Math-Net.Ru

Общероссийский математический портал

Л. В. Кузьмин, О ℓ -адических логарифмах гауссовых сумм, *Изв. РАН. Сер. матем.*, 2014, том 78, выпуск 3, 111–134

DOI: <https://doi.org/10.4213/im8085>

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., 07:14:35

УДК 519.4

Л. В. Кузьмин

О ℓ -адических логарифмах гауссовых сумм

Для гауссовой суммы $S(\chi)$, соответствующей характеру χ порядка $\ell^m d$ мультипликативной группы $\mathbb{F}_q$ конечного поля характеристики p , получена приближенная формула для ℓ -адического логарифма числа $S(\chi)$. Строится специальный базис для группы логарифмов и определяются коэффициенты разложения $\log_\ell(S(\chi))$ по модулю ℓ^m (по модулю ℓ^{m-1} при $\ell = 2$). Эти значения коэффициентов определяются в терминах степенных вычетов некоторых круговых чисел в точках, лежащих над p .

Библиография: 5 наименований.

Ключевые слова: гауссова сумма, круговые единицы, теория Ивасавы, законы взаимности.

DOI: 10.4213/im8085

§ 1. Введение

Пусть $\mathbb{F}_q$ – конечное поле характеристики p из $q = p^r$ элементов, ξ_p – первообразный корень из единицы степени p и $\chi: \mathbb{F}_q^\times \rightarrow \mu_{q-1}$ – характер порядка r , делящего $q - 1$, мультипликативной группы поля $\mathbb{F}_q$, где $\mu_{q-1} \subset \overline{\mathbb{Q}}$ – группа всех корней из единицы степени $q - 1$. Тогда, как и в [1], соответствующая χ гауссова сумма определяется формулой

$$S(\chi) = \sum_{a \in \mathbb{F}_q^\times} \chi(a) \xi_p^{\text{Sp}(a)}, \quad (1.1)$$

где Sp – отображение следа из $\mathbb{F}_q$ в $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. Считая, что значения всех характеров лежат в фиксированном алгебраическом замыкании $\overline{\mathbb{Q}}$, мы можем рассматривать $S(\chi)$ как элемент кругового поля $L = \mathbb{Q}(\xi_r, \xi_p) \subset \overline{\mathbb{Q}}$, где ξ_r – первообразный корень из единицы степени r . Таким образом, при заданном простом ℓ мы можем, зафиксировав вложение $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, где $\mathbb{Q}_\ell$ – поле рациональных ℓ -адических чисел, рассматривать $S(\chi)$ как элемент локального поля $\mathbb{Q}_\ell(\xi_r, \xi_p)$ или как элемент алгебры $L_\ell = L \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{v|\ell} L_v$, где L_v означает v -пополнение L .

Итак, возникает задача характеризации гауссовой суммы $S(\chi)$ как элемента поля $\mathbb{Q}_\ell(\xi_r, \xi_p)$, или как элемента алгебры L_ℓ . В случае $\ell = p$ эта задача была решена Б. Гроссом и Н. Коблицем [2]. С другой стороны, Х. Микки в случае $\ell \neq p$ (см. [3] и библиографию в этой работе) рассмотрел случай $r = \ell^n$ при некотором n и получил сравнение, выражающее $S(\chi) \pmod{\pi^\ell}$ в терминах круговых единиц поля $\mathbb{Q}(\xi_r)$, где $\pi = 1 - \xi_r$. Он дал также ряд приложений этого сравнения.

Работа выполнена при финансовой поддержке РФФИ (грант № 11-01-00588-а).

В настоящей работе мы рассматриваем существенно другую задачу. Мы получаем приближенное вычисление ℓ -адического логарифма гауссовой суммы, поэтому наши результаты трудно сопоставить с результатами [3]. В частности, по мнению автора, ни в одном частном случае не удастся ни вывести наши результаты из результатов [3], ни получить результаты Микки из результатов этой работы. Отметим также, что и используемые методы совершенно различны.

Возникает вопрос: можно ли получить какую-либо нетривиальную информацию о гауссовой сумме $S(\chi)$, если не предполагать никакой связи между числами p , r и ℓ ? Автор не знает ответа, если не считать таковым формулу (1.1).

Наша цель – дать в случае $\ell \neq p$ характеристику ℓ -адического логарифма элемента $S(\chi)$ в предположении, что $r = \ell^m d$, где $(d, \ell) = 1$ и $m \geq 1$ при $\ell \neq 2$, $m \geq 2$ при $\ell = 2$. Точнее, положим

$$K := \mathbb{Q}(\xi_r), \quad K_\ell := K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{v|\ell} K_v,$$

где K_v – v -пополнение K и v пробегает все точки, лежащие над ℓ . Тогда для любой точки $v|\ell$ имеется логарифмическое отображение $\log_v : U(K_v) \rightarrow K_v$, где $U(K_v)$ – группа единиц поля K_v . Это отображение определяется на группе главных единиц $U^{(1)}(K_v) \subset U(K_v)$ при помощи обычного степенного ряда для логарифма. Любая единица $u \in U(K_v)$ представима в виде $u = u_1 u_2$, где $u_1 \in U^{(1)}(K_v)$, $u_2 \in \mu(K_v)$ и $\mu(K_v)$ – группа всех корней из единицы в поле K_v . Тогда $\log_v(u) = \log_v(u_1)$. Мы определяем отображение $\log_\ell : \prod_{v|\ell} U(K_v) \rightarrow K_\ell$ формулой

$$\log_\ell := \prod_{v|\ell} \log_v : \prod_{v|\ell} U(K_v) \rightarrow \prod_{v|\ell} K_v \cong K_\ell. \quad (1.2)$$

Пусть $u_v \in U^{(1)}(K_v)$ – такой элемент, что $K_v(\sqrt[m]{u_v})/K_v$ является неразветвленным расширением степени ℓ^m . Тогда мы определим модуль Галуа $V(K_v)$ относительно действия группы Галуа $G(K_v/\mathbb{Q}_\ell)$ как подгруппу мультипликативной группы $U^{(1)}(K_v) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, порожденную группой главных единиц $U^{(1)}(K_v)$ и элементом $\sqrt[m]{u_v}$. Легко видеть, что $V(K_v)$ не зависит от выбора элемента u_v , т. е. определен корректно. Таким образом, $V(K_v)$ является $\mathbb{Z}_\ell$ -модулем без кручения, и имеется вложение $U(K_v)/\mu(K_v) \hookrightarrow V(K_v)$, причем имеется изоморфизм $G(K_v/\mathbb{Q}_\ell)$ -модулей $V(K_v)/(U(K_v)/\mu(K_v)) \cong \mu_{\ell^m}$ (неканонически). Иногда мы будем использовать аддитивные обозначения для записи групповой операции в $V(K_v)$. Отметим также, что $S(\chi)^r \in K \subset K_\ell$ (см. [1, теорема 1.3]) и расширение L_v/K_v не разветвлено для любой точки $v|\ell$. Поскольку для любой точки $v|\ell$ расширение $K_v(S(\chi)^d)/K_v$ не разветвлено и имеет степень, делящую ℓ^m , а d взаимно просто с ℓ , мы можем рассматривать $S(\chi)$ как элемент модуля $V(K) := \prod_{v|\ell} V(K_v)$. Отображение (1.2) продолжается по линейности до отображения $\log_\ell : V(K) \hookrightarrow \prod_{v|\ell} K_v$, и наша цель – охарактеризовать $\log_\ell S(\chi)$ как элемент модуля Галуа $\log_\ell V(K)$. Чтобы сделать это, мы положим

$$V(K_v)^0 = \{x \in V(K_v) \mid N_{K_v/\mathbb{Q}_\ell}(x) = 1\}, \quad V(K)^0 = \prod_{v|\ell} V(K_v)^0,$$

где $N_{K_v/\mathbb{Q}_\ell}$ – отображение нормы относительно группы $G(K_v/\mathbb{Q}_\ell)$, действующей на модуль $V(K_v)$.

Хорошо известное соотношение $S(\chi)\overline{S(\chi)} = q$ (см. [1]), где черта означает комплексное сопряжение, показывает, что в $V(K)$ выполняется равенство $N_{K/\mathbb{Q}}(S(\chi)) = q^{(1/2)[K:\mathbb{Q}]}$. Следовательно, полагая $S(\chi)_1 = q^{-1/2}S(\chi) = S(\chi)^{(1-\sigma_{-1})/2}$ при $\ell \neq 2$ и $S(\chi)_1 = q^{-1}S(\chi)^2 = S(\chi)^{1-\sigma_{-1}}$ при $\ell = 2$, где σ_{-1} – автоморфизм, действующий на любой корень из единицы ξ по правилу $\xi^{\sigma_{-1}} = \xi^{-1}$, получаем $\sigma_{-1}(S(\chi)_1) = S(\chi^{-1})_1^{-1}$ и

$$N_{K/\mathbb{Q}}(S(\chi)_1) = 1 \quad (1.3)$$

(напомним, что мы рассматриваем $S(\chi)_1$ как элемент модуля $V(K)$).

Мы доказываем (предложение 2.12), что $S(\chi)_1$ является элементом группы $V(K)^0$ (если в K имеется единственная точка $v|\ell$, то условие $S(\chi)_1 \in V(K)^0$ следует из (1.3)). В [4] было показано, что $V(K)^0$ является циклическим модулем Галуа над $\mathbb{Z}_\ell[G]$, где $G = G(K/\mathbb{Q})$, а также построен элемент $\eta(K) \in V(K)^0$ такой, что $\eta(K)$ порождает $V(K)^0$ как $\mathbb{Z}_\ell[G]$ -модуль, и было получено явное выражение для $\log_\ell(\eta(K))$. Таким образом, $S(\chi)_1$ можно представить в виде

$$S(\chi)_1 = \sum_{\sigma \in G} a_\sigma \sigma(\eta(K)), \quad a_\sigma \in \mathbb{Z}_\ell. \quad (1.4)$$

В силу предложения 2.12 набор коэффициентов a_σ в (1.4) определен не однозначно. Именно, пусть G_ℓ – подгруппа разложения ℓ в группе G . Тогда вектор $\{a_\sigma\}_{\sigma \in G}$ определен однозначно с точностью до слагаемого, координаты которого b_σ зависят только от класса смежности σ по G_ℓ . Поэтому мы вводим соответствующее отношение эквивалентности и для элементов $x, y \in \mathbb{Z}_\ell[G]$ или $x, y \in \mathbb{Z}/\ell^m\mathbb{Z}[G]$ пишем $x \sim y$, если $x - y = \alpha \sum_{\sigma \in G_\ell} \sigma$ для некоторого $\alpha \in \mathbb{Z}_\ell[G]$. Наш основной результат (теорема 3.2) выражает коэффициенты a_σ по модулю ℓ^m (по модулю ℓ^{m-1} при $\ell = 2$) в терминах степенного вычета степени ℓ^m , соответствующего некоторой фиксированной точке $\mathfrak{p}_0|p$ от некоторых круговых единиц поля K .

Работа построена следующим образом. В §2 мы напомним некоторые результаты из [4], которые потребуются нам в дальнейшем, и доказываем вышеупомянутое предложение 2.12.

В §3 мы доказываем существование нужных нам круговых единиц (точнее, круговых чисел) и формулируем основной результат (теорема 3.2).

Используя явные формулы для символа норменного вычета и уточнение теоремы Ивасава о круговых единицах, полученное в [4], мы доказываем ослабленный вариант теоремы 3.2 (предложение 3.3). Цель дальнейшего – показать, что из предложения 3.3, справедливого для любого характера, можно вывести теорему 3.2 для исходного характера χ .

В §4 показываем, что элемент $S(\chi)_1$ можно аппроксимировать некоторой гауссовой суммой $S(\chi_1)$, связанной с характером χ_1 , являющимся ℓ^t -й степенью некоторого другого характера χ_2 порядка $\ell^{m+t}d$, где t можно выбрать сколь угодно большим. Доказывается ряд утверждений о взаимосвязи между $S(\chi)$ и $S(\chi_2)$.

В §5 мы применяем предложение 3.3 к гауссовой сумме $S(\chi_2)$ и, опираясь на результаты §4, доказываем, что при достаточно большом t из неточной формы

теоремы 3.2, даваемой предложением 3.3, следует утверждение теоремы 3.2 для исходной гауссовой суммы $S(\chi)$. Доказательство этого факта опирается на свойства элементов Штикельберга и периодических Γ -модулей.

Среди специалистов существует мнение, что гауссовы суммы и круговые единицы – это объекты, в каком-то смысле двойственные друг другу. Результаты этой работы дают еще одно подтверждение справедливости этого мнения.

Автор благодарен рецензенту, замечания которого помогли исправить ряд неточностей и сделать изложение более четким.

§ 2. Некоторые вспомогательные результаты

Мы принимаем здесь обозначения из [4]. Напомним некоторые результаты этой работы. Начнем с локального случая. Для заданного n обозначим через ζ_n первообразный корень из единицы степени ℓ^m , где $m = n + 1$ при $\ell \neq 2$ и $m = n + 2$ при $\ell = 2$. Мы предполагаем, что корни ζ_n выбраны согласовано, т. е. $\zeta_{n+1}^\ell = \zeta_n$ при любом n . Для заданного натурального d , взаимно простого с ℓ , положим $H = \mathbb{Q}_\ell(\mu_d)$, $K_n = \mathbb{Q}_\ell(\zeta_n, \mu_d)$ для $n \geq 0$. Таким образом, K_n – это пополнение того поля, которое во введении обозначалось через K . Тогда $K_\infty := \bigcup_{n=0}^\infty K_n$ является круговым $\mathbb{Z}_\ell$ -расширением поля K_0 и H является максимальным неразветвленным подполем поля K_n при любом n . Пусть $\mathcal{O}_H$ – кольцо целых поля H . Мы фиксируем некоторую пару элементов $\alpha, \beta \in \mathcal{O}_H$, порождающих взаимные целые нормальные базисы поля H , т. е. такие, что

$$\mathrm{Sp}_{H/\mathbb{Q}_\ell}(\sigma(\alpha)\tau(\beta)) = \begin{cases} 1 & \text{при } \sigma = \tau, \\ 0 & \text{при } \sigma \neq \tau \end{cases}$$

для любых $\sigma, \tau \in G(H/\mathbb{Q}_\ell)$. Пусть φ – автоморфизм Фробениуса расширения $H/\mathbb{Q}_\ell$. Определим идемпотент $e_n = 1 - |G_n|^{-1} \mathrm{Sp}_{G_n}$, где $G_n = G(K_n/\mathbb{Q}_\ell)$ и $\mathrm{Sp}_{G_n} = \sum_{\sigma \in G_n} \sigma$.

