Министерство образования и науки Российской Федерации
Федеральное государственное автономное
образовательное учреждение высшего образования
Московский физико-технический институт
(государственный университет)

На правах рукописи

Мороз Борис Зеликович

Аналитические задачи в алгебраической теории чисел и диофантовой геометрии

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация
на соискание ученой степени
доктора физико-математических наук

Москва
2017

Оглавление

Стр.

Введение

0.1 Содержание диссертации

Диссертация состоит из введения, четырёх глав, заключения и списка литературы.

1. В первой главе изучаются аналитические свойства скалярных произведений L - рядов Артина - Вейля над полем алгебраических чисел; эта тематика восходит к моей кандидатской диссертации [26] - [30]. Изложение основано на моих работах 1980-ых годов [121], [123], [132], [133] (см. также [124], [128]). Сформулируем основные результаты этой главы.

Зафиксируем поле алгебраических чисел k и обозначим через $I_0(k)$ моноид ненулевых целых идеалов этого поля. Будем называть ряд Дирихле

$$(L_1 * \cdots * L_r)(s) := \sum_{\mathfrak{n} \in I_0(k)} N_{k/\mathbb{Q}}\mathfrak{n}^{-s} \prod_{i=1}^{r} a_i(\mathfrak{n})$$

скалярным произведением (формальных) рядов Дирихле

$$L_i(s) := \sum_{\mathfrak{n} \in I_0(k)} a_i(\mathfrak{n}) N_{k/\mathbb{Q}}\mathfrak{n}^{-s},\ 1 \leq i \leq r,$$

над полем k. Положим

$$\mathbb{C}_0 := \{x + iy | (x, y) \in \mathbb{R}^2,\ x > 0\} \ \text{ и } \ \mathbb{C}^{(0)} := \{iy | y \in \mathbb{R}\}.$$

При $1 \leq i \leq r$ рассмотрим (непрерывные) конечномерные нормированные представления

$$\rho_i \colon W(k) \to \mathrm{GL}(d_i, \mathbb{C})$$

группы Вейля $W(k)$ поля k и отвечающие этим представлениям L - функции Вейля $L(\chi_i,\ s)$, $\chi_i := \mathrm{tr}\ \rho_i$. Положим

$$L_i(s) := L(\chi_i, s),\ \vec{\chi} := (\chi_1, ..., \chi_r) \ \text{ и } \ L(\vec{\chi}, s) := (L_1 * \cdots * L_r)(s).$$

Предположим, не нарушая общности, что степени d_i представлений ρ_i удовлетворяют следующему условию:

$$r \geq 2 \text{ и } d_1 \geq d_2 \geq ... \geq d_r \geq 2. \tag{0.1.1}$$

Теорема 0.1.1. *Если $d_1 = d_2 = r = 2$, то функция $s \mapsto L(\vec{\chi}, s)$ мероморфна на всей комплексной плоскости $\mathbb{C}$; в противном случае, эта функция мероморфна в полуплоскости $\mathbb{C}_0$, а прямая $\mathbb{C}^{(0)}$ является её естественной границей.*

При $1 \leq i \leq r$ рассмотрим конечные расширения полей $k_i|k$ степени $d_i := [k_i : k]$, положим $L_i(s) := L(\psi_i, s)$, где $L(\psi_i, s)$ есть L - ряд Hecke поля k_i с характером ψ_i; пусть

$$\vec{\psi} := (\psi_1, ..., \psi_r) \text{ и } L(\vec{\psi}, s) := (L_1 * \cdots * L_r)(s).$$

Предположим, не нарушая общности, что степени d_i расширений $k_i|k$ удовлетворяют условию (1).

Теорема 0.1.2. *Если $d_1 = d_2 = r = 2$, то функция $s \mapsto L(\vec{\psi}, s)$ мероморфна на всей комплексной плоскости $\mathbb{C}$; в противном случае, эта функция мероморфна в полуплоскости $\mathbb{C}_0$, а прямая $\mathbb{C}^{(0)}$ является её естественной границей.*

Теорема 1 есть основной результат второй главы диссертации; важной технической леммой при доказательстве теоремы 1 является полученное в этой главе обобщение теоремы плотности Чеботарёва (ср. [132]). Теорема 2 легко следует из теоремы 1.

Несколько слов об истории проблемы, рассматриваемой в этой главе. В 1950 г. Ю.В. Линник определил скалярное произведение L-рядов Гекке над полем рациональных чисел. Весной 1962 года Юрий Владимирович Линник предложил мне заняться изучением свойств скалярных произведений L - рядов Гекке двух квадратичных полей, и я написал кандидатскую диссертацию на

эту тему. В 1965 г. А.И. Виноградов продолжил скалярное произведение L-рядов Гекке в полуплоскость

$$\mathbb{C}_{1/2} := \{x + iy | (x, y) \in \mathbb{R}^2,\ x > 1/2\},$$

а в 1971 г. П.К.Й. Дракслу усилил результат Виноградова, продолжив эту функцию в полуплоскость $\mathbb{C}_0$. Через несколько лет после этого стало ясно (см., например, [121]), что скалярное произведение L - рядов Гекке двух квадратичных полей над любым полем алгебраических чисел выражается через обычные L - ряды Гекке. С другой стороны, теорема 5 показывает, что в общем случае результат Дракслу неулучшаем: за исключением случая двух квадратичных полей, прямая $\mathbb{C}^{(0)}$ есть естественная граница определяемой скалярным произведением L - рядов Гекке (и мероморфной в $\mathbb{C}_0$) функции. Идея доказательства теорем 4 и 5, восходящая к классическим работам Ландау - Вальфиша и Эстермана (ср. [122]), принадлежит Н. Курокава (см. [107], [108]). Приведённое в диссертации доказательство теорем 4 и 5 использует технику, развитую в моих работам [121], [123], [124], [128], [127], [132] и [133]. В работе Курокава [109] эти теоремы доказаны по-иному.

2. Во второй главе изучается распределение целых точек на аффинных торических многообразиях, определённых над кольцом целых рациональных чисел. Простейшие многообразия такого рода - это квадрики вида $\mathrm{Spec}\ \mathbb{Z}[x]/(F(x))$, где $f(x_1, x_2)$ и $g(x_3, x_4)$ суть бинарные положительно определённые квадратичные формы с целыми рациональными коэффициентами и $F(x) := f(x_1, x_2) - g(x_3, x_4)$. Распределение целых точек на таких гиперповерхностях изучалось в моих первых работах [26] - [30]. В работах [129], [130], [136] исследуется множество целых точек норменных многообразий; целые точки аффинных торических многообразий изучаются в работах [137] - [140] и в §4 этой главы. Определённое над полем алгебраических чисел торическое многообразие имеет, вообще говоря, много попарно неизоморфных моделей над кольцом целых этого поля. Целые модели алгебраических

торов и аффинных торических многообразий изучаются в совместных работах [14], [6], [15]. В §2 этой главы приводятся некоторые определения и результаты, связанные с теорией алгебраических торов и аффинных торических многообразий, определённых над произвольным полем нулевой характеристики. Рассмотрим алгебраический тор T, определённый над полем алгебраических чисел k, и обозначим через $\mathfrak{o}$ кольцо целых поля k. В §3 строятся естественная явно заданная $\mathfrak{o}$ - целая модель $\mathcal{T}$ алгебраического тора T и соответствующие целые модели аффинных T - торических многообразий. Построенная $\mathfrak{o}$ - схема $\mathcal{T}$ является приведённой строго плоской схемой; более того, если тор T расщепляется над (конечным) алгебраическим расширением поля k без высшего ветвления, то связная компонента единицы схемы $\mathcal{T}$ изоморфна связной компоненте единицы модели Нерона-Рейно тора T [6, теорема 3]. В общем случае гладкую $\mathfrak{o}$ - целую модель тора T можно получить из схемы $\mathcal{T}$ разрешением особенностей. Изложение в §2 и §3 следует нашей совместной с Б.Э. Кунявским работе [15].

3. В третьей главе обсуждаются теоремы о бесконечности числа простых чисел, представимых полиномами третьей степени от двух переменных, и некоторые следствия этих теорем. Упомянутые теоремы (и их следствия) доказаны в двух совместных с Д.Р. Хис-Брауном работах [97], [98].

Рассмотрим неприводимую примитивную бинарную кубическую форму $f(x),\ x := (x_1, x_2)$, с целыми рациональными коэффициентами. Положим

$$\varepsilon(f) := \text{ н.о.д. } \{f(a) | a \in \mathbb{N}^2\};$$

можно показать, что $\varepsilon(f) \in \{1, 2\}$. Пусть

$$X \in \mathbb{R},\ X \geq 3,\ \tau := (\log\log X)^{-1/6},\ \eta := (\log X)^{-c_0},$$

где c_0 есть фиксированное вещественное положительное число, зависящее

лишь от f (или от F в теореме 4), и

$$I(X) := \{a | a \in \mathbb{Z}^2,\ X < a_1, a_2 \leq X(1+\eta)\}.$$

Обозначим через P множество простых чисел.

Теорема 0.1.3. *Пусть* $\varepsilon(f) = 1$ *и* $f(1,1) > 0$. *Тогда*

$$\pi_f(X) = \sigma(f)\ \frac{\eta^2 X^2}{3\log X}\ (1 + O((\log\log X)^{-1/6}))\ \ c\ \ \sigma(f) > 0$$

при $X \to \infty$, *где*

$$\pi_f(X) := card\ \{p | p \in P,\ (\exists\ x \in I(X))\ f(x) = p\}.$$

Следствие 0.1.1. *Пусть* $\varepsilon(f) = 2$ *и* $f(2,1) > 0$. *Тогда*

$$\pi_{f,1}(X) = \sigma(g)\ \frac{\eta^2 X^2}{3\log X}\ (1 + O((\log\log X)^{-1/6}))$$

при $X \to \infty$, *где*

$$\pi_{f,1}(X) := card\ \{p | p \in P,\ (\exists\ b \in \mathbb{Z}^2)\ p = \frac{f(b)}{2},\ (b_1/2, b_2) \in I(X)\}$$

и

$$g(y_1, y_2) := \frac{1}{2} f(2y_1, y_2).$$

Рассмотрим кубическое поле k, т.е. поле алгебраических чисел под условием $[k : \mathbb{Q}] = 3$, и обозначим через $\mathfrak{o}$ кольцо целых этого поля. Пусть

$$\{\omega_1,\ \omega_2\} \subseteq \mathfrak{o} \setminus \{0\},\ k = \mathbb{Q}(\omega_2\omega_1^{-1}),\ d \in \mathbb{N},\ a \in \mathbb{Z}^2\ \text{ и }\ 0 \leq a_1, a_2 < d.$$

Предположим, что н.о.д. $(a_1,\ a_2,\ d) = 1$, введём в рассмотрение идеал

$$\mathfrak{d}(a) := (a_1\omega_1 + a_2\omega_2,\ d\omega_1,\ d\omega_2)$$

кольца $\mathfrak{o}$ и положим

$$F(x) := N_{k(x)/\mathbb{Q}(x)}((a_1 + dx_1)\omega_1 + (a_2 + dx_2)\omega_2) N\mathfrak{d}(a)^{-1}.$$

Ясно, что $F(x) \in \mathbb{Z}[x]$; положим

$$\varepsilon(F) := \text{н.о.д. } \{F(a) | a \in \mathbb{N}^2\}.$$

Можно показать, что $\varepsilon(F) \in \{1, 2, 3, 6\}$.

Теорема 0.1.4 . *Пусть* $\varepsilon(F) = 1$. *Тогда*

$$\pi_F(X) = \sigma(F)\,\frac{\eta^2 X^2}{3\log X}\,(1 + O((\log\log X)^{-1/6}))\ \ c\ \ \sigma(F) > 0$$

при $X \to \infty$, *где*

$$\pi_F(X) := card\,\{p | p \in P,\ (\exists\, x \in I(X))\ F(x) = p\}.$$

Гипотеза 0.1.1 . *Пусть* $a \in \mathbb{N}$; *обозначим через* $r(a)$ *ранг эллиптической кривой*

$$x^3 + y^3 = az^3$$

и через $R(a)$ *аналитический ранг (т.е. порядок нуля в точке* $s = 1$ *дзета - функции Хассе - Вейля* $L_a(s)$*) этой кривой. Имеет место соотношение*

$$(\forall\, a \in \mathbb{N})\ r(a) = R(a)\ (mod\ \ 2).$$

Гипотеза 1 следует из известной гипотезы Бёрча и Свиннертона-Дайера, но пока не доказана.

Следствие 0.1.2 . *Пусть*

$$\{a_i | 0 \le i \le 4\} \subseteq \mathbb{Z}, \quad \prod_{i=0}^{4} a_i \neq 0\ (mod\ \ 3)$$

и

$$(\forall\, p \in \{q | q \in P,\ q = 2\ (mod\ \ 3)\})\ a_i \neq 0\ (mod\ \ p^2)\ \ при\ \ 0 \le i \le 4.$$

Тогда из справедливости гипотезы 1 *вытекает, что гиперповерхность*

$$H_1 : \sum_{i=0}^{4} a_i x_i^3 = 0\ \ в\ \ \mathbb{P}^4(\mathbb{Q})$$

удовлетворяет принципу Хассе.

Следствие 0.1.3 . *Пусть* $\{a,\ b\} \subseteq \mathbb{Z}$; *рассмотрим поверхность*

$$H_2 : x_0^3 + 2x_1^3 + ax_2^3 + bx_3^3 = 0\ \ в\ \ \mathbb{P}^3(\mathbb{Q}),$$

обозначим через $\bar{y}$ *остаток при делении числа* y, $y \in \mathbb{Z}$, *на* 9 *и предположим, что*

$$н.о.д.\ (a,b) = 1 \ \ и \ \ \{\overline{a+b},\ \overline{a-b}\} \cap \{0\} \neq \emptyset \tag{0.1.2}$$

или

$$н.о.д.\ (a,b) = 1 \ \ и \ \ \{\bar{a},\ \bar{b}\} \cap \{2,\ 3,\ 6,\ 7\} \neq \emptyset. \tag{0.1.3}$$

Тогда

$$H_2(\mathbb{Q}) \neq \emptyset. \tag{0.1.4}$$

В работе Хис-Брауна [95] теорема 3 доказана для полинома $x^3 + 2y^3$, в этом случае $k = \mathbb{Q}(\sqrt[3]{3})$; разработанная в этой работе стратегия доказательства обобщается в наших совместных работах [97], [98] (и в диссертации) на произвольные кубические поля.

4. В четвёртой главе (приложение) собраны заметки, написанные в разные годы. Первая заметка "О распределении степенных вычетов и невычетов" есть слегка переработанный вариант моей дипломной работы [25], написанной под руководством Ю.В. Линника (ср. [8, гл. 9]). Во второй заметке в предположении гипотезы Римана получена асимптотическая формула для числа целых точек с взаимно простыми координатами в плоских "звёздообразных"множествах (ср. [126]). В третьей заметке получена асимптотическая формула для числа рациональных точек ограниченной высоты на проективной кубической поверхности, заданной уравнением

$$X_0^3 = X_1X_2X_3$$

(изложение в этом параграфе основано на совместной работе [96]). В основу четвёртой заметки положена работа [134], задуманная как введение в аналитическую теорию положительно определённых квадратичных форм, см. также [135]. В пятом параграфе обсуждаются L - функции эллиптических кривых, определённых над мнимыми квадратичными полями (здесь мы следуем совместной работе [67]). В шестой заметке уточняется формулировка

известной теоремы Берча [49] (изложение в этом параграфе основано на совместной работе [43]). В последнем параграфе этой главы воспроизводится с небольшими изменями заметка [58] (совместная работа с М. Карлом); в этой заметке коротко описывается конструкция диофантовых уравнений, кодирующих доказуемость в формальной математике, ср. [57]. Сформулируем три из доказанных в этой главе теорем.

Пусть p - нечётное простое число; $l|p-1$; χ - мультипликативный характер степени l; $\varepsilon_1, ..., \varepsilon_s$ - корни l-ой степени из единицы; $\Phi(t)$ - неприводимый полином степени f с коэффициентами в конечном поле $\mathbb{F}_p$ из p элементов. Положим

$$E(\varepsilon, \Phi) := \text{card } \{x | x \in \mathbb{F}_p,\ \chi(\Phi(x+i)) = \varepsilon_i \text{ при } 1 \leq i \leq s\}.$$

Теорема 0.1.5. *Имеет место следующее неравенство:*

$$|E(\varepsilon, \Phi) - \frac{p}{l^s}| < sflp^{1/2}.$$

Эта теорема, доказанная в 1961-м году, обобщает и усиливает более ранние результаты Дэвенпорта.

Рассмотрим открытое множество

$$U : X_0 \neq 0$$

на проективной кубической поверхности

$$S : X_0^3 = X_1 X_2 X_3.$$

Ясно, что

$$U(\mathbb{Q}) = \{[x] | x \in \mathbb{Z}^4,\ x_0 > 0,\ x_0^3 = x_1 x_2 x_3,\ \text{н.о.д. } (x_0, ..., x_3) = 1\},$$

где $[x] := \{tx | t \in \mathbb{Q}\}$ - прямая в $\mathbb{Q}^4$, проходящая через точки 0 и x. Положим

$$h([x]) := \max \{|x_i|\ | 0 \leq i \leq 3\} \text{ при } [x] \in U(\mathbb{Q})$$

и

$$\mathcal{N}(H) := \text{card}\ \{y | y \in U(\mathbb{Q}),\ h(y) < H\}.$$

Теорема 0.1.6. *При $H \to \infty$ имеет место следующая асимптотическая формула:*

$$\mathcal{N}(H) = \frac{H(\log H)^6}{6!} \prod_{p \in P} l_p + O(H(\log H)^5),$$

где

$$l_p := (1 - \frac{1}{p})^7 (1 + \frac{7}{p} + \frac{1}{p^2}).$$

Теорема 6, доказанная в совместной работе [96], показывает, что поверхность S удовлетворяет гипотезе Батырева - Манина.

Будем называть натуральное число n квадратично полным, если

$$(\forall\ p \in P)\ p|n\ \Rightarrow\ p^2|n.$$

Теорема 0.1.7. *Любое достаточно большое натуральное число есть сумма двух квадратов и квадратично полного числа.*

В работе [135] эта теорема, впервые доказанная Хис-Брауном, выводится из общей теории положительно определённых квадратичных форм.

0.2 Разное

Актуальность темы. К началу двадцатого века в теории чисел сложились два основных направления: алгебраическая теория чисел (см., например, монографию Гильберта о полях алгебраических чисел,
1897 г.) и аналитическая теория чисел (см., например, монографию
Ландау о распределении простых чисел, 1909 г.). В последующие десятилетия в работах Ландау, Гекке, Артина и других авторов была постреана аналитическая теория числовых полей, так что, например, теорема плотности Чеботарёва получила чисто аналитическое доказательство (ср. §4 гл. I этой

работы). Полученные А. Вейлем как следствие доказанного им аналога гипотезы Римана для глобальных полей простой характеристики оценки тригонометрических сумм нашли применение в различных задачах классической теории чисел (ср. гл. IV, §1 и §4). В работах Хули, Хис-Брауна и других авторов применяются оценки кратных тригонометрических сумм, вытекающие из доказанных Гротендиком и Делинем гипотез Вейля. Гипотеза Хассе-Вейля о мероморфности арифметических L-функций является одной из центральных проблем современной диофантовой геометрии; достаточно сказать, что теорема Ферма есть следствие этой гипотезы для определённых над $\mathbb{Q}$ эллиптических кривых, доказанной в 1990-ые (эта гипотеза для эллиптических кривых, определённых над мнимым квадратичным полем, обсуждается в §5 главы IV). Доказанные в гл. I теоремы о непродолжимости эйлеровских произведений показывают, что (в предположении гипотезы Хассе-Вейля) класс арифметических L-функций не замкнут относительно "естественной" операции скалярного произведения рядов Дирихле. Изучение распределения целых и рациональных точек, определённых над кольцом целых алгебраических чисел, есть классическая проблема теории чисел. Как показывает теорема Матиясевича (см., например, гл. IV, §7), эта проблема не допускает "окончательного" решения на языке современной математики. В §3 главы IV изучается распределение рациональных точек на одной кубической поверхности, а в §4 этой главы - распределение целых точек на квадриках; в §4 главы II рассматриваются целые точки аффинных торических многообразий. Классическая гипотеза В.Я. Буняковского (1854 г.) утверждает, что неприводимый полином $f(x)$ с целыми рациональными коэффициентами принимает бесконечно много простых значений, коль скоро старший коэффициент этого полинома положителен и

$$\text{н.о.д. } \{f(a)|a \in \mathbb{N}\} = 1;$$

эта гипотеза до сих пор не доказана ни для одного нелинейного полинома.

Теоремы, доказанные в третьей главе диссертации, являются в настоящий момент одним из самых сильных результатов в направлении гипотезы Буняковского (ср. [33]).

Цель работы. Привести несколько примеров эффективности применения аналитических методов в диофантовой геометрии. Исследовать поведение скалярных произведений L-рядов Артина - Вейля. Построить естественные целые модели алгебраических торов и аффинных торических многообразий и изучить распределение целых точек этих моделей. Доказать новые теоремы о представимости простых чисел кубическими полиномами от двух переменных.

Методы исследования. В первой главе для доказательства основных теорем привлекается весь аппарат аналитической арифметики полей алгебраических чисел. Во второй главе аналитические методы комбинируются с довольно тонкими диофантово-геометрическими рассуждениями. В третьей главе метод решета применяется для изучения трёхмерной арифметики (в смысле Гекке) кубических полей. В первых четырёх параграфах четвёртой главы используется стандартная техника аналитической теории чисел. В пятом параграфе с помощью теории полей классов изучаются двумерные l-адические представления групп Галуа на модулях Тэйта эллиптических кривых. В шестом параграфе мы изучаем подмногообразия особых точек алгебраических многобразий, определённых над полем рациональных чисел, пользуясь методами и результатами коммутативной алгебры. Методы седьмого параграфа суть комбинаторно-алгебраические рассмотрения, используемые при решении десятой проблемы Гильберта.

Научная новизна. Перечислим основные новые результаты диссертации, выносимые на защиту.

1. Исследована проблема продолжимости скалярных произведений L-рядов Артина - Вейля.

2. Доказано обобщение теоремы плотности Чеботарёва.
3. Доказаны теоремы о распределении целых точек некоторых аффинных торических многообразий.
4. Построены "естественные" целые модели алгебраических торов и аффинных торических многообразий (в соавторстве с Воскресенским и Кунявским).
5. Доказаны теоремы о бесконечности множеств вида

$$\{f(a)|a \in \mathbb{Z}^2\} \cap P,$$

где P есть множество простых натуральных чисел, для широкого класса кубических полиномов $f(x)$, $x := (x_1, x_2)$, от двух переменных (в соавторстве с Хис-Брауном).
6. Доказана гипотеза Батырева - Манина для одной кубической поверхности (в соавторстве с Хис-Брауном).
7. Получено новое доказательство теоремы Хис-Брауна о представимости достаточно больших натуральных чисел суммой трёх квадратично полных чисел.
8. Построен полином, кодирующий доказуемость в теории множеств (в соавторстве с Карлом).

Теоретическая и практическая ценность. Работа носит теоретический характер. Её результаты и методы могут быть использованы в аналитической и алгебраической теории чисел, теории алгебраических групп, диофантовой геометрии и других областях.

Апробация работы. Основные результаты диссертации докладывались и обсуждались на семинарах и/или конференциях в следующих городах: Москва, Санкт-Петербург (Ленинград), Владимир, Вильнюс, Паланга, Варшава, Познань, Будапешт, Братислава, Вена, Грац, Женева, Цюрих, Генуя,

Барселона, Иерусалим, Тель-Авив, Беэр-Шева, Реховот, Натания, Эйлат, Париж, Бордо, Лилль, Лимож, Люмини, Мец, Страсбург, Гент, Нордвейкерхаут, Копенгаген, Бонн, Бохум, Гейдельберг, Гёттинген, Дармштадт, Лейпциг, Марбург, Мюнстер, Обервольфах, Лондон, Кардифф, Кембридж, Ноттингем, Оксфорд, Монреаль, Токио.

Публикации. Диссертация опубликована [35]; основная цель монографии [35] - привлечь внимание широкого круга читателей, интересующихся теорией чисел, к рассматриваемым в диссертации проблемам.

Основные результаты диссертации опубликованы в работах [6], [14], [15], [25] - [34], [43], [57], [58], [67], [96] - [98], [121] - [140]. В цитируемых совместных работах вклад соавторов одинаков.

0.3 Обозначения

Как обычно, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$ и $\mathbb{C}$ суть поля рациональных, p - адических, вещественных и комплексных чисел; $\mathbb{Z}$ и $\mathbb{Z}_p$ суть кольца целых рациональных и целых p - адических чисел; $\mathbb{N}$ и $\mathcal{P}$ суть множества положительных целых и простых рациональных чисел; $\mathbb{F}_q$ есть конечное поле из q элементов при $q \in \{p^n | p \in \mathcal{P},\ n \in \mathbb{N}\}$; $\mu : \mathbb{N} \to \{0,\ \pm 1\}$ есть функция Мёбиуса, определяемая соотношениями:

$$\mu(1) = 1,\ \mu(n_1 n_2) = \mu(n_1)\mu(n_2) \ \text{ при } \ (n_1, n_2) = (1)$$

и $\mu(p) = -1,\ \mu(p^k) = 0$ при $p \in \mathcal{P},\ k \in \mathbb{N} \setminus \{1\}$ (заметим, что буква μ используется также для обозначения меры Хаара). Положим

$$\mathbb{N}_0 := \mathbb{N} \cup \{0\},\ \mathbb{C}_\sigma := \{x + iy | \{x, y\} \subseteq \mathbb{R},\ x > \sigma\} \text{ при } \sigma \in \mathbb{R},$$

$$\mathbb{R}_+ := \{x | x \in \mathbb{R},\ x \geq 0\} \ \text{ и } \ \mathbb{R}_+^* := \mathbb{R}_+ \setminus \{0\}.$$

Число элементов (мощность) множества T обозначается через $|T|$ или $\mathrm{card}\ T$.

Для произвольного множества T положим

$$M_{mn}(T) := \{A|A = (a_{ij})_{1\leq i\leq m,\, 1\leq j\leq n}\ ,\ a_{ij} \in T\ \text{ при }\ 1 \leq i \leq m,\ 1 \leq j \leq n\}$$

при $\{m, n\} \subseteq \mathbb{N}$ и

$$T^n := M_{n1}(T),\ M_n(T) := M_{nn}(T)\ \text{ при }\ n \in \mathbb{N};$$

введём операцию траспонирования $A \mapsto A^t,\ x \mapsto x^t$, положив

$$A^t = (b_{ij})_{1\leq i,j\leq n}\ ,\ b_{ij} = a_{ji}\ \text{ при }\ A \in M_n(T),\ A = (a_{ij})_{1\leq i,j\leq n}$$

и $x^t = (x_1, ..., x_n)$ при $x \in T^n,\ n \in \mathbb{N}$. Рассмотрим кольцо R и пусть $\mathcal{Q} \subseteq R$; обозначим через $(\mathcal{Q})_R$ (или просто $(\mathcal{Q})$) идеал кольца R, порождённый множеством $\mathcal{Q}$; как обычно, строка $(a_1, ..., a_n)$ служит для обозначения идеала кольца R, порожденного элементами $a_1, ..., a_n$ этого кольца, а R^* есть группа единиц кольца R;

$$a = b\ (\mathfrak{a}) := (a - b) \in \mathfrak{a}\ \text{ при }\ \{a, b\} \subseteq R$$

для любого идеала $\mathfrak{a}$ кольца R и

$$a = b\ (c) := (a - b) \in (c)\ \text{ при }\ \{a, b, c\} \subseteq R,$$

так что, например, равенство $(a, b) = (1)$ при $\{a, b\} \subseteq \mathbb{Z}$ означает, что числа a и b взаимно просты, а равенство $a = b\ (m)$ при $m \in \mathbb{N}$ означает, что $a - b$ делится m. Если кольцо R является коммутативным кольцом с единицей "1", то $G_{m,R}$ и $G_{a,R}$ обозначают соответственно мультипликативную и аддитивную алгебраические группы, определённые над R,

$$\mathrm{GL}_n(R) := \{A|A \in M_n(R),\ |A| \in R^*\},$$

и

$$\mathrm{SL}_n(R) := \{A|A \in M_n(R),\ |A| = 1\},$$

где $|A|$ есть определитель матрицы A. Обозначим через $(G : H)$ индекс подгруппы H в группе G, а через $S^G := \{a|a \in S,\ g \cdot a = a\}$ множество неподвижных точек действия группы G на множестве S. Положим

$$|x| := (\sum_{i=1}^{n} x_i^2)^{1/2} \text{ при } x \in \mathbb{R}^n$$

и обозначим через S_n единичную сферу в $\mathbb{R}^{n+1}$:

$$S_n := \{x|x \in \mathbb{R}^{n+1},\ |x| = 1\};$$

одномерная единичная сфера часто отождествляется с единичной окружностью в комплексной плоскости:

$$S_1 = \{z|z \in \mathbb{C},\ |z| = 1\}.$$

Рассмотрим топологическое пространство T и пусть $U \subseteq T$; обозначим через $\bar{U}$ замыкание множества U и через

$$\partial U := \bar{U} \cap \overline{T \setminus U}$$

(топологическую) границу этого множества.

