЛЕДСТВИЕ 3.1. При произвольном $b \geq 1$ имеет место сравнение

$$(\gamma_p - 1)\eta_{p+1}(\beta, b) \equiv \begin{cases} 0 \pmod{\pi_0\lambda_\nu^{b-\delta-1}} & \text{при } \ell \neq 2, \\ 0 \pmod{2\lambda_\nu^{b-\delta-1}} & \text{при } \ell = 2, \end{cases}$$

где $\nu = p + 1$ при $b - \delta - 1 \geq 0$ и $\nu = p$ при $b - \delta - 1 < 0$.

ДОКАЗАТЕЛЬСТВО. Действительно, при $\ell \neq 2$ это непосредственно следует из (3.2)–(3.4), если учесть, что из условия $x \equiv 0 \pmod{\pi_0\lambda_\nu^{b-\delta}}$ следует $x \equiv 0 \pmod{\pi_0\lambda_\nu^{b-\delta-1}}$. Далее, при $b - \delta - 1 \geq 0$ из условия $x \equiv 0 \pmod{\pi_0\lambda_p^{b-\delta-1}}$ следует $x \equiv 0 \pmod{\pi_0\lambda_{p+1}^{b-\delta-1}}$, а при $b - \delta - 1 < 0$ из условия $x \equiv 0 \pmod{\pi_0\lambda_{p+1}^{b-\delta-1}}$ следует $x \equiv 0 \pmod{\pi_0\lambda_p^{b-\delta-1}}$.

В случае $\ell = 2$ все рассуждения аналогичны, но нужно еще воспользоваться (3.7) для оценки члена $(\gamma_p - 1)B$.

Очевидно, что для любых $x \in K_{p+1}$ и $z \in K_p$ мы имеем $\text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}(z \times (\gamma_p - 1)x) = 0$, поэтому для вычисления элемента $C(\alpha, a, \beta, b)$ в (3.1) достаточно знать $\eta_{p+1}(\alpha, a)$ с точностью до произвольного слагаемого $z \in K_p$.

ПРЕДЛОЖЕНИЕ 3.2. Пусть натуральный индекс a таков, что $c(a, \delta) := a\ell - (\ell - 1)(\delta + 1) < 0$. Тогда для заданного $\alpha \in \mathcal{O}_H$ найдется $z \in K_p$ такой, что справедливо сравнение

$$\eta_{p+1}(\alpha, a) + z \equiv a\iota\varphi(\alpha)\lambda_{p+1}^{c(a, \delta)} \pmod{\lambda_{p+1}^{c(a, \delta)+1}},$$

где ι имеет тот же смысл, что и в предложении 2.3. В частности, $\nu_\ell(u) = 0$.

Для любых $\alpha \in \mathcal{O}_H$ и $a' > a$ найдется $z' \in K_p$ такой, что справедливо сравнение

$$\eta_{p+1}(\alpha, a') + z' \equiv 0 \pmod{\lambda_{p+1}^{c(a, \delta)+1}}.$$

ДОКАЗАТЕЛЬСТВО. Используя теорему 2.1 для $\eta_{p+1}(\alpha, a)$, получаем

$$\eta_{p+1}(\alpha, a) = \alpha\lambda_{p+1}^a + a\ell^{-1}S_p(\alpha, a)\varepsilon_{p+1} + \ell^{-1}\eta_p(\varphi(\alpha), a) + A + B, \quad (3.8)$$

где $S_p(\alpha, a)$ определяется так же, как и $S_p(\beta, b)$ в доказательстве предложения 3.1.

Поскольку $a \geq 1$ и $c(a, \delta) + 1 \leq 0$, мы имеем $\alpha\lambda_{p+1}^a \equiv A \equiv 0 \pmod{\lambda_{p+1}^{c(a, \delta)+1}}$. Далее, $\eta_p(\varphi(\alpha), a) \in K_p$, т. е. это слагаемое можно отнести к z . Таким образом, остается оценить в (3.8) только слагаемые $a\ell^{-1}S_p(\alpha, a)\varepsilon_{p+1}$ и B , причем случай $B \neq 0$ возможен только при $\ell = 2$.

Используя (2.13) и определение $S_p(\alpha, a)$, получаем

$$a\ell^{-1}S_p(\alpha, a)\varepsilon_{p+1} = a\varphi(\alpha)\lambda_p^{a-1}(u\lambda_{p+1}^{-\ell\delta+\delta+1} + z'' + \dots),$$

где $z'' \in K_p$, $\nu_\ell(u) = 0$ и многоточием обозначены члены с более высоким ℓ -адическим показателем. Из определения ε_{p+1} следует, что $\lambda_p^{a-1} \equiv$

$\lambda_{p+1}^{\ell a - \ell} \pmod{\varepsilon_{p+1}}$. Наше условие, налагаемое на a , означает, что $a - 1 < \delta$, поэтому $\nu_\ell(\lambda_p^{a-1}) < 1/2$. Поскольку $\nu_\ell(\varepsilon_{p+1}) > 1/2$, из последнего сравнения следует, что разложение λ_p^{a-1} по степеням λ_{p+1} начинается с члена $\lambda_{p+1}^{\ell a - \ell}$. Таким образом,

$$a\ell^{-1}S_p(\alpha, a)\varepsilon_{p+1} = au\varphi(\alpha)\lambda_{p+1}^{c(a, \delta)} + z' + \dots,$$

где $z' \in K_p$ и многоточием обозначены более высокие степени λ_{p+1} . Этим доказана справедливость первого сравнения предложения при $\ell \neq 2$.

В случае $\ell = 2$ мы должны оценить слагаемое B . Согласно (2.13) $\varepsilon_{p+1} = x + z$, где $x \equiv 0 \pmod{\ell\lambda_{p+1}^{-\ell\delta + \delta + 1}}$, $z \equiv 0 \pmod{\ell\lambda_p^{-\delta}}$ и $z \in K_p$ (заметим, что при $\ell = 2$ мы имеем $-\ell\delta + \delta + 1 = 1 - \delta$). Тогда $\varepsilon_{t+1}^2 = x^2 + 2xz + z^2$, причем $z^2 \in K_p$ и $2xz \equiv 0 \pmod{8\lambda_{p+1}^{1-\delta}\lambda_p^{-\delta}}$. Учитывая, что $p > q$, мы получаем $\nu_\ell(2xz) \geq 2\frac{1}{2}$.

Далее, $x = \sum_{i=1-\delta}^{\infty} 2a_i\lambda_{p+1}^i$, где $a_i \in \mathcal{O}_H$, откуда следует, что

$$x^2 = \sum_{i=1-\delta}^{\infty} 4a_i^2\lambda_{p+1}^{2i} + 8 \sum_{\substack{i,j \\ j > i, i=1-\delta}}^{\infty} a_i a_j \lambda_{p+1}^{i+j}. \quad (3.9)$$

Заметим, что $\lambda_{p+1}^2 = \lambda_p + \varepsilon_{p+1}$ и $\lambda_{p+1}^{-2} = \lambda_p^{-1}(1 + \varepsilon_{p+1}\lambda_p^{-1})^{-1} = \lambda_p^{-1} - \varepsilon_{p+1}\lambda_p^{-2} + \dots$. Поэтому из (2.3) следует, что при $i \geq 1 - \delta$ мы имеем $\lambda_{p+1}^{2i} \equiv \lambda_p^i \pmod{2\lambda_p^{-\delta-3}}$. Если $p > q + 1$, то $\nu_2(\lambda_p^{\delta+3}) < 1/2$, поэтому из (3.9) следует, что $x^2 = x_1 + z_1$, где $z_1 = \sum_{i=1-\delta}^{\infty} 4a_i^2\lambda_p^i \in K_p$ и $\nu_2(x_1) \geq 5/2$. Этим полностью доказано первое утверждение предложения.

Предположим теперь, что задан некоторый индекс $a' > a$. Повторяя все предыдущие рассуждения для $\eta_{p+1}(\alpha, a')$, мы убеждаемся в справедливости второго сравнения предложения. Предложение доказано полностью.

Теперь мы можем сформулировать и доказать первый основной результат работы.