ПРЕДЛОЖЕНИЕ 2.1 [4, теорема 1.1]. *Для целого $n \geq 0$ пусть группа $V(K_n)^0$ определена, как в § 1. Тогда существует пара элементов $\eta(K_n) = \eta_n(\alpha, 1)$, $\eta'(K_n) = \eta_n(\beta, -1) \in V(K_n)^0$ таких, что каждый из этих элементов порождает $V(K_n)^0$ как модуль Галуа. При этом их ℓ -адические логарифмы $\log(\eta_n(\alpha, 1)), \log(\eta_n(\beta, -1)) \in K_n$ задаются в явном виде формулами*

$$\begin{aligned} & \log(\eta_n(\alpha, 1)) \\ &= e_n \left[-\delta \ell^{1-m} \alpha + \sum_{s=0}^{m-1} \ell^{-s} \zeta_n^{-\ell^s} \varphi^{s+1-m}(\alpha) - \ell^{2-m} \frac{\varphi^{-1}}{1 - \ell \varphi^{-1}}(\alpha) \right], \end{aligned} \quad (2.1)$$

$$\begin{aligned} & \log(\eta_n(\beta, -1)) \\ &= e_n \left[-\delta \ell^{1-m} \beta + \sum_{s=0}^{m-1} \ell^{-s} \zeta_n^{\ell^s} \varphi^{s+1-m}(\beta) - \ell^{2-m} \frac{\varphi^{-1}}{1 - \ell \varphi^{-1}}(\beta) \right], \end{aligned} \quad (2.2)$$

где $\delta = 1$ при $\ell \neq 2$ и $\delta = 0$ при $\ell = 2$. Отметим, что $(1 - \ell \varphi^{-1})^{-1} = (1 - \ell^f)^{-1} \sum_{i=0}^{f-1} \varphi^{-i} \ell^i$, где $f = [H : \mathbb{Q}]$.

ЗАМЕЧАНИЕ 2.2. В случае $\ell \neq 2$ умножение на e_n в (2.1) и (2.2) можно не учитывать. Кроме того, эти формулы показывают, что элементы $\eta_n(\alpha, 1)$ и $\eta_n(\beta, -1)$ согласованы для различных n относительно норменных отображений.

Отметим, что $V(K_n)^0 \cong \mathbb{Z}_\ell[G_n]/\mathbb{Z}_\ell \text{Sp}_{G_n}$ как модуль Галуа. Действительно, этот модуль порождается одним элементом (например, $\eta(\alpha, 1)$ или $\eta(\beta, -1)$). В этом модуле выполняется соотношение $N_{K_n/\mathbb{Q}_\ell}(x) = 1$ для любого $x \in V(K_n)^0$, и его $\mathbb{Z}_\ell$ -ранг равен $[K_n:\mathbb{Q}_\ell] - 1$. Таким образом, для всякого $n \geq 0$ любые два элемента $x, y \in V(K_n)^0$ могут быть представлены в виде

$$x = \sum_{\sigma \in G_n} x_\sigma \sigma(\eta(\alpha, 1)), \quad y = \sum_{\sigma \in G_n} y_\sigma \sigma(\eta(\beta, -1)), \quad x_\sigma, y_\sigma \in \mathbb{Z}_\ell. \quad (2.3)$$

При этом коэффициенты x_σ (соответственно, y_σ) определены однозначно с точностью до произвольной аддитивной постоянной $c \in \mathbb{Z}_\ell$.

Рассмотрим символ норменного вычета степени ℓ^m

$$K_n \times K_n \rightarrow \mu_{\ell^m}, \quad (a, b) = \vartheta(a)(\sqrt[m]{b})/\sqrt[m]{b} = \zeta_n^t, \quad a, b \in K_n^\times, \quad (2.4)$$

где $\vartheta(a)$ – автоморфизм, соответствующий элементу a согласно локальной теории полей классов. Положим

$$U(K_n)^0 = (U(K_n)/\mu(K_n)) \cap V(K_n)^0. \quad (2.5)$$

Поскольку $N_{K_n/\mathbb{Q}_\ell}(U(K_n)^0) = 1$ и любые корни из единицы порождают абелево расширение поля $\mathbb{Q}_\ell$, спаривание $U(K_n)^0 \times \mu(K_n)$, индуцированное произведением (2.4), тривиально, поэтому спаривание (2.4) индуцирует корректно определенное спаривание

$$U(K_n)^0 \times U(K_n)^0 \rightarrow \mu_{\ell^m}. \quad (2.6)$$

ПРЕДЛОЖЕНИЕ 2.3 [4, теорема 1.2]. Пусть $x, y \in V(K_n)^0$. Тогда $x \in U(K_n)^0$ (соответственно, $y \in U(K_n)^0$), если и только если коэффициенты x_σ (соответственно, y_σ) в (2.3) удовлетворяют соотношению $\sum_{\sigma \in G_n} \kappa(\sigma) x_\sigma \equiv 0 \pmod{\ell^m}$ (соответственно, $\sum_{\sigma \in G_n} \kappa(\sigma) y_\sigma \equiv 0 \pmod{\ell^m}$), где $\kappa: G_n \rightarrow (\mathbb{Z}/\ell^m\mathbb{Z})^\times$ – круговой характер, определенный условием $\sigma(\zeta_n) = \zeta_n^{\kappa(\sigma)}$ для любого $\sigma \in G_n$.

ПРЕДЛОЖЕНИЕ 2.4 [4, теорема 1.3]. Для $x, y \in U(K_n)^0$ пусть x_σ, y_σ – коэффициенты, определенные в (2.3). Пусть $(x, y)_n = \zeta_n^t$ – значение спаривания, определенного в (2.6). Тогда

$$t \equiv - \sum_{\sigma \in G_n} \kappa(\sigma) x_\sigma y_\sigma \pmod{\ell^m}.$$

Для $x, y \in U(K_n)^0$ мы положим

$$\langle x, y \rangle_n := \sum_{\sigma \in G_n} (\sigma^{-1}(x), y)_n \sigma \in \mathbb{Z}/\ell^m\mathbb{Z}[G_n],$$

где $(x, y)_n$ определено в (2.6) и μ_{ℓ^m} отождествляется с $\mathbb{Z}/\ell^m\mathbb{Z}$ при помощи сопоставления $\zeta_n \leftrightarrow 1$. Пусть w – автоморфизм кольца $\mathbb{Z}/\ell^m\mathbb{Z}[G_n]$ такой, что w

оставляет на месте все элементы из $\mathbb{Z}/\ell^m\mathbb{Z}$ и $w(\sigma) = \varkappa(\sigma)\sigma^{-1}$ для любого $\sigma \in G_n$.

В качестве непосредственного следствия из предложения 2.4 мы получаем

ПРЕДЛОЖЕНИЕ 2.5. *Для $x, y \in U(K_n)^0$ пусть x_σ, y_σ определены так же, как в (2.3). Положим*

$$a = \sum_{\sigma \in G_n} \bar{x}_\sigma \sigma, \quad b = \sum_{\sigma \in G_n} \bar{y}_\sigma \sigma \in \mathbb{Z}/\ell^m\mathbb{Z}[G_n],$$

где $\bar{x}_\sigma$ и $\bar{y}_\sigma$ — соответственно вычеты x_σ и y_σ по модулю ℓ^m . Тогда в кольце $\mathbb{Z}/\ell^m\mathbb{Z}[G_n]$ справедливо равенство

$$\langle x, y \rangle_n = -a \cdot w(b).$$

Теперь мы рассмотрим глобальный случай. Пусть $K_n = \mathbb{Q}(\zeta_n, \mu_d)$. Положим

$$V(K_n) = \prod_{v|\ell} V(K_{n,v}), \quad V(K_n)^0 = \prod_{v|\ell} V(K_{n,v})^0, \quad U(K_n)^0 = \prod_{v|\ell} U(K_{n,v})^0.$$

Эти группы мы будем рассматривать как модули относительно группы Галуа $G_n = G(K_n/\mathbb{Q})$, и как таковые они изоморфны индуцированным модулям $\text{ind}_{G_{n,v}}^{G_n}$ для $G_{n,v}$ -модулей $V(K_{n,v})$, $V(K_{n,v})^0$ и $U(K_{n,v})^0$ соответственно, где $G_{n,v}$ — подгруппа разложения точки $v|\ell$ в группе G_n . В качестве непосредственного следствия из предложения 2.1 мы получаем

ПРЕДЛОЖЕНИЕ 2.6. *В глобальном случае положим $G_n = G(K_n/\mathbb{Q})$, где $K_n = \mathbb{Q}(\zeta_n, \mu_d)$. Тогда $V(K_n)^0$ является циклическим $\mathbb{Z}_\ell[G_n]$ -модулем. Зафиксируем некоторую точку $v_n|\ell$ поля K_n . Тогда любой из элементов $\eta(K_{n,v_n}) = \eta_n(\alpha, 1), \eta'(K_{n,v_n}) = \eta_n(\beta, -1) \in V(K_{n,v_n})^0$, определенных в предложении 2.1, порождает $V(K_n)^0$ как модуль Галуа, где $V(K_{n,v_n})^0$ рассматривается как подгруппа группы $V(K_n)^0$.*

Если $\mathbf{x}, \mathbf{y} \in U(K_n)^0$ и $\mathbf{x} = \prod_{v|\ell} x_v$, $\mathbf{y} = \prod_{v|\ell} y_v$, где $x_v, y_v \in U(K_{n,v})^0$, то спаривания (2.6) для всех $v|\ell$ определяют произведение $(\cdot, \cdot)_{\ell,n}$:

$$U(K_n)^0 \times U(K_n)^0 \rightarrow \mu_{\ell^m}, \quad (\mathbf{x}, \mathbf{y})_{\ell,n} = \prod_{v|\ell} (x_v, y_v)_n, \quad (2.7)$$

где $(x_v, y_v)_n$ означает спаривание (2.6), а группы $\mu_{\ell^m} \subset K_n$ и $\mu_{\ell^m} \subset K_{n,v}$ отождествлены при помощи канонического включения $K_n \subset K_{n,v}$. Следующее предложение непосредственно вытекает из предложения 2.4.

ПРЕДЛОЖЕНИЕ 2.7. *Пусть $\mathbf{x}, \mathbf{y} \in U(K_n)^0$, где*

$$\mathbf{x} = \sum_{\sigma \in G_n} x_\sigma \sigma(\eta(K_{n,v_n})), \quad \mathbf{y} = \sum_{\sigma \in G_n} y_\sigma \sigma(\eta'(K_{n,v_n})), \quad x_\sigma, y_\sigma \in \mathbb{Z}_\ell.$$

Тогда произведение $(\mathbf{x}, \mathbf{y})_{\ell,n}$ в (2.7) задается в явном виде формулой

$$(\mathbf{x}, \mathbf{y})_{\ell,n} = \zeta_n^t, \quad \text{где } t \equiv - \sum_{\sigma \in G_n} \varkappa(\sigma) x_\sigma y_\sigma \pmod{\ell^m}.$$

Обозначим $\mathbb{Z}/\ell^m\mathbb{Z}[G_n]$ через $\mathfrak{R}_n$. Для $\mathbf{x}, \mathbf{y} \in U(K_n)^0$ положим

$$\langle \mathbf{x}, \mathbf{y} \rangle_{\ell, n} = \sum_{\sigma \in G_n} (\sigma^{-1}(\mathbf{x}), \mathbf{y})_{\ell, n} \sigma \in \mathfrak{R}_n, \quad (2.8)$$

где $(\sigma^{-1}(\mathbf{x}), \mathbf{y})_{\ell, n}$ – произведение, определенное в (2.7), и группа μ_{ℓ^m} отождествлена с $\mathbb{Z}/\ell^m\mathbb{Z}$, как и выше. Следующее предложение непосредственно вытекает из предложения 2.7.

ПРЕДЛОЖЕНИЕ 2.8. Пусть $\mathbf{x}, \mathbf{y} \in U(K_n)^0$ имеют тот же смысл, что и в предложении 2.7. Положим

$$\mathbf{a} = \sum_{\sigma \in G_n} \bar{x}_\sigma \sigma, \quad \mathbf{b} = \sum_{\sigma \in G_n} \bar{y}_\sigma \sigma \in \mathfrak{R}_n,$$

где $\bar{x}_\sigma$ и $\bar{y}_\sigma$ – соответственно вычеты x_σ и y_σ по модулю ℓ^m . Тогда

$$\langle \mathbf{x}, \mathbf{y} \rangle_{\ell, n} = -\mathbf{a} \cdot w(\mathbf{b}),$$

где w – автоморфизм кольца $\mathfrak{R}_n$, оставляющий на месте $\mathbb{Z}/\ell^m\mathbb{Z}$ и такой, что $w(\sigma) = \varkappa(\sigma)\sigma^{-1}$ для любого $\sigma \in G_n$.

Теперь рассмотрим глобальное круговое $\mathbb{Z}_\ell$ -расширение K_∞/K_0 , где $K_0 = \mathbb{Q}(\zeta_0, \mu_d)$. Положим $V(K_\infty) = \varprojlim V(K_n) = \varprojlim V(K_n)^0$, где проективные пределы берутся относительно норменных отображений. Отметим, что $V(K_\infty)$ является R_∞ -модулем, где $R_\infty = \mathbb{Z}_\ell[[G(K_\infty/\mathbb{Q})]] = \varprojlim \mathbb{Z}_\ell[G_n]$. В соответствии с разложением $G_\infty := G(K_\infty/\mathbb{Q}) = G_0 \times \Gamma$, где $G_0 \cong G(K_0/\mathbb{Q}) \cong G(K_\infty/\mathbb{Q}_\infty)$ и $\Gamma \cong G(K_\infty/K_0) \cong G(\mathbb{Q}_\infty/\mathbb{Q})$, мы имеем $R_\infty \cong \Lambda[G_0]$, где $\Lambda = \mathbb{Z}_\ell[[\Gamma]]$.