Обозначим через $\bar{K}$ алгебраическое замыкание поля K, через $[L : K]$ степень конечного расширения полей $K \subseteq L$, через $\mathrm{Gal}(L|K)$ группу Галуа нормального расширения полей $K \subseteq L$ и через $G_K := \mathrm{Gal}(\bar{K}|K)$ (абсолютную) группу Галуа поля K. Если $\mathbb{Q} \subseteq K$ и $[K : \mathbb{Q}] < \infty$, будем называть K полем алгебраических чисел; обозначим через d_K, h_K и $\mathfrak{o}(K)$ дискриминант, число классов и кольцо целых элементов поля K. Положим

$$\mathcal{P}(K) := \mathrm{Spec}\ \mathfrak{o}(K) \setminus \{(0)\},$$

так что

$$\mathcal{P}(\mathbb{Q}) = \mathrm{Spec}\ \mathbb{Z} \setminus \{(0)\} = \{(p)|p \in \mathcal{P}\}.$$

Обозначим через $I(K)$ группу дробных идеалов поля K и положим

$$I_0(K) := \{\mathfrak{a} | \mathfrak{a} \in I(K),\ \mathfrak{a} \subseteq \mathfrak{o}(K)\};\ |\mathfrak{A}| := N_{K/\mathbb{Q}}\mathfrak{A} \text{ при } \mathfrak{A} \in I(K).$$

Изоморфные объекты часто отождествляются, если это не может привести к недоразумению.

Как обычно, (I.1.1):="формула (1) в §1 гл. I" , (1.1):="формула (1) в §1 той же главы" и (1):="формула (1) того же параграфа".

Остальные обозначения вводятся по ходу изложения (или являются самоочевидными/общепринятыми).

Глава 1

Скалярные произведения L-рядов Гекке и Артина - Вейля.

1.1 Введение

1. В этой главе изучаются аналитические свойства скалярных произведений L - рядов Артина-Вейля над полем алгебраических чисел k. Будем называть ряд Дирихле

$$(L_1 * \cdots * L_r)(s) := \sum_{\mathfrak{n} \in I_0(k)} |\mathfrak{n}|^{-s} \prod_{i=1}^{r} a_i(\mathfrak{n})$$

скалярным произведением (формальных) рядов Дирихле

$$L_i(s) := \sum_{\mathfrak{n} \in I_0(k)} a_i(\mathfrak{n}) |\mathfrak{n}|^{-s},\ 1 \leq i \leq r,$$

над полем k. Согласно [41, стр. 232], в 1950 г. Ю.В. Линник определил скалярное произведение L-рядов Гекке над полем $\mathbb{Q}$. Весной 1962 года Юрий Владимирович Линник [16] предложил мне заняться изучением свойств скалярных произведений L - рядов Гекке двух квадратичных полей [26] - [30]. В 1965 г. А.И. Виноградов [4] продолжил скалярное произведение L-рядов Гекке в полуплоскость $\mathbb{C}_{1/2}$, а в 1971 г. П.К.Й. Дракcл [68] усилил результат Виноградова, продолжив эту функцию в полуплоскость $\mathbb{C}_0$. В 1972 г. О.М. Фоменко [41] доказал, что скалярное произведение L - рядов Гекке двух квадратичных полей над полем $\mathbb{Q}$ мероморфно на всей комплексной плоскости и удовлетворяет функциональному уравнению с четырьмя Γ - факторами. Через несколько лет после этого стало ясно [7], [108], [121], что скалярное произведение L - рядов Гекке двух квадратичных полей над любым полем алгебраических чисел выражается через обычные L - ряды Гекке, а в общем случае результат Дракcла неулучшаем: за исключением случая двух квадратичных полей, прямая

$$\mathbb{C}^{(0)} := \{iy | y \in \mathbb{R}\}$$

есть естественная граница определяемой скалярным произведением L - рядов Гекке (и мероморфной в $\mathbb{C}_0$) функции. Точнее говоря, имеет место следующая теорема [107] - [109], [123], [127], [128], [133].

Теорема 1.1.1. *При $1 \leq i \leq r$ рассмотрим конечные расширения полей $k_i|k$ степени $d_i := [k_i : k]$ и предположим, что*

$$r \geq 2 \ \text{ и } \ d_1 \geq d_2 \geq ... \geq d_r \geq 2. \tag{1.1.1}$$

Положим $L_i(s) := L(\psi_i, s)$, где $L(\psi_i, s)$ есть L - ряд Hecke поля k_i с характером ψ_i, при $1 \leq i \leq r$; пусть

$$\vec{\psi} := (\psi_1, ..., \psi_r) \ \text{ и } \ L(\vec{\psi}, s) := (L_1 * \cdots * L_r)(s).$$

Если $d_1 = d_2 = r = 2$, то функция

$$s \mapsto L(\vec{\psi}, s)$$

мероморфна на всей комплексной плоскости $\mathbb{C}$; в противном случае, эта функция мероморфна в полуплоскости $\mathbb{C}_0$, а прямая $\mathbb{C}^{(0)}$ является её естественной границей.

При $1 \leq i \leq r$, рассмотрим (непрерывные) конечномерные нормированные представления

$$\rho_i \colon W(k) \to \mathrm{GL}(d_i, \mathbb{C})$$

группы Вейля $W(k)$ поля k и отвечающие этим представлениям L - функции Вейля $L(\chi_i,\ s)$, $\chi_i := \mathrm{tr}\ \rho_i$ [166], [40]. Положим

$$L_i(s) := L(\chi_i, s),\ \vec{\chi} := (\chi_1, ..., \chi_r) \ \text{ и } \ L(\vec{\chi}, s) := (L_1 * \cdots * L_r)(s).$$

Не нарушая общности, предположим, что степени d_i представлений ρ_i удовлетворяют условию (1).

Теорема 1.1.2. *Если $d_1 = d_2 = r = 2$, то функция $s \mapsto L(\vec{\chi}, s)$ мероморфна на всей комплексной плоскости $\mathbb{C}$; в противном случае, эта функция мероморфна в полуплоскости $\mathbb{C}_0$, а прямая $\mathbb{C}^{(0)}$ является её естественной границей.*

Теорема 1 вытекает из более общей теоремы 2. Идея доказательства этих теорем, восходящая к классическим работам [110], [75], принадлежит Курокава [107], [108] (ср. [122]). Я докажу эти теоремы, следуя моим работам [123], [132], [133] (см. также [124], [127], [128]); важную роль в этом доказательстве играет доказанная в §4 теорема о распределении простых идеалов поля k. В работе [109] приводится несколько иное доказательство теоремы 2. В работе [131] изучаются суммы коэффициентов рядов Дирихле $L(\vec{\chi}, s)$ и $L(\vec{\psi}, s)$.

2. **Обозначения.** Обозначим через $\hat{G}$ или $G^{\perp}$ множество всех (непрерывных) конечномерных комплексных неприводимых характеров (топологической) группы G. При $\varphi \in \hat{G}$ зафиксируем неприводимое представление $\tilde{\varphi}$ группы G под условием $\operatorname{tr} \tilde{\varphi} = \varphi$ и заметим, что характер φ определяет представление $\tilde{\varphi}$ с точностью до эквивалентности [1, гл. VIII, §12, no.1, предложение 3]. Обозначим через

$$Y(G) := \{\sum_{\varphi \in \hat{G}} m(\varphi)\varphi | m : \hat{G} \to \mathbb{Z},\ |m^{-1}(\mathbb{Z} \setminus \{0\})| < \infty\}$$

группу (по сложению) виртуальных характеров группы G; положим

$$\sup \sum_{\varphi \in \hat{G}} m(\varphi)\varphi := m^{-1}(\mathbb{Z} \setminus \{0\}) \ \text{ при } \ \sum_{\varphi \in \hat{G}} m(\varphi)\varphi \in Y(G)$$

и

$$\varphi \prec a := \varphi \in \sup a \ \text{ при } \ a \in Y(G) \text{ и } \varphi \in \hat{G}.$$

Пусть H - подгруппа конечного индекса группы G; определим гомоморфизм

$$\operatorname{Ind}_H^G \colon Y(H) \to Y(G),$$

положив

$$\operatorname{Ind}_H^G \varphi := \operatorname{tr} \operatorname{Ind}_H^G \tilde{\varphi} \ \text{ при } \ \varphi \in \hat{H},$$

где $\operatorname{Ind}_H^G \tilde{\varphi}$ есть индуцированное представлением $\tilde{\varphi}$ представление группы G.

Определение 1.1.1. *Пусть $\chi \in Y(G)$; характер χ называется мономиальным характером, если*

$$(\exists \varphi \in Y(H))\ \chi = \mathrm{Ind}\ {}_H^G\varphi \ \ и \ \ \varphi(1) = 1$$

для некоторой подгруппы H группы G с $(G : H) < \infty$.

Определим эпиморфизм

$$g : Y(G) \to \mathbb{Z}, \ \text{ положив } \ g(1) = 1 \ \text{ и } \ g(\hat{G} \setminus \{1\}) = \{0\}.$$

По теореме двойственности Фробениуса (см., например, [128, стр. 12, предложение 1]),

$$g(\mathrm{Ind}\ {}_H^G\varphi) = g(\varphi) \ \text{ при } \ \varphi \in Y(H). \tag{1.1.2}$$

Пусть E - поле алгебраических чисел; положим

$$\Pi(E, x) := \{p | p \in \mathcal{P}(E),\ |p| < x\} \ \text{ при } \ x \in \mathbb{R}_+.$$

Определение 1.1.2. *Говорят, что бесконечный ряд (бесконечное произведение) компактно сходится на открытом подмножестве U комплексной плоскости $\mathbb{C}$, если этот ряд (это произведение) абсолютно сходится в каждой точке множества U и равномерно сходится на любом компактном подмножестве этого множества.*

1.2 К теории представлений компактных групп

1. Пусть G - компактная группа и μ - мера Хаара на G под условием $\mu(G) = 1$. В этом случае группа виртуальных характеров $Y(G)$ является кольцом. Пусть $\{\chi, \varphi\} \subseteq Y(G)$; если характеры χ и φ мономиальны, то существуют *мономиальные* характеры $\psi_1, ..., \psi_l$ группы G под условием

$$\chi\varphi = \sum_{i=1}^{l} \psi_i$$

(теорема Макки [115], ср. [128, стр. 15]). Напомним также, что кольцо виртуальных характеров $Y(G)$ *конечной* группы G порождается мономиальными характерами (теорема Брауэра, см., например, [37, часть II, §10]). Обозначим через $L^2(G)$ комплексное гильбертово пространство квадратично μ - интегрируемых функций $f : G \to \mathbb{C}$.

Пусть

$$P(t) \in Y(G)[t],\ P(t) = 1 + \sum_{j=1}^{l} a_j t^j. \tag{1.2.1}$$

При $g \in G$ положим

$$P_g(t) = 1 + \sum_{j=1}^{l} a_j(g) t^j = \prod_{j=1}^{l} (1 - \gamma_j(g)t) \tag{1.2.2}$$

с $\gamma_j(g) \in \mathbb{C}$ при $1 \leq j \leq l$, и пусть

$$\gamma(P) := \sup\{|\gamma_j(g)|\ |1 \leq j \leq l,\ g \in G\}.$$

Лемма 1.2.1. *Если* $P(t) \neq 1$, *то* $(\exists\, B(P) \in \mathbb{R})\ 1 \leq \gamma(P) \leq B(P)$.

Доказательство. Предположим, не нарушая общности, что $a_l \neq 0$. Из соотношений (1) и (2) следует, что

$$\gamma(P)^l \geq \prod_{j=1}^{l} |\gamma_j(g)| = |a_l(g)|.$$

Пусть

$$a_j = \sum_{\varphi \in \hat{G}} m_j(\varphi)\varphi,\ m_j(\varphi) \in \mathbb{Z}\ \text{ при }\ 1 \leq j \leq l.$$

Ясно, что

$$\gamma(P)^{2l} \geq \int\limits_G |a_l(g)|^2 d\mu(g) = \sum_{\varphi \in \hat{G}} m_l(\varphi)^2 \geq 1 \tag{1.2.3}$$

и, значит, $\gamma(P) \geq 1$. С другой стороны, если $P_g(\alpha^{-1}) = 0$ и $|\alpha| \geq 1$, то

$$\alpha^l + \sum_{j=1}^{l} a_j \alpha^{l-j} = 0,\ |\alpha| \leq \sum_{j=1}^{l} |a_j(g)| = \sum_{1 \leq j \leq l,\ \varphi \in \hat{G}} |m_j(\varphi)\varphi(g)| \leq B_1,$$

где

$$B_1 := \sum_{1\le j\le l,\ \varphi\in\hat{G}} |m_j(\varphi)|\varphi(1),$$

так как $|\varphi(g)| \le \varphi(1)$ при $g \in G$. Таким образом, $\gamma(P) \le B(P)$ при $B(P) := 1 + B_1$. Лемма доказана.

Пусть $P(t) \in Y(G)[t]$ и $P(0) = 1$; будем говорить, что полином $P(t)$ *унитарен*, если $\gamma(P) = 1$.

Следствие 1.2.1. *Полином $P(t)$ унитарен тогда и только тогда, когда*

$$(\forall g \in G)\ P_g(\alpha) \neq 0 \ \ при\ \ |\alpha| \neq 1,\ \alpha \in \mathbb{C}. \tag{1.2.4}$$

Доказательство. Ясно, что унитарность полинома $P(t)$ следует из условия (4). Обратно, пусть $\gamma(P) = 1$ и полином $P(t)$ удовлетворяет соотношению (2), тогда

$$|a_l(g)| = \prod_{j=1}^{l} |\gamma_j(g)| \le 1 \text{ при } g \in G. \tag{1.2.5}$$

Если, с другой стороны, $|\gamma_j(g_0)| < 1$ каких-либо j и g_0, то

$$|a_l(g_0)| < 1. \tag{1.2.6}$$

Из соотношений (5) и (6) следует однако неравенство

$$\int_G |a_l(g)|^2 d\mu(g) < 1,$$

противоречивающее неравенствам (3). Значит,

$$(\forall g \in G)\ |\gamma_j(g)| = 1 \text{ при } 1 \le j \le l.$$

Следствие доказано.

Лемма 1.2.2. *Пусть $A \in \mathrm{GL}(n, \mathbb{C})$ и предположим, что матрица A диагонализуема. Тогда*

$$\det (1 - tA)^{-1} = \sum_{m=1}^{\infty} t^m \mathrm{tr}\ (S^m A) \text{ и } \det (1 - tA) = \sum_{m=1}^{n} (-1)^m t^m \mathrm{tr}\ (\Lambda^m A),$$

где $S^m A$ и $\Lambda^m A$ суть m-ая симметрическая и внешняя степень матрицы A.

Доказательство. Это утверждение хорошо известно (см., например, [128, стр. 17, лемма 4]).

Следствие 1.2.2. *Пусть $\varphi \in \hat{G}$; тогда*

$$\det\,(1-t\tilde{\varphi})^b \in Y(G)[[t]] \text{ при } b \in \mathbb{Z}. \tag{1.2.7}$$

Доказательство. Поскольку матрицы $\tilde{\varphi}(g)$ при $g \in G$ диагонализуемы, соотношение (7) следует из леммы 2.

Предложение 1.2.1. *Пусть $P(t) \in Y(G)[t]$, $P(0) = 1$ и $P(t) \neq 1$. Тогда найдётся последовательность функций*

$$b_n \colon \hat{G} \to \mathbb{Z},\ n \in \mathbb{N}$$

под условием

$$|b_n^{-1}(\mathbb{Z} \setminus \{0\})| < \infty \text{ при } n \in \mathbb{N} \tag{1.2.8}$$

и таких, что

$$P(t) = \prod_{n=1}^{\infty} \prod_{\varphi \in \hat{G}} \det\,(1-t^n\tilde{\varphi})^{b_n(\varphi)} \ \text{ в } \ Y(G)[[t]]. \tag{1.2.9}$$

Более того, при $g \in G$ бесконечное произведение

$$P_g(t) = \prod_{n=1}^{\infty} \prod_{\varphi \in \hat{G}} \det\,(1-t^n\tilde{\varphi}(g))^{b_n(\varphi)} \tag{1.2.10}$$

абсолютно сходится в круге $|t| < \gamma(P)^{-1}$ и имеют место следующие неравенства:

$$|\sum_{\varphi \in \hat{G}} b_n(\varphi)\varphi(g)| \leq \frac{\tau(n)}{n}\, l\gamma(P)^n \tag{1.2.11}$$

и

$$\sum_{n \geq M} |\sum_{\varphi \in \hat{G}} \log\det\,(1-t^n\tilde{\varphi}(g))^{b_n(\varphi)}| \leq \frac{l(\gamma(P)|t|)^M}{(1-\gamma(P)|t|)^2} \ \text{ при } \ |t| < \gamma(P)^{-1}, \tag{1.2.12}$$

где $\tau(n) := |\{d | d \in \mathbb{N},\ d|n\}|$, $n \in \mathbb{N}$ и $l := \deg P(t)$.

Доказательство. Положим $F_0(t) = 1$ и $b_0 = 0$. Построим по индукции последовательности

$$b_n\colon \hat{G} \to \mathbb{Z},\ F_n(t) \in Y(G)[t],\ n \in \mathbb{N},$$

удовлетворяющие следующим условиям:

$$F_{n-1}(t) = P(t) \bmod t^n \ \text{ и } \ F_{n-1}(t) = \prod_{\nu=0}^{n-1} \prod_{\varphi\in\hat{G}} \det\,(1 - t^\nu\tilde{\varphi})^{b_\nu(\varphi)} \text{ при } n \in \mathbb{N},$$

положив

$$F_{n-1}(t) = (1 + bt^n)P(t) \bmod t^{n+1} \text{ с } b \in Y,\ b = \sum_{\varphi\in\hat{G}} b_n(\varphi)\varphi \text{ при } n \in \mathbb{N}.$$

Построенная таким образом последовательность $\{b_n\}$ удовлетворяет соотношениям (8) и (9). Не нарушая общности, предположим, что полином $P(t)$ удовлетворяет соотношениям (1) и (2) с $a_l \neq 0$. Применяя оператор

$$-t\frac{\partial}{\partial t}\log : Y(G)[[t]] \to Y(G)[[t]]$$

к обеим частям тождества

$$\prod_{j=1}^{l}(1 - \gamma_j t) = \prod_{n=1}^{\infty} \prod_{\varphi\in\hat{G}} \det\,(1 - t^n\tilde{\varphi})^{b_n(\varphi)}$$

и воспользовавшись соотношением $\log \circ \det\ = \mathrm{tr}\ \circ \log$, легко находим

$$\sum_{j=1}^{l} \frac{t\gamma_j}{(1 - t\gamma_j)} = \sum_{n=1}^{\infty} \sum_{\varphi\in\hat{G}} nb_n \mathrm{tr}\ (t^n\tilde{\varphi}(1 - t^n\tilde{\varphi})^{-1}) \ \text{ в } \ Y(G)[[t]]. \tag{1.2.13}$$

Положим

$$\sigma(m, g) := \sum_{j=1}^{l} \gamma_j(g)^m \ \text{ и } \ h_n(g) := n \sum_{\varphi\in\hat{G}} b_n(\varphi)\varphi(g) \ \text{ при } \ g \in G.$$

Соотношение (13) даёт:

$$\sum_{m=1}^{\infty} t^m\sigma(m, g) = \sum_{m,n=1}^{\infty} t^{mn}h_n(g^m) \ \text{ в } \ \mathbb{C}[[t]],$$

или

$$\sigma(m,g)=\sum_{mm'=n} h_n(g^{m'}) \text{ при } n\in\mathbb{N},\ g\in G.$$

Применяя формулу обращения Мёбиуса, получим

$$h_n(g)=\sum_{mm'=n}\mu(m)\sigma(m',g^m) \text{ при } n\in\mathbb{N},\ g\in G. \tag{1.2.14}$$

Так как $|\sigma(n,g)|\le l\gamma(P)^n$ при $n\in\mathbb{N}$ и $g\in G$, неравенство (11) следует из тождества (14). Оценка (12) легко выводится из (11) и упомянутого выше соотношения $\log\circ\det = \mathrm{tr}\circ\log$, а сходимость произведения (10) круге $|t|<\gamma(P)^{-1}$ следует из неравенства (12). Предложение доказано.

Следствие 1.2.3. *Сохраняя обозначения и условия предложения 1, предположим, что полином $P(t)$ унитарен. Тогда*

$$(\exists N\in\mathbb{N})\ b_n(\varphi)=0 \text{ при } n>N$$

и потому

$$P(t)=\prod_{n=1}^{N}\prod_{\varphi\in\hat{G}}\det\,(1-t^n\tilde{\varphi})^{b_n(\varphi)} \text{ в } Y(G)[[t]]. \tag{1.2.15}$$

Доказательство. Так как, по предположению, $\gamma(P)=1$, из неравенства (11) и соотношений ортогональности следует, что

$$\sum_{\varphi\in\hat{G}} b_n(\varphi)^2=\int\limits_G|\sum_{\varphi\in\hat{G}} b_n(\varphi)\varphi(g)|^2 d\mu(g)\to 0 \text{ при } n\to\infty$$

и, значит, $(\exists N\in\mathbb{N})\ b_n(\varphi)=0$ при $n>N$, ибо $b_n(\hat{G})\subseteq\mathbb{Z}$ при $n\in\mathbb{N}$. Утверждение доказано.

2. Пусть теперь группа G является расширением конечной группы H вещественным n-мерным тором $\mathcal{T}$, так что имеет место точная последовательность (топологических) групп

$$1\to\mathcal{T}\to G\xrightarrow{j} H\to 1,$$

где

$$\mathcal{T} := \{z | z \in \mathbb{C}^n,\ |z_j| = 1 \text{ при } 1 \leq j \leq n\}$$

и $|H| < \infty$. Положим

$$G = \bigcup_{h \in H} \mathcal{T}\gamma_h,\ \gamma_1 = 1.$$

Обозначим через $[G]$ множество классов сопряжённых элементов группы G, введём в рассмотрение счётное множество Π и две функции

$$\sigma \colon \Pi \to [G],\ p \mapsto \sigma_p \text{ при } p \in \Pi$$

и

$$|\cdot| \colon \Pi \to \mathbb{R}_+^*.$$

Положим

$$\Pi(x) := \{p | p \in \Pi,\ |p| < x\} \text{ при } x \in \mathbb{R}_+^*$$

и пусть

$$\mathcal{N}(\mathcal{A}, x) := \text{card } \{p | p \in \Pi(x),\ \sigma_p \cap \mathcal{A} \neq \emptyset\} \tag{1.2.16}$$

при $\mathcal{A} \subseteq G$ и $x \in \mathbb{R}_+^*$. Определим метрику

$$\rho \colon G \times G \to \mathbb{R}_+^* \cup \{\infty\}$$

на группе G, положив

$$\rho(g_1, g_2) = \infty \text{ при } j(g_1) \neq j(g_2) \text{ и } \rho(g_1, g_2) = \rho_0(g_1 g_2^{-1}, 1) \text{ при } j(g_1) = j(g_2),$$

где $\{g_1, g_2\} \subseteq G$ и ρ_0 - естественная инвариантная метрика на торе $\mathcal{T}$.

Определение 1.2.1. *Назовём подмножество $\mathcal{A}$ группы G инвариантным, если*

$$(\forall\, \tau \in G)\ \tau^{-1}\mathcal{A}\tau = \mathcal{A};$$

функция $f \colon G \to \mathbb{C}$ называется инвариантной, если

$$(\forall\, \{x, \tau\} \subseteq G)\ f(\tau^{-1}x\tau) = f(x).$$

Обозначим через $I(G)$ множество инвариантных функций на группе G, положим

$$L_0^2(G) := L^2(G) \cap I(G)$$

и заметим, что элементы множества $\hat{G}$ образуют ортонормированный базис пространства $L_0^2(G)$. Обозначим через $C^\infty(G)$ множество комплекснозначных бесконечно дифференцируемых функций на G и положим

$$C_0^\infty(G) := C^\infty(G) \cap I(G);$$

ясно, что $C_0^\infty(G) \subseteq L_0^2(G)$. При $a \in [G],\ g \in a$ и $f \in I(G)$ положим $f(a) := f(g)$.

Пусть $x \in G$ и $\mathcal{B} \subseteq G$; положим

$$\rho(x, \mathcal{B}) := \inf\{\rho(x, y) | y \in \mathcal{B}\}.$$

Ясно, что $\rho(x, \mathcal{B}) \leq \rho(x, \bar{\mathcal{B}})$. Так как множество $\bar{\mathcal{B}}$ компактно,

$$\rho(x, \bar{\mathcal{B}}) = \min\{\rho(x, y) | y \in \bar{\mathcal{B}}\}. \tag{1.2.17}$$

Пусть

$$\rho(x, \bar{\mathcal{B}}) = \rho(x, y_0),\ y_0 \in \bar{\mathcal{B}},\ \{y_n | n \in \mathbb{N}\} \subseteq \mathcal{B} \text{ и } y_n \to y_0 \text{ при } n \to \infty,$$

тогда

$$\rho(x, y_n) \to \rho(x, y_0) \text{ при } n \to \infty \text{ и } (\forall\, n \in \mathbb{N})\ \rho(x, y_n) \geq \rho(x, y_0).$$

Значит,

$$\rho(x, y_0) = \inf\{\rho(x, y_n) | n \in \mathbb{N}\} \geq \inf\{\rho(x, y) | y \in \mathcal{B}\} = \rho(x, \mathcal{B}).$$

Таким образом,

$$\rho(x, \mathcal{B}) = \rho(x, \bar{\mathcal{B}}). \tag{1.2.18}$$

Из соотношений (17) и (18) следует, что

$$\rho(x, \mathcal{B}) = 0 \Leftrightarrow x \in \bar{\mathcal{B}}.$$

Пусть $\rho(x, \mathcal{B}) = a,\ a \in \mathbb{R}_+^*$; тогда, в силу (17) и (18),

$$(\exists\ y_0 \in \bar{\mathcal{B}})\ \rho(x, y_0) = a.$$

Обозначим через $[y_0, x]$ отрезок геодезической, соединяющий точки y_0 и x. Пусть $y_1 \in [y_0, x] \cap \partial\mathcal{B}$ и $y_1 \neq y_0$, тогда

$$\rho(y_1, x) < \rho(y_0, x) = \rho(x, \mathcal{B}),$$

что невозможно, значит $y_1 = y_0$, то-есть, $y_0 \in \partial\mathcal{B}$ и потому $\rho(x, \partial\mathcal{B}) = a$. Отсюда следует, что

$$x \notin \mathcal{B} \Rightarrow \rho(x, \mathcal{B}) = \rho(x, \partial\mathcal{B}). \tag{1.2.19}$$

Положим

$$U_\delta(\mathcal{B}) := \{x | x \in G,\ \rho(x, \mathcal{B}) < \delta\} \text{ и } V_\delta(\mathcal{B}) := \bigcap_{g \in G} g^{-1} U_\delta(\mathcal{B}) g$$

при $\mathcal{B} \subseteq G$ и $\delta > 0$. При любых $\mathcal{B} \subseteq G$ и $\delta > 0$ множество $U_\delta(\mathcal{B})$ является открытым подмножеством группы G, а множество $V_\delta(\mathcal{B})$ - инвариантным подмножеством этой группы. Легко видеть, что

$$V_\delta(\mathcal{B}) = \bigcap_{h \in H} \gamma_h^{-1} U_\delta(\mathcal{B}) \gamma_h. \tag{1.2.20}$$

Действительно, пусть

$$g \in \bigcap_{h \in H} \gamma_h^{-1} U_\delta(\mathcal{B}) \gamma_h,\ \tau \in G,\ \tau = u\gamma_h \ \text{ с } \ u \in \mathcal{T},$$

положим $g_1 := \tau g \tau^{-1}$, тогда

$$(\exists\ g_2 \in U_\delta(\mathcal{B}))\ g = \gamma_h^{-1} g_2 \gamma_h,$$

так что

$$\gamma_h^{-1} g_2 \gamma_h = \tau^{-1} g_1 \tau = \gamma_h^{-1} u^{-1} g_1 u \gamma_h,\ g_2 = u^{-1} g_1 u,\ g_1 = u g_2 u^{-1} = g_2,$$

ибо $\{g_2, u\} \subseteq \mathcal{T}$, и, значит,

$$g_1 \in U_\delta(\mathcal{B}),\ g \in \tau^{-1} U_\delta(\mathcal{B}) \tau,\ \bigcap_{h \in H} \gamma_h^{-1} U_\delta(\mathcal{B}) \gamma_h \subseteq V_\delta(\mathcal{B});$$

обратное включение

$$V_\delta(\mathcal{B}) \subseteq \bigcap_{h \in H} \gamma_h^{-1} U_\delta(\mathcal{B}) \gamma_h$$

очевидно.

Следствие 1.2.4. *Множество $V_\delta(\mathcal{B})$ открыто (при любых $\mathcal{B} \subseteq G$ и $\delta > 0$).*

Доказательство. Так как конечное пересечение открытых множеств открыто, доказываемое утверждение следует из равенства (20).