ТЕОРЕМА 3.1. Пусть K – произвольное конечное расширение поля $\mathbb{Q}_\ell$, содержащее первообразный корень степени ℓ из единицы (степени 4 при $\ell = 2$). Пусть K характеризуется параметрами δ и q , определенными, как в предложении 2.1. Пусть $\ell \geq 3$, причем в случае $\ell = 3$ мы предполагаем, что $\delta > 1$. Тогда для любого $p > q$ и любого $n \geq p+1$ группы $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$ отличны от нуля. Более того, справедлива оценка

$$|\mathcal{A}_{p+1}^{(p)}| = |\mathcal{B}_{p+1}^{(p)}| \geq \ell^{2\rho f},$$

где $\rho = \left(\left\lceil \frac{(\ell-2)(\delta+1)}{\ell} \right\rceil - \left\lceil \frac{(\ell-2)(\delta+1)}{\ell^2} \right\rceil \right)$, $[x]$ – целая часть x и $f = [H : \mathbb{Q}_\ell]$.

ДОКАЗАТЕЛЬСТВО. Согласно [7, предложение 2.1] для любого $n > p+1$ существуют эпиморфизмы $\mathcal{A}_n^{(p)} \rightarrow \mathcal{A}_{p+1}^{(p)}$, $\mathcal{B}_n^{(p)} \rightarrow \mathcal{B}_{p+1}^{(p)}$, поэтому достаточно доказать теорему только для случая $n = p+1$. Мы рассмотрим элемент $C(\alpha, a, \beta, b)$ в случае, когда $b > \delta + 1$ и индексы a и b связаны соотношением $a\ell + b = (\ell - 1)(\delta + 1)$, причем $(a, \ell) = 1$ (условие $(b, \ell) = 1$ также выполняется и следует из указанного соотношения, поскольку $\delta \not\equiv -1 \pmod{\ell}$). Применяя для вычисления $C(\alpha, a, \beta, b)$ предложения 3.1 и 3.2 и полагая $B(\alpha, a, \beta, b) = \eta_{p+1}(\alpha, a)\ell^{-p-2}(\gamma_p - 1)\eta_{p+1}(\beta, b)$, мы получаем

$$B(\alpha, a, \beta, b) = \ell^{-p-2}\pi_0 au\varphi(\alpha)\beta bv\lambda_{p+1}^{-\delta-1} + z(\gamma_p - 1)\eta_{p+1}(\beta, b) + \dots, \quad (3.10)$$

где многоточие обозначает члены с более высоким ℓ -адическим показателем.

Из (2.1) следует, что

$$\mathcal{D}(K_{p+1}/\mathbb{Q}_\ell) = \mathcal{D}(K_{p+1}/H) = \mathcal{D}(K_{p+1}/k_{p+1})\mathcal{D}(k_{p+1}/H) = (\ell^{p+2}\pi_0^{-1}\lambda_{p+1}^\delta).$$

Таким образом, след из K_{p+1} в H любого слагаемого, обозначенного в (3.10) многочлином, является целым. Наоборот, предположим, что $\nu_\ell(\alpha) = \nu_\ell(\beta) = 0$. Тогда $\nu_\ell(a\alpha\varphi(\alpha)\beta bv) = 0$, поэтому первый член имеет нецелый след в H , т. е., полагая $D := \text{Sp}_{K_{p+1}/H}(B(\alpha, a, \beta, b))$, мы получаем $D = \varphi(\alpha)\beta c$, где

$$c := \text{Sp}_{K_{p+1}/H}(\ell^{-p-2}\pi_0 aubv\lambda_{p+1}^{-\delta-1}) \in \ell^{-1}\mathcal{O}_H \setminus \mathcal{O}_H.$$

Таким образом, при фиксированном α мы всегда можем подобрать β такой, чтобы, например, выполнялось условие $C(\alpha, a, \beta, b) = \text{Sp}_{H/\mathbb{Q}_\ell}(D) = \ell^{-1}$. Следовательно, $\ell^{-p-2}(\gamma_p - 1)\eta_{p+1}(\beta, b)$ представляет ненулевой элемент группы $\mathcal{A}_{p+1}^{(p)}$.

Теперь мы выясним, когда уравнение (относительно неизвестных a, b)

$$b + a\ell = (\ell - 1)(\delta + 1) \quad (3.11)$$

имеет решение (a, b) такое, что a, b – натуральные числа, взаимно простые с ℓ , и $b > \delta + 1$. Мы найдем также число таких решений (мы будем называть их допустимыми).

Подставляя в (3.11) $a = 1$, мы получаем $b = (\ell - 1)\delta - 1$. Таким образом, указанная пара (a, b) является допустимым решением тогда и только тогда, когда $(\ell - 2)\delta \geq 3$. Последнее условие всегда выполняется при $\ell \geq 5$ или в случае $\ell = 3$ и $\delta \neq 1$ (заметим, что ввиду условия $\delta \not\equiv -1 \pmod{\ell}$ случай $\ell = 3, \delta = 2$ невозможен).

Определим теперь число допустимых решений уравнения (3.11). Сделав замену $b' = b - (\delta + 1)$, мы получаем, что пара натуральных чисел (a, b') удовлетворяет уравнению

$$b' + a\ell = (\ell - 2)(\delta + 1), \quad (3.12)$$

причем при $\ell > 2$ из равенства (3.12) следует, что $(b', \ell) = 1$. Таким образом, необходимо найти число решений (3.12) в натуральных числах, причем нас интересуют только те решения, для которых $(a, \ell) = 1$. Если забыть о последнем условии, то всего имеется $\varkappa = \left\lfloor \frac{(\ell-2)(\delta+1)}{\ell} \right\rfloor$ решений, которым соответствуют значения $a = 1, \dots, \varkappa$. Среди этих $\varkappa$ значений a имеется ровно $\left\lfloor \frac{\varkappa}{\ell} \right\rfloor = \left\lfloor \frac{(\ell-2)(\delta+1)}{\ell^2} \right\rfloor$ значений, делящихся на ℓ . Таким образом, уравнение (3.11) имеет всего $\rho = \left\lfloor \frac{(\ell-2)(\delta+1)}{\ell} \right\rfloor - \left\lfloor \frac{(\ell-2)(\delta+1)}{\ell^2} \right\rfloor$ допустимых решений.

Отметим также, что согласно (3.12) всегда $a < \delta + 1$. Следовательно, для любых двух допустимых решений (a, b) и (a_1, b_1) , не обязательно различных, мы имеем

$$b > a_1, \quad b_1 > a. \quad (3.13)$$

Теперь мы оценим порядок группы $\mathcal{A}_{p+1}^{(p)}$. Для натурального i обозначим через $\mathcal{A}_{p+1}^{(p)}(i)$ подгруппу группы $\mathcal{A}_{p+1}^{(p)}$, порожденную образами элементов $(\gamma_p - 1)\Phi_{p+1}(p)\eta_{p+1}(\beta, b)$, где $\beta \in \mathcal{O}_H$ и $b \geq i$. Тогда группы $\mathcal{A}_{p+1}^{(p)}(i)$ образуют нестрого убывающую последовательность, причем $\mathcal{A}_{p+1}^{(p)}(1) = \mathcal{A}_{p+1}^{(p)}$ и $\mathcal{A}_{p+1}^{(p)}(i) = 0$ для некоторого достаточно большого i . Действительно, в качестве примарного элемента ω поля K_{p+1} мы можем выбрать примарный элемент

кругового поля k_{p+1} , но $\mathcal{A}_{p+1}^{(p)}(k_{p+1}) = 0$ согласно теореме А, поэтому группа $\mathcal{A}_{p+1}^{(p)}$ совпадает с группой

$$\mathcal{A}_{p+1}^{(p)}(1) = (\gamma_p - 1)\Phi_{p+1}(p) \log U(K_{p+1})/\mathcal{M}_{p+1}^{(p)}.$$

Мы покажем, что для всякого b , входящего в некоторое допустимое решение (a, b) , выполняется равенство

$$[\mathcal{A}_{p+1}^{(p)}(b) : \mathcal{A}_{p+1}^{(p)}(b+1)] = \ell^f, \quad f = [H : \mathbb{Q}_\ell]. \quad (3.14)$$

Действительно, используя (3.10), мы получаем, что для любых $\alpha, \beta \in \mathcal{O}_H$ и заданных индексов (a, b) , образующих допустимое решение уравнения (3.11), справедливо сравнение

$$C(\alpha, a, \beta, b) \equiv \text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}(\ell^{-p-2}\pi_0 a u \varphi(\alpha) \beta b v \lambda_{p+1}^{-\delta-1}) \pmod{\mathbb{Z}_\ell},$$

причем элемент $c := \text{Sp}_{K_{p+1}/H}(\ell^{-p-2}\pi_0 a u b v \lambda_{p+1}^{-\delta-1})$ принадлежит $\ell^{-1}\mathcal{O}_H \setminus \mathcal{O}_H$.