Будем предполагать, что выделенные точки $v_n|\ell$ полей K_n согласованы. Тогда точка $v_\infty|\ell$, определенная условием $v_\infty = \varprojlim v_n$, является выделенной точкой поля K_∞ , и мы положим $\eta(K_\infty, v_\infty) = \varprojlim \eta(K_n, v_n)$, $\eta'(K_\infty, v_\infty) = \varprojlim \eta'(K_n, v_n) \in V(K_\infty)$. Для любого $\xi \in \mu_d$ имеется представление вида

$$\xi = \sum_{\sigma \in G_{-1}} a_\sigma \sigma(\alpha), \quad a_\sigma \in \mathbb{Z}_\ell,$$

где $G_{-1} = G(\mathbb{Q}(\mu_d)/\mathbb{Q})$ и α имеет тот же смысл, что и выше. Тогда существует элемент $\eta_n(\xi, 1)$ такой, что его логарифм

$$\log_\ell(\eta_n(\xi, 1)) \in \prod_{v|\ell} K_{n,v}$$

определяется формулой (2.1) с заменой α на ξ . Элементы $\eta_n(\xi, 1)$, где $n = 1, 2, \dots$, образуют согласованную последовательность относительно норменных отображений и определяют после перехода к пределу элемент $\eta_\infty(\xi, 1) = \varprojlim \eta_n(\xi, 1) \in V(K_\infty)$. Аналогичным образом можно определить элемент $\eta_\infty(\xi, -1) \in V(K_\infty)$. Отметим, что элементы $\eta_\infty(\xi, 1)$ и $\eta_\infty(\xi, -1)$ сопряжены относительно действия группы Галуа. Именно, пусть $\tau \in G_\infty$ – такой элемент, что $\tau(\xi) = \xi$ для любого $\xi \in \mu_d$ и $\tau(\zeta_n) = \zeta_n^{-1}$ для любого n . Тогда $\eta_\infty(\xi, -1) = \tau(\eta_\infty(\xi, 1))$.

ПРЕДЛОЖЕНИЕ 2.9 [4, предложение 2.1]. *Элементы $\eta_\infty(\xi, 1)$, где $\xi \in \mu_d$ (соответственно, $\eta_\infty(\xi, -1)$, где $\xi \in \mu_d$), порождают $V(K_\infty)$ как модуль Галуа.*

Для кругового поля $K_n = \mathbb{Q}(\zeta_n, \mu_d)$ пусть $P(K_n)$ – группа круговых чисел, т.е. $P(K_n)$ – подгруппа в $K_n^\times$, порожденная элементами $1 - \xi\zeta_n^i$, где $\xi \in \mu_d$, $i = 1, \dots, \ell^m$, $\xi\zeta_n^i \neq 1$. Положим

$$\overline{P}(K_n) = (P(K_n)/\mu(K_n)) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell.$$

Для заданного $\xi \in \mu_d$ положим $\varepsilon_n(\xi) = 1 - \varphi^{1-m}(\xi)\zeta_n$, где φ – автоморфизм Фробениуса, т.е. $\varphi(\xi) = \xi^\ell$. Тогда при заданном ξ элементы $\varepsilon_n(\xi)$ образуют согласованную последовательность относительно норменных отображений и определяют элемент

$$\varepsilon_\infty(\xi) = \varprojlim \varepsilon_n(\xi) \in P(K_\infty) := \varprojlim \overline{P}(K_n).$$

Отметим, что $(\sigma - 1)P(K_\infty) \subset V(K_\infty)$ для любого $\sigma \in G_\infty$.

ПРЕДЛОЖЕНИЕ 2.10 [4, предложение 2.3]. *Элементы $\varepsilon_\infty(\xi)$, $\xi \in \mu_d$, порождают $P(K_\infty)$ как модуль Галуа.*

Как и в [5], для целого числа a мы определяем элемент Штикельбергера формулой

$$s(a, \ell^m d) = \sum_{\substack{i \bmod \ell^m d \\ (i, \ell d) = 1}} \left\langle -\frac{ai}{\ell^m d} \right\rangle \sigma_i^{-1} \in \mathbb{Q}_\ell[G_n], \quad (2.9)$$

где через $\langle x \rangle$ означена дробная часть числа $x \in \mathbb{Q}$ и элемент $\sigma_i \in G_n$ определяется условием $\sigma_i(x) = x^i$ для любого $x \in \mu(K_n)$. Отметим, что мы будем также использовать формулу (2.9) в случае $d \equiv 2 \pmod{4}$. В этом случае

$$s(a, \ell^m d) = (1 - \sigma_2^{-1})s(a, \ell^m d/2).$$

Положим $e^+ = (1 + \sigma_{-1})/2$, $e^- = (1 - \sigma_{-1})/2$, где σ_{-1} – автоморфизм комплексного сопряжения. Хорошо известно, что при заданном i и любом n мы имеем $(\sigma_i - i)s(a, \ell^m d) \in \mathbb{Z}_\ell[G_n]$. Также хорошо известно [1], [5], что элементы $e^- s(a, \ell^m d)$ согласованы относительно естественных проекций $\mathbb{Q}[G_{n_2}] \rightarrow \mathbb{Q}[G_{n_1}]$ при $n_2 > n_1$. Таким образом, мы можем рассматривать элементы

$$s(a, \ell^\infty d) := \varprojlim e^- s(a, \ell^m d) \in \varprojlim \mathbb{Q}_\ell[G_n] \quad (2.10)$$

как элементы алгебры $M[G_0]$, где M – поле частных кольца Λ . Пусть w – автоморфизм кольца R_∞ , оставляющий на месте $\mathbb{Z}_\ell$ и такой, что $w(\sigma) = \varkappa(\sigma)\sigma^{-1}$ для любого $\sigma \in G_\infty$, где $\varkappa: G_\infty \rightarrow \mathbb{Z}_\ell^\times$ – круговой характер, определенный условием $\sigma(\zeta_n) = \zeta_n^{\varkappa(\sigma)}$ для любого n . Заметим, что при любом n автоморфизм w кольца R_∞ согласован с автоморфизмом w кольца $\mathfrak{R}_n$ из предложения 2.8.

ПРЕДЛОЖЕНИЕ 2.11 [4, теорема 2.1]. *Пусть $\xi \in \mu_d$ и $\xi^\delta = 1$ для некоторого $\delta | d$. Тогда*

$$w(s(1, \ell^\infty \delta))(\eta_\infty(\xi, -1)) = - \sum_{f | \delta} f^{-1} \mu(f) \sigma(f)(\varepsilon_\infty(\xi^f)),$$

где f пробегает все делители δ , включая δ и 1, а $\mu(f)$ – функция Мёбиуса и $\sigma(f)$ – элемент группы $G(K_\infty/K_{-1})$ такой, что $\varkappa(\sigma(f)) = f$.

Отметим, что δ не обязан быть точным порядком ξ .

Следующее предложение показывает, что интересующий нас элемент $S(\chi)_1 \in V(K)$ фактически принадлежит подгруппе $V(K)^0$.

ПРЕДЛОЖЕНИЕ 2.12. Пусть $S(\chi)$ – гауссова сумма из (1.1), где χ – характер порядка $r = \ell^m d$, и $S(\chi)_1$ имеет тот же смысл, что и в (1.3). Пусть G_ℓ – подгруппа разложения ℓ в группе $G = G(K/\mathbb{Q})$, где $K = \mathbb{Q}(\xi_r)$, ξ_r – первообразный корень из единицы степени r . Тогда

$$\mathrm{Sp}_{G_\ell}(\log_\ell S(\chi)_1) = 0. \quad (2.11)$$

ДОКАЗАТЕЛЬСТВО. Прежде всего заметим, что достаточно проверить существование равенства главных дивизоров

$$(N_{G_\ell}(S(\chi)_1)) = 1. \quad (2.12)$$

Действительно, (2.12) означает, что $N_{G_\ell}(S(\chi)_1)$ является единицей. Поскольку $j(S(\chi)_1) = S(\chi)_1^{-1}$, где j – автоморфизм комплексного сопряжения, мы получаем, что $N_{G_\ell}(S(\chi)_1)$ – корень из единицы, откуда следует предложение.

Чтобы доказать (2.12), заметим, что согласно теореме Штикельбергера [1, гл. 2, теорема 2.2] мы имеем

$$(S(\chi_1)) = \mathfrak{p}^{\delta e^- s(a, \ell^m d)}, \quad (2.13)$$

где $\mathfrak{p}$ – простой дивизор над p в поле K такой, что χ является характером поля вычетов $\mathbb{F}_q = \mathcal{O}_K/\mathfrak{p}$, $\delta = 1$ при $\ell \neq 2$, $\delta = 2$ при $\ell = 2$, число a определяется из равенства $\chi = \omega^{a(q-1)/\ell^m d}$ для характера Тейхмюллера ω и элемент $s(a, \ell^m d)$ определен в (2.9). Заметим, что $(a, \ell d) = 1$. Если $\mathfrak{p}_1 = N_{G_\ell}(\mathfrak{p})$, то

$$N_{G_\ell}((S(\chi)_1)) = \mathfrak{p}_1^{\pi(\delta e^- s(a, \ell^m d))},$$

где π означает естественную проекцию $\pi: \mathbb{Q}_\ell[G] \rightarrow \mathbb{Q}_\ell[G/G_\ell]$. Таким образом, достаточно проверить, что

$$\pi(e^- s(a, \ell^m d)) = 0.$$

Заметим, что согласно [5, формула (3.3)]

$$e^- s(a, \ell^m d) = \sum_{\substack{i \bmod \ell^m d \\ (i, \ell d) = 1}} \left(- \left\langle \frac{ai}{\ell^m d} \right\rangle + \frac{1}{2} \right) \sigma_i^{-1}. \quad (2.14)$$

Пусть T_ℓ – подгруппа инерции ℓ в G . Тогда $(\mathbb{Z}/\ell^m \mathbb{Z})^\times \cong T_\ell \subseteq G_\ell$ и G_ℓ/T_ℓ – циклическая группа, порожденная автоморфизмом Фробениуса φ_ℓ , соответствующим ℓ . Мы имеем $\pi = \pi_2 \cdot \pi_1$, где π_1, π_2 – естественные проекции,

$$\pi_1: \mathbb{Q}_\ell[G] \rightarrow \mathbb{Q}_\ell[G/T_\ell], \quad \pi_2: \mathbb{Q}_\ell[G/T_\ell] \rightarrow \mathbb{Q}_\ell[G/G_\ell].$$

Заметим, что функция $u(x) = -\langle ax \rangle + \frac{1}{2}$ является распределением на группе $\frac{1}{\ell^m d} \mathbb{Z}/\mathbb{Z}$. Таким образом, учитывая, что $m \geq 1$ при $\ell \neq 2$ ($m \geq 2$ при $\ell = 2$), и рассуждая, как в доказательстве леммы 2.1 из [5], мы получаем

$$\pi_1(e^- s(a, \ell^m d)) = (1 - \varphi_\ell^{-1})e^- s(a, d).$$

Если $G_\ell = T_\ell$, то $\varphi_\ell = 1$, откуда следует наше утверждение. В противном случае

$$\pi(e^-s(a, \ell^m d)) = \pi_2((1 - \varphi_\ell^{-1})e^-s(a, d)) = 0.$$

Это означает, что $(N_{G_\ell}(S(\chi)_1)) = 1$, что и требовалось доказать.

§ 3. Основная теорема

ПРЕДЛОЖЕНИЕ 3.1. Пусть $K_n = \mathbb{Q}(\zeta_n, \mu_d)$ и $K_\infty = \bigcup_{n=1}^\infty K_n$. Тогда существуют элементы $\eta_\infty, \eta'_\infty \in V(K_\infty)$, $\varepsilon_\infty \in P(K_\infty)$, удовлетворяющие следующим условиям:

- (i) каждый из элементов $\eta_\infty, \eta'_\infty$ порождает $V(K_\infty)$ как модуль Галуа;
- (ii) если η_n (соответственно, η'_n) – образ η_∞ (соответственно, η'_∞) относительно естественной проекции $V(K_\infty) \rightarrow V(K_n)$ при некотором n , то для любых $x, y \in U(K_n)^0$ произведение (2.8) определяется формулой

$$\langle x, y \rangle_{\ell, n} = -\mathbf{a} \cdot w(\mathbf{b}), \quad (3.1)$$

где для $x = \mathbf{a}_1 \eta_n$, $y = \mathbf{b}_1 \eta'_n$, $\mathbf{a}_1, \mathbf{b}_1 \in \mathbb{Z}_\ell[G_n]$, мы обозначаем через $\mathbf{a}$ и $\mathbf{b}$ образы в $\mathfrak{R}_n$ элементов $\mathbf{a}_1$ и $\mathbf{b}_1$ соответственно;

- (iii) элемент η'_∞ и круговое число ε_∞ связаны соотношением

$$-w(s(1, \ell^\infty d))(\eta'_\infty) = \varepsilon_\infty. \quad (3.2)$$

ДОКАЗАТЕЛЬСТВО. Если $d = 1$, т.е. $K_n = \mathbb{Q}(\zeta_n)$ для любого n , то $V(K_\infty) = V(K_{\infty, v_\infty})$, где v_∞ – единственная точка над ℓ в поле K_∞ . В этом случае мы можем положить $\eta_\infty = \eta_\infty(1, 1)$, $\eta'_\infty = \eta_\infty(1, -1)$, $\varepsilon_\infty = \varepsilon_\infty(1) = \varprojlim (1 - \zeta_n)$. Тогда предложение 2.9 показывает, что элементы $\eta_\infty, \eta'_\infty$ удовлетворяют условию (i). Условие (ii) следует из предложения 2.8, а (iii) является следствием предложения 2.11.