Более того, из соотношений (18) и (19) следует, что

$$U_\delta(\mathcal{B}) \setminus \mathcal{B} := \{x | x \in G \setminus \mathcal{B},\ \rho(x, \mathcal{B}) < \delta\} = \{x | x \in G \setminus \mathcal{B},\ \rho(x, \partial\mathcal{B}) < \delta\} \subseteq$$

$$\{x | x \in G,\ \rho(x, \partial\mathcal{B}) < \delta\} = U_\delta(\partial\mathcal{B}) \text{ и } U_\delta(\partial\mathcal{B}) \subseteq U_\delta(\mathcal{B}).$$

Таким образом,

$$U_\delta(\mathcal{B}) = \mathcal{B} \cup U_\delta(\partial\mathcal{B}). \tag{1.2.21}$$

Лемма 1.2.3. *Предположим, что подмножество $\mathcal{A}$ группы G является инвариантным. Тогда*

$$V_\delta(\mathcal{A}) = \mathcal{A} \cup V_\delta(\partial\mathcal{A}), \tag{1.2.22}$$

и

$$\beta \in \mathcal{A} \cap \gamma V_\delta(\{1\}) \Rightarrow \gamma \in V_\delta(\mathcal{A}) \ \ \textit{при}\ \ \{\beta, \gamma\} \subseteq G. \tag{1.2.23}$$

Доказательство. Ввиду (21), имеем

$$V_\delta(\mathcal{B}) = \bigcap_{g \in G} g^{-1} U_\delta(\mathcal{A}) g = \bigcap_{g \in G} g^{-1} (\mathcal{A} \cup U_\delta(\partial\mathcal{A})) g = \bigcap_{g \in G} (g^{-1} \mathcal{A} g \cup g^{-1} U_\delta(\partial\mathcal{A}) g)$$

$$= \bigcap_{g\in G}(\mathcal{A}\cup g^{-1}U_\delta(\partial\mathcal{A})g) = \mathcal{A}\cup(\bigcap_{g\in G}(g^{-1}U_\delta(\partial\mathcal{A})g) = \mathcal{A}\cup V_\delta(\partial\mathcal{A}).$$

Тем самым, доказано равенство (22). Пусть

$$g\in G,\ \beta\in\mathcal{A} \text{ и } \gamma^{-1}\beta\in V_\delta(\{1\}),$$

тогда

$$\rho(g^{-1}\gamma g, g^{-1}\beta g) = \rho_0(g^{-1}\gamma^{-1}\beta g, 1) < \delta$$

и, значит, $\rho(g^{-1}\gamma g,\mathcal{A})<\delta$, так как $g^{-1}\beta g\in\mathcal{A}$ в силу инвариантности множества $\mathcal{A}$. Таким образом,

$$(\forall\ g\in G)\ g^{-1}\gamma g\in U_\delta(\mathcal{A})$$

и, следовательно, $\gamma\in V_\delta(\mathcal{A})$. Лемма доказана.

Ясно, что

$$\hat{\mathcal{T}} = \{\prod_{j=1}^{n}\xi_j^{m_j}|m\in\mathbb{Z}^n\},$$

где

$$\xi_j\colon\hat{\mathcal{T}}\to\mathbb{C},\ \xi_j\colon z\mapsto z_j \text{ при } 1\le j\le n.$$

Определим функцию $w\colon\hat{G}\to\mathbb{N}$, положив

$$w(\prod_{j=1}^{n}\xi_j^{m_j}) := \max\{|m_j|+1|1\le j\le n\} \text{ при } m\in\mathbb{Z}^n$$

и

$$w(\chi) := \max\{w(\lambda_i)|1\le i\le l\}$$

при

$$\chi\in\hat{G},\ l:=\chi(1),\ \chi|_{\mathcal{T}} = \sum_{i=1}^{l}\lambda_i,\ \text{ с } \{\lambda_i|1\le i\le l\}\subseteq\hat{\mathcal{T}}$$

и заметим, что

$$\lambda\prec\chi|_{\mathcal{T}}\Leftrightarrow\chi\prec\operatorname{Ind}\tfrac{G}{\mathcal{T}}\lambda \text{ при } \lambda\in\hat{\mathcal{T}} \text{ и } \chi\in\hat{G}, \tag{1.2.24}$$

см., например, [128, стр. 12, предложение 1].

Определение 1.2.2. *Пусть* $\alpha \in \mathbb{R}_+$. *Измеримое подмножество* $\mathcal{A}$ *группы* G *называется* α*-гладким, если*

$$(\exists\, C(\mathcal{A}))\ \mu(U_\delta(\partial\mathcal{A})) < C(\mathcal{A})\delta^\alpha \ \ \textit{при}\ \ 0 < \delta < 1. \tag{1.2.25}$$

Предложение 1.2.2. *Пусть функции*

$$B\colon \mathbb{R}_+ \to \mathbb{R},\ b\colon \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R},\ b_1\colon \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}_+$$

удовлетворяют следующим условиям:

$$B(x) > 1,\ b(x,y) > 1,\ \sum_{m=1}^{\infty} b(x,m)m^{-\nu} = b_1(x,\nu) \ \ \textit{при}\ \ \{x, y, \nu - 1\} \subseteq \mathbb{R}_+$$

и

$$(\forall\, \chi \in \hat{G}) \sum_{p\in\Pi(x)} \chi(\sigma_p) = g(\chi)B(x) + O(b(x, w(\chi)) \ \ \textit{при}\ \ x \to \infty. \tag{1.2.26}$$

Тогда для любого инвариантного α*-гладкого подмножества* $\mathcal{A}$ *группы* G *имеет место асимптотическая формула*

$$\mathcal{N}(\mathcal{A}, x) =$$

$$\mu(\mathcal{A})B(x) + O(C(\mathcal{A})b_1(x, \nu - n + 1)^{\alpha(\alpha+2n\nu)^{-1}} B(x)^{2n\nu(\alpha+2n\nu)^{-1}}) \tag{1.2.27}$$

при $\nu \geq n$ *и* $x \to \infty$.

Доказательство. Пусть $0 < \delta < 1/4$. Определим следующие функции:

$$f_0\colon \mathbb{R}_+ \to [0,1],\ f_0(t) = \begin{cases} \exp(t(t-1)^{-1}) & \text{при } 0 \leq t < 1 \\ 0 & \text{при } t \geq 1, \end{cases}$$

$$f_\delta\colon \mathcal{T} \to [0,1],\ f_\delta(z) = f_0(\delta^{-2}|\varphi|^2) \ \text{ при } \ z \in \mathcal{T},$$

где $\varphi \in \mathbb{R}^n,\ z_j = \exp(2\pi i\varphi_j)$ и $-1/2 < \varphi_j \leq 1/2$ при $1 \leq j \leq n$. Положим

$$\psi_\delta^{(1)}\colon G \to [0,1],\ \psi_\delta^{(1)}(z) = f_\delta(z) \text{ при } z \in \mathcal{T} \ \text{ и } \ \psi_\delta^{(1)}(G \setminus \mathcal{T}) = \{0\}$$

и

$$\psi_\delta\colon G \to [0,1],\ \psi_\delta(g) = \frac{1}{|H|} \sum_{h\in H} \psi_\delta^{(1)}(\gamma_h^{-1} g \gamma_h) \ \text{ при } \ g \in G.$$

Ясно, что

$$\psi_\delta \in C_0^\infty(G) \ \text{ и } \ \psi_\delta(G \setminus V_\delta(\{1\})) = \{0\}.$$

Положим

$$J_\delta := \int\limits_G \psi_\delta(g) d\mu(g)$$

и заметим, что

$$J_\delta = c_0 \delta^n \ \text{ с } \ c_0 > 0, \tag{1.2.28}$$

ибо

$$J_\delta = \frac{1}{|H|} \sum_{h \in H} \int\limits_G \psi_\delta^{(1)}(\gamma_h^{-1} g \gamma_h) d\mu(g) = \int\limits_G \psi_\delta^{(1)}(g) d\mu(g) = \int\limits_{\mathcal{T}} f_\delta(z) d\mu(z) =$$

$$\int\limits_{\mathcal{T}} f_0(\delta^{-2}|\varphi|^2) d\mu(z) = \int\limits_{\delta K_n} f_0(|\varphi/\delta|^2) d\varphi = c_0 \delta^n,$$

где $K_n := \{x | x \in \mathbb{R}^n, \ |x| \le 1\}$ и $c_0 := \int\limits_{K_n} f_0(|x|^2) dx > 0$.

Обозначим через

$$f[\mathcal{B}] \colon G \to \{0,1\}, \ f[\mathcal{B}](g) = 1 \Leftrightarrow g \in \mathcal{B} \text{ при } g \in G,$$

характеристическую функцию подмножества $\mathcal{B}$ группы G; положим

$$f_+ := f[V_\delta(\mathcal{A})] \ \text{ и } \ f_- := f[\mathcal{A} \setminus V_\delta(\partial \mathcal{A})].$$

Определим функции

$$g_\pm \colon G \to [0,1], \ g_\pm(\beta) := \int\limits_G f_\pm(\gamma) \psi_\delta(\gamma^{-1}\beta) d\mu(\gamma) \ \text{ при } \ \beta \in G$$

и заметим, что

$$g_\pm(h^{-1}\beta h) = \int\limits_G f_\pm(\gamma) \psi_\delta(\gamma^{-1} h^{-1} \beta h) d\mu(\gamma) =$$

$$\int\limits_G f_\pm(\gamma) \psi_\delta((h^{-1}\gamma h)^{-1}\beta) d\mu(\gamma) = g_\pm(\beta) \ \text{ при } \ \{\beta, \gamma\} \subseteq G,$$

так как $\{f_\pm, \psi_\delta\} \subseteq I(G)$. Значит, $g_\pm \in C_0^\infty(G)$ и потому

$$g_\pm = \sum_{\chi \in \hat{G}} c_\pm(\chi)\chi, \text{ где } c_\pm(\chi) = \int\limits_G g_\pm(\beta)\overline{\chi(\beta)}d\mu(\beta). \tag{1.2.29}$$

Из соотношения (29), в частности, следует, что

$$c_\pm(1) = \int\limits_G g_\pm(\beta)d\mu(\beta) = \int\limits_{G\times G} f_\pm(\gamma)\varphi_\delta(\gamma^{-1}\beta)d\mu(\gamma)d\mu(\beta).$$

Но

$$\int\limits_G \varphi_\delta(\gamma^{-1}\beta)d\mu(\beta) = J_\delta,$$

так что

$$c_\pm(1) = J_\delta \int\limits_G f_\pm(\gamma)d\mu(\gamma),\ c_+(1) = J_\delta\ \mu(V_\delta(\mathcal{A})) \text{ и } c_-(1) = J_\delta\ \mu(\mathcal{A} \setminus V_\delta(\partial\mathcal{A})).$$

В силу равенства (22),

$$\mu(V_\delta(\mathcal{A})) = \mu(\mathcal{A} \cup V_\delta(\partial\mathcal{A})) \le \mu(\mathcal{A}) + \mu(V_\delta(\partial\mathcal{A}));$$

таким образом,

$$\mu(\mathcal{A}) \le J_\delta^{-1}c_+(1) \le \mu(\mathcal{A}) + \mu(V_\delta(\partial\mathcal{A}))$$

и

$$\mu(\mathcal{A}) - \mu(V_\delta(\partial\mathcal{A})) \le J_\delta^{-1}c_-(1) \le \mu(\mathcal{A}).$$

Так как, по условию, множество $\mathcal{A}$ является α-гладким, отсюда следует, что

$$J_\delta^{-1}c_\pm(1) = \mu(\mathcal{A}) + O(\mu(V_\delta(\partial\mathcal{A}))) = \mu(\mathcal{A}) + O(C(\mathcal{A})\delta^\alpha). \tag{1.2.30}$$

Заметим также, что

$$g_-(\beta) \le J_\delta \text{ при } \beta \in G, \tag{1.2.31}$$

$$g_+(\beta) = J_\delta \text{ при } \beta \in \mathcal{A} \text{ и } g_-(\beta) = 0 \text{ при } \beta \in G \setminus \mathcal{A}. \tag{1.2.32}$$

Действительно,

$$g_-(\beta) \le \int\limits_G \psi_\delta(\gamma^{-1}\beta)d\mu(\gamma) = J_\delta.$$

Пусть $\beta \in \mathcal{A}$, тогда

$$g_+(\beta) = \int\limits_G f_+(\gamma)\psi_\delta(\gamma^{-1}\beta)d\mu(\gamma) = \int\limits_G \psi_\delta(\gamma^{-1}\beta)d\mu(\gamma) = J_\delta,$$

так как, с одной стороны, из $\psi_\delta(\gamma^{-1}\beta) \neq 0$ следует, что $\gamma^{-1}\beta \in V_\delta(\{1\})$ и, значит, в силу леммы 3, $\gamma \in V_\delta(\mathcal{A})$, ибо $\beta \in \mathcal{A}$, а, с другой стороны, $f_+(\mathcal{A}) = 1$. Наконец, пусть

$$\beta \in G \setminus \mathcal{A} \ \text{ и } \ \mathcal{B} := V_\delta(G \setminus \mathcal{A}) \cap (\mathcal{A} \setminus V_\delta(\partial\mathcal{A})),$$

тогда

$$g_-(\beta) = \int\limits_G f_-(\gamma)\psi_\delta(\gamma^{-1}\beta)d\mu(\gamma) = \int\limits_{\mathcal{B}} \psi_\delta(\gamma^{-1}\beta)d\mu(\gamma),$$

так как из $\psi_\delta(\gamma^{-1}\beta) \neq 0$ следует, что $\gamma^{-1}\beta \in V_\delta(\{1\})$ и, значит, в силу леммы 3, $\gamma \in V_\delta(G \setminus \mathcal{A})$, ибо $\beta \in G \setminus \mathcal{A}$. С другой стороны, из соотношения (22) вытекает, что

$$V_\delta(G \setminus \mathcal{A}) \cap (\mathcal{A} \setminus V_\delta(\partial\mathcal{A})) = ((G \setminus \mathcal{A}) \cup V_\delta(\partial(G \setminus \mathcal{A}))) \cap (\mathcal{A} \setminus V_\delta(\partial\mathcal{A})) =$$

$$V_\delta(\partial(G \setminus \mathcal{A}))) \cap (\mathcal{A} \setminus V_\delta(\partial\mathcal{A})) = V_\delta(\partial\mathcal{A})) \cap (\mathcal{A} \setminus V_\delta(\partial\mathcal{A})) = \emptyset,$$

значит, $\mathcal{B} = \emptyset$ и $g_-(\beta) = 0$.

Так как $\mathcal{A} \in I(G)$ из определения (16) следует, что

$$\mathcal{N}(\mathcal{A}, x) = \sum_{p \in \Pi(x)} \sum_{\sigma_p \subseteq \mathcal{A}} 1$$

и потому, ввиду соотношений (30) и (31),

$$\sum_{p \in \Pi(x)} g_-(\sigma_p) \leq J_\delta\, \mathcal{N}(\mathcal{A}, x) \leq \sum_{p \in \Pi(x)} g_+(\sigma_p).$$

Из этих неравенств, соотношения (29) и соотношения (30) вытекает, что

$$\mathcal{N}(\mathcal{A}, x) = \mu(\mathcal{A})B(x) + O(B(x)C(\mathcal{A})\delta^\alpha) + O(|S_\pm(\mathcal{A}, x)|), \qquad (1.2.33)$$

где

$$S_{\pm}(\mathcal{A},x) := J_{\delta}^{-1} \sum_{\chi\in\hat{G}\setminus\{1\}} c_{\pm}(\chi) \sum_{p\in\Pi(x)} \chi(\sigma_p).$$

Соотношение (26) даёт:

$$S_{\pm}(\mathcal{A},x) \ll J_{\delta}^{-1} \sum_{\chi\in\hat{G}\setminus\{1\}} |c_{\pm}(\chi)| b(x,w(\chi)) \text{ при } x\to\infty. \tag{1.2.34}$$

Положим

$$A_m := \{\chi|\chi\in\hat{G},\ w(\chi)=m\}.$$

Пусть $m\in\mathbb{N},\ \chi\in A_m$ и $\chi|\tau = \sum_{i=1}^{l}\lambda_i$; из соотношения (29) следует тогда, что

$$\overline{c_{\pm}(\chi)} = \frac{1}{|H|}\sum_{h\in H}\int\limits_{\mathcal{T}} g_{\pm}(\alpha\gamma_h)(\sum_{i=1}^{l}\lambda_i(\alpha\gamma_h))d\mu(\alpha),$$

откуда, интегрируя ν раз по частям и рассуждая также, как и при выводе равенства (28), получим оценку

$$c_{\pm}(\chi) = O_{\nu}(J_{\delta}\delta^{-2n\nu}m^{-\nu}) \text{ при } \nu\in\mathbb{N}. \tag{1.2.35}$$

Из соотношений (34) и(35) следует, что

$$S_{\pm}(\mathcal{A},x) \ll_{\nu} \delta^{-2n\nu}\sum_{m=1}^{\infty} b(x,m)|A_m|m^{-\nu} \text{ при } \nu\in\mathbb{N} \text{ и } x\to\infty.$$

Но $|A_m| \ll m^{n-1}$, как легко вывести из соотношения (24), и, значит,

$$S_{\pm}(\mathcal{A},x) \ll_{\nu} \delta^{-2n\nu} b_1(x,\nu-n+1)| \text{ при } \nu\geq n \text{ и } x\to\infty. \tag{1.2.36}$$

Формула (27) вытекает из соотношений (33) и (36) при

$$\delta = (b_1(x,\nu-n+1)B(x)^{-1})^{1/(\alpha+2n\nu)}.$$

Предложение 2 доказано.

Пусть $\mathfrak{N}\subseteq\hat{G},\ g_0\in G$ и $0<u<1$. Положим

$$\mathcal{A}(\mathfrak{N};u,g_0) := \{g|g\in G,\ (\forall\chi\in\mathfrak{N})\ |\chi(g)-\chi(g_0)|<u\}.$$

Лемма 1.2.4. *Предположим, что множество* $\mathfrak{N}$ *конечно. Тогда*

$$(\exists\, c_1(\mathfrak{N}) \in \mathbb{R})\ \mu(U_\delta(\partial\mathcal{A}(\mathfrak{N}; u, g_0))) < c_1(\mathfrak{N})\delta \ \ \textit{при}\ \ 0 < \delta < 1. \tag{1.2.37}$$

Доказательство. Ясно, что

$$\mathcal{A}(\mathfrak{N}; u, g_0) = \bigcap_{\chi\in\mathfrak{N}} \mathcal{A}(\{\chi\}; u, g_0) \tag{1.2.38}$$

и

$$\mathcal{A}(\{\chi\}; u, g_0) = \bigcup_{h\in H} \{\alpha\gamma_h | \alpha \in \mathcal{B}(h)\} \tag{1.2.39}$$

с

$$\mathcal{B}(h) := \{\alpha | \alpha \in \mathcal{T},\ |\chi(\alpha\gamma_h) - \chi(g_0)| < u\}.$$

Полагая

$$\tilde{\chi}(g) = (r_{ik}(g))_{1\le i,k\le l},$$

легко находим

$$\chi(\alpha\gamma_h) = \sum_{j=1}^{l} \lambda_j(\alpha) r_{jj}(\gamma_h) \ \text{ с } \ \lambda_j(\alpha) = \prod_{\nu=1}^{n} \alpha_\nu^{m_{j\nu}},\ m_{j\nu} \in \mathbb{Z}$$

при $1 \le j \le l,\ 1 \le \nu \le n$ и $\alpha \in \mathcal{T}$, так что

$$\mathcal{B}(h) = \{(x,y) | (x,y) \in \mathcal{T},\ |\sum_{j=1}^{l} r_{jj} \prod_{\nu=1}^{n} (x_\nu + iy_\nu)^{m_{j\nu}} - \chi(g_0)|^2 < u^2\} \tag{1.2.40}$$

и

$$\mathcal{T} = \{(x,y) | \{x,y\} \subseteq \mathbb{R}^n,\ x_\nu^2 + y_\nu^2 = 1 \ \text{ при } \ 1 \le \nu \le n\}.$$

Соотношения (38) - (40) показывают, что вычисление меры

$$\mu(U_\delta(\partial\mathcal{A}(\mathfrak{N}; u, g_0)))$$

сводится к вычислению объёма полуалгебраического подмножества пространства $\mathbb{R}^{2n}$; поэтому соотношение (37) следует из теорем И.Н. Иомдина [169, следствие 4.5], [170, теорема 5.6].

Лемма 1.2.5. *Предположим, что множество* $\mathfrak{N}$ *конечно. Тогда*

$$(\exists\, c_2(\mathfrak{N}) \in \mathbb{R}_+^*)\mu(\mathcal{A}(\mathfrak{N}; u, g_0)) \geq c_2(\mathfrak{N})u^n. \tag{1.2.41}$$

Доказательство. Пусть $0 < u_1 < 1$; положим

$$\mathcal{B}(u_1) := \{\alpha | \alpha \in \mathcal{T},\ |\alpha_\nu - 1| < u_1 \ \text{ при } \ 1 \leq \nu \leq n\}.$$

Ясно, что

$$(\exists\, c_3(n) \in \mathbb{R}_+^*)\ \mu(\mathcal{B}(u_1)) \geq c_3(n)\mu(\mathcal{T})u_1^n. \tag{1.2.42}$$

Положим

$$\tilde{\chi}(g) = (r_{ik\chi}(g))_{1 \leq i,k \leq \chi(1)}$$

и

$$\chi|\tau = \sum_{j=1}^{\chi(1)} \lambda_{j\chi}, \ \text{ с } \ \lambda_{j\chi}(\alpha) = \prod_{\nu=1}^{n} \alpha_\nu^{m_{j\nu}(\chi)},\ m_{j\nu}(\chi) \in \mathbb{Z}$$

при $\chi \in \hat{G},\ \alpha \in \mathcal{T},\ g \in G,\ 1 \leq j \leq l,\ 1 \leq \nu \leq n$; так как группа G компактна, не нарушая общности, можно предполагать, что представления $\check{\chi}$ унитарны и потому

$$|r_{ik\chi}(g)| \leq 1 \ \text{ при } \ 1 \leq i,k \leq \chi(1),\ \chi \in \hat{G},\ g \in G. \tag{1.2.43}$$

Положим

$$\mathcal{B}_1(u_2, \mathfrak{N}) := \{\alpha | \alpha \in \mathcal{T},\ |\lambda_{j\chi}(\alpha) - 1| < u_2 \ \text{ при } \ 1 \leq j \leq \chi(1),\ \chi \in \mathfrak{N}\}$$

и

$$c_4(\mathfrak{N}) := \max\{\chi(1) | \chi \in \mathfrak{N}\}.$$

Из неравенства (43) следует, что

$$|\chi(\alpha g_0) - \chi(g_0)| = |\sum_{j=1}^{\chi(1)} r_{jj\chi}(g_0)(\lambda_{j\chi}(\alpha) - 1)| \leq \chi(1)u_2 \leq c_4(\mathfrak{N})u_2$$

при $\alpha \in \mathcal{B}_1(u_2, \mathfrak{N})$ и $\chi \in \mathfrak{N}$; значит, ввиду (38) и (39),

$$\{\alpha g_0 | \alpha \in \mathcal{B}_1(c_4(\mathfrak{N})^{-1}u, \mathfrak{N})\} \subseteq \mathcal{A}(\mathfrak{N}; u, g_0) \ \text{ при } \ 0 < u < 1.$$

Таким образом,

$$\mu(\mathcal{A}(\mathfrak{N};u,g_0)) \geq \mu(\mathcal{B}_1(c_4(\mathfrak{N})^{-1}u,\mathfrak{N})) \text{ при } 0<u<1. \tag{1.2.44}$$

С другой стороны, по построению,

$$(\exists\, c_5(\mathfrak{N}) \in \mathbb{R}_+^*)\ \mathcal{B}(c_5(\mathfrak{N})u) \subseteq \mathcal{B}_1(u,\mathfrak{N})$$

и потому

$$\mu(\mathcal{B}_1(u,\mathfrak{N})) \geq \mathcal{B}(c_5(\mathfrak{N})u) \text{ при } 0<u<1. \tag{1.2.45}$$

Доказываемое неравенство (41) следует из неравенств (42), (44) и (45).

1.3 О полиномах над кольцом характеров группы Вейля и связанных с ними L - функциях

1. Пусть k - поле алгебраических чисел. Группа Вейля $W(E|k)$ конечного нормального расширения $E|k$ есть расширение группы Галуа $\mathrm{Gal}(E|k)$ группой классов иделей $C(E)$ поля E, отвечающее каноническому классу когомологий теории полей классов; это групповое расширение определяет точную последовательность (топологических) групп

$$1 \to C(E) \to W(E|k) \to \mathrm{Gal}(E|k) \to 1.$$

Группа Вейля $W(k)$ поля k определяется как проективный предел

$$W(k) = \varprojlim W(E|k)$$

групп Вейля $W(E|k)$ конечных нормальных расширений $E|k$; при этом

$$\mathrm{Gal}(E|k) \cong W(k)/W(E),\ \ W(E|k) \cong W(k)/W(E)^c$$

и

$$C(E) \cong W(E)/W(E)^c,$$

где $W(E)^c$ есть замыкание коммутатора группы $W(E)$. Любое непрерывное представление

$$\rho\colon W(k) \to \mathrm{GL}(V),\ (\exists\, d \in \mathbb{N})\ V \cong \mathbb{C}^d, \tag{1.3.1}$$

пропускается через группу $W(E|k)$ для некоторого конечного нормального расширения $E|k$ и, значит, для любого конечного нормального расширения $E_1|k$ с $E \subseteq E_1$ (см. [166], [40]). Как известно,

$$C(E) \cong \mathbb{R}_+^* \times C_1(E),$$

где $C_1(E)$ есть группа классов иделей единичной нормы, и потому

$$W(E|k) \cong \mathbb{R}_+^* \times W_1(E|k),$$

где $W_1(E|k)$ есть групповое расширение, определяемое точной последовательностью

$$1 \to C_1(E) \to W_1(E|k) \to \mathrm{Gal}(E|k) \to 1.$$

Группа $C_1(E)$ и, значит, группа $W_1(E|k)$ компактны. Обозначим через

$$\tau(E,k) : W(k) \to W_1(E|k)$$

естественный эпиморфизм с

$$\mathrm{Ker}\ \tau(E,k) \cong \mathbb{R}_+ \times W(E)^c.$$

Будем говорить, что представление (1) *нормировано*, если это представление пропускается через одну из групп $W_1(E|k)$, т.е. если $\rho = \rho_1 \circ \tau(E,k)$ для некоторого конечного нормального расширения $E|k$ и некоторого представления ρ_1 группы $W_1(E|k)$. Обозначим через $X_0(k)$ совокупность нормированных неприводимых характеров группы $W(k)$ и через

$$X(k) := \{ \sum_{\varphi \in X_0(k)} m(\varphi)\varphi | m : X_0(k) \to \mathbb{Z},\ |m^{-1}(\mathbb{Z} \setminus \{0\})| < \infty \}$$

кольцо виртуальных нормированных характеров этой группы.

Пусть $p \in \mathcal{P}(k)$; обозначим через I_p подгруппу инерции группы $W(k)$ в точке p и через σ_p класс Фробениуса в этой точке [166], [40] (см. также [128, гл. 1, §3]). Пусть $\psi \in X_0(k)$ и

$$\tilde{\psi}\colon W(k) \to \mathrm{GL}(V)$$

есть представление с характером ψ; положим

$$V(p) := \{x | x \in V,\ \tilde{\psi}(g)x = x \text{ при } g \in I_p\},\ S(\psi) := \{p | p \in \mathcal{P}(k),\ V(p) \neq V\}$$

и

$$S(a) := \bigcup_{\varphi \in \sup a} S(\varphi) \text{ при } a \in X(k).$$

Как известно, множества $S(\psi)$ и, следовательно, $S(a)$ конечны. По определению,

$$I_p \subseteq \mathrm{Ker}\ \tilde{\psi} \ \text{ при } \ p \in \mathcal{P}(k) \setminus S(\psi). \tag{1.3.2}$$

Более того,

$$\mathrm{tr}\ (\tilde{\psi}(g)|V(p)) \ \text{ и } \ \det\ (1 - t\tilde{\psi}(g)|V(p))$$

не зависят от выбора элемента g в σ_p; положим

$$\psi(\sigma_p) := \mathrm{tr}\ (\rho(g)|V(p)) \ \text{ и } \ \det\ (1 - t\tilde{\psi}(\sigma_p)) := \det\ (1 - t\tilde{\psi}(g)|V(p))$$

при $g \in \sigma_p$ и распространим это определение по линейности на все элементы кольца $X(k)$. Мероморфная функция $s \mapsto L(\psi, s)$ определяется абсолютно сходящимся в полуплоскости $\mathbb{C}_1$ эйлеровским произведением

$$L(\psi, s) := \prod_{p \in \mathcal{P}(k)} \det\ (1 - \tilde{\psi}(\sigma_p)|p|^{-s})^{-1}$$

и называется L - функцией Гекке - Артина - Вейля (или просто L - *функцией Вейля*) [166].