Пусть элементы $\beta_1, \dots, \beta_f$ образуют базис $\mathbb{Z}_\ell$ -модуля $\mathcal{O}_H$. Тогда $c\beta_1, \dots, c\beta_f$ образуют базис $\mathbb{Z}_\ell$ -модуля $\ell^{-1}\mathcal{O}_H$. Выберем элементы $\alpha_1, \dots, \alpha_f \in \mathcal{O}_H$ так, чтобы они образовывали базис, взаимный к базису $c\beta_1, \dots, c\beta_f$, т.е. чтобы выполнялось условие

$$\text{Sp}_{H/\mathbb{Q}_\ell}(\alpha_i \cdot c\beta_j) = \ell^{-1}\delta_{ij},$$

где $1 \leq i, j \leq f$ и δ_{ij} – символ Кронекера. Тогда мы получаем $C(\alpha_i, a, \beta_j, b) \equiv \ell^{-1}\delta_{ij} \pmod{\mathbb{Z}_\ell}$. Следовательно, образы элементов $(\gamma_p - 1)\Phi_{p+1}(p)\eta_{p+1}(\beta_j, b)$, $j = 1, \dots, f$, которые порождают группу $\mathcal{A}_{p+1}^{(p)}(b)/\mathcal{A}_{p+1}^{(p)}(b+1)$, линейно независимы в этой группе над полем из ℓ элементов, что доказывает (3.14). С другой стороны, для любого автоморфизма σ поля K_{p+1} и любых $x, y \in K_{p+1}$ мы имеем

$$\text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}(x \cdot \sigma y) = \text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}(\sigma^{-1}x \cdot y),$$

поэтому

$$\begin{aligned} & \text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}[\eta_{p+1}(\alpha, a)(\gamma_p - 1)\Phi_{p+1}(p)\eta_{p+1}(\beta, b)] \\ &= -\text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}[\gamma_p(\eta_{p+1}(\beta, b))(\gamma_p - 1)\Phi_{p+1}(p)\eta_{p+1}(\alpha, a)]. \end{aligned} \quad (3.15)$$

Легко можно показать, что для любого i группа $\mathcal{A}_{p+1}^{(p)}(i)$ является подмодулем Галуа в $\mathcal{A}_{p+1}^{(p)}$. В частности, образы элементов $\gamma_p(\eta_{p+1}(\beta_j, b))$, $j = 1, \dots, f$, порождают группу $\mathcal{A}_{p+1}^{(p)}(b)/\mathcal{A}_{p+1}^{(p)}(b+1)$. Тогда из (3.15) и из приведенного выше доказательства (3.14) следует, что

$$[\mathcal{A}_{p+1}^{(p)}(a) : \mathcal{A}_{p+1}^{(p)}(a+1)] = \ell^f \quad (3.16)$$

для любого допустимого решения (a, b) . Согласно (3.13) для имеющихся ρ допустимых решений $(a_1, b_1), \dots, (a_\rho, b_\rho)$ все 2ρ чисел $a_1, \dots, a_\rho, b_1, \dots, b_\rho$ различны. Тогда из (3.14) и (3.16) следует, что $|\mathcal{A}_{p+1}^{(p)}| \geq \ell^{2\rho f}$. Согласно формуле (2.3) работы [7] порядки групп $\mathcal{A}_{p+1}^{(p)}$ и $\mathcal{B}_{p+1}^{(p)}$ совпадают, что завершает доказательство теоремы.

Следующее утверждение позволит нам получить из теоремы 3.1 оценку снизу для минимального числа образующих групп $\mathcal{A}_{p+1}^{(p)}$ и $\mathcal{B}_{p+1}^{(p)}$.

ПРЕДЛОЖЕНИЕ 3.3. Для простого $\ell \geq 3$ и любого индекса $p > q$ группы $\mathcal{A}_{p+1}^{(p)}$ и $\mathcal{B}_{p+1}^{(p)}$ аннулируются умножением на ℓ . Это же утверждение остается верным при $\ell = 2$, если $p > q + 1$.

ДОКАЗАТЕЛЬСТВО. Покажем сначала, что группа $\mathcal{A}_{p+1}^{(p)}$ имеет период ℓ . Для этого достаточно проверить, что для любых α, a, β, b имеется включение $\ell C(\alpha, a, \beta, b) \in \mathbb{Z}_\ell$.

Если $\ell \neq 2$, то согласно следствию 3.1

$$(\gamma_p - 1)\eta_{p+1}(\beta, b) \equiv 0 \pmod{\pi_0 \lambda_\nu^{b-\delta-1}},$$

где $\nu = p + 1$ при $b - \delta - 1 \geq 0$ и $\nu = p$ при $b - \delta - 1 < 0$. В любом случае

$$\nu_\ell((\gamma_p - 1)\eta_{p+1}(\beta, b)) \geq \nu_\ell(\pi_0 \lambda_p^{-\delta}) \geq \frac{1}{\ell - 1} - \frac{1}{2\ell} > \frac{1}{2\ell}.$$

Если $c(a, \delta) < 0$, то согласно предложению 3.2 для любого $\eta_{p+1}(\alpha, a)$ существует $z \in K_p$ такое, что выполняется сравнение $\eta_{p+1}(\alpha, a) + z \equiv 0 \pmod{\lambda_{p+1}^{c(a, \delta)}}$, причем $c(a, \delta) > -(\ell - 1)(\delta + 1)$.

Если $c(a, \delta) \geq 0$, то существует $a_1 < a$ такое, что $c(a_1, \delta) < 0$, и тогда выполняется сравнение $\eta_{p+1}(\alpha, a) + z \equiv 0 \pmod{\lambda_{p+1}^{c(a_1, \delta)}}$ для некоторого $z \in K_p$. Поскольку справедливы неравенства $c(a, \delta) > -2\ell\delta$, $c(a_1, \delta) > -2\ell\delta$, $\nu_\ell(\lambda_q)^{2\delta} \leq 1$ и $p > q$, мы имеем $\nu_\ell(\lambda_{p+1}^{c(a, \delta)}) > -1/\ell$ и $\nu_\ell(\lambda_{p+1}^{c(a_1, \delta)}) > -1/\ell$. Это означает, что

$$\nu_\ell(\eta_{p+1}(\alpha, a)(\gamma_p - 1)\eta_{p+1}(\beta, b)) > -\frac{1}{2\ell} > \nu_\ell(\pi_0^{-1}).$$

Тогда из (3.1) следует, что $\ell C(\alpha, a, \beta, b) \in \mathbb{Z}_\ell$, т. е. $\mathcal{A}_{p+1}^{(p)}$ аннулируется умножением на ℓ . Случай $\ell = 2$ рассматривается аналогично.

Теперь мы докажем, что $\mathcal{B}_{p+1}^{(p)}$ аннулируется умножением на ℓ . Пусть $y \in \text{Ker } \text{Sp}_{K_{p+1}/K_p}(V_{p+1}^\perp)$ – представитель некоторого элемента из группы $\mathcal{B}_{p+1}^{(p)}$. Мы должны доказать, что ℓy представляет 0 в $\mathcal{B}_{p+1}^{(p)}$, т. е.

$$\ell y \in (\gamma_p - 1)\Phi_{p+1}(p) \log V_{p+1} = (\gamma_p - 1)\ell^{-m(p+1)} \log V_{p+1}. \quad (3.17)$$

Пусть $\mathcal{O}_{p+1}$ – кольцо целых поля K_{p+1} . Рассмотрим в K_{p+1} аддитивную подгруппу $Y := \pi_0 \lambda_{p+1} \mathcal{O}_{p+1}$ ($Y := 2\lambda_{p+1} \mathcal{O}_{p+1}$ при $\ell = 2$). Как хорошо известно, любой элемент из Y является логарифмом некоторой единицы, поэтому $Y \subseteq \log V_{p+1}$. С другой стороны, из определения дифференты $\mathcal{D}_{p+1}$ расширения $K_{p+1}/\mathbb{Q}_\ell$ и ее явного вида, указанного в (2.2), мы получаем $\mathcal{O}_{p+1}^\perp = \mathcal{D}_{p+1}^{-1} = (\ell^{-p-2} \pi_0 \lambda_{p+1}^{-\delta})$ ($\mathcal{D}_{p+1}^{-1} = (\ell^{-p-2} \lambda_{p+1}^{-\delta})$ при $\ell = 2$). Следовательно, $Y^\perp = \ell^{-p-2} \lambda_{p+1}^{-\delta-1} \mathcal{O}_{p+1} \supset V_{p+1}^\perp$. В частности, мы получаем $y \in \ell^{-p-2} \lambda_{p+1}^{-\delta-1} \mathcal{O}_{p+1}$. Тогда $\ell y = \ell^{-p-2} y_1$, где $y_1 \in \ell \lambda_{p+1}^{-\delta-1} \mathcal{O}_{p+1}$ (при $\ell = 2$ мы имеем $2y = 2^{-p-3} y_1$, где $y_1 \in 4\lambda_{p+1}^{-\delta-1} \mathcal{O}_{p+1}$).