Если $d > 1$, то можно выбрать $\alpha, \beta \in A := \mathbb{Q}(\mu_d) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ такие, что $\alpha = \sum_{\xi \in \mu_d} a_\xi \xi$, $\beta = \sum_{\xi \in \mu_d} b_\xi \xi$, $a_\xi, b_\xi \in \mathbb{Z}_\ell$, и α, β порождают нормальные взаимные базисы алгебры A . Тогда можно положить

$$\eta_\infty = \eta_\infty(\alpha, 1) = \prod_{\xi \in \mu_d} \eta_\infty(\xi, 1)^{a_\xi}, \quad \eta'_\infty = \eta_\infty(\beta, -1) = \prod_{\xi \in \mu_d} \eta_\infty(\xi, -1)^{b_\xi}.$$

Далее, в качестве ε_∞ мы можем, пользуясь предложением 2.11, взять элемент (в аддитивной записи)

$$\varepsilon_\infty = -w(s(1, \ell^\infty d))\eta'_\infty = \sum_{\xi \in \mu_d} b_\xi \sum_{f|d} f^{-1} \mu(f) \sigma(f)(\varepsilon_\infty(\xi^f)),$$

где обозначения имеют тот же смысл, что и в предложении 2.11. Предложение доказано.

Через ε_n мы будем обозначать проекцию ε_∞ в $\bar{P}(K_n)$. Итак, пусть $S(\chi)$ – гауссова сумма, определенная в (1.1), где χ – характер порядка $r = \ell^m d$ мультипликативной группы $\mathbb{F}_q^\times$ конечного поля $\mathbb{F}_q$ характеристики p . Если $\mathfrak{P}$ – фиксированная точка над p в поле $E := \mathbb{Q}(\mu_{q-1})$, то мы можем отождествить χ

с характером поля вычетов $\mathcal{O}_E/\mathfrak{P}$, где $\mathcal{O}_E$ – кольцо целых поля E , поскольку $\mathcal{O}_E/\mathfrak{P} \cong \mathbb{F}_p(\mu_{q-1}) \cong \mathbb{F}_q$. Пусть $\omega: \mathcal{O}_E/\mathfrak{P} \rightarrow \mu_{q-1}$ – характер Тейхмюллера, т.е. $\omega(a) \equiv a \pmod{\mathfrak{P}}$ для любого $a \in \mathcal{O}_E/\mathfrak{P}$. Заметим, что любой характер порядка $\ell^m d$ сопряжен относительно действия группы Галуа с характером $\chi_0 = \omega^{-(q-1)/\ell^m d}$. Действительно, любой такой характер χ имеет вид $\chi = \chi_0^t$ для некоторого t , взаимно простого с ℓd . Если σ_t – автоморфизм поля K_n такой, что $\sigma_t(\xi) = \xi^t$ для любого $\xi \in \mu(K_n)$, то $\chi = \chi_0^t$ и $S(\chi)_1 = \sigma_t(S(\chi_0)_1)$.

Пусть $\mathfrak{p}_n$ – точка поля K_n такая, что $\mathfrak{P}|\mathfrak{p}_n$. Пусть ε_n – проекция элемента ε_∞ в $\overline{P}(K_n)$. Если некоторый $x \in \overline{P}(K_n)$ является всюду локальной универсальной нормой в расширении K_∞/K_n , то x является локальной единицей относительно любой точки, не делящей ℓ . В частности, ε_n является локальной единицей в K_n для любой точки $\mathfrak{p}|p$. Зафиксируем первообразный корень степени u из единицы $\theta \in \mathcal{O}_{K_n}/\mathfrak{p}_n$ такой, что $\theta^{u/\ell^m} \equiv \zeta_n \pmod{\mathfrak{p}_n}$, где $u = N(\mathfrak{p}_n) - 1 = |(\mathcal{O}_{K_n}/\mathfrak{p}_n)^\times|$. Для любого $\sigma \in G_n$ мы определим элемент $c_\sigma \in \mathbb{Z}/u\mathbb{Z}$ формулой

$$\sigma^{-1}(\varepsilon_n) \equiv \theta^{c_\sigma} \pmod{\mathfrak{p}_n}. \quad (3.3)$$

Положим $\bar{c}_\sigma = c_\sigma \pmod{\ell^m}$. Заметим, что $\bar{c}_\sigma$ не зависит от выбора θ . Таким образом, любой единице ε_n соответствует элемент $\mathbf{c}(\varepsilon_n) = \sum_{\sigma \in G_n} \bar{c}_\sigma \sigma \in \mathfrak{R}_n$. Кроме того, $w(\zeta_n) \sim 0$, поэтому элемент $w(\mathbf{c}(\varepsilon_n))$ определен корректно с точностью до отношения $\sim$. Положим

$$\mathbf{a} = \sum_{\sigma \in G_n} \bar{a}_\sigma \sigma, \quad \mathbf{c} = \mathbf{c}(\varepsilon_n) = \sum_{\sigma \in G_n} \bar{c}_\sigma \sigma \in \mathfrak{R}_n, \quad (3.4)$$

где $\bar{a}_\sigma = a_\sigma \pmod{\ell^m}$ и a_σ – коэффициенты, входящие в формулу (1.4).

Заметим, что для любого $x \in \mathcal{O}_{K_n} \setminus \mathfrak{p}_n$ можно аналогичным образом определить элемент $\mathbf{c}(x) \in \mathfrak{R}_n$, причем для $x, y \in \mathcal{O}_{K_n} \setminus \mathfrak{p}_n$ мы имеем $\mathbf{c}(xy) = \mathbf{c}(x) + \mathbf{c}(y)$ и для любого $\sigma \in G_n$ имеем $\mathbf{c}(\sigma(x)) = \sigma(\mathbf{c}(x))$.

ТЕОРЕМА 3.2. Пусть $S(\chi_0)$ – гауссова сумма, соответствующая характеру $\chi_0 = \omega^{-(q-1)/\ell^m d}$, где ω – характер Тейхмюллера по модулю $\mathfrak{P}$. Тогда элементы $\mathbf{a}, \mathbf{c} \in \mathfrak{R}_n$, определенные в (3.4), удовлетворяют соотношению

$$\mathbf{a} \sim -\delta w(\mathbf{c}),$$

где $\delta = 1$ при $\ell \neq 2$ и $\delta = 2$ при $\ell = 2$. Если $S(\chi)$ – гауссова сумма, соответствующая характеру $\chi = \chi_0^t$, и $\mathbf{a}(\chi)$ – соответствующий ей элемент группового кольца $\mathfrak{R}_n$, определенный в (3.4), то

$$\mathbf{a}(\chi) \sim \sigma_t(-\delta w(\mathbf{c})).$$

Заметим, что достаточно доказать первое утверждение теоремы 3.2. Зафиксируем топологическую образующую $\gamma \in \Gamma = G(K_\infty/K_0)$. Например, мы можем положить $\gamma = \sigma_{i_0}$, где $i_0 = 1 + \ell d$ при $\ell \neq 2$ и $i_0 = 1 + 4d$ при $\ell = 2$. Докажем сначала ослабленный вариант теоремы 3.2, а затем покажем, что теорема 3.2 выводится из этого результата.

ПРЕДЛОЖЕНИЕ 3.3. В условиях и обозначениях теоремы 3.2 справедливо равенство

$$(\gamma - i_0)((i_0 \gamma^{-1} - 1)e^{-s(1, \ell^m d)})(\mathbf{a} + \delta w(\mathbf{c})) \sim 0,$$

где $\delta = 1$ при $\ell \neq 2$ и $\delta = 2$ при $\ell = 2$.

ДОКАЗАТЕЛЬСТВО. Положим $S(\chi)_2 = S(\chi)_1^{\gamma-i_0}$. Хорошо известно (см. [1], [5]), что $S(\chi)^{\sigma_i-i} \in K_n$. Более того, поскольку согласно предложению 2.12 имеем $S(\chi)_1 \in V(K_{n,v})^0$ для любой точки $v|\ell$ и $(\sigma_i - i)V(K_{n,v}) \subseteq U(K_{n,v})/\mu(K_{n,v})$, мы получаем

$$S(\chi)_2 \in U(K_{n,v})^0 \quad \forall v: v|\ell.$$

Следовательно, мы можем рассматривать $S(\chi)_2$ как элемент группы $U(K_n)^0 = \prod_{v|\ell} U(K_{n,v})^0$. Положим $\varepsilon'_n = \varepsilon_n^{\gamma-1}$. Тогда мы можем рассматривать ε'_n как элемент группы $U(K_n)^0$. Следовательно, определено произведение $\langle S(\chi)_2, \varepsilon'_n \rangle_{\ell,n} \in \mathfrak{R}_n$ (см. (2.8)).

С другой стороны, мы можем рассматривать $S(\chi)_2$ и ε'_n как элементы алгебры Галуа $K_{n,p} = K_n \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{\mathfrak{p}|p} K_{n,\mathfrak{p}}$, где произведение берется по всем точкам $\mathfrak{p}|p$ поля K_n . Заметим, что символ норменного вычета

$$K_{n,\mathfrak{p}}^\times \times K_{n,\mathfrak{p}}^\times \rightarrow \mu_{\ell^m} \quad (3.5)$$

определен для любой точки $\mathfrak{p}|p$. Следовательно, мы можем определить спаривание

$$K_{n,p}^\times \times K_{n,p}^\times \rightarrow \mu_{\ell^m}, \quad \mathbf{x}, \mathbf{y} \rightarrow (\mathbf{x}, \mathbf{y})_{p,n},$$

где, как и в случае $v|\ell$, мы полагаем

$$(\mathbf{x}, \mathbf{y})_{p,n} = \prod_{\mathfrak{p}|p} (x_{\mathfrak{p}}, y_{\mathfrak{p}}) \in \mu_{\ell^m}, \quad (3.6)$$

а также спаривание

$$\langle \mathbf{x}, \mathbf{y} \rangle_{p,n} = \sum_{\sigma \in G_n} (\sigma^{-1}(\mathbf{x}), \mathbf{y})_{p,n} \sigma \in \mathfrak{R}_n, \quad (3.7)$$

где

$$\mathbf{x}, \mathbf{y} \in K_{n,p}, \quad \mathbf{x} = \prod_{\mathfrak{p}|p} x_{\mathfrak{p}}, \quad \mathbf{y} = \prod_{\mathfrak{p}|p} y_{\mathfrak{p}}, \quad x_{\mathfrak{p}}, y_{\mathfrak{p}} \in K_{n,\mathfrak{p}}.$$

Из определения $\langle \mathbf{x}, \mathbf{y} \rangle_{p,n}$ следует, что (в аддитивной записи)

$$\langle \alpha \mathbf{x}, \beta \mathbf{y} \rangle_{p,n} = \bar{\alpha} w(\bar{\beta}) \langle \mathbf{x}, \mathbf{y} \rangle_{p,n} \quad (3.8)$$

для любых $\alpha, \beta \in \mathbb{Z}_{\ell}[G_n]$, где $\bar{\alpha}, \bar{\beta}$ – образы соответственно α и β в $\mathfrak{R}_n$.

Заметим, что

$$\langle S(\chi)_2, \varepsilon'_n \rangle_{\ell,n} = -\langle S(\chi)_2, \varepsilon'_n \rangle_{p,n}. \quad (3.9)$$

Действительно, используя (3.6), можно определить произведение $(\mathbf{x}, \mathbf{y})_{q,n}$ для любого простого q и любых $\mathbf{x}, \mathbf{y} \in K_n^\times$. Поскольку $\mathbf{x}$ и $\mathbf{y}$ – главные идеалы, закон взаимности для символов норменного вычета приводит к равенству

$$\prod_q (\mathbf{x}, \mathbf{y})_{q,n} = 1, \quad (3.10)$$

где произведение берется по всем рациональным простым q (заметим, что K_n – мнимое абелево поле, поэтому символ норменного вычета тривиален для любой

архимедовой точки). Так как ε'_n – единица и $S(\chi)_2$ – p -единица, мы получаем, что $(\sigma(S(\chi)_2), \varepsilon'_n)_{q,n} = 1$ для любых $\sigma \in G_n$ и $q \neq p, \ell$. Итак, в нашем случае (3.10) сводится к равенству (в аддитивной записи)

$$(\sigma(S(\chi)_2), \varepsilon'_n)_{\ell,n} = -(\sigma(S(\chi)_2), \varepsilon'_n)_{p,n}, \quad (3.11)$$

откуда следует (3.9).

Мы вычислим обе части (3.9) в явном виде. Прежде всего заметим, что из соотношения (3.2) следует равенство

$$\varepsilon'_\infty := \varepsilon_\infty^{\gamma^{-1}} = -w(s(1, \ell^\infty d))(\gamma - 1)\eta'_\infty = -w((i_0\gamma^{-1} - 1)s(1, \ell^\infty d))\eta'_\infty. \quad (3.12)$$

Мы имеем $(i_0\gamma^{-1} - 1)s(1, \ell^m d) \in R_\infty$. Следовательно, взяв проекции обеих частей (3.12) в $V(K_n)$, мы получаем

$$\varepsilon'_n = -\pi_n(w((i_0\gamma^{-1} - 1)s(1, \ell^\infty d)))\eta'_n,$$

где π_n – естественная проекция $R_\infty \rightarrow \mathbb{Z}_\ell[G_n]$. Заметим, что

$$\pi_n(w((i_0\gamma^{-1} - 1)s(1, \ell^\infty d))) \bmod \ell^m = w((i_0\gamma^{-1} - 1)e^-s(1, \ell^m d)) \bmod \ell^m \in \mathfrak{R}_n.$$

Отметим также, что при $\ell = 2$ элемент $(i_0\gamma^{-1} - 1)e^-s(1, \ell^m d)$ принадлежит $\mathbb{Z}_2[G_n]$. Действительно,

$$e^-s(1, \ell^m d) = s(1, \ell^m d) - \frac{1}{2} \sum_{\sigma \in G_n} \sigma.$$

С другой стороны,

$$(i_0\gamma^{-1} - 1)\frac{1}{2} \sum_{\sigma \in G_n} \sigma = (i_0 - 1)\frac{1}{2} \sum_{\sigma \in G_n} \sigma \in \mathbb{Z}_2[G_n].$$

Таким образом, применяя (3.1) и учитывая, что w – инволюция кольца $\mathfrak{R}_n$, получаем равенство

$$\langle S(\chi)_2, \varepsilon'_n \rangle_{\ell,n} = (\gamma - i_0)\mathbf{a}((i_0\gamma^{-1} - 1)e^-s(1, \ell^m d)), \quad (3.13)$$

где $\mathbf{a}$ имеет тот же смысл, что и в теореме 3.2.