2. Пусть

$$\Phi(t) \in X(k)[t],\ \Phi(t) = 1 + \sum_{j=1}^{l} a_j t^j.$$

Положим

$$\Phi_g(t) := 1 + \sum_{j=1}^{l} a_j(g)t^j = \prod_{j=1}^{l}(1 - \gamma_j(g)t)$$

с $\gamma_j(g) \in \mathbb{C}$ при $g \in W(k),\ 1 \le j \le l$. Пусть

$$\gamma(\Phi) := \sup\{|\gamma_j(g)|\ |1 \le j \le l,\ g \in W(k)\}.$$

Назовём полином $\Phi(t)$ унитарным, если

$$(\forall g \in W(k))\ \Phi_g(\alpha) \neq 0 \ \text{ при } \ |\alpha| \neq 1,\ \alpha \in \mathbb{C}.$$

Положим далее

$$\mathcal{X}_0(\Phi) := \bigcup_{j=1}^{l} \sup a_j \ \text{ и } \ S(\Phi) := \bigcup_{j=1}^{l} S(a_j).$$

Ясно, что множества $\mathcal{X}_0(\Phi)$ и $S(\Phi)$ конечны.

Предложение 1.3.1. *Пусть* $\Phi(t) \in X(k)[t],\ \Phi(0) = 1$ *и* $\Phi(t) \neq 1$. *Тогда*

(i) $(\exists\, B(\Phi) \in \mathbb{R})\ 1 \le \gamma(\Phi) \le B(\Phi)$;

(ii) *полином* $\Phi(t)$ *унитарен* $\Leftrightarrow \gamma(\Phi) = 1$;

(iii) *найдётся последовательность функций*

$$b_n \colon X_0(k) \to \mathbb{Z},\ n \in \mathbb{N}$$

и последовательность конечных подмножеств $X_n(\Phi),\ n \in \mathbb{N}$, *множества* $X_0(k)$, *удовлетворяющих следующим условиям:*

$$b_n(X_0(k) \setminus X_n(\Phi)) = \{0\} \ \text{ при } \ n \in \mathbb{N};$$

$$I_p \subseteq \operatorname{Ker} \tilde{\psi} \ \text{ при } \ \psi \in \bigcup_{n\in\mathbb{N}} X_n(\Phi),\ p \in \mathcal{P}(k) \setminus S(\Phi);$$

$$\Phi(t) = \prod_{n=1}^{\infty} \prod_{\varphi \in X_0(k)} \det\,(1 - t^n\tilde{\varphi})^{b_n(\varphi)} \ \text{ в } \ X(k)[[t]];$$

при $g \in W(k)$ *бесконечное произведение*

$$\Phi_g(t) = \prod_{n=1}^{\infty} \prod_{\varphi \in X_0(k)} \det\,(1 - t^n \tilde{\varphi}(g))^{b_n(\varphi)} \tag{1.3.3}$$

абсолютно сходится в круге $|t| < \gamma(\Phi)^{-1}$;

при $g \in W(k)$ *и* $m \in \mathbb{N}$ *имеет место неравенство*

$$|\sum_{\varphi \in X_0(k)} b_m(\varphi)\varphi(g)| \leq \frac{\tau(m)}{m}\, l\gamma(\Phi)^m, \tag{1.3.4}$$

где $\tau(m) := |\{d | d \in \mathbb{N},\ d|m\}|$ *и* $l := \deg\,\Phi(t)$;

наконец,

$$\sum_{n \geq M} |\sum_{\varphi \in X_0(k)} \log\det\,(1 - t^n \tilde{\varphi}(g))^{b_n(\varphi)}| \leq \frac{l(\gamma(\Phi)|t|)^M}{(1 - \gamma(\Phi)|t|)^2} \tag{1.3.5}$$

при $g \in W(k),\ m \in \mathbb{N}$ *и* $|t| < \gamma(\Phi)^{-1}$.

Доказательство. Пусть $\Phi(t) \in X(k)[t],\ \Phi(0) = 1$ и $\Phi(t) \neq 1$; положим

$$\Phi(t) = 1 + \sum_{j=1}^{l} a_j t^j \ \text{ с } \ a_l \neq 0.$$

Так как множество $\mathcal{X}_0(\Phi)$ конечно, существует конечное нормальное расширение $K|k$ под условием

$$(\forall\ \psi \in \mathcal{X}_0(\Phi))\ \mathrm{Ker}\ \tau(K|k) \subseteq \mathrm{Ker}\ \tilde{\psi}. \tag{1.3.6}$$

С другой стороны,

$$(\forall\ \psi \in \mathcal{X}_0(\Phi),\ p \in \mathcal{P}(k) \setminus S(\Phi))\ I_p \subseteq \mathrm{Ker}\ \tilde{\psi}. \tag{1.3.7}$$

Обозначим через H замкнутый нормальный делитель группы $W(k)$, порождённый множеством

$$\mathrm{Ker}\ \tau(K|k) \cup (\bigcup_{p \in \mathcal{P}(k) \setminus S(\Phi))} I_p),$$

и через $\lambda\colon W(k) \to G$ естественный эпиморфизм с $G := W(k)/H$. Из соотношений (6) и (7) следует, что

$$(\exists\, c_j \in Y(G))\ a_j = c_j \circ \lambda \ \text{ при } \ 1 \le j \le l$$

положим

$$P(t) = 1 + \sum_{j=1}^{l} c_j t^j,\ P(t) \in Y(G)[t].$$

Ясно, что $\Phi_g(t) = P_{\lambda g}(t)$ при $g \in W(k)$ и, значит, $\gamma(\Phi) = \gamma(P)$. Так как

$$W(K)^c \subseteq \operatorname{Ker} \tau(K|k)$$

и, следовательно, группа G компактна, утверждения $(i) - (iii)$ вытекают из леммы 1, следствия 1 и предложения 1 в §2. Предложение 1 доказано.

Следствие 1.3.1. *Сохраняя обозначения и условия предложения 1, предположим, что полином $\Phi(t)$ унитарен. Тогда*

$$(\exists n_0 \in \mathbb{N})\ X_n(\varphi) = \emptyset \ \ \textit{при} \ \ n > n_0$$

и потому

$$\Phi(t) = \prod_{n=1}^{n_0} \prod_{\varphi \in X_0(k)} \det\,(1 - t^n \tilde{\varphi})^{b_n(\varphi)} \ \textit{в}\ X(k)[[t]]. \tag{1.3.8}$$

Доказательство. Это утверждение вытекает из следствия 2.3.

3. Пусть

$$\Phi(t) := 1 + \sum_{j=1}^{l} a_j t^j,\ \Phi(t) \in X(k)[t].$$

Положим

$$\Phi_p(t) := 1 + \sum_{j=1}^{l} a_j(\sigma_p) t^j \ \text{ при } \ p \in \mathcal{P}(k)$$

и заметим, что

$$\Phi_p(t) = \Phi_g(t) \ \text{ при } \ p \in \mathcal{P}(k) \setminus S(\Phi) \text{ и } g \in \sigma_p. \tag{1.3.9}$$

Положим далее

$$L(\Phi; s) := \prod_{p \in \mathcal{P}(k)} \Phi_p(|p|^{-s})^{-1} \text{ при } s \in \mathbb{C}_1. \tag{1.3.10}$$

Ясно, что

$$L(\psi; s) = L(Q, s) \text{ при } \psi \in X_0(k) \text{ и } Q(t) := \det(1 - \tilde{\psi}\, t).$$

Положим

$$f_{n,p}(t) := \prod_{\psi \in X_0(k)} \det(1 - t^n \tilde{\psi}(\sigma_p))^{b_n(\psi)} \text{ при } n \in \mathbb{N} \text{ и } p \in \mathcal{P}(k).$$

По определению,

$$\prod_{p \in \mathcal{P}(k)} f_{n,p}(|p|^{-s})^{-1} = \prod_{\psi \in X_0(k)} L(\psi; ns)^{b_n(\psi)} \text{ при } s \in \mathbb{C}_{1/n}. \tag{1.3.11}$$

Следствие 1.3.2. *Имеет место следующее соотношение:*

$$\Phi_p(t) = \prod_{n=1}^{\infty} f_{n,p}(t) \text{ при } p \in \mathcal{P}(k) \setminus S(\Phi) \text{ и } |t| < \gamma(\Phi)^{-1}. \tag{1.3.12}$$

Доказательство. Соотношение (12) следует из соотношений (3) и (9).

Следствие 1.3.3. *Если полином $\Phi(t)$ унитарен, то функция*

$$s \mapsto L(\Phi; s)$$

мероморфно продолжима на всю комплексную плоскость.

Доказательство. Из соотношений (8) - (10) и определения функций Вейля следует, что

$$L(\Phi; s) = L_1(\Phi, s) \text{ при } s \in \mathbb{C}_1,$$

где

$$L_1(\Phi, s) := \prod_{p \in S(\Phi)} \prod_{n=1}^{n_0} f_{n,p}(|p|^{-s}) \Phi_p(|p|^{-s})^{-1} \prod_{n=1}^{n_0} \prod_{\varphi \in X_0(k)} L(\varphi; ns)^{b_n(\varphi)}.$$

Так как функции Вейля $L(\varphi, s)$ суть мероморфные функции и множество $S(\Phi)$ конечно, функция $s \mapsto L_1(\Phi; s)$ мероморфна. Утверждение доказано.

Пусть

$$\{M, N\} \subseteq \mathbb{N},\ N > \max\{|p|, \gamma(\Phi)^M \mid p \in S(\Phi))\}$$

и

$$S_N := \{p | p \in \mathcal{P}(k),\ |p| < N\},\ \text{ так что }\ S(\Phi) \subseteq S_N.$$

Следствие 1.3.4. *Пусть $p \in \mathcal{P}(k) \setminus S(\Phi)$, тогда*

$$\Phi_p(|p|^{-s}) = \prod_{n=1}^{\infty} f_{n,p}(|p|^{-s}) \ \text{ при }\ s \in \mathbb{C}_{1/M}. \tag{1.3.13}$$

Доказательство. Так как

$$|p|^{-\operatorname{Re} s} < \gamma(\Phi))^{-1} \ \text{ при }\ s \in \mathbb{C}_{1/M},\ p \in \mathcal{P}(k) \setminus S_N \tag{1.3.14}$$

и $S(\Phi) \subseteq S_N$, доказываемое утверждение следует из соотношения (12).

Положим

$$Z_N(s) := \prod_{p \in S_N} \Phi_p(|p|^{-s})^{-1} \ \text{ и }\ T_{N,M}(s) := \prod_{n=M}^{\infty} \prod_{p \in \mathcal{P}(k) \setminus S_N} f_{n,p}(|p|^{-s})^{-1}.$$

Лемма 1.3.1. *Произведение $T_{N,M}(s)$ компактно сходится в $\mathbb{C}_{1/M}$.*

Доказательство. Так как

$$f_{n,p}(t) = \prod_{\psi \in X_0(k)} \det\,(1 - t^n \tilde{\psi}(g))^{b_n(\psi)}$$

при $p \in \mathcal{P}(k) \setminus S(\Phi),\ g \in \sigma_p,\ n \in \mathbb{N}$ и $S(\Phi) \subseteq S_N$, из соотношений (14) и (5) следует, что

$$\sum_{n=M}^{\infty} \sum_{p \in \mathcal{P}(k) \setminus S_N} |f_{n,p}(|p|^{-s})| \le \sum_{p \in \mathcal{P}(k) \setminus S_N} \frac{l(\gamma(\Phi)|p|^{-\operatorname{Re} s})^M}{(1 - \gamma(\Phi)|p|^{-\operatorname{Re} s})^2} \le$$

$$\frac{l\gamma(\Phi)^M [k : \mathbb{Q}]}{(1 - \gamma(\Phi) N^{-1/M})^2} \sum_{n=1}^{\infty} n^{-M \operatorname{Re} s}.$$

Лемма доказана.

Положим

$$U_M(s) := \prod_{1 \le n < M} \prod_{\varphi \in X_0(k)} L(\varphi; ns)^{b_n(\varphi)} \ \text{ и }\ R_{N,M}(s) := \prod_{1 \le n < M} \prod_{p \in S_N} f_{n,p}(|p|^{-s}).$$

Лемма 1.3.2. *Равенство*

$$L(\Phi;s)=Z_N(s)T_{N,M}(s)R_{N,M}(s)U_M(s), \tag{1.3.15}$$

определяет мероморфное продолжение функции $s\mapsto L(\Phi;s)$ *в полуплоскость* $\mathbb{C}_{1/M}$.

Доказательство. В силу следствия 2 и соотношения (11), равенство (15) имеет место при $s\in\mathbb{C}_1$, а из леммы 1 следует, что функция

$$s\mapsto Z_N(s)T_{N,M}(s)R_{N,M}(s)$$

мероморфна в полуплоскости $\mathbb{C}_{1/M}$. Поэтому утверждение леммы вытекает из мероморфности L-функций Вейля.

Следствие 1.3.5. *Функция* $s\mapsto L(\Phi;s)$ *мероморфно продолжима в полуплоскость* $\mathbb{C}_0$.

Доказательство. В силу леммы 2, функция $s\mapsto L(\Phi;s)$ мероморфно продолжима в полуплоскость $\mathbb{C}_{1/M}$ при любом $M\in\mathbb{N}$ и, значит, в полуплоскость

$$\mathbb{C}_0=\bigcup_{M=1}^{\infty}\mathbb{C}_{1/M}.$$

Следствие 5 доказано.

1.4 Об одном обобщении теоремы плотности Н. Г. Чеботарёва

1. Пусть $\mathfrak{N}\subseteq X_0(k),\ g\in W(k),\ v\in\mathbb{R}$ и $0<v<1$. Рассмотрим множество

$$\Pi_1(\mathfrak{N},g,v;x):=\{p|p\in\Pi(k,x),\ |\chi(\sigma_p)-\chi(g)|<v \text{ при } \chi\in\mathfrak{N}\};$$

положим $\pi(\mathfrak{N},g,v;x):=|\Pi_1(\mathfrak{N},g,v;x)|$.

В этом параграфе будет доказана следующая теорема (ср. [128], [132]).

Теорема 1.4.1. *Предположим, что множество* $\mathfrak{N}$ *конечно. Тогда*

$$\pi(\mathfrak{N},g,v;x)=c_0(\mathfrak{N},g,v)\int_2^x\frac{du}{\log u}+O(x\exp(-c_1(\mathfrak{N})(\log x)^{1/2})) \tag{1.4.1}$$

при $x \to \infty$, *где*

$$c_0(\mathfrak{N}, g, v) \geq c_2(\mathfrak{N}) v^{c_3(\mathfrak{N})},\ c_j(\mathfrak{N}) \in \mathbb{R}_+^*\ \textit{при}\ 1 \leq j \leq 3 \tag{1.4.2}$$

и O*-константа в* (1) *зависит только от* $\mathfrak{N}$ *(но не от* g, v *и* x*).*

Обозначим через $gr(E)$ группу характеров Гекке поля алгебраических чисел E и пусть

$$gr(E, \mathcal{L}) := \{\chi | \chi \in gr(E),\ \mathfrak{f}(\chi) | \mathcal{L}\}$$

при $\mathcal{L} \in \mathbb{N}$, где $\mathfrak{f}(\chi)$ есть ведущий модуль характера χ. Как известно (см., например, [91, §9], [128, гл. 1, §1]),

$$gr(E) \cong C_1(E)^{\perp},\ gr(E) = \bigcup_{\mathcal{L} \in \mathbb{N}} gr(E, \mathcal{L})\ \text{ и }\ gr(E, \mathcal{L}) \cong \mathbb{Z}^n \oplus \mathfrak{A}(\mathcal{L}), \tag{1.4.3}$$

где $[E : \mathbb{Q}] = n + 1,\ n \in \mathbb{N}_0$ и $|\mathfrak{A}(\mathcal{L})| < \infty$. Элементы группы $gr(E, \mathcal{L})$ суть характеры Гекке по модулю $\mathcal{L}$; напомним конструкцию этих характеров. Пусть

$$U := (\mathbb{R}_+^*)^{r_1} \times (\mathbb{C}^*)^{r_2}\ \text{ и }\ n + 1 = r_1 + 2r_2;$$

ясно, что

$$\hat{U} = \{f | f : U \to S_1,\ f : z \mapsto \prod_{j=1}^{r_1+r_2} |z_j|^{it_j(f)} \prod_{j=r_1+1}^{r_1+r_2} (\frac{z_j}{|z_j|})^{a_j(f)}\}$$

с $t_j(f) \in \mathbb{R}$ при $1 \leq i \leq r_1 + r_2$ и $a_j(f) \in \mathbb{Z}$ при $r_1 + 1 \leq i \leq r_1 + r_2,\ f \in \hat{U}$.

Рассмотрим стандартные вложения

$$\sigma : E \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},\ \sigma_i : E \hookrightarrow \mathbb{C} \text{ при } 1 \leq i \leq r_1 + r_2,\ \ \iota : \mathbb{R}_+^* \hookrightarrow U$$

с

$$\sigma_i(E) \subseteq \mathbb{R} \Leftrightarrow 1 \leq i \leq r_1\ \text{ и }\ \iota(t)_i = t \text{ при } 1 \leq i \leq r_1 + r_2.$$

Положим

$$\mathcal{E}(\mathcal{L}) := \{\varepsilon | \varepsilon \in \mathfrak{o}(E)^*,\ \varepsilon = 1(\mathcal{L}),\ \sigma_i(\varepsilon) > 0 \text{ при } 1 \leq i \leq r_1\};$$

из теоремы Дирихле о единицах следует, что

$$U/(\iota(\mathbb{R}_+^*)\mathcal{E}(\mathcal{L})) \cong \mathcal{T}, \text{ где } \mathcal{T} := \{z | z \in \mathbb{C}^n, \ |z_j| = 1 \text{ при } 1 \le j \le n\}.$$

Пусть

$$\mathcal{F}(\mathcal{L}) := \{f | f \in \hat{U}, \ \iota(\mathbb{R}_+^* \mathcal{E}(\mathcal{L})) \subseteq \operatorname{Ker} f\},$$

так что

$$\mathcal{F}(\mathcal{L}) \cong (U/(\iota(\mathbb{R}_+^*)\mathcal{E}(\mathcal{L}))^{\perp} \text{ и, значит, } \mathcal{F}(\mathcal{L}) \cong \mathbb{Z}^n.$$

Положим

$$I(\mathcal{L}) := \{\mathfrak{a}\mathfrak{b}^{-1} | \{\mathfrak{a}, \mathfrak{b}\} \subseteq I_0, \ (\mathfrak{a}\mathfrak{b}, (\mathcal{L})) = (1)\}$$

и

$$pr(\mathcal{L}) := \{(\alpha) | \alpha \in E^*, \ \alpha = 1(\mathcal{L})\}.$$

По определению,

$$gr(E, \mathcal{L}) :=$$

$$\{\lambda | \lambda \in I(\mathcal{L})^{\perp}, \ \lambda((\alpha)) = f_\lambda(\alpha) \text{ с } f_\lambda \in \mathcal{F}(\mathcal{L}) \text{ при } (\alpha) \in pr(\mathcal{L})\};$$

легко видеть, что

$$gr(E, \mathcal{L}) = gr_0(E, \mathcal{L}) \oplus \mathfrak{A}(\mathcal{L}) \text{ с } gr_0(E, \mathcal{L}) \cong \mathbb{Z}^n \text{ и } \mathfrak{A}(\mathcal{L}) \cong I(\mathcal{L})/pr(\mathcal{L}).$$

Положим

$$w_0(\lambda) := 1 + \sum_{j=1}^{r_1+r_2} |t_j(f_\lambda)| + \sum_{j=r_1+1}^{r_1+r_2} |a_j(f_\lambda)| \text{ при } \lambda \in gr(E, \mathcal{L}).$$

Лемма 1.4.1. *Пусть $\chi \in gr(E, \mathcal{L})$. Тогда*

$$\sum_{p \in \Pi(E,x)} \chi(p) = g(\chi) \int_2^x \frac{du}{\log u} +$$

$$O(x \exp(-c(\mathcal{L}) \frac{\log x}{\log w_0(\chi) + (\log x)^{1/2}})) \text{ при } x \to \infty, \ c(\mathcal{L}) \in \mathbb{R}_+^*, \qquad (1.4.4)$$

где $c(\mathcal{L})$ и O-константа в (4) зависят лишь от E и $\mathcal{L}$ (но не от x).

Доказательство. Это известная теорема Гекке [99] (ср. [128, гл. 1, §5]).

Зафиксировав систему образующих группы $\mathcal{E}(\mathcal{L})$, можно построить канонический базис $\{\mu_j | 1 \leq j \leq n\}$ группы $gr_0(E, \mathcal{L})$ и эпиморфизм

$$\varphi_0(E, \mathcal{L}) : C_1(E) \to \mathcal{T},\ \varphi_0(E, \mathcal{L}) : \alpha \mapsto (\mu_1(\alpha), ..., \mu_n(\alpha))$$

группы классов иделей единичного объёма $C_1(E)$ на n-мерный тор $\mathcal{T}$. Отображение $\varphi_0(E, \mathcal{L})$ естественным образом продолжается до эпиморфизма

$$\varphi(E, \mathcal{L}) : W(E|k) \to \mathfrak{G}$$

группы Вейля $W(E|k)$ на расширение $\mathfrak{G}$ конечной группы

$$\mathfrak{H} := \mathrm{Gal}(E|k) \times \mathfrak{A}(\mathcal{L})$$

тором $\mathcal{T}$; построенные таким образом отображения определяют точную последовательность групп:

$$1 \to \mathcal{T} \to \mathfrak{G} \to \mathfrak{H} \to 1.$$

Положим

$$w(\lambda_0 \prod_{j=1}^{n} \mu_j^{m_j}) := \max\{|m_i| + 1 | 1 \leq i \leq n\} \ \text{ при } \ m \in \mathbb{Z}^n,\ \lambda_0 \in \mathfrak{A}(\mathcal{L});$$

тогда

$$w_0(\lambda) \ll_{\mathcal{L},E} w(\lambda) \ \text{ при } \ \lambda \in gr(E, \mathcal{L}) \tag{1.4.5}$$

и имеет место следующее утверждение.

Лемма 1.4.2. *Рассмотрим конечное расширение полей алгебраических чисел степени $E|E_1$. Пусть*

$$\lambda_1 \in gr(E_1, \mathcal{L}) \ \ u \ \ \lambda := \lambda_1 \circ N_{E/E_1};$$

тогда

$$\lambda \in gr(E, \mathcal{L}) \ \ u \ \ w(\lambda_1) \ll_{\mathcal{L},E,E_1} w(\lambda) \ll_{\mathcal{L},E,E_1} w(\lambda_1).$$

Рассмотрим конечное нормальное расширение $E|k$ и пусть $\mathcal{L} \in \mathbb{N}$; положим

$$\mathcal{X}(E|k) := \{\chi | \chi \in X_0(k),\ W(E)^c \subseteq \mathrm{Ker}\ \tilde{\chi}\},$$

$$\mathcal{X}(E|k, \mathcal{L}) := \{\chi | \chi \in \mathcal{X}(E|k),\ \lambda \prec (\chi \circ \tau(E,k))|_{C_1(E)} \Rightarrow \lambda \in gr(E, \mathcal{L})\}$$

и

$$w(E;\chi) := \max\{w(\lambda) | \lambda \prec (\chi \circ \tau(E,k))|_{C_1(E)}\} \ \text{ при } \ \chi \in \mathcal{X}(E|k, \mathcal{L}).$$

Лемма 1.4.3. *Рассмотрим конечные нормальные расширения $E|k$ и $E_1|k$ под условием $E_1 \subseteq E$. Пусть $\chi \in \mathcal{X}(E_1|k, \mathcal{L})$, тогда*

$$w(E,\chi) \ll_{\mathcal{L},E,E_1} w(E_1;\chi) \ll_{\mathcal{L},E,E_1} w(E,\chi). \tag{1.4.6}$$

Доказательство. Обозначим через

$$j : W_1(E|k) \to W_1(E_1|k)$$

естественный эпиморфизм групп Вейля и заметим, что, по построению (см. [166], [40]),

$$\tau(E_1,k) = \tau(E,k) \circ j \ \text{ и } \ j|_{C_1(E)} = N_{E/E_1}. \tag{1.4.7}$$

Соотношение (6) следует из (7) и леммы 2.

Лемма 1.4.4. *Рассмотрим конечное нормальное расширение $E|k$ и пусть $\chi \in \mathcal{X}(E|k, \mathcal{L})$. Тогда*

$$\sum_{p \in \Pi(k,x)} \chi(\sigma_p) = g(\chi) \int_2^x \frac{du}{\log u} \ +$$

$$O(x \exp(-c(\mathcal{L}) \frac{\log x}{\log w(E,\chi) + (\log x)^{1/2}})) \ \ \textit{при} \ \ x \to \infty, \ \ c(\mathcal{L}) \in \mathbb{R}_+^*, \tag{1.4.8}$$

где $c(\mathcal{L})$ и O-константа в (8) зависят лишь от E и $\mathcal{L}$ (но не от x).

Доказательство. Можно показать, что существуют поле k_1 и характер χ_1 под условием:

$$k \subseteq k_1 \subseteq E,\ \chi_1 \in \mathcal{X}(E|k_1, \mathcal{L}),\ \chi = \mathrm{Ind}\, {}^{W(E|k)}_{W(E|k_1)} \chi_1 \text{ и } \chi_1 = \lambda\psi \tag{1.4.9}$$

с

$$\lambda \in gr(k_1, \mathcal{L}),\ \psi \in \mathcal{X}(E|k_1, \mathcal{L}) \text{ и } C(E) \subseteq \operatorname{Ker} \psi. \tag{1.4.10}$$

По теореме Брауэра, найдутся число l, поля E_i и характеры ψ_i такие, что

$$k_1 \subseteq E_i \subseteq E,\ \psi_i \in gr(E_i, \mathcal{L}),\ w(\psi_i) = 0 \text{ при } 1 \leq i \leq l$$

и

$$\psi = \sum_{i=1}^{l} e_i \operatorname{Ind}_{W(E|E_i)}^{W(E|k_1)} \psi_i,\ e_i \in \{\pm 1\} \text{ при } 1 \leq i \leq l. \tag{1.4.11}$$

Из соотношений (9) и (10) следует, что

$$\sum_{p \in \Pi(k,x)} \chi(\sigma_p) = \sum_{p \in \Pi(k_1,x)} \chi_1(\sigma_p) = \sum_{p \in \Pi(k_1,x)} \lambda(p)\psi(\sigma_p)$$

и потому, в силу (11),

$$\sum_{p \in \Pi(k,x)} \chi(\sigma_p) = \sum_{i=1}^{l} e_i \sum_{p \in \Pi(E_i,x)} \lambda(N_{E_i/k_1} p)\psi_i(p). \tag{1.4.12}$$

С другой стороны, в силу леммы 2,

$$w(E_i, (\lambda \circ N_{E_i/k_1})\psi_i) \ll_{E,\mathcal{L}} w(\lambda) \text{ при } 1 \leq i \leq l \text{ и } w(E, \chi) \gg_{E,\mathcal{L}} w(\lambda), \tag{1.4.13}$$

ибо

$$\chi(\alpha) = \sum_{\tau \in G(k_1|k)} \chi_1(\tau^{-1}\alpha\tau) = \sum_{\tau \in G(k_1|k)} \lambda(N_{E/k_1}\alpha) \text{ при } \alpha \in C(E),$$

где $G(k_1|k)$ есть совокупность классов смежности группы $\operatorname{Gal}(E|k)$ по подгруппе $\operatorname{Gal}(E|k_1)$. Доказываемое утверждение вытекает из леммы 1 и соотношений (12), (13), (1.2).

Доказательство теоремы 1. Так как множество $\mathfrak{N}$ конечно, существуют конечное нормальное расширение $K|k$ и натуральное число $\mathcal{L}$ под условием $\mathfrak{N} \subseteq \mathcal{X}(K|k, \mathcal{L})$; положим

$$n + 1 := [K : k],\ n \in \mathbb{N}_0,\ \mathfrak{H} := \operatorname{Gal}(K|k) \times \mathfrak{A}(\mathcal{L})$$

и

$$\mathcal{T} := \{z | z \in \mathbb{C}^n,\ |z_j| = 1 \text{ при } 1 \leq j \leq n\}.$$

По построению,

$$(\forall \chi \in \mathfrak{N}\ \exists \psi(\chi) \in \hat{\mathfrak{G}})\ \chi = \varphi(K, \mathcal{L})\tau(K|k)\psi(\chi),$$

где $\mathfrak{G}$ есть расширение конечной группы $\mathfrak{H}$ тором $\mathcal{T}$, определяемое точной последовательностью

$$1 \to C(K) \to W(K|k) \to \mathrm{Gal}(K|k) \to 1$$

и гомоморфизмом $\varphi(K, \mathcal{L})$; более того, $w(\psi(\chi)) = w(K, \chi)$. Асимптотическая формула (1) следует из леммы 4, леммы 2.4 и предложения 2.2 с

$$B(x) = \int_2^x \frac{du}{\log u},\ b(x, m) = x \exp(-c(\mathcal{L})\frac{\log x}{\log m + (\log x)^{1/2}}),\ \alpha = 1,$$

$C(\mathcal{A}) = c_1(\mathfrak{N})$ и $\nu = n+1$; оценка (2) следует из леммы 2.5. Теорема доказана.

2. Имеют место следующие две леммы о нулях L - функций Вейля.