Мы покажем, что при $\ell \neq 2$ всегда выполнено неравенство

$$\nu_\ell(\ell \lambda_{p+1}^{-\delta-1}) \geq \nu_\ell(\pi_0 \lambda_{p+1}). \quad (3.18)$$

Действительно, пусть $\ell > 3$. Тогда

$$\nu_\ell(\lambda_{p+1}^{\delta+1}) \leq \nu_\ell(\lambda_{p+1}^{2\delta}) \leq \frac{1}{\ell} \nu_\ell(\lambda_q^{2\delta}) \leq \frac{1}{\ell}.$$

С другой стороны, $\nu_\ell(\pi_0) = \frac{1}{\ell-1}$ и $\nu_\ell(\lambda_{p+1}) \leq \frac{1}{2(\ell-1)}$. Следовательно,

$$\nu_\ell(\pi_0 \lambda_{p+1}) \leq \frac{3}{2(\ell-1)} < 1 - \frac{1}{\ell} \leq \nu_\ell(\ell \lambda_{p+1}^{-\delta-1}),$$

т. е. выполняется неравенство (3.18).

В случае $\ell = 3$ предположим сначала, что $\delta > 1$. Тогда $\delta \geq 3$, что вместе с условием $\nu_\ell(\lambda_q^\delta) \leq 1/2$ дает $\nu_\ell(\lambda_{p+1}^\delta) \leq 1/6$ и $\nu_\ell(\lambda_{p+1}) \leq 1/18$. Следовательно, в этом случае

$$\nu_\ell(\pi_0 \lambda_{p+1}) \leq \frac{5}{9} < \frac{7}{9} \leq \nu_\ell(\ell \lambda_{p+1}^{-\delta-1}),$$

т. е. выполняется неравенство (3.18).

Наконец, если $\ell = 3$ и $\delta = 1$, то $\nu_\ell(\lambda_q) \leq 1/2$ и $\nu_\ell(\pi_0) = 1/4$. Тогда $\nu_\ell(\lambda_{p+1}) \leq 1/12$ и $\nu_\ell(\ell \lambda_{p+1}^{-\delta-1}) \geq 5/6$. С другой стороны, $\nu_\ell(\pi_0 \lambda_{p+1}) \leq 7/12$, т. е. снова выполняется неравенство (3.18).

Пусть теперь $\ell = 2$. В этом случае $\delta \geq 2$, $\nu_\ell(\lambda_{p+1}^\delta) \leq 1/4$ и $\nu_\ell(\lambda_{p+1}) \leq 1/8$, откуда следует, что

$$\nu_\ell(\lambda_{p+1}) \leq \nu_\ell(4 \lambda_{p+1}^{-\delta-1}). \quad (3.19)$$

Неравенства (3.18) и (3.19) означают, что элемент y_1 является логарифмом некоторой единицы, т. е. существует единица $u \in U(K_{p+1})$ такая, что $\log u = y_1$. Поскольку $\text{Sp}_{K_{p+1}/K_p}(y_1) = 0$ и группа всех корней из единицы $\mu(K_{p+1})$ в поле K_{p+1} кохомологически тривиальна как $G(K_{p+1}/K_p)$ -модуль, мы можем считать, что $N_{K_{p+1}/K_p}(u) = 1$. Согласно теореме 90 Гильберта тогда существует элемент $v \in K_{p+1}^\times$ такой, что $u = v^{\gamma_p-1}$. Элемент v можно записать в виде $v = \lambda_{p+1}^a u_1$ с некоторым целым a и некоторой единицей u_1 . Если $a \equiv 0 \pmod{\ell}$, то $a = a_1 \ell$ и $v = \lambda_{p+1}^{a_1} u_2$ для некоторой единицы $u_2 \in U(K_{p+1})$. Тогда $u = u_2^{\gamma_p-1}$, т. е. $y_1 = \log u = (\gamma_p - 1) \log u_2$, что доказывает (3.17). Если $a \not\equiv 0 \pmod{\ell}$, то, полагая $u_3 = N_{K_{p+1}/k_{p+1}}(v)$, мы получаем, что $u_3 = v_1^{\gamma_p-1}$ и $v_1 = \pi_{p+1}^a u_4$, где π_{p+1} — униформизирующий элемент кругового поля k_{p+1} и $u_4 \in U(k_{p+1})$. Условие $a \not\equiv 0 \pmod{\ell}$ означает, что $\log u_3 \notin (\gamma_p - 1) \log U(k_{p+1})$, но тогда из кохомологической тривиальности $G(k_{p+1}/k_p)$ -модуля $V(k_{p+1})/\log U(k_{p+1}) \cong \mu_\ell(k_{p+1})$ следует, что $\log u_3 \notin (\gamma_p - 1) \log V(k_{p+1})$. С другой стороны, очевидно, что $\ell^{-m(p+1)} \log u_3 \in \text{Ker } \text{Sp}_{k_{p+1}/k_p}(V(k_{p+1})^\perp)$, и мы получаем противоречие с тем, что для кругового поля k_{p+1} справедлива теорема А. Предложение доказано.

Из предложения 3.3 и теоремы 3.1 немедленно следует

ТЕОРЕМА 3.2. *Для конечной абелевой ℓ -группы A пусть $d(A)$ — минимальное число образующих группы A . Тогда в условиях и обозначениях теоремы 3.1 справедливо неравенство*

$$d(\mathcal{A}_{p+1}^{(p)}) = d(\mathcal{B}_{p+1}^{(p)}) \geq \ell^{2pf}.$$

Отметим также, что равенство $d(\mathcal{A}_{p+1}^{(p)}) = d(\mathcal{B}_{p+1}^{(p)})$ было доказано в теореме 2.1 работы [7] при более сильных ограничениях на p .

Другое интересное следствие из предложения 3.3 получится, если скомбинировать его с теоремой 2.1 работы [7].

ТЕОРЕМА 3.3. *Для заданного поля K , являющегося конечным расширением поля $\mathbb{Q}_\ell$, найдется индекс r , зависящий только от K , такой, что для любых $n > p \geq r$ конечные абелевы ℓ -группы $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$ изоморфны.*

Заметим, что r имеет здесь тот же смысл, что и в теореме 2.1 из [7].

Наш метод позволяет также получить оценку сверху порядка групп $\mathcal{A}_{p+1}^{(p)}$ и $\mathcal{B}_{p+1}^{(p)}$.

ТЕОРЕМА 3.4. *В обозначениях теоремы 3.1 пусть $p > q$ при $\ell \neq 2$ и $p > q+1$ при $\ell = 2$. Тогда для любого простого ℓ справедлива оценка*

$$|\mathcal{A}_{p+1}^{(p)}| = |\mathcal{B}_{p+1}^{(p)}| \leq \ell^{\tau f},$$

где $\tau = (\ell - 1)\delta - 1 - \left\lfloor \frac{(\ell-1)\delta-1}{\ell} \right\rfloor$ при $\ell \neq 2$ и $\tau = \frac{\delta}{2} - 1$ при $\ell = 2$.