Теперь мы вычислим $\langle S(\chi)_2, \varepsilon'_n \rangle_{p,n}$. Прежде всего мы вычислим $\langle \pi, \varepsilon_n \rangle_{p,n}$, где $\pi \in K_{n,p}$ – элемент вида $\pi = \prod_{\mathfrak{p}|p} \pi_{\mathfrak{p}}$, где $\pi_{\mathfrak{p}} \in K_{n,\mathfrak{p}}$, $\pi_{\mathfrak{p}_n}$ – униформизирующий элемент поля $K_{n,\mathfrak{p}_n}$ и $\pi_{\mathfrak{p}} = 1$ для $\mathfrak{p} \neq \mathfrak{p}_n$. Заметим, что ε_n – локальная единица для любой точки $\mathfrak{p}|p$. Следовательно, $\langle \pi, \varepsilon_n \rangle_{p,n}$ не зависит от конкретного выбора локального параметра $\pi_{\mathfrak{p}_n}$. Положим $K' = K_{n,\mathfrak{p}_n}(\theta')$, где $\theta' = \sqrt[\ell^m]{\theta}$ и θ имеет тот же смысл, что и в (3.3). Автоморфизм $\varphi_{\mathfrak{p}_n}$ расширения $K'/K_{n,\mathfrak{p}_n}$, соответствующий согласно локальной теории полей классов элементу $\pi_{\mathfrak{p}_n}$, совпадает с автоморфизмом Фробениуса. Следовательно, $\varphi_{\mathfrak{p}_n}(\theta') \equiv (\theta')^u \pmod{\mathfrak{p}_n}$, где $u = |\mathcal{O}_{K_n}/\mathfrak{p}_n|$. Тогда

$$(\pi, \theta)_{p,n} = \varphi_{\mathfrak{p}_n}(\theta')/\theta' \equiv (\theta')^{u-1} \equiv \theta^{(u-1)/\ell^m} \equiv \zeta_n \pmod{\mathfrak{p}_n}.$$

Таким образом, $(\pi, \theta)_{p,n} = \zeta_n$ и $(\pi, \varepsilon_n) = \zeta_n^{c_1}$, где c_1 определен в (3.3) (для $\sigma = 1$). Если σ – произвольный элемент группы G_n , то, рассуждая, как и выше, и полагая $\rho = \sigma^{-1}$, мы получаем

$$(\rho(\pi), \varepsilon_n)_{p,n} = (\pi, \sigma(\varepsilon_n)^{\varkappa(\rho)})_{p,n} = (\pi, \theta^{c_\rho})_{p,n}^{\varkappa(\rho)} = (\pi, \theta)^{\varkappa(\rho)c_\rho}_{p,n} = \zeta_n^{\varkappa(\rho)c_\rho}.$$

Тогда из (3.7) следует

$$\langle \pi, \varepsilon_n \rangle_{p,n} = \sum_{\sigma \in G_n} \varkappa(\sigma^{-1})_{c_{\sigma^{-1}}\sigma} = w(\mathbf{c}) \in \mathfrak{R}_n. \quad (3.14)$$

Согласно теореме Штикельбергера мы имеем $(S(\chi)) = \mathfrak{p}^{s(1, \ell^m d)}$. Таким образом, главный дивизор $(S(\chi)_2)$ определяется формулой

$$(S(\chi)_2) = \mathfrak{p}^{(\gamma - i_0)\delta e^- s(1, \ell^m d)},$$

где $\delta = 1$ при $\ell \neq 2$ и $\delta = 2$ при $\ell = 2$. Учитывая, что $\langle S(\chi)_2, \varepsilon_n \rangle_{p,n}$ зависит только от главного дивизора $(S(\chi)_2)$, и применяя (3.8), мы получаем

$$\langle S(\chi)_2, \varepsilon_n \rangle_{p,n} = ((\gamma - i_0)\delta e^- s(1, \ell^m d)) \langle \pi, \varepsilon_n \rangle_{p,n} = ((\gamma - i_0)\delta e^- s(1, \ell^m d)) w(\mathbf{c}). \quad (3.15)$$

Заметим, что $\varepsilon'_n = \varepsilon_n^{\gamma^{-1}}$ по определению. Поскольку $w(\gamma - 1) = i_0\gamma^{-1} - 1$, из (3.15) мы получаем

$$\langle S(\chi)_2, \varepsilon'_n \rangle_{p,n} = ((\gamma - i_0)\delta e^- s(1, \ell^m d))(i_0\gamma^{-1} - 1)w(\mathbf{c}). \quad (3.16)$$

Подставляя соотношения (3.13) и (3.16) в (3.11), мы получаем

$$(\gamma - i_0)((i_0\gamma^{-1} - 1)e^- s(1, \ell^m d))\mathbf{a} = ((\gamma - i_0)\delta e^- s(1, \ell^m d))(i_0\gamma^{-1} - 1)w(\mathbf{c}). \quad (3.17)$$

Поскольку

$$(i_0\gamma^{-1} - 1)e^- s(1, \ell^m d) = \gamma^{-1}(i_0 - \gamma)e^- s(1, \ell^m d),$$

из (3.17) получаем

$$(\gamma - i_0)((i_0\gamma^{-1} - 1)e^- s(1, \ell^m d))(\mathbf{a} + \delta w(\mathbf{c})) = 0. \quad (3.18)$$

Предложение доказано.

Таким образом, теорема 3.2 доказана с точностью до умножения на элемент

$$(\gamma - i_0)(i_0\gamma^{-1} - 1)e^- s(1, \ell^m d).$$

ПРЕДЛОЖЕНИЕ 3.4. Пусть $w(\mathbf{c}) = w(\mathbf{c}(\varepsilon_n))$ имеет тот же смысл, что и в теореме 3.2. Тогда $2w(\mathbf{c}) \sim (1 - j)w(\mathbf{c})$, где j – автоморфизм комплексного сопряжения.

ДОКАЗАТЕЛЬСТВО. Пусть $\varepsilon_n(\alpha) = 1 - \alpha\zeta_n$, где $\alpha \in \mu_d$. Тогда $j(\varepsilon_n(\alpha)) = 1 - \alpha^{-1}\zeta_n^{-1}$. Следовательно, $\mathbf{c}(j(\varepsilon_n(\alpha))) = \mathbf{c}(-1) + \mathbf{c}(\alpha^{-1}) + \mathbf{c}(\zeta_n^{-1}) + \mathbf{c}(\varepsilon_n(\alpha))$. Поскольку $\alpha \in \mu_d$, мы имеем $\mathbf{c}(\alpha^{-1}) = 0$, $\mathbf{c}(-1) = 0$ при $\ell \neq 2$ и $\mathbf{c}(-1) = \ell^{m-1} \sum_{\sigma \in G_n} \sigma$ при $\ell = 2$. Если $\zeta_n^{-1} \equiv \theta^h \pmod{\mathfrak{p}_n}$, где θ имеет тот же смысл,

что и в (3.3), то $\sigma^{-1}(\zeta_n^{-1}) = \zeta_n^{-\varkappa(\sigma^{-1})} = \theta^{h\varkappa(\sigma^{-1})}$, т. е. $\mathbf{c}(\zeta_n^{-1}) = \sum_{\sigma \in G_n} h_\sigma \sigma$, где $h_\sigma = h\varkappa(\sigma^{-1}) \pmod{\ell^m}$. Таким образом, мы получаем

$$w(\mathbf{c}(\zeta^{-1})) = \sum_{\sigma \in G_n} h_\sigma \varkappa(\sigma) \sigma^{-1} = h \sum_{\sigma \in G_n} \sigma.$$

Следовательно,

$$\mathbf{c}(j(\varepsilon_n(\alpha))) \sim \mathbf{c}(\varepsilon_n(\alpha)).$$

С другой стороны, $\mathbf{c}(j(\varepsilon_n(\alpha))) = j(\mathbf{c}(\varepsilon_n(\alpha)))$, т. е.

$$2(\mathbf{c}(\varepsilon_n(\alpha))) \sim (1+j)\mathbf{c}(\varepsilon_n(\alpha)), \quad 2w(\mathbf{c}(\varepsilon_n(\alpha))) \sim (1-j)w(\mathbf{c}(\varepsilon_n(\alpha))). \quad (3.19)$$

Согласно предложению 2.11 элемент ε_n является произведением элементов вида $\varepsilon_n(\alpha)$ и элементов, сопряженных с ними. Таким образом, из (3.19) следует $2w(\mathbf{c}) \sim (1-j)w(\mathbf{c})$. Предложение доказано.

§ 4. Продолжение доказательства теоремы 3.2

Мы хотим показать, что теорема 3.2 следует из предложения 3.3. Для этого нам необходимы следующие рассмотрения. Пусть X – группа Галуа максимального абелева ℓ -расширения поля K_n , не разветвленного вне ℓ . Пусть $\mathfrak{A}$ – дивизор поля K_n , взаимно простой с ℓ . Тогда согласно глобальной теории полей классов существует однозначно определенный элемент $\vartheta(\mathfrak{A}) \in X$, называемый *символом Артина*, такой, что для любого простого дивизора $\mathfrak{q}$ поля K_n элемент $\vartheta(\mathfrak{q})$ совпадает с автоморфизмом Фробениуса, соответствующим $\mathfrak{q}$, и для любых $\mathfrak{A}_1, \mathfrak{A}_2$, взаимно простых с ℓ , выполняется равенство $\vartheta(\mathfrak{A}_1 \mathfrak{A}_2) = \vartheta(\mathfrak{A}_1) \vartheta(\mathfrak{A}_2)$. Пусть W – подгруппа группы X , порожденная подгруппами инерции всех точек, лежащих над ℓ . Тогда $X/W \cong \text{Cl}(K_n)_\ell$, где $\text{Cl}(K_n)_\ell$ – ℓ -компонента группы классов поля K_n . В частности, W имеет конечный индекс в X . Согласно глобальной теории полей классов группа W естественно изоморфна группе $(\prod_{v|\ell} U(K_{n,v})[\ell])/U(K_n)[\ell]$, где $U(K_n)$ (соответственно, $U(K_{n,v})$) – группа единиц поля K_n (соответственно, локального поля $K_{n,v}$) и $[\ell]$ означает про- ℓ -пополнение. Группа W конечно порождена над $\mathbb{Z}_\ell$, поэтому согласно теореме плотности Чеботарёва любой элемент из X можно приблизить по модулю W^{ℓ^t} для любого заданного t элементом вида $\vartheta(\mathfrak{q})$, где $\mathfrak{q}$ – некоторый простой дивизор поля K_n , взаимно простой с ℓd и вполне распадающийся в расширении $K_n/\mathbb{Q}$. В частности, мы можем выбрать $\mathfrak{q}$ таким, чтобы выполнялось сравнение

$$\vartheta(\mathfrak{q}) \equiv \vartheta(\mathfrak{p}_n)^{1-j} \pmod{W^{\ell^t}}.$$

Таким образом, дивизор

$$\mathfrak{B} = \mathfrak{q}^{-1} \mathfrak{p}_n^{1-j} \quad (4.1)$$

является главным, т. е. $\mathfrak{B} = (\tilde{b})$ для некоторого $\tilde{b} \in K_n^\times$, где $\tilde{b}$, рассматриваемый как элемент группы $\prod_{v|\ell} U(K_{n,v})[\ell]$, имеет вид

$$\tilde{b} = u u_1^{\ell^t}, \quad u \in U(K_n), \quad u_1 \in \prod_{v|\ell} U(K_{n,v})[\ell].$$

Полагая $b = \tilde{b}u^{-1}$, мы можем считать, что

$$\mathfrak{B} = (b), \quad b \in \left(\prod_{v|\ell} U(K_{n,v})[\ell] \right)^{\ell^t}. \quad (4.2)$$

Имеется естественная проекция $\pi: X \rightarrow \Gamma_n = G(K_\infty/K_n)$. Поскольку j действует тривиально на группе Γ_n , мы получаем, что $\pi(\vartheta(\mathfrak{p}_n^{1-j})) = 1$. Тогда из (4.1) и (4.2) следует, что $\pi(\vartheta(\mathfrak{q})) \in \Gamma_{n+t}$. Таким образом, $\mathfrak{q}$ вполне распадается в K_{n+t}/K_n .

Пусть ω_1 – характер Тейхмюллера поля $\mathcal{O}(K_n)/\mathfrak{q}$. Положим $q = N(\mathfrak{q}) = |\mathcal{O}(K_n)/\mathfrak{q}|$. Таким образом, в отличие от обозначений из введения, здесь q – простое число, лежащее под $\mathfrak{q}$. Тогда $q - 1 \equiv 0 \pmod{\ell^m d}$ и $\chi_1 := \omega_1^{(q-1)/(\ell^m d)}$ является характером группы $(\mathcal{O}(K_n)/\mathfrak{q})^\times$ порядка $\ell^m d$.

Рассмотрим гауссову сумму $S(\chi_1)$, соответствующую характеру χ_1 и определенной, как в (1.1). Тогда $S(\chi_1) \in K_n(\xi_q)$ и $S(\chi_1)^{\ell^m d} \in K_n$, где ξ_q – первообразный корень из единицы степени q . Поскольку расширение $K_n(S(\chi_1))/K_n$ не разветвлено во всех точках v , лежащих над ℓ , мы получаем $S(\chi_1) \in V(K_n)$. Напомним, что согласно определению групп $V(K_{n,v})$ и $V(K_{n,v})^0$, данному во введении, мы имеем $V(K_{n,v})/V(K_{n,v})^0 \cong \mathbb{Z}_\ell$, т. е. $V(K_n)/V(K_n)^0 \cong \mathbb{Z}_\ell^f$, где f – число точек поля K_n , лежащих над ℓ .