Лемма 1.4.5. *Пусть $\chi \in gr(E, \mathcal{L})$. При $T \in \mathbb{R}_+$ положим*

$$R(T, \chi) := \{s | s \in \mathbb{C},\ 0 \leq \mathrm{Re}\ s \leq 1,\ |\mathrm{Im}\ s| \leq T,\ L(\chi, s) = 0\}$$

и

$$\mathcal{N}(T, \chi) := \sum_{s \in R(T, \chi)} \nu(s),$$

где $\nu(s)$ есть кратность нуля s функции $s \mapsto L(\chi, s)$. Тогда

$$\mathcal{N}(T+1, \chi) = \mathcal{N}(T, \chi) + O(\log(\mathcal{L} w_0(\chi)(1+T)^{n+1})). \tag{1.4.14}$$

Доказательство. Это утверждение хорошо известно (см., например, [128, предложение 2 на стр. 55]).

Лемма 1.4.6. *Рассмотрим конечное нормальное расширение $E|k$ и пусть $\chi \in \mathcal{X}(E|k, \mathcal{L})$; при $T \in \mathbb{R}_+$ положим*

$$\mathcal{N}_0(T, \chi) := |\{s | s \in \mathbb{C},\ L(\chi, s) \in \{0, \infty\},\ 0 \leq \operatorname{Re} s \leq 1,\ |\operatorname{Im} s| \leq T\}|.$$

Тогда

$$\mathcal{N}_0(T, \chi) \ll_{\mathcal{L}, E} (T+1) \log((1+T) w(E, \chi)). \tag{1.4.15}$$

Доказательство. Из соотношений (9) - (11) следует, что

$$L(\chi, s) = \prod_{i=1}^{l} L(\psi_i(\lambda \circ N_{E_i/k_1}), s)^{e_i}. \tag{1.4.16}$$

Оценка (15) есть результат применения асимптотической формулы (14) к каждому из сомножителей произведения (16). Лемма доказана.

Замечание. В недавней работе [12] подробно изучается поведение параметра $c(\mathcal{L})$ и O - константы в асимптотической формуле (8).

1.5 Непродолжимость эйлеровских произведений, определяемых неунитарными полиномами, в правую полуплоскость

1. Пусть

$$\Phi(t) \in X(k)[t],\ \Phi(t) = 1 + \sum_{j=1}^{l} a_j t^j,\ l \in \mathbb{N},\ \Phi(t) \neq 1,$$

$$a_j = \sum_{\psi \in \mathcal{X}_0(\Phi)} m_j(\psi) \psi \ \text{ при } \ 1 \leq j \leq l,$$

$$\Phi_g(t) = \prod_{j=1}^{l} (1 - \gamma_j(g) t) \ \text{ и } \ \sigma(m, g) := \sum_{j=1}^{l} \gamma_j(g)^m \text{ при } g \in W(k),\ m \in \mathbb{N}.$$

Обозначим через $\mathcal{X}_1(\Phi)$ подкольцо кольца $X(k)$, порождённое множеством $\mathcal{X}_0(\Phi)$. Как уже было отмечено в §4, из конечности этого множества следует, что

$$\mathcal{X}_0(\Phi) \subseteq \mathcal{X}(K|k, \mathcal{L})$$

и потому

$$\mathcal{X}_1(\Phi) \subseteq \mathcal{X}(K|k, \mathcal{L}) \tag{1.5.1}$$

для некоторого конечного нормального расширения $K|k$ и натурального числа $\mathcal{L}$; положим $n := [K : k]$ и

$$w(\Phi) := \max\{w(K, \psi)|\psi \in \mathcal{X}_0(\Phi)\}.$$

Лемма 1.5.1. *Имеют место следующие соотношения:*

$$X_m(\Phi) \subseteq \mathcal{X}_1(\Phi) \ \ u \ \ |X_m(\Phi)| \ll_\Phi m^n \ \ при \ \ m \in \mathbb{N}.$$

Доказательство. Пусть $m \in \mathbb{N}$. Выражая суммы $\sigma(m, g)$ через коэффициенты полинома $\Phi_g(t)$ и воспользовавшись тождеством (2.14), получим

$$m \sum_{\psi \in X_m(\Phi)} b_m(\psi)\psi(g) = \sum_{uv=m} \mu(u) f_v(a(g^u)) \ \text{ при } \ g \in W(k), \tag{1.5.2}$$

где $f_v(t)$ есть полином степени v от l переменных $t := (t_1, ..., t_l)$ с целыми рациональными коэффициентами. Из соотношений (1) и (2) следует, что

$$X_m(\Phi) \subseteq \mathcal{X}_1(\Phi) \subseteq \mathcal{X}(K|k, \mathcal{L}) \tag{1.5.3}$$

и, более того,

$$w(K; \psi) \leq m\, w(\Phi) \ \text{ при } \ \psi \in X_m(\Phi). \tag{1.5.4}$$

Остаётся заметить, что

$$|\{\psi|\psi \in \mathcal{X}(K|k, \mathcal{L}),\ w(K; \psi) \leq T\}| \ll_\Phi (T + 1)^n \ \text{ при } \ T \in \mathbb{R}_+.$$

Лемма доказана.

При

$$\nu \in \mathbb{N},\ \{t_0, \delta\} \subseteq \mathbb{R},\ t_0(t_0 + \delta) \geq 0 \text{ и } 0 < \delta < 1$$

положим

$$D(\nu; \delta, t_0) := \{s|s \in \mathbb{C},\ (\nu + 1)^{-1} < \mathrm{Re}\ \ s < \nu^{-1},\ t_0 < \mathrm{Im}\ \ s < t_0 + \delta\}.$$

Пусть

$$M := (\nu+1)^{-1} \text{ и } N > \max\{|p|,\ \gamma(\Phi)^M | p \in S(\Phi)\};$$

в обозначениях §3 положим

$$A_1(\nu;\delta,t_0) := |\{s | s \in D(\nu;\delta,t_0),\ U_M(s) = 0\}|$$

и

$$A_2(\nu;\delta,t_0) := |\{s | s \in D(\nu;\delta,t_0),\ Z_N(s)^{-1} = 0\}|.$$

Предложение 1.5.1. *Имеет место следующая оценка:*

$$A_1(\nu;\delta,t_0) \ll_{t_0,\Phi} \nu^{n+3}.$$

Доказательство. В обозначениях леммы 4.6, имеем

$$A_1(\nu;\delta,t_0) \le \sum_{m=1}^{M} \sum_{\varphi \in X_m(\Phi)} \mathcal{N}_0(m(|t_0|+2),\varphi)$$

и, значит, в силу соотношений (3), (4), (4.15) и леммы 1,

$$A_1(\nu;\delta,t_0) \ll_\Phi \sum_{m=1}^{M} |X_m(\Phi)| m(|t_0|+3)\log m(|t_0|+3)) \ll_{\Phi,t_0} \sum_{m=1}^{M} m^{n+2}.$$

Тем самым, предложение доказано.

Пусть

$$|\alpha| = \gamma(\Phi),\ \Phi_g(t) = (1-\alpha t)^b F(g;t) \text{ и } F(g,\alpha^{-1}) \neq 0$$

при некоторых g в $W(k)$, α в $\mathbb{C}$, $F(g;t)$ в $\mathbb{C}[t]$ и b в $\mathbb{N}$ (существование таких α, b и g следует из определения $\gamma(\Phi)$ и компактности группы $W_1(K|k)$). Положим

$$\Pi_0(\Phi;h,v) := \{p | p \in \mathcal{P}(k) \setminus S(\Phi),\ |\psi(\sigma_p) - \psi(h)| < v \text{ при } \psi \in \mathcal{X}(\Phi)\}.$$

Лемма 1.5.2. *Существует положительное вещественное число $v_0(\Phi)$ такое, что для любого v в интервале $0 < v < v_0(\Phi)$ и любого p из $\Pi_0(\Phi;g,v^{b+2})$ найдётся $\kappa(p)$ под условием*

$$\kappa(p) \in \mathbb{C}^*,\ \Phi_p(\kappa(p)^{-1}) = 0 \ \text{ и } \ |\log|\kappa(p)| - \log\gamma(\Phi)| < v. \tag{1.5.5}$$

Доказательство. Пусть $0 < v_1 < 1$ и $F(g;t) \neq 0$ при $|t-\alpha^{-1}| \leq v_1$; положим

$$w := \min \{|F(g;t)| \mid |t-\alpha^{-1}| \leq v_1\}.$$

Ясно, что $w \in \mathbb{R}_+^*$ и

$$|\Phi_g(t)| \geq w v^b \gamma(\Phi)^b \text{ при } 0 < v < v_1 \text{ и } |t-\alpha^{-1}| = v, \tag{1.5.6}$$

ибо

$$|\Phi_g(t)| = |(1-\alpha t)^b F(g;t)| \geq w|1-\alpha t|^b \text{ при } |t-\alpha^{-1}| \leq v_1.$$

Пусть

$$w_1 := \max\{\sum_{\psi \in \mathcal{X}_0(\Phi)} |m_j(\psi)| \mid 1 \leq j \leq l\},$$

тогда $w_1 \in \mathbb{R}_+^*$ и имеет место следующее соотношение:

$$|a_j(\sigma_p) - a_j(g)| < w_1 v \text{ при } p \in \Pi_0(\Phi; g, v),\ 1 \leq j \leq l \text{ и } v \in \mathbb{R}_+^*. \tag{1.5.7}$$

Положим $h_p(t) := \Phi_p(t) - \Phi_g(t)$; из соотношения (7) следует, что

$$|h_p(t)| < 2^l l w_1 v^{b+1} \text{ при } 0 < v < 1,\ |t-\alpha^{-1}| = v \text{ и } p \in \Pi_0(\Phi; g, v^{b+1}), \tag{1.5.8}$$

так как при этих условиях

$$|\Phi_p(t) - \Phi_g(t)| \leq$$

$$\sum_{j=1}^{l} |t|^j |a_j(\sigma_p) - a_j(g)| < w_1 v^{b+1} \sum_{j=1}^{l} (v + \gamma(\Phi)^{-1})^j \leq 2^l l w_1 v^{b+1}.$$

Положим

$$v_2 := \min \{1,\ v_1,\ w\gamma(\Phi)^b (2^l l w_1)^{-1}\};$$

из соотношений (8) и (6) следует, что при $0 < v < v_2$, $|t-\alpha^{-1}| = v$ и $p \in \Pi_0(\Phi; g, v^{b+1})$ имеют место неравенства

$$|h_p(t)| < w\gamma(\Phi)^b v^b \leq |\Phi_g(t)|$$

и, значит, по теореме Руше (см., например, [39, no. 3.4.2]),

$$|\{\beta | \beta \in \mathbb{C},\ \Phi_p(\beta) = 0,\ |\beta - \alpha^{-1}| \leq v\}| =$$

$$|\{\beta|\beta \in \mathbb{C},\ \Phi_g(\beta) = 0,\ |\beta - \alpha^{-1}| \leq v\}| = 1.$$

Таким образом, для любого v в интервале $0 < v < v_2$ и любого p из $\Pi_0(\Phi; g, v^{b+1})$ найдётся $\kappa(p)$ под условием

$$\kappa(p) \in \mathbb{C}^*,\ \Phi_p(\kappa(p)^{-1}) = 0 \ \text{ и } \ |\kappa(p)^{-1} - \alpha^{-1}| \leq v.$$

Несложное вычисление позволяет теперь построить искомое число $v_0(\Phi)$. Лемма доказана.

Предложение 1.5.2. *Пусть* $\gamma(\Phi) > 1$, *тогда*

$$(\exists\ \{c_1(\Phi), c_2(\Phi)\} \subseteq \mathbb{R}_+^*)\ A_2(\nu; \delta, t_0) > \exp(c_1(\Phi)\nu^{1/2}) \tag{1.5.9}$$

при $\nu > c_2(\Phi)$.

Доказательство. Пусть

$$\nu > \max\{2\pi(\delta \log \gamma(\Phi))^{-1},\ (\log v_0(\Phi))^2\}. \tag{1.5.10}$$

Положим $v_\nu := \exp(-\nu^{1/2})$ и

$$Q(\nu) := \{p|p \in \Pi_0(\Phi; g, v_\nu^{b+2}),\ (\gamma(\Phi)e^{v_\nu})^\nu \leq |p| < (\gamma(\Phi)e^{-v_\nu})^{\nu+1}\}.$$

Так как $0 < v_\nu < v_0(\Phi)$, в силу леммы 1, для любого p в Q_ν найдётся $\kappa(p)$, удовлетворяющее условию (5). Положим

$$\kappa(p) = |p|^{s(p)} \tag{1.5.11}$$

с

$$s(p) \in \{\sigma(p) + i(\tau(p) + 2\pi n(\log |p|)^{-1})|n \in \mathbb{Z}\},\ \{\sigma(p), \tau(p)\} \subseteq \mathbb{R}. \tag{1.5.12}$$

Из условия (5) следует, что

$$Z_N(s(p))^{-1} = 0 \ \text{ и } \ (\nu+1)^{-1} < \sigma(p) < \nu^{-1} \ \text{ при } \ p \in Q(\nu).$$

Неравенство (10) даёт:

$$2\pi(\log |p|)^{-1} < \delta \ \text{ при } \ p \in Q(\nu);$$

следовательно, при $p \in Q(\nu)$ найдётся $s(p)$ под условием

$$t_0 < \mathrm{Im}\ \ s(p) < t_0 + \delta.$$

Таким образом,

$$(\forall\ p \in Q(\nu)\ \exists\ s(p) \in D(\nu; \delta, t_0))\ Z_N(s(p))^{-1} = 0. \tag{1.5.13}$$

Положим $\lambda := 2(\nu+1)v_\nu$; из соотношений (5), (11) и (12) следует, что

$$s(p) = s(q) \Rightarrow |\log|p| - \log|q|| < \lambda \ \text{ при } \ \{p, q\} \subseteq Q(\nu). \tag{1.5.14}$$

Пусть

$$J := \{j | j \in \mathbb{Z},\ 0 \le j \le \lambda^{-1} \log \gamma(\Phi) - 2\};$$

при $j \in J$ положим

$$Q_j(\nu) := \{p | p \in \Pi_0(\Phi; g, v_\nu^{b+2}),\ (\gamma(\Phi)e^{v_\nu})^\nu e^{j\lambda} \le |p| < (\gamma(\Phi)e^{v_\nu})^\nu e^{(j+1)\lambda}\}.$$

Легко видеть, что

$$\bigcup_{j \in J} Q_j(\nu) \subseteq Q(\nu) \ \text{ и } \ Q_j \cap Q_{j'} = \emptyset \text{ при } j \ne j'; \tag{1.5.15}$$

более того из теоремы 4.1 следует, что

$$(\exists\ \ c_3(\Phi) \in \mathbb{R})\ Q_j \ne \emptyset \ \text{ при } \ j \in J \text{ и } \nu > c_3(\Phi). \tag{1.5.16}$$

По построению,

$$(\exists\ \{c_4(\Phi), c_5(\Phi)\} \subseteq \mathbb{R}_+^*)\ |J| > \exp(c_4(\Phi)\nu^{1/2}) \ \text{ при } \ \nu > c_5(\Phi), \tag{1.5.17}$$

а из соотношения (14) следует, что

$$s(p) \ne s(q) \ \text{ при } \ p \in Q_j,\ q \in Q_{j'},\ \{j, j'\} \subseteq J \text{ и } |j - j'| \ge 2. \tag{1.5.18}$$

Доказываемое утверждение вытекает из соотношений (13) и (15) - (18).

Следствие 1.5.1. *Предположим, что полином* $\Phi(t)$ *не является унитарным полиномом и обозначим через*

$$\mathcal{A} := \{s | s \in \mathbb{C}_0,\ L(\Phi, s) = \infty\}$$

множество полюсов функции $s \mapsto L(\Phi, s)$. *Имеет место соотношение*

$$\bar{\mathcal{A}} = \mathbb{C}^{(0)} (:= \{iy | y \in \mathbb{R}\}). \tag{1.5.19}$$

Доказательство. Пусть $s_0 \in \mathbb{C}^{(0)},\ r \in \mathbb{R}_+^*$ и

$$K(s_0, r) := \{s | s \in \mathbb{C}_0,\ |s - s_0| < r\}.$$

Ясно, что

$$K(s_0, r) \supseteq \bigcup_{\nu=\nu_0}^{\infty} D(\nu; \delta, t_0)$$

при некоторых $\delta,\ t_0$ и ν. С другой стороны, из предложений 1, 2 и предложения 3.1 (ii) следует, что

$$(\exists\ \nu_0 \in \mathbb{N})\ A_2(\nu; \delta, t_0) > A_1(\nu; \delta, t_0) \ \text{ при } \ \nu \geq \nu_0,$$

а из леммы 3.1 и определения произведения $R_{N,M}(s)$ следует, что

$$T_{N,M}(s) R_{N,M}(s) \neq 0 \ \text{ при } \ s \in \mathbb{C}_{1/M}.$$

Поэтому соотношение (3.15) показывает, что круг $K(s_0, r)$ содержит полюс функции $s \mapsto L(\Phi, s)$ при любом r в $\mathbb{R}_+^*$; следовательно, $s_0 \in \bar{\mathcal{A}}$ и, значит,

$$\bar{\mathcal{A}} \subseteq \mathbb{C}^{(0)}.$$

Обратное включение следует из мероморфности рассматриваемой функции в полуплоскости $\mathbb{C}_0$. Утверждение доказано.

Теорема 1.5.1. *Если полином* $\Phi(t)$ *унитарен, то функция* $s \mapsto L(\Phi, s)$ *мероморфно продолжима на всю комплексную плоскость. Если полином* $\Phi(t)$ *не является унитарным полиномом, то эта функция мероморфно продолжима в полуплоскость* $\mathbb{C}_0$, *а прямая* $\mathbb{C}^{(0)}$ *есть естественная рассматриваемой функции (так что функция* $s \mapsto L(\Phi, s)$ *не может быть продолжена влево от этой прямой).*

Доказательство. Утверждение теоремы вытекает из следствия 1, следствия 3.3 и следствия 3.5.

1.6 Доказательство основных теорем

1. Определим свёртку Адамара [87] в кольце формальных степенных рядов $\mathbb{C}[[t]]$ по формуле:

$$(\sum_{n=0}^{\infty} a_n t^n) * (\sum_{n=0}^{\infty} b_n t^n) := \sum_{n=0}^{\infty} a_n b_n t^n.$$

Обозначим через

$$\mathcal{A} := \{\det (1 - tA)^{-1} | A \in \bigcup_{n}^{\infty} M(n, \mathbb{C})\}$$

подгруппу "эйлеровских произведений" группы $(\mathbb{C}[[t]])^*$ и положим

$$(f_1 \circ f_2)(t) := \det (1 - t(A_1 \otimes A_2))^{-1},$$

где

$$f_i := \det (1 - tA_i)^{-1},\ f_i \in \mathcal{A}_i \ \text{ при } \ i = 1, 2.$$

Обозначим степень полинома $f(t)$ в $\mathbb{C}[t]$ через $\delta(f)$.

Предложение 1.6.1. *Пусть*

$$f_j(t) := \det (1 - tA_j)^{-1},\ A_j \in M(d_j, \mathbb{C}) \ \textit{при} \ 1 \leq j \leq r,$$

$$d_1 \geq ... \geq d_r \geq 1,\ d := \prod_{j=1}^{r} d_j \ \ u \ \ n := 1 - r + \sum_{j=1}^{r} d_j.$$

Тогда

$$(f_1 * ... * f_r)(t) = (f_1 \circ ... \circ f_r)(t) h(t)$$

с

$$h(t) \in \mathbb{C}[t],\ h(t) = 1\ (mod\, t^2) \ \ u \ \ \delta(h) \leq d - 1;$$

при этом

$$d_1 = d_2 = r = 2 \ \Rightarrow h(t) = (1 - |A_1 A_2| t^2). \tag{1.6.1}$$

Более того, если $f_j(t) := (1-t)^{-d_j}$ *при* $1 \le j \le r$, *то*

$$(f_1 * ... * f_r)(t) = (1-t)^{-n} f(t)$$

с

$$f(t) \in \mathbb{C}[t],\ f(t) = 1 + (d-n)t\ (mod\, t^2)\ \ и\ \ \delta(f) \le n - d_1. \tag{1.6.2}$$

Доказательство. Это утверждение доказывается несложными вычислениями в кольце $\mathbb{C}[[t]]$, см. [123, §3], [128, стр. 78 - 82 и 108 - 109].

Следствие 1.6.1. *Сохраняя обозначения и условия предложения 1, допустим, что*

$$(r \ge 2\ \ и\ \ d_1 > d_2 \ge 2)\ \ или\ \ (r \ge 3\ \ и\ \ d_3 \ge 2). \tag{1.6.3}$$

Тогда

$$(\exists \beta \in \mathbb{C})\ f(\beta) = 0\ и\ \ |\beta| < 1$$

Доказательство. Из соотношений (2) следует, что

$$f(t) = \prod_{1 \le j \le n-d_1} (1 + \beta_j t)\ \ \text{с} \sum_{1 \le j \le n-d_1} \beta_j = d - n$$

и, в частности,

$$\max\{|\beta_j|\ |1 \le j \le (n-d_1)\} \ge (d-n)(n-d_1)^{-1}.$$

Неравенство $(d-n) > (n-d_1)$ вытекает из условия (3). Следствие доказано.

2. Возвращаясь к обозначениям §1, no. 1, рассмотрим конечномерные нормированные представления

$$\rho_i \colon W(k) \to \mathrm{GL}(d_i, \mathbb{C}),\ 1 \le i \le r;$$

положим

$$\chi_i := \mathrm{tr}\ \rho_i\ \ \text{при}\ \ 1 \le i \le r,\ \vec{\chi} := (\chi_1, ..., \chi_r),$$

$$\rho := \rho_1 \otimes ... \otimes \rho_r,\ \chi := \mathrm{tr}\ \rho,\ \chi = \prod_{i=1}^{r} \chi_i,$$

и пусть

$$F_i(t) := \det\,(1 - t\rho_i)^{-1}\ \text{ при }\ 1 \le i \le r\ \text{ и }\ F(t) := \det\,(1 - t\rho)^{-1},$$

так что

$$\{F(t), F_i(t) | 1 \le i \le r\} \subseteq X(k)[t].$$

Пусть $g \in W(k)$ и $p \in \mathcal{P}(k)$; в соответствии с обозначениями §3 положим

$$F_{ig}(t) := \det\,(1 - t\rho_i(g))^{-1}\ \text{ и }\ F_{ip}(t) := \det\,(1 - t\rho_i(\sigma_p))^{-1}\ \text{ при }\ 1 \le i \le r,$$

$$F_g(t) := \det\,(1 - t\rho(g))^{-1}\ \text{ и }\ F_p(t) := \det\,(1 - t\rho(\sigma_p))^{-1}.$$

Ясно, что

$$F_g(t) = (F_{1g} \circ ... \circ F_{rg})(t)\ \text{ и }\ F_p(t) = (F_{1p} \circ ... \circ F_{rp})(t).$$

Пусть

$$G_g(t) := (F_{1g} * ... * F_{rg})(t)\ \text{ и }\ G_p(t) := (F_{1p} * ... * F_{rp})(t);$$

тогда, в силу предложения 1,

$$G_g(t) = F_g(t)h_g(t)\ \text{ с }\ h_g(t) \in \mathbb{C}[t],\ h_g(t) = 1\ (\mathrm{mod}\ t^2)\ \text{ и }\ \delta(h_g) \le d - 1. \tag{1.6.4}$$

и

$$G_p(t) = F_p(t)h_p(t)\ \text{ с }\ h_p(t) \in \mathbb{C}[t],\ h_p(t) = 1\ (\mathrm{mod}\ t^2)\ \text{ и }\ \delta(h_p) \le d-1. \tag{1.6.5}$$

По определению,

$$L(\vec{\chi}, s) = \prod_{p \in \mathcal{P}} G_p(|p|^{-s})\ \text{ и }\ L(\chi, s) = \prod_{p \in \mathcal{P}} F_p(|p|^{-s})\ \text{ при }\ s \in \mathbb{C}_1. \tag{1.6.6}$$

Лемма 1.6.1. *Существует полином* $\Phi(t)$ *в* $X(k)[t]$ *под условием*

$$\Phi_g(t) = h_g(t)\ \ \textit{при}\ \ g \in W(k). \tag{1.6.7}$$

Доказательство. В силу леммы 2.2,

$$G_g(t) = \sum_{m=1}^{\infty} t^m \prod_{i=1}^{r} \mathrm{tr}\ (S^m \rho_i)(g) \tag{1.6.8}$$

и

$$F_g(t)^{-1} = \sum_{m=1}^{\infty} (-1)^m t^m \mathrm{tr}\ (\Lambda^m \rho)(g) \tag{1.6.9}$$

при $g \in W(k)$. Положим

$$\Phi(t) := 1 + \sum_{l=1}^{d-1} b_l t^l \quad \text{с} \quad b_l := \sum_{l_1=1}^{l} (-1)^{l_1} \mathrm{tr}\ (\Lambda^{l_1} \rho) \prod_{i=1}^{r} \mathrm{tr}\ (S^{l-l_1} \rho_i).$$

Соотношение (7) следует из соотношений (8) и (9). Лемма доказана.

Положим

$$S(\vec{\chi}) := \bigcup_{i=1}^{r} S(\chi_i)$$

и заметим, что

$$|S(\vec{\chi})| < \infty \ \text{ и } \ S(\chi) \subseteq S(\vec{\chi}). \tag{1.6.10}$$

Следствие 1.6.2. *Имеет место соотношение*

$$(\forall p \in \mathcal{P}(k) \setminus S(\vec{\chi}))\ \Phi_p(t) = h_p(t). \tag{1.6.11}$$

Доказательство. Это утверждение непосредственно вытекает из леммы 1 и определений.

Предположим, не нарушая общности, что (ср. (1.1))

$$r \geq 2 \ \text{ и } \ d_1 \geq d_2 \geq \ldots \geq d_r \geq 2. \tag{1.6.12}$$

Следствие 1.6.3. *В предположении* (12) *построенный в лемме* 1 *полином* $\Phi(t)$ *унитарен тогда и только тогда, когда*

$$d_1 = r = 2. \tag{1.6.13}$$

Доказательство. Пусть $d_1 = r = 2$. Из соотношений (1), (4) и (7) следует тогда, что

$$\Phi_g(t) = 1 - \det(\rho_1(g)\rho_2(g))t^2 \text{ при } g \in W(k).$$

Но представления ρ_1 и ρ_2 эквивалентны унитарным представлениям, так что $|\det(\rho_1(g)\rho_2(g))| = 1$. Значит, $\gamma(\Phi) = 1$, и потому полином $\Phi(t)$ унитарен. Допустим, что условие (13) не выполняется; тогда из неравенств (12) следует, что имеет место соотношение (3). С другой стороны, при $f_j(t) := (1-t)^{-d_j}$, $1 \le j \le r$, из предложения 1 и равенства (7) вытекает, что

$$\Phi_1(t) = h_1(t) = (f_1 * ... * f_r)(t)(1-t)^d = (1-t)^{d-n}f(t)$$

с $f(t)$ под условием (2). Значит, в силу следствия 1 полином $\Phi(t)$ не унитарен. Следствие 3 доказано.

Доказательство теоремы 1.2. Из соотношений (5), (6), (10) и (11) следует, что

$$L(\vec{\chi}, s) = L(\chi, s) \prod_{p \in \mathcal{P}(k) \setminus S(\vec{\chi})} \Phi_p(|p|^{-s}) \prod_{p \in S(\vec{\chi})} G_p(|p|^{-s}) F_p(|p|^{-s})^{-1}. \qquad (1.6.14)$$

Ввиду соотношений (10) и (14) утверждение теоремы вытекает из следствия 3 и теоремы 5.1.

Доказательство теоремы 1.1. Пусть $\psi_i \in gr(k_i)$ при $1 \le i \le r$. Отождествив характер ψ_i с одномерным представлением группы $W(k_i)$, положим

$$\chi_i := \operatorname{Ind}_{W(k_i)}^{W(k)} \psi_i \text{ при } 1 \le i \le r.$$

Так как

$$d_i = \chi_i(1) = [k_i : k] \text{ при } 1 \le i \le r,$$

утверждение теоремы 1.1 вытекает из теоремы 1.2.

При $d_1 = r = 2$ равенство (14) принимает особенно простой вид.

Теорема 1.6.1. *Пусть* $d_1 = d_2 = r = 2$ *и* $\psi_i \in gr(k_i)$ *при* $i = 1, 2$. *Если* $k_1 \neq k_2$, *то*

$$L(\vec{\psi}, s) = L(\psi, s)L(\psi_0, 2s)^{-1} \prod_{p|D} f_p(|p|^{-s}),$$

где

$$D := (D(k_1|k), D(k_2|k)),\ f_p(t) \in \mathbb{C}[t],\ \delta(f_p) \leq 3,$$

$D(k_i|k)$ *есть дискриминант расширения* $k_i|k$ *при* $i = 1, 2$,

$$\psi := (\psi_1 \circ N_{K/k_1})(\psi_2 \circ N_{K/k_2}),\ K := k_1 \cdot k_2 \ \text{ и } \ \psi_0 \in gr(k).$$

При $k_1 = k_2 =: K$ *имеем*

$$L(\vec{\psi}, s) = L(\psi_1\psi_2, s)L(\psi_1\bar{\psi_2}(\psi_2 \circ N_{K/k}), s)L(\psi_0, 2s)^{-1} \prod_{p|D(K|k)} f_p(|p|^{-s})^{-1},$$

где $\psi_0 \in gr(k)$ *и* $f_p(t) := 1 + t(\psi_1\psi_2)(\mathfrak{p})$ *при* $p = \mathfrak{p}^2,\ \mathfrak{p} \in \mathcal{P}(K),\ p \in \mathcal{P}(k)$.