ДОКАЗАТЕЛЬСТВО. Как было показано в доказательстве теоремы 3.1, $\mathcal{A}_{p+1}^{(p)} \cong \mathcal{A}_{p+1}^{(p)}(1)/\mathcal{A}_{p+1}^{(p)}(b_0)$ для некоторого достаточно большого b_0 , где $\mathcal{A}_{p+1}^{(p)}(i)$ – подгруппа в $\mathcal{A}_{p+1}^{(p)}$, порожденная образами элементов $\theta(\beta, b) := (\gamma_p - 1)\Phi_{p+1}(p) \times \eta_{p+1}(\beta, b)$ при $\beta \in \mathcal{O}_H$ и $b \geq b_0$. Согласно следствию из предложения 3.1 для любого $a \geq 1$ и любого $\alpha \in \mathcal{O}_H$ справедливо сравнение

$$(\gamma_p - 1)\eta_{p+1}(\alpha, a) \equiv \begin{cases} 0 \pmod{\pi_0 \lambda_p^{-\delta}} & \text{при } \ell \neq 2, \\ 0 \pmod{2\lambda_p^{-\delta}} & \text{при } \ell = 2. \end{cases} \quad (3.20)$$

Заметим, что $C(\alpha, a, \beta, b) \equiv 0 \pmod{\mathbb{Z}_\ell}$ при любых $\alpha, \beta \in \mathcal{O}_H$, $\alpha \geq 1$ и $b \geq b_0$ тогда и только тогда, когда $C(\beta, b, \alpha, a) \equiv 0 \pmod{\mathbb{Z}_\ell}$ при тех же условиях на α, a, β, b . Учитывая, что $\mathcal{D}(K_{p+1}/\mathbb{Q}_\ell) = (\ell^{p+2}\pi_0^{-1}\lambda_{p+1}^\delta)$ и $(\gamma_p - 1)\Phi_{p+1}(p) = \ell^{-p-2}(\gamma_p - 1)$ при $\ell \neq 2$ ($\mathcal{D}(K_{p+1}/\mathbb{Q}_\ell) = (2^{p+2}\lambda_{p+1}^\delta)$, $(\gamma_p - 1)\Phi_{p+1}(p) = \ell^{-p-3}(\gamma_p - 1)$ при $\ell = 2$), и применяя (3.20), мы получаем, что $C(\beta, b, \alpha, a) \equiv 0 \pmod{\mathbb{Z}_\ell}$, если при некотором $z \in K_p$ справедливо сравнение

$$\eta_{p+1}(\beta, b) + z \equiv 0 \pmod{\lambda_{p+1}^{(\ell-1)\delta}}. \quad (3.21)$$

Применим к $\eta_{p+1}(\beta, b)$ равенство (3.8). Сравнение $\beta\lambda_{p+1}^b \equiv 0 \pmod{\lambda_{p+1}^{(\ell-1)\delta}}$ выполняется при $b \geq (\ell - 1)\delta$.

Согласно (2.13) для некоторого $z_1 \in K_p$ справедливо сравнение $\varepsilon_{p+1} + z_1 \equiv 0 \pmod{\lambda_{p+1}^{-b\delta+\delta+1}}$. Таким образом, сравнение $b\ell^{-1}S_p(\beta)\varepsilon_{p+1} + z_2 \equiv 0 \pmod{\lambda_{p+1}^{(\ell-1)\delta}}$ выполняется для некоторого $z_2 \in K_p$, если $b\ell \geq 2\ell\delta - 2\delta - 1$. Легко видеть, что второе неравенство следует из первого, т. е., полагая $b_0 = (\ell - 1)\delta$, мы получаем, что при $b \geq b_0$ первые два слагаемые в правой части формулы (3.8), примененной к $\eta_{p+1}(\beta, b)$, не влияют на значение $C(\beta, b, \alpha, a) \pmod{\mathbb{Z}_\ell}$.

Рассмотрим теперь добавочный член A . Согласно теореме 2.1 при $b \geq b_0 = (\ell - 1)\delta$ справедливо сравнение $A \equiv 0 \pmod{\ell\lambda_p^{b_0-\varkappa(\delta+1)}}$, где $\varkappa = 2$ при $\ell > 3$, $\varkappa = 3$ при $\ell = 3$ и $\varkappa = 4$ при $\ell = 2$. Таким образом, A удовлетворяет сравнению $A \equiv 0 \pmod{\lambda_{p+1}^{(\ell-1)\delta}}$, если только $\ell \equiv 0 \pmod{\lambda_p^{\varkappa(\delta+1)}}$. При $\ell \geq 3$ последнее сравнение следует из того, что $\nu_\ell(\lambda_p^{\varkappa(\delta+1)}) \leq \nu_\ell(\lambda_{p-1}^{2\delta}) \leq \nu_\ell(\lambda_q^{2\delta}) \leq 1$, а при $\ell = 2$ последнее сравнение следует из условия $p > q + 1$. Наконец, в случае $\ell = 2$ имеется еще ненулевой член B , который можно оценить так же, как в доказательстве предложения 3.2.

Этим доказано, что при $b \geq b_0 = (\ell - 1)\delta$ мы имеем $C(\alpha, a, \beta, b) \equiv 0 \pmod{\mathbb{Z}_\ell}$ при любых α, a, β . Следовательно, группа $\mathcal{A}_{p+1}^{(p)}$ порождается элементами $\theta(\beta, b)$, где $b = 1, \dots, b_0 - 1$ и β пробегает некоторый $\mathbb{Z}_\ell$ -базис $\mathcal{O}_H$, состоящий из f элементов. Легко видеть, что при $b \equiv 0 \pmod{\ell}$ образ $\theta(\beta, b)$ в $\mathcal{A}_{p+1}^{(p)}$

равен нулю. Следовательно, эта группа имеет не более τf образующих. Согласно предложению 3.3 группа $\mathcal{A}_{p+1}^{(p)}$ аннулируется умножением на ℓ , поэтому $|\mathcal{A}_{p+1}^{(p)}| \leq \ell^{\tau f}$. Теорема доказана.

§ 4. Исключительный случай

В случае $\ell = 3$ и $\delta = 1$ теорема 3.1 не дает никакой информации, поскольку в этом случае уравнение (3.11) не имеет допустимых решений. В настоящем параграфе мы выясним, что происходит в этом исключительном случае, пользуясь тем, что в данном случае поля K_n допускают совершенно явное описание и при каждом n имеется ровно два таких поля.

Именно, если $\delta = 1$ и $\ell \neq 2$, то K_n является квадратичным и, следовательно, слабо разветвленным расширением кругового поля k_n . Таким образом, $K_n = k_n(\sqrt{\alpha})$ для некоторого $\alpha \in k_n$, причем, не ограничивая общности, можно считать, что $\alpha = \varkappa_n \pi_n$, где $\pi_n = 1 - \zeta_n$ – стандартный униформизирующий элемент в поле k_n и $\varkappa_n$ – некоторый корень из единицы в поле H . В частности, это означает, что $\varkappa_n$ – корень степени, взаимно простой с ℓ .

Очевидно, что поле K_n определяет корень $\varkappa_n$ с точностью до квадрата. Следовательно, для любого $n \geq 0$ имеется в точности два различных квадратичных расширения $K_n := k_n(\sqrt{\pi_n})$ и $K'_n := k_n(\sqrt{\mu_n \pi_n})$, где $\mu_n \in H$ – корень из единицы, не являющийся квадратом. Легко видеть, что $K_{n+1} \supset K_n$ и $K'_{n+1} \supset K'_n$ для любого $n \geq 0$. Таким образом, мы имеем два $\mathbb{Z}_3$ -расширения $K_\infty = \bigcup_n K_n$ и $K'_\infty = \bigcup_n K'_n$. Если положить $\lambda_n = \sqrt{\pi_n}$, $\lambda'_n = \sqrt{\mu_n \pi_n}$ и предположить дополнительно, что корни μ_n согласованы условием $\mu_{n+1}^3 = \mu_n$ для всех $n \geq 0$, то мы получим, что системы локальных параметров $\{\lambda_n\}$ и $\{\lambda'_n\}$ для $n \geq 0$ – это те системы, существование которых гарантируется предложением 2.1. Заметим, что для каждого из полей K_∞ и K'_∞ мы имеем $q = 0$ и $\nu_\ell(\lambda_0) = \nu_\ell(\lambda'_0) = 1/4$.

Следующее предложение переносит утверждение теоремы 2.1 на случай $n = 0$.

ПРЕДЛОЖЕНИЕ 4.1. Пусть $\eta_1(\alpha, a)$ – некоторый логарифм Артина–Хассе в поле K_1 . Тогда

$$\eta_1(\alpha, a) = \alpha \lambda_1^a + \frac{a \varepsilon_1}{\ell} S_0(\alpha, a) + \frac{1}{\ell} \eta_0(\varphi(\alpha), a) + A,$$

где $S_0(\alpha, a) = \sum_{r=1}^{\infty} \varphi^r(\alpha) \lambda_0^{a \ell^{r-1}-1}$, $A \in K_1$ и $\nu_\ell(A) \geq 3/4$.

ДОКАЗАТЕЛЬСТВО. Согласно предложению 2.2 имеем

$$\nu_\ell(\varepsilon_1) = \nu_\ell(\ell \lambda_0^{-1} \pi_1) = 1 - \frac{1}{4} + \frac{1}{6} = \frac{11}{12}. \quad (4.1)$$

Оценим показатели $\nu_\ell(A_{r,i})$, где члены $A_{r,i}$ имеют тот же смысл, что и в доказательстве теоремы 2.1.