Таким образом, если элементы $\varrho_1, \dots, \varrho_f \in V(K_n)$ таковы, что их образы составляют базис группы $V(K_n)/V(K_n)^0$, то любой $x \in V(K_n)$ может быть записан в виде

$$x = \sum_{i=1}^f \alpha_i \varrho_i + \sum_{\sigma \in G_n} \beta_\sigma \sigma(\eta(K_n)), \quad \alpha_i, \beta_\sigma \in \mathbb{Z}_\ell, \quad (4.3)$$

причем в этом разложении коэффициенты $\alpha_1, \dots, \alpha_f$ определены однозначно, а коэффициенты β_σ , $\sigma \in G_n$, определены с точностью до функции, постоянной на каждом классе смежности по подгруппе разложения G_ℓ простого ℓ .

ПРЕДЛОЖЕНИЕ 4.1. Пусть

$$S(\chi_1) = \sum_{i=1}^f \alpha_i \varrho_i + \sum_{\sigma \in G_n} \beta_\sigma \sigma(\eta(K_n)), \quad \alpha_i, \beta_\sigma \in \mathbb{Z}_\ell,$$

– разложение вида (4.3) для элемента $S(\chi_1) \in V(K_n)$. Пусть t имеет тот же смысл, что и в формуле (4.2). Тогда

$$\alpha_i \equiv 0 \pmod{\ell^{t-m-1}}, \quad \beta_\sigma \equiv \frac{2}{\delta} a_\sigma + f(\sigma) \pmod{\ell^{t-m-1}} \quad (4.4)$$

для всех i и всех $\sigma \in G_n$, где a_σ – коэффициенты разложения (1.4), $\delta = 1$ при $\ell \neq 2$, $\delta = 2$ при $\ell = 2$ и $f(\sigma)$ – произвольная функция со значениями в $\mathbb{Z}_\ell$, постоянная на классах смежности по G_ℓ . В частности, при $t \geq 2m+1$ сравнения (4.4) выполняются по модулю ℓ^m .

ДОКАЗАТЕЛЬСТВО. Положим $b_1 = b^{s(1, \ell^m d) \ell^m d} \in K_n$ и $b_2 = \sqrt[\ell^m]{b_1}$. Вычисляя главный дивизор элемента b_2 с помощью (4.1), мы получаем

$$(b_2) = \mathfrak{q}^{-s(1, \ell^m d)} \mathfrak{p}_n^{(1-j)s(1, \ell^m d)}.$$

По теореме Штикельбергера такой же дивизор имеет и элемент $S(\chi_1)^{-1} S(\chi)^{1-j}$. Следовательно, для некоторой единицы u такой, что $u^{\ell^m} \in K_n$, выполняется равенство

$$b_2 = S(\chi_1)^{-1} S(\chi)^{1-j} u. \quad (4.5)$$

Из соотношения (4.2) следует, что $b_1 \in (\prod_{v|\ell} U(K_{n,v})[\ell])^{\ell^t}$ и, следовательно, $b_2 \in V(K_n)^{\ell^{t-m}}$. Применим $1+j$ к обеим частям (4.5). Учитывая, что $S(\chi_1)^{1+j} = q \equiv 1 \pmod{\ell^{m+t}}$, мы получаем $q = q_1^{\ell^t}$ для некоторого $q_1 \in \mathbb{Z}_\ell$. Далее, в $V(K_n)$ выполняется равенство $j(u) = u$, т.е. $u^{1+j} = u^2$ и $u \in V(K_n)^{\ell^{t-m-1}}$. Тогда из (4.5) следует, что $S(\chi_1)^{-1} S(\chi)^{1-j} \in V(K_n)^{\ell^{t-m-1}}$. Это означает, что в разложении вида (4.3) для элемента $S(\chi_1)^{-1} S(\chi)^{1-j}$ все коэффициенты сравнимы с 0 по модулю ℓ^{t-m-1} . Учитывая, что $\frac{2}{\delta} a_\sigma$ — коэффициенты разложения (1.4) для элемента $S(\chi)^{1-j}$, мы получаем (4.4). Предложение доказано.

ПРЕДЛОЖЕНИЕ 4.2. Пусть $\mathbf{c} \in \mathfrak{R}_n$ — элемент, определенный в (3.4) для кругового числа ε_n и простого дивизора $\mathfrak{p}_n$, а $\mathbf{c}(\mathfrak{q})$ — аналогичным образом определенный элемент кольца $\mathfrak{R}_n$ для кругового числа ε_n и простого дивизора $\mathfrak{q}$. Тогда в $\mathfrak{R}_n$ выполняется равенство

$$\mathbf{c}(\mathfrak{q}) = (1+j)\mathbf{c}, \quad \text{т.е.} \quad w(\mathbf{c}(\mathfrak{q})) = (1-j)w(\mathbf{c}).$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим в группе идеалей $J(K_n)$ поля K_n главные идеалы ε_n и b , где b имеет тот же смысл, что и в (4.2). Для конечной точки v поля K_n пусть $(b, \varepsilon_n)_{n,v}$ — локальный символ норменного вычета со значением в μ_{ℓ^m} на элементах $b, \varepsilon_n \in K_{n,v}$. Согласно закону взаимности имеем

$$\prod_v (b, \varepsilon_n)_{n,v} = 1, \quad (4.6)$$

где v пробегает все неархимедовы точки поля K_n .

Из (4.2) следует, что $(b, \varepsilon_n)_{n,v} = 1$ для любой точки $v|\ell$, если только $t > m$. Если $v \nmid \ell$, то ε_n является единицей в v , т.е. символ $(b, \varepsilon_n)_{n,v}$ может быть отличен от 1 только в точках $\mathfrak{q}$, $\mathfrak{p}_n$ и $j(\mathfrak{p}_n)$. Таким образом, мы получаем из (4.6), что $(b^{-1}, \varepsilon_n)_{n,\mathfrak{q}} = (b, \varepsilon_n)_{n,\mathfrak{p}_n} (b, \varepsilon_n)_{n,j(\mathfrak{p}_n)}$.

Если в (4.6) элемент ε_n заменить на $\sigma(\varepsilon_n)$ для некоторого $\sigma \in G_n$, то, используя те же рассуждения, что и выше, мы получим

$$(b^{-1}, \sigma(\varepsilon_n))_{n,\mathfrak{q}} = (b, \sigma(\varepsilon_n))_{n,\mathfrak{p}_n} (b, \sigma(\varepsilon_n))_{j(\mathfrak{p}_n)}.$$

Учитывая, что $(b) = \mathfrak{q}^{-1} \mathfrak{p}_n j(\mathfrak{p}_n)^{-1}$, и повторяя рассуждения из доказательства предложения 3.3, мы получаем, что $(b^{-1}, \sigma(\varepsilon_n))_{n,\mathfrak{q}} = \zeta_n^{c_\sigma(\mathfrak{q})}$, где $c_\sigma(\mathfrak{q})$ — коэффициент при σ в элементе $\mathbf{c}(\mathfrak{q})$, и $(b, \sigma(\varepsilon_n))_{n,\mathfrak{p}_n} = (\pi, \sigma(\varepsilon_n))_{n,\mathfrak{p}_n} = \zeta_n^{c_\sigma}$, где π — идеаль, компонента которого в точке $\mathfrak{p}_n$ является униформизирующим элементом

поля K_{n,p_n} , а все остальные компоненты равны 1. Наконец, учитывая, что $\varkappa(j) = -1$, мы получаем

$$(b, \sigma(\varepsilon_n))_{n,j(p_n)} = (j(\pi^{-1}), \sigma(\varepsilon_n))_{n,j(p_n)} = (\pi^{-1}, j\sigma(\varepsilon_n))_{p_n}^{-1} = \zeta_n^{c_{j\sigma}}.$$

Таким образом, $c_\sigma(\mathbf{q}) \equiv c_\sigma + c_{j\sigma} \pmod{\ell^m}$, т. е. $\mathbf{c}(\mathbf{q}) = \mathbf{c} + j\mathbf{c}$. Предложение доказано.

Напомним, что простой дивизор $\mathbf{q}$ из (4.1) вполне распадается в расширении K_{n+t}/K_n . Пусть Ω – простой делитель $\mathbf{q}$ в поле K_{n+t} и $\omega_2: (\mathcal{O}(K_{n+t})/\Omega)^\times \rightarrow K_{n+t}(\xi_s)$ – характер Тейхмюллера, соответствующий Ω , где s – порядок группы $(\mathcal{O}(K_{n+t})/\Omega)^\times$. Тогда $s \equiv 0 \pmod{\ell^{m+t}d}$ и $\chi_2 := \omega_2^{s/(\ell^{m+t}d)}$ – характер порядка $\ell^{m+t}d$ мультипликативной группы конечного поля $\mathcal{O}(K_{n+t})/\Omega$.

ПРЕДЛОЖЕНИЕ 4.3. Пусть $S(\chi_2)$ – гауссова сумма, соответствующая характеру χ_2 , так что $S(\chi_2)^{\ell^{m+t}d} \in K_{n+t}$. Положим $S(\chi_2)_1 := S(\chi_2)^{1-j} \in V(K_{n+t})^0$. Пусть (в аддитивной записи)

$$S(\chi_2)_1 = \sum_{\sigma \in G_{n+t}} x_\sigma \sigma(\eta(K_{n+t})) = \mathbf{x} \cdot \eta(K_{n+t}), \quad x_\sigma \in \mathbb{Z}_\ell, \quad \mathbf{x} \in \mathbb{Z}_\ell[G_{n+t}], \quad (4.7)$$

и пусть $S(\chi_1)_1 = S(\chi_1)^{1-j}$ и (в аддитивной записи)

$$S(\chi_1)_1 = \sum_{\sigma \in G_n} y_\sigma \sigma(\eta(K_n)) = \mathbf{y} \cdot \eta(K_n), \quad y_\sigma \in \mathbb{Z}_\ell, \quad \mathbf{y} \in \mathbb{Z}_\ell[G_n].$$

Кроме того, пусть $\pi: \mathbb{Z}_\ell[G_{n+t}] \rightarrow \mathbb{Z}_\ell[G_n]$ – проекция групповых колец, индуцированная естественным эпиморфизмом $G_{n+t} \rightarrow G_n$. Тогда $\pi(\mathbf{x}) \sim \mathbf{y}$.

ДОКАЗАТЕЛЬСТВО. Согласно теореме Штикельбергера имеется равенство дивизоров

$$(S(\chi_2)_1) = \Omega^{(1-j)s(1, \ell^{m+t}d)}, \quad (S(\chi_1)_1) = \mathbf{q}^{(1-j)s(1, \ell^m d)}.$$

Как хорошо известно (см. [5]), $\pi((1-j)s(1, \ell^{m+t}d)) = (1-j)s(1, \ell^m d)$. Это означает, что имеет место равенство дивизоров

$$N_{K_{n+t}/K_n}((S(\chi_2)_1)) = \mathbf{q}^{\pi((1-j)s(1, \ell^{m+t}d))} = \mathbf{q}^{(1-j)s(1, \ell^m d)} = (S(\chi_1)_1),$$

где N_{K_{n+t}/K_n} – отображение нормы. Следовательно, $N_{K_{n+t}/K_n}(S(\chi_2)_1)$ отличается от $S(\chi_1)_1$ умножением на некоторую единицу u , но, поскольку оба эти элемента аннулируются умножением на $1+j$, единица u должна быть корнем из единицы, т. е. в группе $V(K_n)$ выполняется равенство

$$N_{K_{n+t}/K_n}(S(\chi_2)_1) = S(\chi_1)_1. \quad (4.8)$$

Пусть теперь, как и в (4.7), $S(\chi_2)_1 = \mathbf{x}(\eta(K_{n+t}))$. Тогда, учитывая, что $N_{K_{n+t}/K_n}(\eta(K_{n+t})) = \eta(K_n)$ и $\mathbf{x}(\eta(K_n)) = \pi(\mathbf{x})(\eta(K_n))$, мы получаем из равенства (4.8), что $S(\chi_1)_1 = \mathbf{x}(\eta(K_n)) = \pi(\mathbf{x})(\eta(K_n))$, т. е.

$$(\pi(\mathbf{x}) - \mathbf{y})(\eta(K_n)) = 0, \quad \pi(\mathbf{x}) \sim \mathbf{y}.$$

Предложение доказано.