Доказательство. Это утверждение доказывается прямым вычислением, см. [121], [128, стр. 111 - 114].

Глава 2
Целые точки и целые модели аффинных торических многообразий.

2.1 Введение

В этой главе изучается распределение целых точек на аффинных торических многообразиях, определённых над кольцом целых рациональных чисел. Простейшие многообразия такого рода - это квадрики вида Spec $\mathbb{Z}[x]/(F(x))$, где $f(x_1, x_2)$ и $g(x_3, x_4)$ суть бинарные положительно определённые квадратичные формы с целыми рациональными коэффициентами и $F(x) := f(x_1, x_2) - g(x_3, x_4)$. Распределение целых точек на таких гиперповерхностях изучалось в моих первых работах [26] - [30]. В работах [129], [130], [136] исследуется множество целых точек норменных многообразий; целые точки аффинных торических многообразий изучаются в работах [137] - [140] и в §4 этой главы (теорема 4.1). Определённое над полем алгебраических чисел торическое многообразие имеет, вообще говоря, много попарно неизоморфных моделей над кольцом целых этого поля. Целые модели алгебраических торов и аффинных торических многообразий изучаются в совместных работах [14], [6], [15]. В следующем параграфе приводятся некоторые определения и результаты, связанные с теорией алгебраических торов и аффинных торических многообразий, определённых над произвольным полем нулевой характеристики. Хотя и определение аффинного T - торического многообразия, и теорема 2.1, возможно, известны специалистам, нам не удалось найти в литературе доказательства этой теоремы. В §3 строится естественная явно заданная целая модель алгебраического тора T, определённого над полем алгебраических чисел, и соответствующие целые модели аффинных T - торических многообразий (изложение в §2 и §3 следует нашей совместной с Б.Э. Кунявским работе [15]). Было бы интересно изучить распределение целых

точек на схемах $\mathcal{X}_{\mathfrak{B}}$ (см. §3), определённых над кольцами целых произвольных полей алгебраических чисел; по-видимому, некоторые из описанных в §4 результатов имеют место и в этом случае, ср. [137] - [140].

Обозначения. При $b \in \mathbb{R}$ положим

$$b^+ := \frac{1}{2}\,(|b| + b) \;\text{ и }\; b^- := \frac{1}{2}\,(|b| - b).$$

Рассмотрим два коммутативных кольца A и B под условием $B \subseteq A$ и B - схему Y; положим, для краткости,

$$Y \times_B A := Y \times_{\operatorname{Spec} B} \operatorname{Spec} A.$$

Пусть k - поле алгебраических чисел или конечное расширение поля $\mathbb{Q}_p$, $p \in \mathcal{P}$, $\mathfrak{o}$ - кольцо целых поля k, $\mathfrak{a}$ - идеал кольца $\mathfrak{o}$ и $\alpha \in k$; будем говорить, что $\alpha = 1\ (\mathfrak{a})$, если $\alpha \in k^*$, $\alpha = \alpha_1\alpha_2^{-1}$ с $(\alpha_1 - \alpha_2) \in \mathfrak{a}$ и $(\alpha_2, \mathfrak{a}) = (1)$. Более того, сравнение $\alpha = 1\ (\mathfrak{a})$ при $\alpha \in k^m$ означает, что $\alpha_i = 1\ (\mathfrak{a})$ при $1 \leq i \leq m$.

2.2 Аффинные торические многообразия

1. Рассмотрим d - мерный алгебраический тор T, определённый над полем k характеристики 0 (см., например, [5]). Тор T расщепляется над $\bar{k}$, так что

$$T \times_k \bar{k} \cong G_{m,\bar{k}}^d\,.$$

Проекции

$$\chi_i \colon T \times_k \bar{k} \to G_{m,\bar{k}},\ 1 \leq i \leq d, \tag{2.2.1}$$

определены над конечным нормальным расширением $L|k$; любое такое поле L будем называть *полем расщепления* тора T. Проекции (1) порождают свободную абелеву группу

$$\hat{T} := \operatorname{Hom}(T \times_k \bar{k}, G_{m,\bar{k}})$$

ранга d, группу рациональных характеров тора T. Группа Галуа G_k действует на $\hat{T}$; обозначим через

$$\bar{\rho}\colon G_k \to \mathrm{GL}(d,\mathbb{Z})$$

целочисленное представление, определяемое этим действием. Рассмотрим поле расщепления L тора T; пусть $n := [L:k]$, $\Gamma := \mathrm{Gal}(L|k)$ и $T_L := T \times_k L$. Ясно, что

$$T_L \cong G_{m,L}^d \ .$$

Представление $\bar{\rho}$ пропускается через группу Γ, так что $\bar{\rho} = \rho \circ \tau$ для некоторого представления

$$\rho\colon \mathrm{Gal}(L|k) \to \mathrm{GL}(d,\mathbb{Z}),$$

где τ есть естественный эпиморфизм абсолютной группы Галуа G_k на группу Γ. Представление ρ определяет действие группы Γ на свободном $\mathbb{Z}$-модуле

$$\mathfrak{M} := \mathrm{Hom}(T_L, G_{m,L})$$

ранга d. Рассмотрим $\mathbb{Z}[\Gamma]$-модуль $\mathfrak{M}^\perp$, двойственный к $\mathfrak{M}$, и контрагредиентное к ρ целочисленное представление $\tilde{\rho}$. Выберем $\mathbb{Z}$ - базис $\{e_1, ..., e_d\}$ модуля $\mathfrak{M}^\perp$ и положим

$$\tilde{\rho}(g)\ e_i = \sum_{j=1}^{d} e_j\ r(g)_{ji} \ \text{ при } \ 1 \le i \le d,\ r(g) \in M_d(\mathbb{Z}). \tag{2.2.2}$$

Далее выберем базис $\{\omega_1, ..., \omega_n\}$ расширения $L|k$, под условием $\omega_1 = 1$, и введём в рассмотрение $d+1$ линейных форм

$$t_i := \sum_{j=1}^{n} x_i^{(j)} \omega_j,\ t_i \in L[x] \ \text{ при } \ 0 \le i \le d,$$

от переменных

$$x := (..., x_i^{(j)}, ...),\ 0 \le i \le d,\ 1 \le j \le n.$$

Положим

$$gt_i := \sum_{j=1}^{n} x_i^{(j)} g\omega_j \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma.$$

Соотношения

$$\prod_{i=0}^{d} t_i - 1 = \sum_{j=1}^{n} P_0^{(j)}(x)\,\omega_j$$

и

$$gt_i \prod_{j=1}^{d} t_j^{r(g)_{ji}^-} - \prod_{j=1}^{d} t_j^{r(g)_{ji}^+} = \sum_{j=1}^{n} P_{i,g}^{(j)}(x)\,\omega_j \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma \setminus \{1\}$$

однозначно определяют систему многочленов

$$\mathcal{P}_0 := \{P_0^{(j)}(x),\ P_{i,g}^{(j)}(x) | 1 \le j \le n,\ 1 \le i \le d,\ g \in \Gamma \setminus \{1\}\}$$

с коэффициентами в поле k; пусть

$$I := (\mathcal{P}_0)_{k[x]} \ \text{ и } \ B := k[x]/I.$$

По определению,

$$T = \operatorname{Spec} B; \tag{2.2.3}$$

иными словами, тор T задаётся системой уравнений

$$\prod_{j=0}^{d} t_j = 1,\ gt_i = \prod_{j=1}^{d} t_j^{r(g)_{ji}} \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma,$$

ср. [5], [138]. Положим $B_L := B \otimes_k L$, тогда

$$T_L = \operatorname{Spec} B_L \ \text{ и } \ B_L = L[t, t^{-1}], \tag{2.2.4}$$

где $t^{-1} := (t_1^{-1}, ...,\ t_d^{-1})$. Продолжим действие $g\colon L \to L,\ g \in \Gamma$, группы Галуа Γ на L до автоморфизма k - алгебры B_L, положив

$$g\colon B_L \to B_L,\ g : t_i \mapsto \prod_{j=1}^{d} t_j^{r(g)_{ji}} \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma, \tag{2.2.5}$$

и заметим, что

$$B = (B_L)^{\Gamma}. \tag{2.2.6}$$

2. Определённое над L нормальное многообразие X называется T_L - *торическим многообразием*, если X содержит изоморфное тору T_L плотное открытое подмножество U и определено действие

$$T_L \times X \to X,$$

продолжающее естественное действие

$$T_L \times U \to X,$$

индуцированное операцией умножения на торе T_L, ср. [84, стр. 3]. Рассмотрим строго выпуклый рациональный многогранный конус (сврм-конус) $\sigma(\mathbb{Q})$ в $\mathbb{Q}$-векторном пространстве $V := \mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{Q}$, двойственный к $\sigma(\mathbb{Q})$ конус

$$\sigma(\mathbb{Q})^{\perp} = \{v | v \in V^{\perp},\ (v|u) \geq 0 \ \text{ при } \ u \in \sigma(\mathbb{Q})\}$$

в векторном пространстве $V^{\perp} := \mathfrak{M}^{\perp} \otimes_{\mathbb{Z}} \mathbb{Q}$ и две полугруппы

$$\sigma := \sigma(\mathbb{Q}) \cap \mathfrak{M} \ \text{ и } \ \sigma^{\perp} := \sigma(\mathbb{Q})^{\perp} \cap \mathfrak{M}^{\perp}.$$

Выберем минимальную систему образующих $\{u_1, ..., u_l\}$ полугруппы $\sigma^{\perp}$ (ср. [84, стр. 14]) и обозначим через

$$\mathfrak{R}(\sigma) := \{a | a \in \mathbb{Z}^l,\ \sum_{j=1}^{l} a_j u_j = 0\}$$

группу соотношений между этими образующими. Пусть

$$u_j = \sum_{i=1}^{d} e_i\ c_{ij} \ \text{ при } \ 1 \leq j \leq l,\ c \in M_{dl}(\mathbb{Z}). \tag{2.2.7}$$

Ясно, что

$$\mathfrak{R}(\sigma) = \{a | a \in \mathbb{Z}^l,\ ca = 0\}. \tag{2.2.8}$$

Положим

$$\mathfrak{C}(\sigma) := \{b | b \in M_{ld}(\mathbb{Z}),\ cb = 1\}$$

и заметим, что $\mathfrak{C}(\sigma) \neq \emptyset$, ибо множество образующих $\{u_1, ..., u_l\}$ полугруппы $\sigma^{\perp}$ порождает $\mathbb{Z}$-модуль $\mathfrak{M}^{\perp}$. Рассмотрим кольцо многочленов Laurent'a $L[s, s^{-1}]$ от переменных $s := (s_1, ..., s_l)$, где $s^{-1} := (s_1^{-1}, ..., s_l^{-1})$, и обозначим через

$$\mathcal{L}\{s\} := \{\prod_{j=1}^{l} s_j^{a_j} | a \in \mathbb{Z}^l\} \ \text{ и } \ \mathcal{L}\{t\} := \{\prod_{j=1}^{d} t_j^{a_j} | a \in \mathbb{Z}^d\}$$

множества мономов Laurent'а от переменных s и t. Определим гомоморфизмы L-алгебр:

$$\varphi_0 : L[s, s^{-1}] \to B_L,\ s_j \mapsto \prod_{i=1}^{d} t_i^{c_{ij}} \ \text{ при } \ 1 \le j \le l,$$

и

$$\psi_0(b)\colon B_L \to L[s, s^{-1}],\ t_i \mapsto \prod_{j=1}^{l} s_j^{b_{ji}} \ \text{ при } \ b \in \mathfrak{C}(\sigma) \ \text{ и } \ 1 \le i \le d.$$

Ясно, что $\varphi_0 \circ \psi_0(b) = 1$; следовательно,

$$\varphi_0(\mathcal{L}\{s\}) = \varphi_0(\mathcal{L}\{t\}) \ \text{ и } \ \varphi_0(L[s, s^{-1}]) = B_L. \tag{2.2.9}$$

Положим

$$\mathcal{P}_1(\sigma) := \{h_a(s) | h_a(s) := \prod_{j=1}^{l} s_j^{a_j} - 1,\ a \in \mathfrak{R}(\sigma)\}$$

и пусть

$$\bar{J}_0(\sigma) := (\mathcal{P}_1(\sigma))_{L[s,s^{-1}]}\ .$$

Лемма 2.2.1 . *Имеет место соотношение*

$$\bar{J}_0(\sigma) = \mathrm{Ker}\ \varphi_0\ . \tag{2.2.10}$$

Доказательство. Из соотношения (8) и определения гомоморфизма φ_0 следует, что

$$\bar{J}_0(\sigma) \subseteq \mathrm{Ker}\ \varphi_0\ . \tag{2.2.11}$$

Пусть $q(s) \in \mathrm{Ker}\ \varphi_0$; положим

$$q(s) = \sum_{1 \le i \le R,\ 1 \le j \le S} \alpha_{ij} m_{ij}(s),$$

где

$$\alpha_{ij} \in L,\ m_{ij}(s) \in \mathcal{L}\{s\} \ \text{ при } \ 1 \le i \le R,\ 1 \le j \le S,$$

$$\varphi_0(m_{ij}(s)) = \varphi_0(m_{i1}(s)) \ \text{ при } \ 1 \le i \le R,\ 1 \le j \le S \tag{2.2.12}$$

и

$$\varphi_0(m_{i1}(s)) \ne \varphi_0(m_{k1}(s)) \ \text{ при } \ 1 \le i < k \le R.$$

Так как $\varphi_0(q(s)) = 0$, отсюда следует, что

$$\sum_{1\le j\le S} \alpha_{ij} = 0 \ \text{ при } \ 1 \le i \le R. \tag{2.2.13}$$

С другой стороны, из соотношений (8) и (12) и определения отображения φ_0 вытекает, что

$$m_{ij}(s) = m_{i1}(s) \prod_{h=1}^{l} s_h^{a(i,j)_h} \tag{2.2.14}$$

с

$$a(i,j) \in \mathfrak{R}(\sigma). \tag{2.2.15}$$

В силу равенств (13) и (14) имеет место соотношение

$$q(s) = \sum_{1\le i\le R,\ 1\le j\le S} \alpha_{ij} m_{i1}(s)(\prod_{h=1}^{l} s_h^{a(i,j)_h} - 1). \tag{2.2.16}$$

Соотношения (15) и (16) показывают, что $q(s) \in \bar{J}_0(\sigma)$; таким образом,

$$\text{Ker } \varphi_0 \subseteq \bar{J}_0(\sigma). \tag{2.2.17}$$

Соотношение (10) следует из соотношений (11) и (17). Лемма доказана.

Следствие 2.2.1 . *Имеет место изоморфизм*

$$\psi : B_L \to L[s, s^{-1}]/\bar{J}_0(\sigma),\ B_L \cong L[s, s^{-1}]/\bar{J}_0(\sigma). \tag{2.2.18}$$

Доказательство. Существование изоморфизма ψ вытекает из леммы 1 и соотношения (9).

Положим

$$J_0(\sigma) := \bar{J}_0(\sigma) \cap L[s];$$

ясно, что

$$J_0(\sigma) = (\mathcal{P}_2(\sigma))_{L[s]}\ ,$$

где

$$\mathcal{P}_2(\sigma) := \{f_a(s) | f_a(s) := \prod_{j=1}^{l} s_j^{a_j^+} - \prod_{j=1}^{l} s_j^{a_j^-},\ a \in \mathfrak{R}(\sigma)\}.$$

Следствие 2.2.2. *Пусть* $\{m_1(s), m_2(s)\} \subseteq \mathcal{L}\{s\}) \cap L[s]$, $p(s) \in L[s]$ *и* $q(s) := m_1(s) + p(s)m_2(s)$. *Если* $q(s) \in J_0(\sigma)$, *то*

$$(\exists\, m_3(s) \in (\mathcal{L}\{s\} \cap L[s]),\ a \in \mathfrak{R}(\sigma))\ m_1(s) = m_2(s)m_3(s)\prod_{j=1}^{l} s_j^{a_j}$$

Доказательство. Поскольку $q(s) \in J_0(\sigma)$, в кольце $L[t, t^{-1}]$ имеет место равенство

$$\varphi_0(\frac{m_1(s)}{m_2(s)} + p(s)) = 0.$$

Представим многочлен $p(s)$ в виде

$$p(s) = \sum_{i=1}^{N} \alpha_i n_i(s) \ \text{ с } \ \alpha_i \in L,\ n_i(s) \in \mathcal{L}\{s\}) \cap L[s] \ \text{ при } \ 1 \leq i \leq N.$$

Из этих соотношений следует, что

$$(\exists\, m_3(s) \in \{n_i(s) | 1 \leq i \leq N\})\ \varphi_0(\frac{m_1(s)}{m_2(s)}) = \varphi_0(m_3(s))$$

и потому

$$m_1(s) = m_2(s)m_3(s)\prod_{j=1}^{l} s_j^{a_j} \ \text{ с } \ a \in \mathfrak{R}(\sigma).$$

Утверждение доказано.

Положим

$$A_L(\sigma) := L[s]/J_0(\sigma) \ \text{ и } \ X_L(\sigma) := \operatorname{Spec} A_L(\sigma). \tag{2.2.19}$$

Легко видеть, что $X_L(\sigma)$ есть T_L - торическое многообразие; будем говорить, что это многообразие $X_L(\sigma)$ задаётся сврм-конусом $\sigma(\mathbb{Q})$, ср. [84, стр. 19]. Можно доказать, что любое *аффинное* T_L-торическое многообразие задаётся некоторым сврм-конусом, см., например, [143]. Обозначим через

$$\lambda_1 \colon T_L \to X_L(\sigma)$$

доминантную открытую иммерсию тора T_L в $X_L(\sigma)$.

Пример 1. Легко видеть, что $X_L(\{0\}) \cong T_L$.

3. Пусть $b \in M_{ld}(\mathbb{Z})$, а матрицы $r(g)$ и c определены по формулам (2) и (7); положим

$$\tilde{r}(g,b) := br(g)c \ \text{ при } \ g \in \Gamma \tag{2.2.20}$$

и заметим, что

$$r(g) \in M_d(\mathbb{Z}),\ c \in M_{dl}(\mathbb{Z}),\ \tilde{r}(g,b) \in M_l(\mathbb{Z}).$$

Ясно, что

$$(\forall\, b \in \mathfrak{C}(\sigma))\ \tilde{\rho}(g)\ u_i = \sum_{j=1}^{l} u_j\ \tilde{r}(g,b)_{ji} \ \text{ при } \ 1 \le i \le l. \tag{2.2.21}$$

Лемма 2.2.2. *Пусть* $g \in \Gamma,\ a \in \mathfrak{R}(\sigma),\ m \in \mathbb{N}$ *и* $m \le l$. *Тогда найдётся матрица* b *под условием*

$$b \in M_{ld}(\mathbb{Z}),\ cb = 0\ u\ \tilde{r}(g,b)_{jm} = a_j \ \ при \ \ 1 \le j \le l.$$

Доказательство. Пусть

$$a = \sum_{j=1}^{t} \alpha_j v_j \ \text{ с } \ \alpha \in \mathbb{Z}^t \tag{2.2.22}$$

для некоторого $\mathbb{Z}$ - базиса $\{v_1, ..., v_t\}$ группы $\mathfrak{R}(\sigma)$. Поскольку отображение $b \mapsto br(g)$ есть автоморфизм группы

$$N(\sigma) := \{b \mid \ b \in M_{ld},\ cb = 0\},$$

достаточно найти матрицу b под условием

$$b \in N(\sigma) \ \text{ и } \ (bc)_{jm} = a_j \text{ при } 1 \le j \le l.$$

Но $(c_{1j}, ..., c_{dj}) = (1)$ при $1 \le j \le l$, ибо $\{u_1, \ \ldots, \ u_l\}$ есть минимальная система образующих насыщенной полугруппы $\sigma^{\perp}$, и потому

$$(\exists\, w \in M_{ld})\ \alpha_i = \sum_{j=1}^{d} c_{jm} w_{ji} \ \text{ при } \ 1 \le i \le t. \tag{2.2.23}$$

Положим

$$b^{(i)} = \sum_{j=1}^{d} w_{ij} v_j \text{ при } 1 \leq i \leq d \tag{2.2.24}$$

и обозначим через $b := (b^{(1)}, ..., b^{(d)})$ матрицу со столбцами $b^{(i)}$. По построению, $b \in N(\sigma)$, а из соотношений (22) - (24) вытекает, что

$$a = \sum_{i=1}^{t} b^{(i)} c_{im}$$

и, следовательно,

$$a_j = \sum_{i=1}^{t} b_{ji} c_{im} = (bc)_{jm} \text{ при } 1 \leq j \leq d.$$

Лемма доказана.

Следствие 2.2.3. *Пусть*

$$\mathcal{P}_3(\sigma) := \{s_j - \prod_{i=1}^{l} s_i^{(bc)_{ij}} | b \in \mathfrak{C}(\sigma),\ 1 \leq j \leq l\},$$

тогда

$$\bar{J}_0(\sigma) = (\mathcal{P}_3(\sigma))_{L[s,s^{-1}]}\ .$$

Доказательство. Заметим прежде всего, что

$$\{s_j | 1 \leq j \leq l\} \subseteq (L[s, s^{-1}])^*. \tag{2.2.25}$$

Пусть $b \in \mathfrak{C}(\sigma)$, тогда $(bc - 1) \in \mathfrak{R}(\sigma)$. Но

$$s_j - \prod_{i=1}^{l} s_i^{(bc)_{ij}} = s_j(1 - \prod_{i=1}^{l} s_i^{(bc-1)_{ij}})$$

и потому, ввиду (25),

$$(s_j - \prod_{i=1}^{l} s_i^{(bc)_{ij}}) \subseteq (1 - \prod_{i=1}^{l} s_i^{(bc-1)_{ij}}).$$

Таким образом,

$$(\mathcal{P}_3(\sigma))_{L[s,s^{-1}]} \subseteq (\mathcal{P}_1(\sigma))_{L[s,s^{-1}]}\ .$$

Обратно, пусть $v \in \mathfrak{R}(\sigma)$ и пусть $b_0 \in \mathfrak{C}(\sigma)$, так что $cb_0 = 1$. Положим $b_0 c = 1 + a$, тогда

$$ca = 0,\ a = (a^{(1)}, ..., a^{(l)})\ \text{ с }\ a^{(j)} \in \mathfrak{R}(\sigma)\ \text{ при }\ 1 \leq j \leq l.$$

В силу леммы 2,

$$(\exists\, \beta \in \mathfrak{C}(\sigma))\ (\beta c)_{ij} = v_i - a_i^j\ \text{ при }\ 1 \leq i, j \leq l.$$

Положим $b := b_0 + \beta$. Ясно, что

$$(bc)_{ij} = (b_0 c)_{ij} + (\beta c)_{ij} = (\delta_{ij} + a_i^j) + (v_i - a_i^j) = \delta_{ij} + v_i\ \text{ при }\ 1 \leq i, j \leq l$$

и потому

$$(s_j - \prod_{i=1}^{l} s_i^{(bc)_{ij}}) = (s_j(1 - \prod_{i=1}^{l} s_i^{v_i})) = (1 - \prod_{i=1}^{l} s_i^{v_i}),$$

в силу соотношения (25), так что

$$(\mathcal{P}_1(\sigma))_{L[s,s^{-1}]} \subseteq (\mathcal{P}_3(\sigma))_{L[s,s^{-1}]}\ .$$

Итак,

$$(\mathcal{P}_3(\sigma))_{L[s,s^{-1}]} = (\mathcal{P}_1(\sigma))_{L[s,s^{-1}]} = \bar{J}_0(\sigma).$$

Утверждение доказано.

Пусть $b \in \mathfrak{C}(\sigma)$; продолжим действие $g : L \to L,\ g \in \Gamma$, группы Галуа Γ на L до автоморфизма на k-алгебры $L[s, s^{-1}]/\bar{J}_0(\sigma)$, положив

$$gs_j = \prod_{i=1}^{l} s_i^{\tilde{r}(g,b)_{ij}}\ \text{ при }\ 1 \leq j \leq l,\ g \in \Gamma. \tag{2.2.26}$$

Легко видеть, что $\varphi_0(gs_j) = g\varphi_0(s_j)$ при $1 \leq j \leq l$ и $g \in \Gamma$; поэтому изоморфизм (18) является Γ - изоморфизмом. Отождествим, не нарушая общности, $k[\Gamma]$ - модули B_L и $L[s, s^{-1}]/\bar{J}_0(\sigma)$; в частности, будем считать, что $A_L(\sigma) \subseteq B_L$.

4. Говорят, что отделимая k-схема $Y(\sigma)$ есть аффинное T-*торическое многообразие*, если выполнены следующие условия:

а) существует k-иммерсия

$$\lambda_2 : T \to Y(\sigma);$$

б) определён L-изоморфизм

$$\varphi_1 : Y(\sigma) \times_k L \to X_L(\sigma);$$

в) диаграмма

$$\begin{array}{ccc} T & \xrightarrow{\lambda_2} & Y(\sigma) \\ {\scriptstyle p}\uparrow & & \uparrow{\scriptstyle q} \\ T_L & \xrightarrow{\lambda_1} & X_L(\sigma) \end{array} \qquad (2.2.27)$$

коммутативна (здесь: $p : T_L \to T$ и $p' : Y(\sigma) \times_k L \to Y(\sigma)$ суть естественные проекции, а $q := p' \circ \varphi_1^{-1}$).

Будем говорить, что торическое многообразие $Y(\sigma)$ задаётся сврм-конусом $\sigma(\mathbb{Q})$.

Лемма 2.2.3. *Аффинное T-торическое многообразие есть аффинная k-схема конечного типа.*

Доказательство. Рассмотрим аффинное T-торическое многообразие Y. По определению, существует конечное расширение полей $L|k$ такое, что схема $Y \times_k L$ есть аффинная L-схема конечного типа. Следовательно, схема Y есть аффинная k-схема конечного типа [86, стр. 20] (ср. [164, пример 2 на стр. 23]). Лемма доказана.

Теорема 2.2.1. *Аффинное T-торическое многообразие является аффинной k-схемой конечного типа, содержащей изоморфное тору T открытое плотное подмножество. Для любого поля расщепления L тора T с группой Галуа $\Gamma := \mathrm{Gal}(L|k)$ и любого Γ - инвариантного сврм-конуса существует единственное, с точностью до изоморфизма, аффинное T-торическое многообразие, задаваемое этим конусом. Сврм-конус, задающий аффинное T-торическое многообразие, Γ - инвариантен.*

Доказательство. Рассмотрим аффинное T-торическое многообразие $Y(\sigma)$, задаваемое сврм-конусом $\sigma(\mathbb{Q})$. В силу леммы 3,

$$Y(\sigma) = \operatorname{Spec} B_0(\sigma) \tag{2.2.28}$$

для некоторой конечно порождённой коммутативной k-алгебры $B_0(\sigma)$. Из условия а), соотношения (3) и соотношения (6) следует существование гомоморфизма

$$\lambda_2^* : B_0(\sigma) \to (B_L)^\Gamma,$$

так что из коммутативности диаграммы (27) вытекает, что имеет место следующая коммутативная диаграмма:

$$\begin{array}{ccc} A_L(\sigma) & \xrightarrow{\lambda_1^*} & B_L \\ {\scriptstyle q^*}\uparrow & & \uparrow{\scriptstyle p^*} \\ B_0(\sigma) & \xrightarrow{\lambda_2^*} & (B_L)^\Gamma \end{array} \tag{2.2.29}$$

Поскольку отображения λ_1^*, p^* и q^* в диаграмме (29) суть мономорфизмы, гомоморфизм λ_2^* также является мономорфизмом. Поэтому, не нарушая общности, можно считать, что

$$B_0(\sigma) \subseteq A_L(\sigma) \subseteq B_L \ \text{ и } \ B_0(\sigma) \subseteq (B_L)^\Gamma \subseteq B_L.$$

Следовательно, $B_0(\sigma) \subseteq A_L(\sigma) \cap (B_L)^\Gamma$ и потому

$$B_0(\sigma) \subseteq (A_L(\sigma))^\Gamma, \tag{2.2.30}$$

так как $A_L(\sigma) \cap (B_L)^\Gamma = (A_L(\sigma))^\Gamma$. Более того, согласно условию б), соотношению (19) и соотношению (28), можно считать, что

$$B_0(\sigma) \otimes_k L = A_L(\sigma). \tag{2.2.31}$$

Как легко заметить, из соотношений (30) и (31) вытекает, что

$$B_0(\sigma) = (A_L(\sigma))^\Gamma. \tag{2.2.32}$$

Действительно, пусть $\alpha \in (A_L(\sigma))^{\Gamma}$. Выберем базис $\{\omega_j | 1 \leq j \leq n\}$ расширения $L|k$ под условием $\omega_1 = 1$. Из соотношения (31) следует, что

$$(\exists\, \{a_1, ..., a_n\} \subseteq B_0(\sigma))\ \alpha = \sum_{j=1}^{n} a_j \omega_j. \tag{2.2.33}$$

Ввиду соотношений (30) и (33), имеют место следующие равенства:

$$\alpha = \sum_{j=1}^{n} a_j g\omega_j \ \text{ при } \ g \in \Gamma. \tag{2.2.34}$$

Но

$$\det\,(g\omega_j)_{1\leq j\leq n,\, g\in\Gamma} \neq 0 \ \text{ и } \ (\forall\, g \in \Gamma)\ \alpha = \alpha g\omega_1,$$

так что $a_1 = \alpha,\ a_j = 0 \ \text{ при } \ 2 \leq j \leq n$ и, значит, $\alpha \in B_0(\sigma)$. Равенства (19), (26), (28) и (32) определяют схему $Y(\sigma)$ однозначно с точностью до изоморфизма. По построению, открытое плотное подмножество схемы $Y(\sigma)$, определяемое соотношением

$$\prod_{j=1}^{l} s_j \neq 0,$$

изоморфно тору T. С другой стороны, из соотношений (31) и (32) вытекает, что

$$A_L(\sigma) = (A_L(\sigma))^{\Gamma} \otimes_k L;$$

значит, алгебра $A_L(\sigma)$ является Γ - инвариатной подалгеброй алгебры B_L и, в частности,

$$gs_j \in A_L(\sigma) \ \text{ при } \ 1 \leq j \leq l,\ g \in \Gamma.$$

Иными словами,

$$(\forall\, 1 \leq j \leq l,\ g \in \Gamma)\ (\exists\, h_{g,j}(s) \in L[s])\ (gs_j - h_{g,j}(s)) \in J_0(\sigma).$$

Положим

$$f_{g,j,b}(s) := h_{g,j}(s) \prod_{i=1}^{l} s_i^{\tilde{r}(g,b)_{ij}^{-}} - \prod_{i=1}^{l} s_i^{\tilde{r}(g,b)_{ij}^{+}}.$$

Ввиду (26) имеем

$$f_{g,j,b}(s) \in J_0(\sigma) \ \text{ при } \ 1 \le j \le l, \ g \in \Gamma, \ b \in \mathfrak{C}(\sigma)$$

и, значит, в силу следствия 2,

$$\tilde{r}(g,b)_{ij} = n(g,b,j)_i + a(g,b,j)_i \ \text{ с } \ n(g,b,j) \in \mathbb{N}_0^l \ \text{ и } \ a(g,b,j) \in \mathfrak{R}(\sigma) \quad (2.2.35)$$

при всех i, j, g, b под условием

$$1 \le i, j \le l, \ g \in \Gamma \ \text{ и } \ b \in \mathfrak{C}(\sigma).$$

Из соотношений (21) и (35) вытекает, что

$$gu_j = \sum_{i=1}^{l} u_i \, \tilde{r}(g,b)_{ij} = \sum_{i=1}^{l} u_i \, (n(g,b,j)_i + a(g,b,j)_i) = \sum_{i=1}^{l} u_i \, n(g,b,j)_i$$

с $n(g,b,j) \in \mathbb{N}_0^l$; следовательно, конус $\sigma(\mathbb{Q})^\perp$, а, значит, и конус $\sigma(\mathbb{Q})$ являются Γ - инвариантными.