Если $(i, \ell) = 1$, то $\nu_\ell(A_{r,i}) = \nu_\ell(\ell^{-1} \lambda_0^{a \ell^{r-1}} (\lambda_0 \varepsilon_1)^i)$. Мы имеем $a, r \geq 1$, $i, a \ell^{r-1} \geq 2$, $\nu_\ell(\lambda_0) = 1/4$ и $\nu_\ell(\varepsilon_1) = 11/12$. Следовательно, $\nu_\ell(A_{r,i}) \geq -1 + 1/2 + 4/3 = 5/6 > 3/4$.

Пусть теперь $i \equiv 0 \pmod{3}$, $\nu_\ell(i) = t$ и $t \geq r$. Тогда, как и в (2.17), мы получаем

$$\nu_\ell(A_{r,i}) \geq -r + \nu_\ell(\lambda_0^{a \ell^{r-1}}) + i \nu_\ell(\lambda_0^{-1} \varepsilon_1) \geq -t + \frac{1}{4} a \ell^{r-1} + \frac{2}{3} \ell^t,$$

откуда, как и в доказательстве теоремы 2.1, следует $\nu_\ell(A_{r,i}) > 1 > 3/4$.

Наконец, если $r > t$, то, как и в (2.18), мы имеем

$$\nu_\ell(A_{r,i}) \geq -t - 1 + \nu_\ell(\lambda_0^{a\ell^{r-1}}) + i\nu_\ell(\lambda_0^{-1}\varepsilon_1) \geq -t - 1 + \frac{3}{4} + 2 \cdot 3^{t-1} \geq \frac{3}{4}.$$

Предложение доказано.

ТЕОРЕМА 4.1. Пусть, как и выше, $K_{p+1} = k_{p+1}(\sqrt{\pi_{p+1}})$, где $k_{p+1} = H(\zeta_{p+1})$, $\pi_{p+1} = 1 - \zeta_{p+1}$, ζ_{p+1} — первообразный корень из единицы степени 3^{p+2} и H — конечное неразветвленное расширение поля $\mathbb{Q}_3$.

Равенство $\mathcal{A}_{p+1}^{(p)} = \mathcal{B}_{p+1}^{(p)} = 0$ выполняется тогда и только тогда, когда $[H : \mathbb{Q}_\ell] \leq 2$.

ДОКАЗАТЕЛЬСТВО. Как и в (3.1), положим

$$C(\alpha, a, \beta, b) = \text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}(\eta_{p+1}(\alpha, a) \cdot 3^{-p-2}(\gamma_p - 1)\eta_{p+1}(\beta, b)), \quad (4.2)$$

где для определенности мы будем считать, что γ_p — автоморфизм расширения K_{p+1}/K_p , действующий на корень ζ_{p+1} по правилу $\gamma_p(\zeta_{p+1}) = \zeta_{p+1}\zeta_0$. Мы хотим вычислить $C(\alpha, a, \beta, b) \bmod \mathbb{Z}_\ell$. В частности, покажем, что в случае, когда $a > 1$ или $b > 1$, при любых α и β выполняется равенство $C(\alpha, a, \beta, b) \bmod \mathbb{Z}_\ell = 0$, и исследуем более подробно случай $a = b = 1$.

Рассуждая так же, как в доказательстве предложения 3.1 при выводе сравнений (3.2) и (3.3), мы получаем

$$(\gamma_p - 1)\beta\lambda_{p+1}^b \equiv 0 \pmod{\pi_0\lambda_{p+1}^{b-2}}, \quad b\ell^{-1}S_p(\beta, b)(\gamma_p - 1)\varepsilon_{p+1} \equiv 0 \pmod{\pi_0\lambda_p^{b-2}}.$$

Учитывая, что $b \geq 1$ и $\nu_\ell(\lambda_0) = 1/4$ при $p = 0$, мы, применяя в последнем случае предложение 4.1, получаем

$$\nu_\ell((\gamma_p - 1)\eta_{p+1}(\beta, b)) \geq \nu_\ell(\pi_0\lambda_p^{-1}) = \nu_\ell(\pi_0\lambda_{p+1}^{-3}). \quad (4.3)$$

Поскольку $\mathcal{D}(K_{p+1}/\mathbb{Q}_\ell) = (3^{p+1}\pi_0\lambda_{p+1})$, мы получаем, что для любого $x \in K_{p+1}$ такого, что $\nu_\ell(x) \geq \nu_\ell(\lambda_{p+1}^2)$, выполняется условие

$$\text{Sp}_{K_{p+1}/\mathbb{Q}_\ell}(x \cdot 3^{-p-2}(\gamma_p - 1)\eta_{p+1}(\beta, b)) \in \mathbb{Z}_\ell.$$

Тогда из (4.2) следует, что при заданном $\eta_{p+1}(\beta, b)$ элемент $C_{p+1}(\alpha, a, \beta, b)$ зависит только от $\eta_{p+1}(\alpha, a) \bmod \lambda_{p+1}^2$. Из предложения 4.1 и формулы (4.1) следует, что при $z = -\frac{1}{\ell}\eta_p(\varphi(\alpha), a) \in K_p$ справедливы сравнения

$$\begin{aligned} \eta_{p+1}(\alpha, a) + z &\equiv \alpha\lambda_{p+1}^a + \frac{a\varepsilon_{p+1}}{\ell} \sum_{r=1}^{\infty} \varphi^r(\alpha)\lambda_p^{a\ell^{r-1}-1} \\ &\equiv \alpha\lambda_{p+1}^a + \frac{a\varepsilon_1}{\ell} \varphi(\alpha)\lambda_p^{a-1} \pmod{\lambda_{p+1}^2}. \end{aligned}$$

В частности, если $a > 1$, то $\eta_{p+1}(\alpha, a) + z \equiv 0 \pmod{\lambda_{p+1}^2}$. Следовательно, при $a > 1$ мы имеем $C(\alpha, a, \beta, b) \bmod \mathbb{Z}_\ell = 0$ при любых α, β, b . Тогда из соображений симметрии видно, что и при $b > 1$ выполняется условие $C(\alpha, 1, \beta, b) \bmod \mathbb{Z}_\ell = 0$ при любых α, β . Таким образом, мы можем ограничиться случаем $a = b = 1$.

Поскольку $\varepsilon_{p+1} = \lambda_{p+1}^3 - \lambda_p = \sqrt{\pi_{p+1}^3} - \sqrt{\pi_p}$ и $\pi_p = 1 - (1 - \pi_{p+1})^3 = \pi_{p+1}^3(1 - 3\pi_{p+1}^{-1} + 3\pi_{p+1}^{-2})$, мы получаем

$$\begin{aligned}\sqrt{\pi_{p+1}^3} &= \pi_{p+1}\lambda_{p+1}, \\ \sqrt{\pi_p} &= \pi_{p+1}\lambda_{p+1}\sqrt{1 - 3\pi_{p+1}^{-1} + 3\pi_{p+1}^{-2}} \\ &\equiv \pi_{p+1}\lambda_{p+1} + \frac{1}{2}(3\lambda_{p+1}^{-1} - 3\lambda_{p+1}) \pmod{3\lambda_{p+1}^2}.\end{aligned}$$

Таким образом, при некотором $z \in K_0$

$$\eta_{p+1}(\alpha, 1) + z \equiv \alpha\lambda_{p+1} - \frac{\varphi(\alpha)}{2}(\lambda_{p+1}^{-1} - \lambda_{p+1}) \pmod{\lambda_{p+1}^2}. \quad (4.4)$$

Проведя аналогичные рассуждения для $\eta_{p+1}(\beta, 1)$, мы получаем, что при некотором $z' \in K_0$ выполняется сравнение

$$\eta_{p+1}(\beta, 1) + z' \equiv \beta\lambda_{p+1} - \frac{\varphi(\beta)}{2}(\lambda_{p+1}^{-1} - \lambda_{p+1}) \pmod{\lambda_{p+1}^2}.$$

При нашем выборе автоморфизма γ_p мы имеем

$$\gamma_p(\pi_{p+1}) = \gamma_p(1 - \zeta_{p+1}) = 1 - \zeta_{p+1}\zeta_0 = \pi_{p+1}(1 + \pi_{p+1}^{-1}\pi_0 - \pi_0).$$

Тогда

$$\begin{aligned}\gamma_p(\lambda_{p+1}) &= \sqrt{\gamma_p(\pi_{p+1})} = \lambda_{p+1}\sqrt{1 + \pi_{p+1}^{-1}\pi_0 - \pi_0} \\ &\equiv \lambda_{p+1}\left(1 + \frac{1}{2}(\pi_{p+1}^{-1}\pi_0 - \pi_0)\right) \pmod{\pi_0}.\end{aligned}$$

Аналогично, $\gamma_p(\lambda_{p+1}^{-1}) \equiv \lambda_{p+1}^{-1}(1 - \frac{1}{2}(\pi_{p+1}^{-1}\pi_0 - \pi_0)) \pmod{\pi_0}$.