Теперь мы определим, как и в (3.4), для простого дивизора $\mathfrak{Q}$ поля K_{n+t} и кругового числа ε_{n+t} этого поля элемент $\mathbf{c}(\mathfrak{q}) \in \mathfrak{R}_{n+t}$. Именно, пусть $\vartheta \in \mathcal{O}_{K_{n+t}}$ такой элемент, что $\bar{\vartheta} := \vartheta \pmod{\mathfrak{Q}}$ – первообразный корень из единицы в $\mathcal{O}_{K_{n+t}}/\mathfrak{Q}$ степени $q-1$, где $q = |\mathcal{O}_{K_{n+t}}/\mathfrak{Q}|$, причем мы предполагаем, что $\vartheta^{(q-1)/\ell^{m+t}} \equiv \zeta_{n+t} \pmod{\mathfrak{Q}}$. Для $\sigma \in G(K_{n+t}/\mathbb{Q})$ пусть $\tilde{c}_\sigma \in \mathbb{Z}/\ell^{m+t}\mathbb{Z}$ и $\mathbf{c}(\mathfrak{Q}) \in \mathfrak{R}_{n+t}$ определены условиями

$$\sigma^{-1}(\varepsilon_{n+t}) \equiv \vartheta^{u_\sigma} \pmod{\mathfrak{Q}}, \quad \tilde{c}_\sigma = u_\sigma \pmod{\ell^{m+t}}, \quad \mathbf{c}(\mathfrak{Q}) = \sum_{\sigma \in G_{n+t}} \tilde{c}_\sigma \sigma.$$

ПРЕДЛОЖЕНИЕ 4.4. Пусть $\pi_1: \mathfrak{R}_{n+t} \rightarrow \mathfrak{R}_n$ – естественная проекция групповых колец, и пусть $\mathbf{c}(\mathfrak{q})$ имеет тот же смысл, что и в предложении 4.2. Тогда

$$\pi_1(\mathbf{c}(\mathfrak{Q})) = \mathbf{c}(\mathfrak{q}), \quad \pi_1(w(\mathbf{c}(\mathfrak{Q}))) = w(\mathbf{c}(\mathfrak{q})).$$

ДОКАЗАТЕЛЬСТВО. Пусть λ – идеаль, у которого на $\mathfrak{Q}$ -м месте стоит униформизирующий элемент поля K_{n+t} , а все остальные компоненты равны 1. Тогда, рассуждая, как и в доказательстве предложения 3.3 (см. (3.14)), мы получаем

$$\langle \lambda, \varepsilon_{n+t} \rangle_{q, n+t} = w(\mathbf{c}(\mathfrak{Q})), \quad (4.9)$$

где c_σ определяется условием $(\sigma^{-1}(\lambda), \varepsilon_{n+t})_{q, n+t} = \zeta_{n+t}^{c_\sigma}$ и $(\ , \)_{q, n+t}$ – полулокальный символ норменного вычета по всем точкам над q со значением в $\mu_{\ell^{m+t}}$. Если обозначить $c_\sigma \pmod{\ell^m}$ через $\bar{c}_\sigma$, то

$$\pi_1\left(\sum_{\sigma \in G_{n+t}} c_\sigma \sigma\right) = \sum_{\bar{\sigma} \in G_n} \left(\sum_{\sigma \rightarrow \bar{\sigma}} \bar{c}_\sigma\right) \bar{\sigma},$$

где $\bar{\sigma}$ пробегает все элементы группы G_n и внутренняя сумма берется по всем $\sigma \in G_{n+t}$, которые при естественной проекции $G_{n+t} \rightarrow G_n$ переходят в данный элемент $\bar{\sigma} \in G_n$. Заметим, что $\bar{c}_\sigma$ определяется условием $[\sigma^{-1}(\lambda), \varepsilon_{n+t}]_{q, n} = \bar{c}_\sigma$, где $[\ , \]_{q, n}$ – полулокальный символ норменного вычета на группе идеалей $J(K_{n+t})$ поля K_{n+t} со значениями в μ_{ℓ^m} . Следовательно, элемент $\alpha(\bar{\sigma}) := \sum_{\sigma \rightarrow \bar{\sigma}} \bar{c}_\sigma$ определяется из условия $\alpha(\bar{\sigma}) = [\bar{\sigma}^{-1}N_{K_{n+t}/K_n}(\lambda), \varepsilon_{n+t}]_{q, n}$. Заметим, что $\lambda_1 := N_{K_{n+t}/K_n}(\lambda)$ является элементом группы идеалей $J(K_n)$ поля K_n , у которого на месте $\mathfrak{q}$ стоит униформизирующий элемент поля $K_{n, \mathfrak{q}}$, а все остальные компоненты равны 1. Следовательно,

$$\alpha(\bar{\sigma}) = [\bar{\sigma}^{-1}(\lambda_1), \varepsilon_{n+t}]_{q, n} = (\bar{\sigma}^{-1}(\lambda_1), \varepsilon_n)_{q, n},$$

где $(\ , \)_{q, n}$ – полулокальный символ норменного вычета на группе идеалей $J(K_n)$ со значением в μ_{ℓ^m} . Таким образом, снова применяя (3.14), мы получаем, что $\alpha(\bar{\sigma})$ совпадает с коэффициентом при $\bar{\sigma}$ элемента $w(\mathbf{c}(\mathfrak{q}))$, т.е. $\pi_1(w(\mathbf{c}(\mathfrak{Q}))) = w(\mathbf{c}(\mathfrak{q}))$. Поскольку автоморфизм w коммутирует с π_1 , отсюда следует, что $\pi_1(\mathbf{c}(\mathfrak{Q})) = \mathbf{c}(\mathfrak{q})$. Предложение доказано.

ПРЕДЛОЖЕНИЕ 4.5. Пусть $\mathbf{a}_2 = \mathbf{a}_2(S(\chi_2)_1) \in \mathfrak{R}_{n+t}$ – элемент, который соответствует гауссовой сумме $S(\chi_2)$ так же, как $\mathbf{a}$ из теоремы 3.2 соответствует гауссовой сумме $S(\chi_0)$. Пусть $t > 2m$. Тогда $\pi_1(\mathbf{a}_2) \sim 2\mathbf{a}$, где π_1 – проекция из предложения 4.4.

Для $\ell = 2$ пусть $\pi'_1: \mathfrak{R}_{n+t} \rightarrow \mathbb{Z}/\ell^{m+1}\mathbb{Z}[G_n]$ – естественная проекция групповых колец и $i: \mathfrak{R}_n \hookrightarrow \mathbb{Z}/\ell^{m+1}\mathbb{Z}[G_n]$ – вложение G_n -модулей, индуцированное умножением на 2. Тогда при $t > 2m + 1$ мы имеем $\pi'_1(\mathbf{a}_2) \sim i(\mathbf{a})$.

ДОКАЗАТЕЛЬСТВО. Положим $\mathbf{a}_1 = y \bmod \ell^m \in \mathfrak{R}_n$. Согласно предложению 4.3 мы имеем $\pi_1(\mathbf{a}_2) \sim \mathbf{a}_1$. Используя предложение 4.1 и записывая умножение аддитивно, мы получаем $S(\chi_1) = A + B$, где $A = \ell^{t-m-1} \sum_{i=1}^f \alpha'_i \varrho_i$, $\alpha_i = \ell^{t-m-1} \alpha'_i$, $B = \sum_{\sigma \in G_n} \beta_\sigma \sigma(\eta(K_n))$.

Пусть, как и в предложении 4.1, $S(\chi_1)_1 = e^{-\delta} S(\chi_1) = \mathbf{y} \cdot \eta(K_n)$. Тогда $e^{-\delta} A = S(\chi_1)_1 - e^{-\delta} B$. Согласно предложению 2.12 имеем $S(\chi_1)_1 \in V(K_n)^0$, следовательно, $e^{-\delta} A \in V(K_n)^0$, но $V(K_n)^0$ выделяется прямым слагаемым в $V(K_n)$ как $\mathbb{Z}_\ell$ -модуль, поэтому $e^{-\delta} A$ является ℓ^{t-m-1} -й степенью в $V(K_n)^0$. Пусть теперь $t - m - 1 \geq m$, т.е. $t > 2m$. Полагая $\mathbf{b}' = \sum_{\sigma \in G_n} \beta_\sigma \sigma$ и $\mathbf{b} = \mathbf{b}' \bmod \ell^m$, мы получаем $\mathbf{a}_1 \sim e^{-\delta} \mathbf{b}$. С другой стороны, согласно предложению 4.1 при $t > 2m$ мы имеем $\mathbf{b} \sim 2\mathbf{a}/\delta$. Таким образом, при $\ell \neq 2$ мы получаем $\pi_1(\mathbf{a}_2) \sim \mathbf{a}_1 \sim e^{-\delta} \mathbf{b} \sim 2e^{-\delta} \mathbf{a} \sim 2\mathbf{a}$, где условие $2e^{-\delta} \mathbf{a} \sim 2\mathbf{a}$ выполняется в силу того, что $(S(\chi)_1)^j = (S(\chi)_1)^{-1}$, т.е. $j(\mathbf{a}) = -\mathbf{a}$. Этим наше предложение доказано в случае $\ell \neq 2$.

В случае $\ell = 2$ мы могли бы, повторив все предыдущие утверждения, получить равенство $\pi_1(\mathbf{a}_1) \sim 2\mathbf{a}$, но мы хотим получить более точный результат. Для этого при $\ell = 2$ мы положим $\tilde{\mathbf{a}}_1 = y \bmod \ell^{m+1} \in \mathbb{Z}/\ell^{m+1}\mathbb{Z}[G_n]$. Снова из предложения 4.3 следует, что $\pi'_1(\mathbf{a}_2) \sim \tilde{\mathbf{a}}_1$. Пусть теперь $t > 2m + 1$. Также имеем $S(\chi_1) = A + B$ и $e^{-\delta} A = S(\chi_1)_1 - e^{-\delta} B$, где $e^{-\delta} A - \ell^{m+1}$ -я степень в $V(K_n)^0$. Таким образом, полагая $\tilde{\mathbf{b}} = \mathbf{b}' \bmod \ell^{m+1}$, мы получаем $\tilde{\mathbf{a}}_1 \sim e^{-\delta} \tilde{\mathbf{b}} = (1 - j)\tilde{\mathbf{b}}$.

Согласно предложению 4.1 имеем $\tilde{\mathbf{b}} \sim \tilde{\mathbf{a}}$, где $\tilde{\mathbf{a}}$ определяется так же, как и $\mathbf{a}$, только относительно модуля ℓ^{m+1} . Тогда, учитывая, что $j(\tilde{\mathbf{a}}) = -\tilde{\mathbf{a}}$, мы получаем $\pi'_1(\mathbf{a}_2) \sim (1 - j)\tilde{\mathbf{b}} \sim (1 - j)\tilde{\mathbf{a}} \sim 2\tilde{\mathbf{a}}$. С другой стороны, непосредственно из определения элементов $\mathbf{a}$ и $\tilde{\mathbf{a}}$ следует, что $i(\mathbf{a}) = 2\tilde{\mathbf{a}}$. Предложение доказано полностью.

ПРЕДЛОЖЕНИЕ 4.6. Пусть $\mathbf{c}$ и $\mathbf{c}(\mathfrak{Q})$ имеют тот же смысл, что и в теореме 3.2 и предложении 4.5 соответственно. Пусть π_1, π'_1 и i имеют тот же смысл, что и в предложении 4.5. Тогда для любого $t > 0$ мы имеем $\pi_1(w(\mathbf{c}(\mathfrak{Q}))) \sim 2w(\mathbf{c})$ при $\ell \neq 2$ и $\pi'_1(2w(\mathbf{c}(\mathfrak{Q}))) \sim i(2w(\mathbf{c}))$ при $\ell = 2$.

ДОКАЗАТЕЛЬСТВО. Согласно предложению 3.4 имеем $jw(\mathbf{c}) \sim w(\mathbf{c})$, поэтому из предложений 4.2, 4.4 следует, что $\pi_1(w(\mathbf{c}(\mathfrak{Q}))) \sim w(\mathbf{c}(\mathfrak{q})) = (1 - j)w(\mathbf{c}) \sim 2w(\mathbf{c})$, это доказывает наше предложение при $\ell \neq 2$.

Пусть теперь $\ell = 2$. Из предложения 4.4 мы получаем $\pi'_1(2w(\mathbf{c}(\mathfrak{Q}))) = i(w(\mathbf{c}(\mathfrak{q})))$. Применяя предложения 4.2, 3.4, получаем $w(\mathbf{c}(\mathfrak{q})) \sim (1 - j)w(\mathbf{c}) \sim 2w(\mathbf{c})$, т.е. $i(w(\mathbf{c}(\mathfrak{q}))) = i(2w(\mathbf{c}))$. Предложение доказано.

§ 5. Окончание доказательства теоремы 3.2

Итак, пусть для некоторого t , точное значение которого будет указано ниже, $S(\chi_2)$, $\mathbf{a}$ и $\mathbf{c}(\mathfrak{Q})$ имеют тот же смысл, что и в § 4. Применяя предложение 3.1 к элементу $S(\chi_2)$, мы получаем

$$(\gamma - i_0)((i_0\gamma^{-1} - 1)e^{-s(1, \ell^{m+t}d)})(\mathbf{a}_2 + \delta w(\mathbf{c}(\mathfrak{Q}))) = 0. \quad (5.1)$$

Другими словами, элемент $A_{n+t} := \mathbf{a}_2 + \delta w(\mathbf{c}(\Omega))$ аннулируется умножением на элемент

$$\lambda_{n+t} := (\gamma - i_0)((i_0\gamma^{-1} - 1)e^{-s(1, \ell^{m+t})}) \in \mathfrak{R}_{n+t}. \quad (5.2)$$

Для любой пары индексов $n_2 > n_1$ пусть $\pi(n_2, n_1): \mathfrak{R}_{n_2} \rightarrow \mathfrak{R}_{n_1}$ – естественная проекция. Согласно предложениям 4.5, 4.6 при $\ell \neq 2$ и $t > 2m$ мы имеем $\pi(n+t, n)(\mathbf{a}_2) = 2\mathbf{a}$ и $\pi(n+t, n)(\mathbf{c}(\Omega)) = 2\mathbf{c}$. Таким образом, в этом случае для завершения доказательства теоремы 3.2 достаточно проверить, что при некотором достаточно большом t выполняется равенство

$$\pi(n+t, n)(A_{n+t}) = 0. \quad (5.3)$$

В случае $\ell = 2$ согласно предложениям 4.5, 4.6 достаточно проверить, что для некоторого достаточно большого t выполняется равенство

$$\pi(n+t, n+1)(A_{n+t}) = 0. \quad (5.4)$$

Действительно, отображение π'_1 из предложений 4.5, 4.6 пропускается через $\pi(n+t, n+1)$, поэтому из (5.4) мы получаем $\pi'_1(A_{n+t}) = 0$, откуда следует теорема 3.2 в случае $\ell = 2$.

Отметим, что при любом t мы имеем $j(A_{n+t}) \sim -A_{n+t}$. Действительно, условие $j(\mathbf{a}_2) \sim -\mathbf{a}_2$ следует непосредственно из определения элемента $\mathbf{a}_2$, а условие $j(\mathbf{c}(\Omega)) \sim -\mathbf{c}(\Omega)$ доказано в предложении 3.4.

Итак, для завершения доказательства теоремы 3.2 достаточно проверить, что для любого заданного n найдется индекс t такой, что для любого $x \in \mathfrak{R}_n$, удовлетворяющего условиям $j(x) \sim -x$ и $\lambda_{n+t} \cdot x = 0$, где λ_{n+t} определен в (5.2), мы имеем $\pi(n+t, n+1)(x) = 0$.