Обратно, предположим, что сврм-конус $\sigma(\mathbb{Q})$ и, следовательно, конус $\sigma(\mathbb{Q})^\perp$ являются Γ - инвариантными. Докажем, что схема

$$Y(\sigma) := \operatorname{Spec} \left(A_L(\sigma)\right)^\Gamma$$

есть T - торическое многообразие, задаваемое конусом $\sigma(\mathbb{Q})$. Пусть $g \in \Gamma$; из Γ - инвариантности конуса $\sigma(\mathbb{Q})^\perp$ следует, что

$$\sum_{j=1}^{l} u_i \, \tilde{r}(g,b)_{ji} = gu_i = \sum_{i=1}^{l} u_i \, \beta(g)_{ji} \ \text{ с } \ \beta(g)_{ji} \in \mathbb{N}_0 \ \text{ при } \ 1 \le i, j \le l$$

и, следовательно,

$$\tilde{r}(g,b)_{ji} = \beta(g)_{ji} + a(g,b,i)_j \ \text{ с } \ a(g,b,i) \in \mathfrak{R}(\sigma) \ \text{ при } \ 1 \le i, j \le l.$$

В силу леммы 2, имеем

$$(\exists \, b_1 \in M_{ld}(\mathbb{Z}))\ cb_1 = 0 \ \text{ и } \ \tilde{r}(g,b_1)_{ji} = -a(g,b,i)_j \ \text{ при } \ 1 \le i, j \le l;$$

положим $b_2 := b + b_1$, тогда

$$\tilde{r}(g, b_2)_{ji} = \beta(g)_{ji} \text{ при } 1 \leq i, j \leq l.$$

Из этих соотношений вытекает, что k - алгебра $A_L(\sigma)$ является Γ - инвариатной алгеброй, ибо, по определению,

$$gs_i = \prod_{j=1}^{l} s_j^{\tilde{r}(g,b_2)_{ji}} = \prod_{j=1}^{l} s_j^{\beta(g)_{ji}} \text{ при } 1 \leq i \leq l \text{ и } g \in \Gamma.$$

Таким образом, имеет место коммутативная диаграмма

$$\begin{array}{ccc} A_L(\sigma) & \xrightarrow{\lambda_1^*} & B_L \\ {\scriptstyle q^*}\uparrow & & \uparrow{\scriptstyle p^*} \\ (A_L(\sigma))^\Gamma & \xrightarrow{\lambda_2^*} & (B_L)^\Gamma \end{array}$$

В этой диаграмме отображения λ_1^*, p^*, q^* и λ_2^* суть мономорфизмы. Отсюда легко следует, что схема $Y(\sigma)$ удовлетворяет условиям а) - в) и, значит, является T - торическим многообразием. Теорема доказана.

Положим

$$Y_0(\sigma) := \text{Im } \lambda_2.$$

Следствие 2.2.4. *Для любой коммутативной k - алгебры $\mathcal{A}$ имеют место следующие соотношения:*

$$Y(\sigma)(\mathcal{A}) =$$

$$\{\beta | \beta \in (\mathcal{A} \otimes_k L)^l,\ g\beta_j \prod_{i=1}^{l} \beta_i^{\tilde{r}(g,b)_{ij}^-} = \prod_{i=1}^{l} \beta_i^{\tilde{r}(g,b)_{ij}^+},\ 1 \leq j \leq l,\ b \in \mathfrak{C}(\sigma),\ g \in \Gamma\}$$

и

$$Y_0(\sigma)(\mathcal{A}) =$$

$$\{\beta | \beta \in ((\mathcal{A} \otimes_k L)^*)^l,\ g\beta_j = \prod_{i=1}^{l} \beta_i^{\tilde{r}(g,b)_{ij}},\ 1 \leq j \leq l,\ b \in \mathfrak{C}(\sigma),\ g \in \Gamma\};$$

более того, отображение

$$\lambda_2(\mathcal{A}) : T(\mathcal{A}) \to Y_0(\sigma)(\mathcal{A}),\ \lambda_2(\mathcal{A}) : \alpha \mapsto \beta \ \ c \ \ \beta_j = \prod_{i=1}^{l} \alpha_i^{c_{ij}} \ \ при \ \ 1 \leq j \leq l$$

есть изоморфизм.

Доказательство. Это утверждение непосредственно вытекает из описанной в доказательстве теоремы 1 конструкции схемы $Y(\sigma)$ и определений.

Пример 2. Ясно, что тор T является аффинным T - торическим многообразием, задаваемым *тривиальным* сврм-конусом $\{0\}$, так как

$$T \times_k L \cong X_L(\{0\}),$$

ср. пример 1.

Тор T называется *изотропным*, если векторное пространство V (или, что то же самое, векторное пространство $V^\perp$) содержит ненулевой Γ - инвариатный вектор.

Лемма 2.2.4. *Векторное пространство V содержит нетривиальный Γ - инвариатный сврм-конус тогда и только тогда, когда тор T изотропен.*

Доказательство. Предположим, что тор T изотропен, и пусть

$$z \in V \setminus \{0\} \ \text{ и } \ (\forall\, g \in \Gamma)\ gz = z.$$

Ясно, что нетривиальный сврм-конус

$$\{az | a \in \mathbb{Q},\ a \geq 0\}$$

является Γ - инвариатным. Обратно, рассмотрим Γ - инвариатный сврм-конус $\sigma(\mathbb{Q})$ под условием

$$\sigma(\mathbb{Q}) \subseteq V \ \text{ и } \ \sigma(\mathbb{Q}) \neq \{0\},$$

и пусть $u \in \sigma(\mathbb{Q}) \setminus \{0\}$. Положим

$$z := \sum_{g \in \Gamma} gu,$$

тогда

$$z \in \sigma(\mathbb{Q}) \ \text{ и } \ (\forall\, g \in \Gamma)\ gz = z.$$

Допустим, что $z = 0$; тогда

$$u = -\sum_{g \in \Gamma \setminus \{1\}} gu$$

и потому $u \in \sigma_{\mathbb{Q}} \cap (-\sigma_{\mathbb{Q}})$. Следовательно,

$$\sigma(\mathbb{Q}) \cap (-\sigma(\mathbb{Q})) \neq \{0\},$$

что противоречит строгой выпуклости конуса $\sigma(\mathbb{Q})$. Значит, $z \neq 0$, так что тор T изотропен. Лемма доказана.

Пример 3. Рассмотрим r конечных расширений полей $k_i|k$ степени $n_i := [k_i : k]$, $1 \leq i \leq r$, и положим

$$d := \sum_{i=1}^{r} n_i - r + 1.$$

Равенства

$$T(A) = \{b|b := (b_1, ..., b_r),\ b_i \in B_i^*,\ N_{B_i/A} b_i = N_{B_1/A} b_1 \ \text{ при } \ 1 \leq i \leq r\}$$

и

$$X(A) = \{b|b := (b_1, ..., b_r),\ b_i \in B_i,\ N_{B_i/A} b_i = N_{B_1/A} b_1 \ \text{ при } \ 1 \leq i \leq r\},$$

где A пробегает множество коммутативных k-алгебр, а $B_i := A \otimes_k k_i$, определяют d-мерный k-тор T и T-торическое многообразие X. Любое нормальное расширение L поля k под условием

$$k_i \subseteq L \ \text{ при } \ 1 \leq i \leq r$$

есть поле расщепления тора T, ср. [68], [136].

2.3 О некоторых целых моделях алгебраических торов и аффинных торических многообразий, определённых над полями алгебраических чисел

1. Предположим теперь, что тор T определён над полем алгебраических

чисел k; обозначим через $\mathfrak{o}$ кольцо целых элементов этого поля и через K *минимальное* поле расщепление тора T.

Предложение 2.3.1 . *Обозначим через H гильбертово поле классов поля k и рассмотрим расширение $F|H$ степени $m := [F : H]$. Если $2|m$, то дробные идеалы поля F являются свободными $\mathfrak{o}$-модулями.*

Доказательство. Это теорема М.В. Бондарко [50].

Следствие 2.3.1 . *Существует конечное нормальное расширение $L|k$, удовлетворяющее условию $K \subseteq L$ и такое, что дробные идеалы поля L являются свободными $\mathfrak{o}$-модулями.*

Доказательство. Предложение 1 показывает, что в качестве L можно взять любое нормальное расширение поля k под условием

$$H \cdot K \subseteq L \ \text{ и } \ 2|[L : H].$$

Рассмотрим поле расщепления L тора T, все дробные идеалы которого суть свободные $\mathfrak{o}$-модули (следствие 1 гарантирует существование такого поля). Обозначим через $\mathfrak{O}$ кольцо целых элементов этого поля и положим

$$n := [L : k],\ \mathfrak{O} = \sum_{j=1}^{n} \oplus \omega_j \mathfrak{o} \ \text{ и } \ \Gamma := \mathrm{Gal}(L|k). \tag{2.3.1}$$

Как и в начале §2, введём в рассмотрение $d+1$ линейных форм

$$t_i := \sum_{j=1}^{n} x_i^{(j)} \omega_j,\ t_i \in L[x] \ \text{ при } \ 0 \le i \le d,$$

от переменных

$$x := (..., x_i^{(j)}, ...),\ 0 \le i \le d,\ 1 \le j \le n;$$

положим

$$gt_i := \sum_{j=1}^{n} x_i^{(j)} g\omega_j \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma \tag{2.3.2}$$

и определим множество полиномов

$$\mathcal{P}_0 := \{P_0^{(j)}(x),\ P_{i,g}^{(j)}(x) | 1 \le j \le n,\ 1 \le i \le d,\ g \in \Gamma \setminus \{1\}\}$$

с коэффициентами в поле k по формулам

$$\prod_{i=0}^{d} t_i - 1 = \sum_{j=1}^{n} P_0^{(j)}(x)\,\omega_j$$

и

$$gt_i \prod_{j=1}^{d} t_j^{r(g)^-_{ji}} - \prod_{j=1}^{d} t_j^{r(g)^+_{ji}} = \sum_{j=1}^{n} P_{i,g}^{(j)}(x)\,\omega_j \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma \setminus \{1\}.$$

Ясно, что $\mathcal{P}_0 \subseteq \mathfrak{o}[x]$; положим

$$J := (\mathcal{P}_0)_{\mathfrak{o}[x]},\ A := \mathfrak{o}[x]/J \ \text{ и } \ \mathcal{T} := \operatorname{Spec} A. \tag{2.3.3}$$

Так как, по построению, для любой коммутативной $\mathfrak{o}$-алгебры $\mathcal{A}$ имеет место равенство

$$\mathcal{T}(\mathcal{A}) = \{\alpha | \alpha \in [(\mathcal{A} \otimes_{\mathfrak{o}} \mathfrak{O})^*]^d,\ g\alpha_j = \prod_{i=1}^{d} \alpha_i^{r(g)_{ij}} \ \text{ при } \ 1 \le j \le n,\ g \in \Gamma\}, \tag{2.3.4}$$

схема $\mathcal{T}$ является групповой схемой конечного типа над кольцом $\mathfrak{o}$ и

$$\mathcal{T} \times_{\mathfrak{o}} k \cong T. \tag{2.3.5}$$

Предложение 2.3.2. *Схема $\mathcal{T}$ является приведённой строго плоской $\mathfrak{o}$-схемой.*

Доказательство. Так как

$$\det\,(g\omega_j)_{1 \le j \le n,\, g \in \Gamma} \neq 0,$$

из определения (3), уравнений (2) и соотношений

$$gt_i = \prod_{j=1}^{d} t_j^{r(g)_{ji}} \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma$$

вытекает, что найдутся полиномы $p_{ij}(t),\ 1 \le i \le d,\ 1 \le j \le n$, в $L[t]$, для которых

$$\mathcal{A} \otimes_{\mathfrak{o}} \mathfrak{O} = \mathfrak{O}[t, t^{-1}, p(t)],$$

где

$$t^{-1} := (t_1^{-1}, ..., t_d^{-1}) \text{ и } p(t) := (..., p_{ij}(t), ...)_{1\leq i\leq d,\, 1\leq j\leq n}\ .$$

Следовательно, схема $\mathcal{T}\times_{\mathfrak{o}}\mathfrak{O}$ является приведённой $\mathfrak{O}$-схемой и, значит, схема $\mathcal{T}$ является приведённой $\mathfrak{o}$-схемой, ибо $\mathfrak{o}$-модуль $\mathfrak{O}$ свободен (в силу выбора поля L, ср. (1)). Пусть

$$p \in \mathcal{P}(k),\ \mathfrak{p} \in \mathcal{P}(L) \text{ и } \mathfrak{p}|p;$$

обозначим, соответственно, через k_p, $\mathfrak{o}_p$, $L_{\mathfrak{p}}$ и $\mathfrak{O}_{\mathfrak{p}}$ пополнение поля k в точке p, кольцо целых элементов поля k_p, пополнение поля L в точке $\mathfrak{p}$ и кольцо целых элементов поля $L_{\mathfrak{p}}$. Положим $n_p := [L_{\mathfrak{p}} : k_p]$ и обозначим через $\Gamma_{\mathfrak{p}} := \mathrm{Gal}(L_{\mathfrak{p}}|k_p)$ группу разложения в точке $\mathfrak{p}$, а через

$$\Gamma^{(\mathfrak{p})} := \{g\Gamma_{\mathfrak{p}}|g \in \Gamma\}$$

совокупность классов смежности группы Галуа Γ по подгруппе $\Gamma_{\mathfrak{p}}$. Так как свойство быть приведённой строго плоской схемой является локальным (см., например, [2, гл. II, §3, следствие к предложению 15]), достаточно доказать, что схема

$$\mathcal{T}^{(p)} := \mathcal{T} \times_{\mathfrak{o}} \mathfrak{o}_p$$

является строго плоской $\mathfrak{o}_p$-схемой. Из хорошо известного тождества

$$\mathfrak{o}_p \otimes_{\mathfrak{o}} \mathfrak{O} = \sum_{g\in\Gamma^{(\mathfrak{p})}} \oplus\, \mathfrak{O}_{g\mathfrak{p}}$$

[83, гл. III, формула (1.8)] следует, что

$$\mathcal{A} \otimes_{\mathfrak{o}} \mathfrak{O} = \mathcal{A} \otimes_{\mathfrak{o}_p} \mathfrak{o}_p \otimes_{\mathfrak{o}} \mathfrak{O} = \sum_{g\in\Gamma^{(\mathfrak{p})}} \oplus(\mathcal{A} \otimes_{\mathfrak{o}_p} \mathfrak{O}_{g\mathfrak{p}})$$

и потому

$$[(\mathcal{A} \otimes_{\mathfrak{o}} \mathfrak{O})^*]^d = [\sum_{g\in\Gamma^{(\mathfrak{p})}} \oplus(\mathcal{A} \otimes_{\mathfrak{o}_p} \mathfrak{O}_{g\mathfrak{p}})^*]^d. \tag{2.3.6}$$

Так как

$$\mathcal{T}^{(p)} = \mathrm{Spec}\ (A \otimes_{\mathfrak{o}} \mathfrak{o}_p),$$

множества $\mathcal{A}$-точек $\mathcal{T}(\mathcal{A})$ и $\mathcal{T}^{(p)}(\mathcal{A})$ схем $\mathcal{T}$ и $\mathcal{T}^{(p)}$ можно отождествить. Поэтому из соотношений (4) и (6) следует, что

$$\mathcal{T}^{(p)}(\mathcal{A}) = \{\alpha | \alpha \in [(\mathcal{A} \otimes_{\mathfrak{o}_p} \mathfrak{O}_\mathfrak{p})^*]^d,\ g\alpha_j = \prod_{i=1}^{d} \alpha_i^{r(g)_{ij}},\ 1 \leq j \leq n_p,\ g \in \Gamma_\mathfrak{p}\},$$

и рассуждение, аналогичное приведённому в начале доказательства, показывает, что

$$\mathcal{T}^{(p)} = \mathrm{Spec}\ A_p$$

для некоторой $\mathfrak{o}_p$-алгебры A_p под условием

$$A_p \otimes_{\mathfrak{o}_p} \mathfrak{O}_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}[t,\ t^{-1},\ q(t)], \tag{2.3.7}$$

где $t := (t_1, ..., t_d)$ суть d независимых переменных, $t^{-1} := (t_1^{-1}, ..., t_d^{-1})$, а множество $q(t)$ состоит из dn_p многочленов с коэффициентами в $L_\mathfrak{p}$. Так как $\mathfrak{o}_p$-модуль $\mathfrak{O}_\mathfrak{p}$ является свободным, из соотношения (7) следует, что $\mathfrak{o}_p$-модуль A_p не имеет кручения. Кольцо $\mathfrak{o}_p$ есть область главных идеалов, поэтому модуль A_p является плоским [90, пример 9.1.3 на стр. 254]; более того, поскольку $pA_p \neq A_p$, модуль A_p является строго плоским [2, гл. I, §3, предложение 1]. Предложение 2 доказано.

Групповую $\mathfrak{o}$-схему $\mathcal{T}$ можно рассматривать как "естественную" $\mathfrak{o}$-целую модель k-тора T. В работе [6, предложение 2 и 4] доказано, что эта схема изоморфна схемному замыканию k-тора T относительно естественного вложения этого тора в модель Нерона-Рейно квазиразложимого k-тора $R_{L|k}G_{m,L}^d$. Используя это вложение, можно получить более короткое доказательство плоскости схемы $\mathcal{T}$ [51, стр. 291]. Если расширение $L|k$ не имеет высшего ветвления, связная компонента единицы схемы $\mathcal{T}$ изоморфна связной компоненте единицы модели Нерона-Рейно тора T [6, теорема 3]. В общем случае гладкую $\mathfrak{o}$-целую модель тора T можно получить из схемы $\mathcal{T}$ разрешением особенностей. В следующем примере такая модель описана для норменного тора, определённого над $\mathbb{Q}$ уравнением $x^2 - 2y^2 = 1$.

Пример 1. Пусть

$$k = \mathbb{Q},\ K = \mathbb{Q}(\sqrt{2})\ \text{ и }\ T := \operatorname{Spec} \mathbb{Q}[x,y]/(x^2 - 2y^2 - 1);$$

тогда

$$\mathcal{T} = \operatorname{Spec} \mathbb{Z}[x,y]/(x^2 - 2y^2 - 1).$$

Расширение $K|k$ имеет высшее ветвление в точке 2; редукция

$$\mathcal{T}_2 = \mathcal{T} \times_{\mathbb{Z}} \mathbf{F}_2$$

схемы $\mathcal{T}$ по модулю 2 не является приведённой схемой:

$$\mathcal{T}_2 = \operatorname{Spec} \mathbf{F}_2[x,y]/((x-1)^2),$$

так что схема $\mathcal{T}$ не является гладкой схемой. Обозначим через $\mathcal{T}^{(0)}$ связную компоненту единицы схемы

$$\mathcal{T}^{(1)} := \operatorname{Spec} \mathbb{Z}[x,y]/(x^2 + x - 2y^2),$$

получаемой "сглаживанием" схемы $\mathcal{T}$, а через $\mathcal{N}^{(0)}$ - связную компоненту единицы модели Нерона-Рейно тора T. Можно показать, что

$$\mathcal{N}^{(0)} \cong \mathcal{T}^{(0)}$$

(см., например, [73, пример 4.3], [113, предложение 5.6] и [6, пример 4]). Положим

$$\mathcal{S} = \operatorname{Spec} \mathbb{Z}[x,y]/(x+1,2);$$

легко видеть, что

$$\mathcal{S} \cong\ G_{a,\mathbf{F}_2}\ \text{ и }\ \mathcal{T}^{(0)} = \mathcal{T}^{(1)} \setminus \mathcal{S};$$

более того,

$$\mathcal{T}^{(1)} \setminus \mathcal{S} \cong \operatorname{Spec} \mathbb{Z}[x,y]/(2x^2 + x - 4y^2).$$

Таким образом,

$$\mathcal{N}^{(0)} \cong \operatorname{Spec} \mathbb{Z}[x,y]/(2x^2 + x - 4y^2).$$

Можно доказать, что связная компонента единицы $\mathcal{N}^{(0)}$ модели Нерона-Рейно k-тора T является аффинной схемой (см., например, [15, предложение 3]); явное описать схему $\mathcal{N}^{(0)}$ пока не удаётся. Дальнейшее рассмотрение целых моделей алгебраических торов, определённых над локальными и глобальными полями, выходит за рамки этой работы; более подробно целые модели алгебраических торов обсуждаются в работах [73], [14], [113], [6], [15] и в цитированных в этих работах статьях.

2. Рассмотрим Γ-инвариантный сврм-конус $\sigma(\mathbb{Q})$; введём новые переменные

$$y := (..., y_i^{(j)}, ...),\ 1 \leq i \leq n,\ 1 \leq j \leq l,$$

и положим

$$gs_j := \sum_{i=1}^{n} y_i^{(j)} g\omega_i \ \text{ при } \ 1 \leq j \leq l,\ g \in \Gamma;$$

соотношения

$$gs_j \prod_{i=1}^{l} s_i^{\tilde{r}(g,b)_{ij}^-} - \prod_{i=1}^{l} s_i^{\tilde{r}(g,b)_{ij}^+} = \sum_{h=1}^{n} Q_h^{(j,b,g)}(y)\omega_h,\ Q_h^{(j,b,g)}(y) \in k[y]$$

однозначно определяют множество полиномов

$$\mathcal{P}_4(\sigma) := \{Q_h^{(j,b,g)}(y) | 1 \leq h \leq n,\ 1 \leq j \leq l,\ b \in \mathfrak{C}(\sigma),\ g \in \Gamma\}.$$

По определению, $\mathcal{P}_4(\sigma) \subseteq k[y]$; положим

$$\mathfrak{A} := (\mathcal{P}_4(\sigma))_{k[y]}.$$

Легко видеть, что

$$Y(\sigma) \cong \text{Spec } k[x]/\mathfrak{A}. \tag{2.3.8}$$

Рассмотрим группу

$$\mathfrak{I}(\sigma) :=$$

$$\{\mathfrak{B} | \mathfrak{B} \in I(L)^l,\ g\mathfrak{B}_j = \prod_{i=1}^{l} \mathfrak{B}_i^{\tilde{r}(g,b)_{ij}} \ \text{ при } \ 1 \leq j \leq l,\ b \in \mathfrak{C}(\sigma),\ g \in \Gamma\}$$

последовательностей дробных идеалов (с покомпонентно определённым умножением). Пусть

$$\mathfrak{B} \in \mathfrak{I}(\sigma); \tag{2.3.9}$$

зафиксируем $\mathfrak{o}$-базис $\{\omega_{1j}, ..., \omega_{nj}\}$ идеала $\mathfrak{B}_j$ и $\mathfrak{o}$ - базис $\{\omega_1^{(j,b,g)}, ..., \omega_n^{(j,b,g)}\}$ идеала

$$\prod_{i=1}^{l} \mathfrak{B}_i^{\tilde{r}(g,b)_{ij}^{+}} (= g\mathfrak{B}_j \prod_{i=1}^{l} \mathfrak{B}_i^{\tilde{r}(g,b)_{ij}^{-}}).$$

Положим

$$gz_j := \sum_{i=1}^{n} y_i^{(j)} g\omega_{ij} \ \text{ при } \ 1 \leq j \leq l, \ g \in \Gamma$$

и рассмотрим множество многочленов

$$\mathcal{P}_5(\mathfrak{B}) := \{R_h^{(j,b,g)}(y) | 1 \leq h \leq n, \ 1 \leq j \leq l, \ b \in \mathfrak{C}(\sigma), \ g \in \Gamma\},$$

определяемое следующим соотношением:

$$gz_j \prod_{i=1}^{l} z_i^{\tilde{r}(g,b)_{ij}^{-}} - \prod_{i=1}^{l} z_i^{\tilde{r}(g,b)_{ij}^{+}} = \sum_{h=1}^{n} R_h^{(j,b,g)}(y)\omega_h^{(j,b,g)}, \ R_h^{(j,b,g)}(y) \in \mathfrak{o}[y]$$

при $1 \leq j \leq l, \ b \in \mathfrak{C}(\sigma)$ и $g \in \Gamma$ (в силу предположения (9), многочлены $R_h^{(j,b,g)}(y)$ корректно определены). По построению, $\mathcal{P}_5(\mathfrak{B}) \subseteq \mathfrak{o}[y]$; положим

$$J_1(\mathfrak{B}) := (\mathcal{P}_5(\mathfrak{B}))_{\mathfrak{o}[y]} \ \text{ и } \ \mathcal{X}_{\mathfrak{B}} := \operatorname{Spec} \mathfrak{o}[y]/J_1(\mathfrak{B}). \tag{2.3.10}$$

Из соотношений (8) и (10) следует, что

$$\mathcal{X}_{\mathfrak{B}} \times_{\mathfrak{o}} k \cong Y(\sigma);$$

таким образом, схема $\mathcal{X}_{\mathfrak{B}}$ является $\mathfrak{o}$-целой моделью T-торического многообразия $Y(\sigma)$, задаваемого сврм-конусом $\sigma(\mathbb{Q})$. Более того, хотя схема $\mathcal{T}$, вообще говоря, и не изоморфна открытой подсхеме схемы $\mathcal{X}_{\mathfrak{B}}$, нетрудно определить "естественные" вложение

$$F : \ \mathcal{T} \hookrightarrow \mathcal{X}_{\mathfrak{B}}$$

схемы $\mathcal{T}$ в $\mathcal{X}_{\mathfrak{B}}$ и действие

$$G:\ \mathcal{T}\times_{\mathfrak{o}}\mathcal{X}_{\mathfrak{B}}\to\mathcal{X}_{\mathfrak{B}}$$

этой схемы на $\mathcal{X}_{\mathfrak{B}}$. Действительно, из определения (10) следует, что

$$\mathcal{X}_{\mathfrak{B}}(\mathcal{A})=$$

$$\{\beta|\beta_j\in\mathcal{A}\otimes_{\mathfrak{o}}\mathfrak{B}_j,\ g\beta_j\prod_{i=1}^{l}\beta_i^{\tilde{r}(g,b)_{ij}^{-}}=\prod_{i=1}^{l}\beta_i^{\tilde{r}(g,b)_{ij}^{+}},\ 1\le j\le l,\ b\in\mathfrak{C}(\sigma),\ g\in\Gamma\}$$

для любой коммутативной $\mathfrak{o}$-алгебры $\mathcal{A}$. Определим умножение в $\mathcal{X}_{\mathfrak{B}}(\mathcal{A})$ по формуле

$$(\beta\gamma)_j:=\beta_j\gamma_j\ \text{ при }\ 1\le j\le l,\ \{\beta,\gamma\}\subseteq\mathcal{X}_{\mathfrak{B}}(\mathcal{A});$$

морфизмы F и G задаются на $\mathcal{A}$-точках схем $\mathcal{T}$ и $\mathcal{X}_{\mathfrak{B}}$ следующим образом:

$$F(\mathcal{A}):\ \mathcal{T}(\mathcal{A})\hookrightarrow\mathcal{X}_{\mathfrak{B}}(\mathcal{A}),\ \alpha\mapsto\beta$$

с

$$\beta_j=\prod_{i=1}^{d}\alpha_i^{c_{ij}}\ \text{ при }\ 1\le j\le l$$

и

$$G(\mathcal{A}):\ \mathcal{T}(\mathcal{A})\times\mathcal{X}_{\mathfrak{B}}(\mathcal{A})\to\mathcal{X}_{\mathfrak{B}}(\mathcal{A}),\ (\alpha,\beta)\mapsto F(\mathcal{A})(\alpha)\beta$$

при $(\alpha,\beta)\in\mathcal{T}(\mathcal{A})\times\mathcal{X}_{\mathfrak{B}}(\mathcal{A})$.