Таким образом,

$$\begin{aligned}(\gamma_p - 1)\beta\lambda_{p+1} &\equiv \frac{\beta\lambda_{p+1}}{2}(\pi_{p+1}^{-1}\pi_0 - \pi_0) \equiv \frac{\beta\lambda_{p+1}\pi_{p+1}^{-1}\pi_0}{2} \pmod{\pi_0}, \\ \frac{(\gamma_p - 1)\varepsilon_{p+1}}{3} &\equiv -\frac{1}{2}(\gamma_p - 1)(\lambda_{p+1}^{-1} - \lambda_{p+1}) \\ &\equiv -\frac{1}{4}(-\lambda_{p+1}^{-1}\pi_{p+1}^{-1}\pi_0 + \lambda_{p+1}^{-1}\pi_0 - \lambda_{p+1}\pi_{p+1}^{-1}\pi_0 + \lambda_{p+1}\pi_0) \\ &\equiv \frac{1}{4}\lambda_{p+1}^{-1}\pi_{p+1}^{-1}\pi_0 \pmod{\pi_0}.\end{aligned}$$

Следовательно,

$$(\gamma_p - 1)\eta_{p+1}(\beta, 1) \equiv \frac{\beta}{2}\lambda_{p+1}^{-1}\pi_0 + \frac{\varphi(\beta)}{4}\lambda_{p+1}^{-1}\pi_{p+1}^{-1}\pi_0 \pmod{\pi_0}. \quad (4.5)$$

Из (4.4) и (4.5) следует сравнение

$$\begin{aligned}R &:= \eta_{p+1}(\alpha, 1)(\gamma_p - 1)\eta_{p+1}(\beta, 1) \\ &\equiv \left[\alpha\lambda_{p+1} - \frac{\varphi(\alpha)}{2}(\lambda_{p+1}^{-1} - \lambda_{p+1})\right]\left[\frac{\beta}{2}\lambda_{p+1}^{-1}\pi_0 + \frac{\varphi(\beta)}{4}\lambda_{p+1}^{-1}\pi_{p+1}^{-1}\pi_0\right] \pmod{\pi_0\lambda_{p+1}^{-1}}.\end{aligned}$$

Раскрывая скобки, учитывая, что $\lambda_{p+1}^2 = \pi_{p+1}$, и опуская все члены, сравнимые с нулем по модулю $\pi_0 \lambda_{p+1}^{-1}$, получаем

$$R \equiv \frac{1}{4} \left[-\varphi(\alpha)\beta + \alpha\varphi(\beta) + \frac{1}{2} \varphi(\alpha)\varphi(\beta) \right] \pi_{p+1}^{-1} \pi_0 - \frac{\varphi(\alpha)\varphi(\beta)}{8} \pi_{p+1}^{-2} \pi_0 \pmod{\pi_0 \lambda_{p+1}^{-1}}.$$

ЛЕММА 4.1. Для любого $p \geq 0$ справедливо сравнение

$$3^{-p-2} \text{Sp}_{K_{p+1}/H}(\pi_{p+1}^{-1} \pi_0) \equiv 3^{-p-2} \text{Sp}_{K_{p+1}/H}(\pi_{p+1}^{-2} \pi_0) \equiv \frac{2}{3} \pmod{\mathbb{Z}_\ell}.$$

ДОКАЗАТЕЛЬСТВО. Имеет место сравнение $\pi_p \equiv \pi_{p+1}^3 \pmod{3}$, поэтому

$$3^{-p-2} \text{Sp}_{K_{p+1}/H}(\pi_{p+1}^{-1} \pi_0) \equiv 3^{-p-2} \pi_p^{-1} \pi_0 \text{Sp}_{K_{p+1}/H}(\pi_{p+1}^2) \pmod{\mathbb{Z}_\ell}.$$

Поскольку $\pi_{p+1}^2 = 1 - 2\zeta_{p+1} + \zeta_{p+1}^2$ и $\text{Sp}_{K_{p+1}/K_p}(1) = 3$, $\text{Sp}_{K_{p+1}/K_p}(\zeta_{p+1}) = \text{Sp}_{K_{p+1}/K_p}(\zeta_{p+1}^2) = 0$, мы получаем

$$3^{-p-2} \text{Sp}_{K_{p+1}/H}(\pi_{p+1}^{-1} \pi_0) \equiv 3^{-p-1} \text{Sp}_{K_p/H}(\pi_p^{-1} \pi_0) \pmod{\mathbb{Z}_\ell}.$$

Продолжая этот процесс спуска и учитывая, что $[K_0 : H] = 2$, мы получаем

$$3^{-p-2} \text{Sp}_{K_{p+1}/H}(\pi_{p+1}^{-1} \pi_0) \equiv 3^{-2} \text{Sp}_{K_1/H}(\pi_1^{-1} \pi_0) \equiv 3^{-2} \text{Sp}_{K_1/H}(\pi_1^2) \equiv \frac{2}{3} \pmod{\mathbb{Z}_\ell}.$$

Аналогичное рассуждение применяется и к вычислению $\text{Sp}_{K_{p+1}/H}(\pi_{p+1}^{-2} \pi_0)$. Лемма доказана.

Применяя лемму 4.1 для вычисления $C(\alpha, 1, \beta, 1)$, получаем

$$C(\alpha, 1, \beta, 1) \equiv 3^{-p-2} \text{Sp}_{K_{p+1}/\mathbb{Q}_\ell} R \equiv \frac{1}{6} \text{Sp}_{H/\mathbb{Q}_\ell}(\varphi(\alpha)\beta - \alpha\varphi(\beta)) \pmod{\mathbb{Z}_3}. \quad (4.6)$$

Итак, если $H = \mathbb{Q}_3$, то $\varphi(\alpha)\beta = \alpha\varphi(\beta)$, а если $[H : \mathbb{Q}_3] = 2$, то $\varphi(\alpha)\beta = \varphi(\alpha\varphi(\beta))$ для любых α и β . Следовательно, в каждом из этих двух случаев $C_{p+1}(\alpha, 1, \beta, 1) \pmod{\mathbb{Z}_3} = 0$ и $\mathcal{A}_{p+1}^{(p)} = \mathcal{B}_{p+1}^{(p)} = 0$.

Предположим теперь, что $[H : \mathbb{Q}_3] > 2$. Поскольку $\text{Sp}_{H/\mathbb{Q}_3}(\varphi(\alpha)\beta - \alpha\varphi(\beta)) = \text{Sp}_{H/\mathbb{Q}_3}(\alpha(\varphi^{-1}(\beta) - \varphi(\beta)))$ и $\varphi \neq \varphi^{-1}$, мы можем найти $\beta \in \mathcal{O}_H$ такой, что $\varphi^{-1}(\beta) \not\equiv \varphi(\beta) \pmod{\ell}$, и для такого β найти элемент $\alpha \in \mathcal{O}_H$ такой, что $\text{Sp}_{H/\mathbb{Q}_3}(\alpha(\varphi^{-1}(\beta) - \varphi(\beta))) = 1$. Тогда $C(\alpha, 1, \beta, 1) \pmod{\mathbb{Z}_3} \neq 0$, т.е. $\mathcal{A}_{p+1}^{(p)} \neq 0$ и $\mathcal{B}_{p+1}^{(p)} \neq 0$. Теорема доказана.

ТЕОРЕМА 4.2. Для поля K'_{p+1} равенство $\mathcal{A}^{(p)}(K'_{p+1}) = \mathcal{B}^{(p)}(K'_{p+1}) = 0$ выполняется тогда и только тогда, когда $H = \mathbb{Q}_3$, где H – максимальное неразветвленное подполе поля K'_{p+1} .