Для доказательства последнего утверждения нам потребуются некоторые результаты о периодических Γ -модулях и элементах Штикельбергера. Пусть

$$R_\infty = \varprojlim \mathfrak{R}_n,$$

где предел берется относительно отображений $\pi(n_2, n_1)$ для $n_2 > n_1$. Тогда R_∞ – пополненное групповое кольцо группы $G_\infty = G(K_\infty/\mathbb{Q})$, которое уже встречалось в §2. Напомним, что $R_\infty \cong \Lambda[G_0]$, где $G_0 = G(K_0/\mathbb{Q})$, $K_0 = \mathbb{Q}(\zeta_0, \mu_d)$ и $\Lambda \cong \mathbb{Z}_\ell[[T]]$. При последнем изоморфизме выделенная топологическая образующая $\gamma \in \Gamma$ переходит в $1 + T$.

Элементы λ_n согласованы относительно отображений $\pi(n_2, n_1)$ и в пределе определяют элемент $\lambda_\infty \in R_\infty$.

ПРЕДЛОЖЕНИЕ 5.1. Пусть $R_\infty^- = \{x \in R_\infty \mid j(x) = -x\}$. Тогда $\lambda_\infty \in R_\infty^-$ и $C := R_\infty^-/\lambda_\infty R_\infty^-$ является периодическим Λ -модулем.

ДОКАЗАТЕЛЬСТВО. Из (5.2) следует, что $j(\lambda_n) = -\lambda_n$ при любом n , поэтому $\lambda_\infty \in R_\infty^-$. Для того чтобы доказать периодичность C , достаточно доказать, что для любого неприводимого нечетного характера θ группы G_0 , который можно интерпретировать как гомоморфизм $\theta: R_\infty \rightarrow R_{\infty, \theta} \cong \mathcal{O}_\theta[[T]]$, где $\mathcal{O}_\theta = \mathbb{Z}_\ell[\theta]$, выполняется условие $\lambda_{\infty, \theta} := \theta(\lambda_\infty) \neq 0$. Если θ имеет кондуктор d или $d\ell$, то из определения рядов Ивасава следует, что

$$\lambda_{\infty, \theta} = 2(\gamma - i_0)(i_0\gamma^{-1} - 1)f_\theta(T),$$

где $f_\theta(T)$ – ряд Ивасава, соответствующий нечетному характеру θ (или четному характеру $\bar{\theta}\omega$, где ω – характер Тейхмюллера по модулю ℓ). Поскольку $f_\theta(T) \neq 0$, мы получаем $\lambda_{\infty, \theta} \neq 0$ в этом случае.

Пусть теперь θ – примитивный характер кондуктора d_0 или $d_0\ell$, где d_0 – собственный делитель d . Следующий результат не является новым, но автор не может указать подходящую ссылку.

ЛЕММА 5.2. Пусть $F_{-1} = \mathbb{Q}(\mu_{d_0})$, $F_n = F_{-1}(\zeta_n)$ и $F_\infty = \bigcup_{n=1}^\infty F_n$. Пусть $G_\infty^0 = G(F_\infty/\mathbb{Q})$, $R_\infty^0 = \mathbb{Z}_\ell[[G_\infty^0]]$ и $g: R_\infty \rightarrow R_\infty^0$ – естественная проекция. Пусть элементы $s(1, \ell^\infty d) \in R_\infty$ и $s(1, \ell^\infty d_0) \in R_\infty^0$ определены, как в формуле (2.10). Тогда

$$g(s(1, \ell^\infty d)) = s(1, \ell^\infty d_0) \prod_p (1 - \varphi(p)),$$

где произведение берется по всем простым p таким, что $p|d$ и $p \nmid d_0$, а $\varphi(p)$ – автоморфизм Фробениуса в группе G_∞^0 , соответствующий простому p .

ДОКАЗАТЕЛЬСТВО. Для натурального n пусть $G_n = G(K_n/\mathbb{Q})$, $R_n = \mathbb{Z}_\ell[G_n]$, $G_n^0 = G(F_n/\mathbb{Q})$ и $R_n^0 = \mathbb{Z}_\ell[G_n^0]$. Пусть $g_n: R_n \rightarrow R_n^0$ – естественная проекция. Пусть элементы $e^-s(1, \ell^m d)$ и $e^-s(1, \ell^m d_0)$ определены, как в (2.14). Тогда для доказательства леммы достаточно проверить, что при любом n справедливо равенство

$$g_n(e^-s(1, \ell^m d)) = e^-s(1, \ell^m d_0) \prod_p (1 - \varphi_n(p)), \quad (5.5)$$

где p снова пробегает все простые делители d , не делящие d_0 , и $\varphi_n(p)$ – автоморфизм Фробениуса в группе G_n^0 , соответствующий простому p .

Для доказательства (5.5) достаточно проверить, что любой характер группы G_n^0 принимает одинаковые значения на левой и правой частях данной формулы, но это немедленно следует из [5, лемма 2.1]. Лемма доказана.

Итак, если θ – примитивный нечетный характер кондуктора d_0 или $d_0\ell$, то

$$\theta(s(1, \ell^\infty d)) = \theta(s(1, \ell^\infty d_0)) \prod_p (1 - \theta(\varphi(p))).$$

Мы имеем по определению $\theta(s(1, \ell^\infty d_0)) = 2f_\theta(T) \neq 0$, где $f_\theta(T)$ – ряд Ивасава, соответствующий θ . Далее, $\varphi(p) = \varphi'(p) \times \varphi''(p)$, где $\varphi'(p) \in G(F_\infty/\mathbb{Q}_\infty) \cong G(F_0/\mathbb{Q})$ и $\varphi''(p) \in G(F_\infty/F_0)$. Тогда $\theta(\varphi(p)) = \varphi''(p)\theta(\varphi'(p))$, но $\varphi''(p) \neq 1$, поэтому ни один из множителей $1 - \theta(\varphi(p))$ не равен нулю. Следовательно, $\lambda_{\infty, \theta} \neq 0$ для любого θ . Предложение доказано.

Теперь мы покажем, как завершить доказательство теоремы 3.2 в случае $\ell \neq 2$. В этом случае мы имеем $A_{n+t} = A_{n+t}^+ \oplus A_{n+t}^-$, где $A_{n+t}^\pm = e^\pm A_{n+t}$. Условие $j(A_{n+t}) \sim -A_{n+t}$ показывает, что $A_{n+t}^+ \sim 0$, т.е. без ограничения общности мы можем считать, что $A_{n+t} = A_{n+t}^- \in \mathfrak{R}_n^- = e^- \mathfrak{R}_n$.

Положим $B_n = \lambda_n \mathfrak{R}_n^-$, $D_n = \{x \in \mathfrak{R}_n^- \mid \lambda_n x = 0\}$ и $C_n = \mathfrak{R}_n^-/B_n$. Таким образом, в силу (5.1) имеем $A_{n+t} \in D_n$. Согласно предложению 5.1 группа C является периодическим Λ -модулем. Следовательно, существуют неотрицательные целые числа λ и r такие, что $\ell^r C \cong \mathbb{Z}_\ell^\lambda$ как $\mathbb{Z}_\ell$ -модуль. Согласно теореме Ферреро–Вашингтона имеем $r = 0$ при $\ell \neq 2$, но мы не будем пользоваться этой

теоремой, поскольку доказательство проходит и без ее использования, а в случае $\ell = 2$ мы имеем $r > 0$ (фактически, $r = 1$), так как связь между элементом Штикельбергера и рядом Ивасава (для характера θ кондуктора d) выражается соотношением $s(1, \ell^\infty d)_\theta = 2f_\theta(T)$.

Итак, поскольку C_n является эпиморфным образом группы C , мы получаем, что $\ell^r C_n$ имеет не более λ образующих при любом n .

Следующее простое утверждение об абелевых группах легко доказывается с помощью индукции.

ПРЕДЛОЖЕНИЕ 5.3. Пусть $A \cong (\mathbb{Z}/\ell^s \mathbb{Z})^t$ для некоторых натуральных s и t , и пусть B – некоторая подгруппа группы A и $B \cong \bigoplus_{i=1}^t \mathbb{Z}/\ell^{s_i} \mathbb{Z}$, где $0 \leq s_i \leq s$. Тогда $A/B \cong \bigoplus_{i=1}^t \mathbb{Z}/\ell^{s-s_i} \mathbb{Z}$.

СЛЕДСТВИЕ 5.4. При любом n абелевы группы C_n, D_n изоморфны.

ДОКАЗАТЕЛЬСТВО. Достаточно применить предложение 5.3 к точным последовательностям абелевых групп

$$0 \longrightarrow D_n \longrightarrow \mathfrak{R}_n^- \xrightarrow{\lambda_n} B_n \longrightarrow 0,$$

$$0 \longrightarrow B_n \longrightarrow \mathfrak{R}_n^- \longrightarrow C_n \longrightarrow 0.$$

Следствие доказано.

Таким образом, следствие 5.4 показывает, что при любом n группа $\ell^r D_n$ имеет не более λ образующих.

Рассмотрим теперь для некоторого $t \geq r$ отображение $\pi(n+t, n+t-r): \mathfrak{R}_{n+t}^- \rightarrow R_{n+t-r}^-$. Поскольку $\pi(n+t, n+t-r)$ аннулирует все элементы порядка не выше ℓ^r , мы, полагая $n+t-r = s$, получаем, что группа $D'_s := \pi(n+t, s)(D_{n+t})$ имеет не более λ образующих. Отметим также, что D'_s является Γ -модулем.

Пусть V – векторное пространство над полем $\mathbb{F}_\ell$ из ℓ элементов размерности не выше λ . Если на V действует группа Γ , то существует индекс u , зависящий только от λ и такой, что подгруппа Γ_u группы Γ индекса ℓ^u действует на V тривиально.

ПРЕДЛОЖЕНИЕ 5.5. Пусть r, s, u имеют тот же смысл, что и выше, и t удовлетворяет неравенству

$$n+t-r = s \geq 2 \max\{u, n\} + 4. \quad (5.6)$$

Пусть $f = [s/2] + 2$, где $[\cdot]$ означает целую часть числа. Тогда отображение $\pi(s, s-f): \mathfrak{R}_s^- \rightarrow \mathfrak{R}_{s-f}^-$ аннулирует группу D'_s .

ДОКАЗАТЕЛЬСТВО. Согласно (5.6) мы имеем

$$s-f \geq \frac{s}{2} - 2 \geq \max\{u, n\}. \quad (5.7)$$

Отображение $\pi(s, s-f): \mathfrak{R}_s^- \rightarrow \mathfrak{R}_{s-f}^-$ можно представить как композицию естественной проекции $\pi_1: \mathfrak{R}_s^- \rightarrow (\mathbb{Z}/\ell^{s+1}\mathbb{Z}[G_{s-f}])^-$ и отображения факторизации

по ℓ^{s-f+1} -м степеням $\pi_2: \mathbb{Z}/\ell^{s+1}\mathbb{Z}[G_{s-f}] \rightarrow \mathfrak{R}_{s-f}^-$. Положим ${}_\ell D'_s = \{x \in D'_s \mid \ell x = 0\}$. Тогда ${}_\ell D'_s$ – векторное пространство над $\mathbb{F}_\ell$ размерности не выше λ . В силу (5.7) группа Γ_{s-1}/Γ_s действует на это пространство тривиально. Следовательно, норма N_1 относительно группы Γ_{s-1}/Γ_s аннулирует ${}_\ell D'_s$. Поскольку $\mathfrak{R}_s^-$ кохомологически тривиален как Γ_{s-1}/Γ_s -модуль, мы имеем $\pi_1(s, s-1)(D'_s) \cong N_1(D'_s) := D''_s$ и $\ell^s D''_s = 0$. Обозначая через N_2 норму относительно группы $\Gamma_{s-2}/\Gamma_{s-1}$ и повторяя предыдущее рассуждение, мы получаем, что группа $D'''_s := N_2(D''_s)$ аннулируется умножением на ℓ^{s-1} . Повторяя это рассуждение f раз и учитывая, что отображение нормы $N = N_f \circ \dots \circ N_1$ относительно группы Γ_{s-f}/Γ_s совпадает с π_1 , мы получаем, что $\pi_1(D'_s)$ аннулируется умножением на ℓ^{s-f} . Следовательно, $\pi_2(\pi_1(D'_s)) = 0$. Предложение доказано.

Согласно (5.7) мы имеем $s-f \geq n$, т. е. $\pi(s, n)$ пропускается через $\pi(s, s-f)$. Следовательно, $\pi(s, n)$ аннулирует D'_s , и $\pi(n+t, n)$ аннулирует D_{n+t} . Таким образом, выполняется (5.3), что завершает доказательство теоремы 3.2 в случае $\ell \neq 2$.

Случай $\ell = 2$ разбирается аналогично.

Список литературы

1. S. Lang, “Cyclotomic fields I and II”, Grad. Texts in Math., **121**, Springer-Verlag, New York, 1990.
2. B. H. Gross, N. Koblitz, “Gauss sums and the p -adic Γ -function”, *Ann. of Math.* (2), **109**:3 (1979), 569–581.
3. H. Miki, “On the l -adic expansion of certain Gauss sums and its applications”, *Galois representations and arithmetic algebraic geometry* (Kyoto 1985/Tokyo 1986), Adv. Stud. Pure Math., **12**, North-Holland, Amsterdam, 1987, 87–118.
4. Л. В. Кузьмин, “Некоторые явные вычисления в локальных и глобальных круговых полях”, *Теория чисел, алгебра и алгебраическая геометрия*, Сб. статей. К пятидесятилетию со дня рождения академика Игоря Ростиславовича Шафаревича, Тр. МИАН, **208**, Наука, Физматлит, М., 1995, 202–223; англ. пер.: L. V. Kuz'min, “Some explicit calculations in local and global cyclotomic fields”, *Proc. Steklov Inst. Math.*, **208** (1995), 179–197.
5. W. Sinnott, “On the Stickelberger ideal and the circular units of a cyclotomic field”, *Ann. of Math.* (2), **108**:1 (1978), 107–134.

ЛЕОНИД ВИКТОРОВИЧ КУЗЬМИН
(LEONID V. KUZ'MIN)
Национальный исследовательский центр
“Курчатовский институт”, г. Москва
E-mail: helltiapa@mail.ru

Поступило в редакцию
26.12.2012
08.07.2013