ДОКАЗАТЕЛЬСТВО. Пусть H' – единственное неразветвленное квадратичное расширение поля H . Тогда в H' любой корень μ_n является квадратом, т.е. $\mu_n = \xi_n^2$, причем мы можем считать, что корни из единицы ξ_n выбраны так, что

выполняется условие $\xi_{n+1}^3 = \xi_n$ для всех $n \geq 0$. Положим $L_n = K_n \cdot H' = K'_n \cdot H'$. Пусть

$$\eta'_n(\alpha, a) = \sum_{r=0}^{\infty} \ell^{-r} \varphi^r(\alpha) \lambda_n^{a \ell^r}, \quad \eta'_n(\beta, b) = \sum_{r=0}^{\infty} \ell^{-r} \varphi^r(\beta) \lambda_n^{b \ell^r}.$$

Тогда в L_n выполняются равенства $\lambda'_n = \xi_n \lambda_n$ и

$$\eta'_n(\alpha, a) = \eta_n(\alpha \xi_n, a), \quad \eta'_n(\beta, b) = \eta_n(\beta \xi_n, b), \quad (4.7)$$

где

$$\eta_n(\alpha \xi_n, a) = \sum_{r=0}^{\infty} \ell^{-r} \varphi^r(\alpha \xi_n) \lambda_n^{a \ell^r}, \quad \eta_n(\beta \xi_n, b) = \sum_{r=0}^{\infty} \ell^{-r} \varphi^r(\beta \xi_n) \lambda_n^{b \ell^r}.$$

Вернемся теперь к полю K'_{p+1} . Очевидно, что

$$\begin{aligned} C'(\alpha, a, \beta, b) &:= \text{Sp}_{K'_{p+1}/\mathbb{Q}_3}(\eta'_{p+1}(\alpha, a) \cdot 3^{-p-2}(\gamma_p - 1) \eta'_{p+1}(\beta, b)) \\ &= \frac{1}{2} \text{Sp}_{L_{p+1}/\mathbb{Q}_\ell}(\eta_{p+1}(\alpha \xi_1, a) \cdot 3^{-p-2}(\gamma_p - 1) \eta_{p+1}(\beta \xi_1, b)). \end{aligned} \quad (4.8)$$

В частности, из теоремы 4.1, примененной к полю L_1 , следует, что неравенство $C(\alpha, a, \beta, b) \pmod{\mathbb{Z}_3} \neq 0$ может выполняться только при $a = b = 1$.

Применяя (4.6) и (4.8), мы получаем

$$C(\alpha, 1, \beta, 1) \equiv \frac{1}{12} \text{Sp}_{H'/\mathbb{Q}_3}(\varphi(\alpha \xi_1) \beta \xi_1 - \alpha \xi_1 \varphi(\beta \xi_1)) \pmod{\mathbb{Z}_3}.$$

Учитывая, что $\varphi(\xi_1) = \xi_1^3$ и $\xi_1^2 = \mu_1$, получаем $\varphi(\alpha \xi_1) \beta \xi_1 - \alpha \xi_1 \varphi(\beta \xi_1) = \mu_1^2(\varphi(\alpha) \beta - \alpha \varphi(\beta))$. Следовательно,

$$\frac{1}{12} \text{Sp}_{H'/\mathbb{Q}_3}(\varphi(\alpha \xi_1) \beta \xi_1 - \alpha \xi_1 \varphi(\beta \xi_1)) = \frac{1}{6} \text{Sp}_{H/\mathbb{Q}_3}(\mu_1^2(\varphi(\alpha) \beta - \alpha \varphi(\beta))).$$

Таким образом, условие $C'(\alpha, 1, \beta, 1) \not\equiv 0 \pmod{\mathbb{Z}_3}$ для некоторых α, β будет выполняться тогда и только тогда, когда в поле вычетов $\mathbb{F}_q$ поля H ($q = 3^r$) найдутся элементы x, y, μ такие, что μ не является квадратом в $\mathbb{F}_q$ и $\text{Sp}_{\mathbb{F}_q/\mathbb{F}_3}(\mu^2(\varphi(x)y - x\varphi(y))) \neq 0$.

Если $r = 1$, т.е. $\mathbb{F}_q = \mathbb{F}_3$, то $\varphi(x)y - x\varphi(y) = 0$ для любых x, y , т.е. всегда $C'(\alpha, 1, \beta, 1) \equiv 0 \pmod{\mathbb{Z}_3}$.

Если $r = 2$, то $F_q = F_3(i)$, где $i = \sqrt{-1}$. Полагая $\mu = 1 + i$, $x = i$ и $y = 1$, мы получаем $\mu^2(\varphi(x)y - x\varphi(y)) = 1$, т.е. в этом случае для подходящих α и β

$$C'(\alpha, 1, \beta, 1) \not\equiv 0 \pmod{\mathbb{Z}_3}.$$

Наконец, в случае $r \geq 3$ мы докажем, что множество $V := \{\mu^2(\varphi(x)y - x\varphi(y)) \mid x, y \in \mathbb{F}_q\}$ совпадает с $\mathbb{F}_q$. Поскольку $\mu \neq 0$, достаточно проверить, что с $\mathbb{F}_q$ совпадает множество $W := \{\varphi(x)y - x\varphi(y) \mid x, y \in \mathbb{F}_q\}$. Мы имеем точную последовательность $\mathbb{F}_3$ -пространств

$$0 \longrightarrow (\varphi - 1)\mathbb{F}_q \xrightarrow{i} \mathbb{F}_q \xrightarrow{\text{Sp}} \mathbb{F}_3 \longrightarrow 0,$$

где i – естественное вложение и Sp – отображение следа.

Таким образом, $(\varphi - 1)\mathbb{F}_q$ является подпространством коразмерности 1 в $\mathbb{F}_q$. Очевидно, что $(\varphi - 1)\mathbb{F}_q = \{\varphi(x)y - x\varphi(y) \mid x \in \mathbb{F}_q, y = 1\}$. Следовательно, $(\varphi - 1)\mathbb{F}_q \subseteq W$. С другой стороны, в доказательстве теоремы 4.1 мы показали, что W содержит элемент с ненулевым следом. Следовательно, $\mathbb{F}_3$ -пространство W совпадает с $\mathbb{F}_q$. Теорема доказана.

Полученные результаты ставят ряд открытых вопросов, которые мы сейчас сформулируем.

1. Как ведет себя величина $d(\mathcal{A}_n^{(p)})$ при фиксированном p и растущем n ? Может ли она неограниченно возрастать?

2. Каким образом связаны между собой $\mathcal{A}_n^{(p)}$ и $\mathcal{B}_n^{(p)}$ как модули Галуа?

3. Пусть имеет место исключительный случай, т.е. $\ell = 3$ и $\delta = 1$. Пусть $\mathcal{A}_{p+1}^{(p)} = 0$. Существует ли n такое, что $\mathcal{A}_n^{(p)} \neq 0$?

4. Что происходит в случае $\ell = 2$?

Последние два вопроса можно суммировать следующим образом.

5. Верно ли, что условие $\mathcal{A}^{(p)}(K_n) = 0$ выполняется для некоторого p и всех $n > p$ тогда и только тогда, когда K – круговое поле?

Список литературы

1. Iwasawa K., “On some modules in the theory of cyclotomic fields”, *J. Math. Soc. Japan*, **16** (1964), 42–82.
2. Кузьмин Л. В., “Некоторые замечания о ℓ -адическом регуляторе. II”, *Изв. АН СССР. Сер. матем.*, **53**:4 (1989), 782–813.
3. Кузьмин Л. В., “Аналог формулы Римана–Гурвица для одного типа ℓ -расширений полей алгебраических чисел”, *Изв. АН СССР. Сер. матем.*, **54**:2 (1990), 316–338.
4. Кузьмин Л. В., “Новые явные формулы для символа норменного вычета и их приложения”, *Изв. АН СССР. Сер. матем.*, **54**:6 (1990), 1196–1228.
5. Кузьмин Л. В., “Новое доказательство одной теоремы двойственности о ℓ -адических логарифмах локальных единиц”, *Итоги науки и техники. Совр. математика и ее прилож.*, **45** (1997), 72–81.
6. Кузьмин Л. В., “Некоторые замечания о ℓ -адическом регуляторе. III”, *Изв. РАН. Сер. матем.*, **63**:6 (1999), 29–82.
7. Кузьмин Л. В., “Некоторые замечания о ℓ -адическом регуляторе. IV”, *Изв. РАН. Сер. матем.*, **64**:2 (2000), 43–88.
8. Wintenberger J.-P., “Le corps des normes de certaines extensions infinies de corps locaux; applications”, *Ann. Sci. École Norm. Sup. (4)*, **16**:1 (1983), 59–89.

Л. В. Кузьмин (L. V. Kuz'min)
 Российский научный центр
 “Курчатовский институт”,
 Институт информационных технологий
 E-mail: helltiapa@mail.ru

Поступило в редакцию
 27.04.2005