Заметим, что

$$Y_0(\sigma)(\mathbb{Q})=$$

$$\{\alpha|\alpha\in(L^*)^l,\ g\alpha_j=\prod_{i=1}^{l}\alpha_i^{\tilde{r}(g,b)_{ij}}\ \text{ при }\ 1\le j\le l,\ b\in\mathfrak{C}(\sigma),\ g\in\Gamma\},$$

и положим

$$\mathfrak{I}(\sigma)_{pr}:=\{(\alpha)|\alpha\in Y_0(\sigma)(\mathbb{Q})\},$$

где $(\alpha):=((\alpha_1),...,(\alpha_l))$. Ясно, что $\mathfrak{I}(\sigma)_{pr}\subseteq\mathfrak{I}(\sigma)$; пусть

$$H(\sigma):=\mathfrak{I}(\sigma)/\mathfrak{I}(\sigma)_{pr}\ .$$

Предложение 2.3.3. *Группа $H(\sigma)$ конечна и, более того,*

$$\mathcal{X}_{\mathfrak{B}} \cong \mathcal{X}_{\mathfrak{B}'} \ \textit{при} \ \{\mathfrak{B},\ \mathfrak{B}'\} \subseteq \mathfrak{I}(\sigma) \ \textit{и} \ \mathfrak{B}^{-1}\mathfrak{B}' \in \mathfrak{I}(\sigma)_{pr}. \tag{2.3.11}$$

Доказательство. Пусть $\mathfrak{B} \in \mathfrak{I}(\sigma),\ \mathfrak{B}' = (\alpha)\mathfrak{B},\ (\alpha) \in \mathfrak{I}(\sigma)_{pr}$ и

$$\mathfrak{B}_j = \sum_{j=1}^{n} \oplus \omega_{ij}\mathfrak{o} \ \text{ при } \ 1 \leq j \leq l.$$

Тогда

$$\mathfrak{B}'_j = \sum_{j=1}^{n} \oplus \alpha_j\omega_{ij}\mathfrak{o} \ \text{ при } \ 1 \leq j \leq l$$

и, значит, аффинные $\mathfrak{o}$-схемы $\mathcal{X}_{\mathfrak{B}}$ и $\mathcal{X}_{\mathfrak{B}'}$ определяются одной и той же системой уравнений (10). Тем самым утверждение (11) доказано. Обозначим через $I(L)_{pr}$ группу отличных от нуля главных идеалов поля L и положим

$$\mathfrak{I}(\sigma)^{(1)}_{pr} := \mathfrak{I}(\sigma) \cap I(L)^{l}_{pr}\ .$$

Ясно, что

$$\mathfrak{I}(\sigma)_{pr} \subseteq \mathfrak{I}(\sigma)^{(1)}_{pr}.$$

Группа

$$\mathfrak{I}(\sigma)/\mathfrak{I}(\sigma)^{(1)}_{pr}$$

изоморфна подгруппе конечной группы

$$(I(L)/I(L)_{pr})^{l}$$

и, следовательно, конечна. Остаётся доказать конечность группы

$$H_0(\sigma) := \mathfrak{I}(\sigma)^{(1)}_{pr}/\mathfrak{I}(\sigma)_{pr}.$$

Положим, для краткости,

$$g\alpha := (g\alpha_1, ..., g\alpha_l) \ \text{ и } \ \alpha^g := (\beta_1, ..., \beta_l) \ \text{ с } \ \beta_j := \prod_{i=1}^{l} \alpha_i^{\tilde{r}(g,b)_{ij}}$$

при $\alpha \in (L^*)^l,\ 1 \le j \le l$. Пусть $(\alpha) \in \mathfrak{I}(\sigma)^{(1)}_{pr}$, тогда

$$g\alpha = \varepsilon_\alpha(g) \ \text{ с } \ \varepsilon_\alpha(g) \in (\mathfrak{O}^*)^l \ \text{ при } \ g \in \Gamma.$$

Функции $\varepsilon_\alpha : \Gamma \to (\mathfrak{O}^*)^l$ удовлетворяют следующим соотношениям:

$$\varepsilon_{\alpha\beta} = \varepsilon_\alpha \varepsilon_\beta \ \text{ при } \ \{\alpha, \beta\} \subseteq (L^*)^l;$$

$$\varepsilon_\alpha(g_1 g_2) = g_1 \varepsilon_\alpha(g_2) \varepsilon_\alpha(g_1)^{g_2} \ \text{ при } \ \{g_1, g_2\} \subseteq \Gamma,\ \alpha \in (L^*)^l \tag{2.3.12}$$

и

$$(\exists\ \lambda_\alpha \in (\mathfrak{O}^*)^l)\ (\forall\ g \in \Gamma)\ \varepsilon_\alpha(g) = \frac{g\lambda_\alpha}{\lambda_\alpha^g} \Longleftrightarrow (\alpha) \in \mathfrak{I}(\sigma)_{pr} \tag{2.3.13}$$

при $\alpha \in (L^*)^l$. Из соотношения (12) следует, что

$$\varepsilon_\alpha(g)^n = \frac{g\lambda_\alpha}{\lambda_\alpha^g} \ \text{ с } \ \lambda_\alpha := \prod_{h \in \Gamma} h^{-1} \varepsilon_\alpha(h) \ \text{ при } \ g \in \Gamma,\ \alpha \in (L^*)^l. \tag{2.3.14}$$

С другой стороны, в силу теоремы Дирихле о единицах, группа $(\mathfrak{O}^*)^l$ является конечно порождённой абелевой группой и потому

$$|(\mathfrak{O}^*)^l / (\mathfrak{O}^*)^{ln}| < \infty;$$

положим

$$N := |(\mathfrak{O}^*)^l / (\mathfrak{O}^*)^{ln}|.$$

Из соотношений (13) и (14) следует, что $|H_0(\sigma)| < |\Gamma|^N$. Предложение 3 доказано.

Следствие 2.3.2. *Число* $\mathfrak{o}$*-целых моделей многообразия* $Y(\sigma)$ *вида* $\mathcal{X}_{\mathfrak{B}}$ *конечно.*

Доказательство. Из предложения 3 вытекает, что число таких моделей не превосходит $|H(\sigma)|$.

Пример 2. Возвращаясь к описанной в примере 3 предыдущего параграфа ситуации, предположим, что поле k есть поле алгебраических чисел и

обозначим кольца целых элементов полей k и k_i через $\mathfrak{o}$ и $\mathfrak{o}_i$, $1 \leq i \leq r$. Соотношение

$$\mathcal{T}(\mathcal{A}) :=$$

$$\{b|b := (b_1, ..., b_r),\ b_i \in \mathfrak{B}_i^*,\ N_{\mathfrak{B}_i/\mathcal{A}} b_i = N_{\mathfrak{B}_1/\mathcal{A}} b_1 \ \text{ при } \ 1 \leq i \leq r\},$$

где $\mathcal{A}$ пробегает множество коммутативных $\mathfrak{o}$-алгебр и $\mathfrak{B}_i := \mathcal{A} \otimes_{\mathfrak{o}} \mathfrak{o}_i$, определяет $\mathfrak{o}$-целую модель $\mathcal{T}$ тора T. Рассмотрим последовательность дробных идеалов

$$\mathfrak{B} := (\mathfrak{B}_1, ..., \mathfrak{B}_r),\ \mathfrak{B}_i \in I(k_i) \ \text{ при } \ 1 \leq i \leq r,$$

и, для любой коммутативной $\mathfrak{o}$-алгебры $\mathcal{A}$, положим

$$\mathcal{X}_{\mathfrak{B}}(\mathcal{A}) :=$$

$$\{b|b := (b_1, ..., b_r),\ b_i \in \mathfrak{B}_i,\ N_{\mathfrak{B}_i/\mathcal{A}} b_i = N_{\mathfrak{B}_1/\mathcal{A}} b_1 \ \text{ при } \ 1 \leq i \leq r\}, \qquad (2.3.15)$$

где $\mathfrak{B}_i := \mathcal{A} \otimes_{\mathfrak{o}} \mathfrak{B}_i$. Соотношение (15) определяет $\mathfrak{o}$-целую модель $\mathcal{X}_{\mathfrak{B}}$ многообразия X, описанного в рассматриваемом примере 3 из §2.

2.4 О распределении целых точек аффинных торических многообразий, определённых над полем рациональных чисел

1. Многомерная арифметика поля алгебраических чисел k (см., например, [99], [13], [120]) может рассматриваться как аналитическая теория чисел на торе $R_{k|\mathbb{Q}}\, G_{m,k}$. В этом параграфе предпринята попытка обобщить эту теорию на произвольные торы, определённые над полем рациональных чисел (ср. [68], [136] - [140]). Сохраняя предыдущие обозначения, предположим, что $k = \mathbb{Q}$ и отождествим ненулевые идеалы кольца $\mathbb{Z}$ с натуральными числами. Пусть $p \in \mathcal{P},\ \mathfrak{p} \in \mathcal{P}(L)$ и $\mathfrak{p}|p$; обозначим через $e(p)$ индекс ветвления простого числа p в поле L, через

$$\Gamma_{\mathfrak{p}} := \{g|g \in \Gamma,\ g\mathfrak{p} = \mathfrak{p}\}$$

группу разложения идеала $\mathfrak{p}$ и через

$$\Gamma^{(\mathfrak{p})} := \{g\Gamma_{\mathfrak{p}} | g \in \Gamma\}$$

совокупность классов смежности группы Галуа Γ по подгруппе $\Gamma_{\mathfrak{p}}$, так что

$$p = \prod_{h \in \Gamma^{(\mathfrak{p})}} (h\mathfrak{p})^{e(p)}.$$

Положим

$$|\mathfrak{B}| := \prod_{i=1}^{l} |\mathfrak{B}_i| \ \text{ при } \ \mathfrak{B} \in \mathfrak{I}(\sigma), \ \ \mathfrak{I}_0(\sigma) := \mathfrak{I}(\sigma) \cap I(L)_0^l \ ,$$

$$I^{(p)}(\sigma) := \{\mathfrak{A}_a | \mathfrak{A}_a := (..., \prod_{h \in \Gamma^{(\mathfrak{p})}} (h\mathfrak{p})^{(u_i|ha)}, ...), \ a \in \mathfrak{M}^{\Gamma_{\mathfrak{p}}}\},$$

$$\sigma_{\mathfrak{p}} := \sigma \cap \mathfrak{M}^{\Gamma_{\mathfrak{p}}} \ \text{ и } \ I_p(\sigma) := \{\mathfrak{A}_a | \mathfrak{A}_a \in I^{(p)}(\sigma), \ a \in \sigma_{\mathfrak{p}}\}.$$

Легко видеть, что

$$|\mathfrak{A}_a| = p^{(z|a)/e(p)} \ \text{ при } \ \mathfrak{A}_a \in I^{(p)}(\sigma). \tag{2.4.1}$$

Лемма 2.4.1 . *Имеют место следующие соотношения:*

$$\mathfrak{I}(\sigma) = \prod_{p \in \mathcal{P}} I^{(p)}(\sigma) \ \ u \ \ \mathfrak{I}_0(\sigma) = \prod_{p \in \mathcal{P}} I_p(\sigma). \tag{2.4.2}$$

Доказательство. Пусть

$$\mathfrak{B} \in \mathfrak{I}(\sigma) \ \text{ и } \ \mathfrak{B}_j = \prod_{p \in \mathcal{P}} \mathfrak{B}_j^{(p)}$$

с

$$\mathfrak{B}_j^{(p)} = \prod_{h \in \Gamma^{(\mathfrak{p})}} (h\mathfrak{p})^{m_j(h)}, \ m_j(h) \in \mathbb{Z} \ \text{ при } \ 1 \le j \le l, \ \mathfrak{p} \in \mathcal{P}(L), \ \mathfrak{p}|p. \tag{2.4.3}$$

Тогда

$$g\mathfrak{B}_j^{(p)} = \prod_{i=1}^{l} (\mathfrak{B}_i^{(p)})^{\tilde{r}(g,b)_{ij}} \ \text{ при } \ 1 \le j \le l, \ b \in \mathfrak{C}(\sigma), \ g \in \Gamma. \tag{2.4.4}$$

Положим $m(h) := (m_1(h), ..., m_l(h))$; из соотношений (3) и (4) следует, что

$$m(g^{-1}h) = m(h)\tilde{r}(g, b) \text{ при } b \in \mathfrak{C}(\sigma),\ g \in \Gamma,\ h \in \Gamma^{(\mathfrak{p})} \tag{2.4.5}$$

и, в частности, $m(h) = m(h)bc$, так как $\tilde{r}(1, b) = bc$. Положим

$$a(h) := m(h)b,$$

тогда $m(h) = a(h)c$ и, значит,

$$m_i(h) = \sum_{j=1}^{l} a(h)_j c_{ji} = \sum_{j=1}^{l}\sum_{k=1}^{d}(e_k c_{ki})_j a(h)_j = \sum_{j=1}^{l} u_{ij} a(h)_j = (u_i|a(h)).$$

С другой стороны, из соотношения (5) следует, что $m(h) = m(1)\tilde{r}(h^{-1}, b)$; следовательно,

$$m_i(h) = (u_i|a(h)) = m_i(h) = (m(1)\tilde{r}(h^{-1}, b))_i = \sum_{j=1}^{l} m_j(1)\tilde{r}(h^{-1}, b)_{ji} =$$

$$\sum_{j=1}^{l}(u_j|a(1))\tilde{r}(h^{-1}, b)_{ji} = (h^{-1}u_i|a(1)) = (u_i|ha(1)) \text{ при } h \in \Gamma^{(\mathfrak{p})},\ 1 \le i \le l.$$

Таким образом,

$$m_i(h) = (u_i|ha) \text{ с } a \in \mathfrak{M}^{\Gamma_{\mathfrak{p}}} \text{ при } h \in \Gamma^{(\mathfrak{p})},\ 1 \le i \le l. \tag{2.4.6}$$

Из соотношений (3) и (6) следует, что

$$\mathfrak{I}(\sigma) = \prod_{p \in \mathcal{P}} I^{(p)}(\sigma).$$

Более того,

$$(\forall\, a \in \mathfrak{M}^{\Gamma_{\mathfrak{p}}})\ (a \in \sigma \Leftrightarrow (u_i|ha) \ge 0 \text{ при } h \in \Gamma^{(\mathfrak{p})},\ 1 \le i \le l)$$

ввиду Γ-инвариантности сврм-конуса $\sigma(\mathbb{Q})$. Лемма доказана.

Положим

$$z := (\sum_{g \in \Gamma} g)(\sum_{i=1}^{l} u_i)$$

и заметим, что

$$z = 0 \Leftrightarrow \sigma(\mathbb{Q}) = \{0\}.$$

В дальнейшем предполагается, что

$$\sigma(\mathbb{Q}) \neq \{0\} \text{ и, значит, } z \neq 0. \tag{2.4.7}$$

Как известно,

$$(\exists\, q \in \mathbb{N},\ \{v_i | 1 \leq i \leq q\} \subseteq \mathfrak{M})\ \sigma = \{\sum_{i=1}^{q} m_i v_i | m \in \mathbb{N}_0^q\};$$

предположим, что $\{v_i | 1 \leq i \leq q\}$ есть *минимальная* система образующих полугруппы σ. Положим

$$\sigma(m) := \{a | a \in \sigma,\ (z|a) = m\} \text{ и } \sigma_{\mathfrak{p}}(m) := \sigma_{\mathfrak{p}} \cap \sigma(m) \text{ при } m \in \mathbb{N}$$

и

$$\kappa := \min \{m | m \in \mathbb{N},\ \sigma(m) \neq \emptyset\}.$$

Пусть $m \in \mathbb{N}$; ясно, что $\sigma(m)$ есть конечное Γ - инвариантное множество. Обозначим через $B(m)$ число Γ - орбит множества $\sigma(m)$.

Пусть $\mathfrak{f}_0 \in \mathbb{N}$; обозначим через $\Delta(\mathfrak{f}_0, \sigma)$ множество комплекснозначных гомоморфизмов $\chi : \mathfrak{I}_0(\sigma) \to \mathbb{C}$ полугруппы $\mathfrak{I}_0(\sigma)$ под условием

$$|\chi(\mathfrak{A})| \in \{0, 1\} \text{ при } \mathfrak{A} \in \mathfrak{I}_0(\sigma) \text{ и } \chi^{-1}(\{0\}) = \prod_{p|\mathfrak{f}_0} I_p(\sigma),$$

положим

$$\Delta(\sigma) := \bigcup_{\mathfrak{f}_0 \in \mathbb{N}} \Delta(\mathfrak{f}_0, \sigma)$$

и, при $\chi \in \Delta(\sigma)$, определим два (формальных) ряда Дирихле:

$$L(\sigma; \chi, s) := \sum_{\mathfrak{A} \in \mathfrak{I}_0(\sigma)} \chi(\mathfrak{A}) |\mathfrak{A}|^{-s/\kappa} \tag{2.4.8}$$

и

$$L_p(\sigma; \chi, s) := \sum_{\mathfrak{A} \in I_p(\sigma)} \chi(\mathfrak{A}) |\mathfrak{A}|^{-s/\kappa}. \tag{2.4.9}$$

Лемма 2.4.2. *Пусть* $\chi \in \Delta(\sigma)$, *тогда ряд* (9) *компактно сходится в полуплоскости* $\mathbb{C}_0$ *и, более того,*

$$L_p(\sigma;\chi,s) = 1 + O(p^{-(\operatorname{Re} s)/e(p)}) \ \text{ при } \ s \in \mathbb{C}_0. \tag{2.4.10}$$

Доказательство. По определению,

$$L_p(\sigma;\chi,s) = \sum_{m=0}^{\infty} p^{-sm/e(p)\kappa} \sum_{a\in\sigma_{\mathfrak{p}}(m)} \chi(\mathfrak{A}_a),$$

или

$$L_p(\sigma;\chi,s) = 1 + \sum_{m=\kappa}^{\infty} p^{-sm/e(p)\kappa} \sum_{a\in\sigma_{\mathfrak{p}}(m)} \chi(\mathfrak{A}_a). \tag{2.4.11}$$

Равенство (11) даёт

$$|L_p(\sigma;\chi,s)| \le 1 + \sum_{m=\kappa}^{\infty} |\sigma(m)| p^{-(\operatorname{Re} s)m/e(p)\kappa} \ \text{ при } \ s \in \mathbb{C}_0.$$

Но $|\sigma(m)| \le (m+1)^q$, так как, в силу нашего предположения, $(z|v_i) \in \mathbb{N}$ при $1 \le i \le q$; поэтому ряд (9) мажорируется компактно сходящемся в полуплоскости $\mathbb{C}_0$ рядом

$$\sum_{m=0}^{\infty} (m+1)^q p^{-(\operatorname{Re} s)m/e(p)\kappa}$$

и, более того,

$$L_p(\sigma;\chi,s) = 1 + O(\sum_{m=\kappa}^{\infty} (m+1)^q p^{-(\operatorname{Re} s)m/e(p)\kappa}) = 1 + O(p^{-(\operatorname{Re} s)/e(p)})$$

при $s \in \mathbb{C}_0$. Лемма доказана.

Следствие 2.4.1. *Пусть* $\chi \in \Delta(\sigma)$, *тогда*

$$L(\sigma;\chi,s) = \prod_{p\in\mathcal{P}} L_p(\sigma;\chi,s); \tag{2.4.12}$$

при этом ряд (8) *и бесконечное произведение в равенстве* (12) *компактно сходятся в полуплоскости* $\mathbb{C}_1$.

Доказательство. Тождество (12) вытекает из леммы 1 и определений (8) и (9); сходимость ряда Дирихле (8) и бесконечного произведения (12) в полуплоскости $\mathbb{C}_1$ следует из соотношения (10), так как

$$|\{p|p \in \mathcal{P},\ e(p) \neq 1\}| < \infty.$$

Определим множества простых идеалов

$$\mathcal{P}(\sigma) := \{\mathfrak{P}|\mathfrak{P} \in \mathfrak{I}_0(\sigma),\ (\forall\ \mathfrak{a} \in \mathfrak{I}_0(\sigma) \setminus \{0\})\ \mathfrak{a}|\mathfrak{P} \Rightarrow\ \mathfrak{a} = \mathfrak{P}\}$$

и строго простых идеалов

$$\mathcal{P}_0(\sigma) :=$$

$$\{\mathfrak{P}|\mathfrak{P} \in \mathfrak{I}_0(\sigma),\ (\forall\ \mathfrak{a} \in \mathfrak{I}_0(\sigma),\ n \in \mathbb{N})\ \mathfrak{a}|\mathfrak{P}^n \Rightarrow\ (\exists\ m \in \mathbb{N}_0)\ \mathfrak{a} = \mathfrak{P}^m\}$$

относительно естественно определяемого отношения делимости $\mathfrak{a}|\mathfrak{b}$ на полугруппе $\mathfrak{I}_0(\sigma)$. Ясно, что

$$\{\mathfrak{A}_a|a \in \sigma_{\mathfrak{p}}(\kappa),\ p \in \mathcal{P}\} \subseteq \mathcal{P}(\sigma). \tag{2.4.13}$$

Следствие 2.4.2. *Имеют место следующие соотношения:*

$$\mathcal{P}_0(\sigma) \subseteq \mathcal{P}(\sigma) \subseteq I_{\mathcal{P}}(\sigma)\ \ c\ \ I_{\mathcal{P}}(\sigma) := \bigcup_{p \in \mathcal{P}} I_p(\sigma) \tag{2.4.14}$$

и

$$L(\sigma;\chi,s) = \prod_{\mathfrak{P} \in \mathcal{P}_0(\sigma)} (1-\chi(\mathfrak{P})|\mathfrak{P}|^{-s/\kappa})^{-1} \prod_{p \in \mathcal{P}_0} Q_p(p^{-s/e(p)\kappa})\ \ при\ \ s \in \mathbb{C}_1, \tag{2.4.15}$$

где $Q_p(t) \in \mathbb{C}[t]$ *и* $Q_p(t) = 1 \pmod{t^\kappa}$.

Доказательство. Соотношение (14) непосредственно следует из определении множеств $\mathcal{P}(\sigma)$, $\mathcal{P}_0(\sigma)$ и $I_p(\sigma)$. Заметим, что

$$L_p(\sigma;\chi,s) = \sum_{a \in \sigma_{\mathfrak{p}}} (\prod_{j=1}^{q} \chi(\mathfrak{A}^{(j)})|\mathfrak{A}^{(j)}|^{-s/\kappa})^{a_j}$$

при

$$a = \sum_{j=1}^{q} a_j v_j\ \ и\ \ \mathfrak{A}^{(j)} := (..., \prod_{h \in \Gamma^{(\mathfrak{p})}} (h\mathfrak{p})^{(u_i|hv_j)}, ...).$$

Поэтому равенство (15) вытекает из соотношения (14), леммы 1, следствия 1 и известной теоремы о решениях линейных диофантовых уравнений [160, теорема 2.5], ибо элементы множества $\mathcal{P}_0(\sigma) \cap I_p(\sigma)$ отвечают "фундаментальным" (в смысле работы [160]) решениям $(a_1, ..., a_q)$ системы уравнений

$$\sum_{j=1}^{q} a_j g v_j = \sum_{j=1}^{q} a_j v_j \ \text{ при } \ g \in \Gamma_{\mathfrak{p}}.$$

Следствие 2 доказано.

Замечание. В силу леммы 1, элементы множества $\mathfrak{I}_0(\sigma)$ ("целые идеалы") однозначно разлагаются на "примарные идеалы"(элементы множества $I_{\mathcal{P}}(\sigma)$); разложение примарных идеалов на простые, вообще говоря, не является однозначным (см. [160]).

2. Обозначим $\mathbb{Z}$ - ранг группы Γ - инвариантов $\mathfrak{M}^{\Gamma}$ через μ. Из предположения (7) и Γ - инвариантности сврм-конуса $\sigma(\mathbb{Q})$ следует, что $\mu \in \mathbb{N}$. Легко видеть, что

$$T(\mathbb{R}) = (\mathbb{R}_+^*)^{\mu} \times T^{(1)}(\mathbb{R}),$$

где

$$T^{(1)}(\mathbb{R}) := (\mathbb{R}_+^*)^r \times S_1^{d_1} \times (\mathbb{Z}/2\mathbb{Z})^{\nu},\ \{d_1, r, \nu\} \subseteq \mathbb{N}_0,\ d_1 + r + \mu = d,\ \nu \leq \mu + r.$$

Лемма 2.4.3. *Имеет место изоморфизм*

$$\mathcal{T}(\mathbb{Z}) \cong \mathbb{Z}^r \times \mathfrak{A} \ \ c \ \ |\mathfrak{A}| < \infty.$$

Доказательство. Это известная теорема Оно [158, теорема 4].

Обозначим через

$$\iota : T(\mathbb{R}) \to (\mathbb{Z}/2\mathbb{Z})^{\nu}$$

проекцию группы $T(\mathbb{R})$ на группу $(\mathbb{Z}/2\mathbb{Z})^{\nu}$, через $\mathfrak{o}_{\mathfrak{p}}$ кольцо целых элементов поля $L_{\mathfrak{p}}$ и через π один из простых элементов этого кольца.

Из соотношений

$$T(\mathbb{Q}_p) = \{\alpha | \alpha \in (L_{\mathfrak{p}}^*)^d,\ g\alpha_i = \prod_{j=1}^{d} \alpha_j^{r(g)_{ji}} \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma_{\mathfrak{p}}\}$$

и

$$\mathcal{T}(\mathbb{Z}_p) = \{\varepsilon | \varepsilon \in (\mathfrak{o}_{\mathfrak{p}}^*)^d,\ g\varepsilon_i = \prod_{j=1}^{d} \varepsilon_j^{r(g)_{ji}} \ \text{ при } \ 1 \le i \le d,\ g \in \Gamma_{\mathfrak{p}}\}$$

следует, что

$$T(\mathbb{Q}_p)/\mathcal{T}(\mathbb{Z}_p) \cong T(\pi) \ \text{ с } \ T(\pi) := \{\pi^a | a \in \mathfrak{M}^{\Gamma_{\mathfrak{p}}}\}, \pi^a := (\pi^{a_1}, ..., \pi^{a_d}).$$

Обозначим через A алгебру аделей поля $\mathbb{Q}$ и заметим, что

$$T(A) = \{(\alpha^{(\infty)}, ..., \alpha^{(p)}, ...) | \alpha^{(\infty)} \in T(\mathbb{R}),\ \alpha^{(p)} \in T(\mathbb{Q}_p) \ \text{ при } \ p \in \mathcal{P},$$

$$|\{p | p \in \mathcal{P},\ \alpha^{(p)} \notin \mathcal{T}(\mathbb{Z}_p)\}| < \infty\}.$$

Будем считать, как обычно, что $T(\mathbb{Q}) \subseteq T(A_{\mathbb{Q}})$, и положим

$$T^{(1)}(A) := \{\alpha | \alpha \in T(A),\ |v(\alpha)| = 1 \ \text{ при } \ v \in \mathfrak{M}^{\Gamma}\};$$

как известно,

$$T(A) = (\mathbb{R}_+^*)^{\mu} \times T^{(1)}(A) \ \text{ и } \ T(\mathbb{Q}) \subseteq T^{(1)}(A),$$

а фактор-группа $T^{(1)}(A)/T(\mathbb{Q})$ компактна (см., например, [5], [158]). По определению, нормализованный *гроссенхарактер* тора T есть непрерывный гомоморфизм

$$\chi : T(A) \to S_1$$

под условием

$$T(\mathbb{Q}) \cdot (\mathbb{R}_+^*)^{\mu} \subseteq \mathrm{Ker}\ \chi\ ;$$

обозначим через $Gr(T)$ группу нормализованных гроссенхарактеров тора T. Ясно, что группа $Gr(T)$ изоморфна группе (непрерывных) характеров группы $T^{(1)}(A_{\mathbb{Q}})/T(\mathbb{Q})$.

Обозначим через F множество пар $\mathfrak{f} := (\mathfrak{f}_0,\ \mathfrak{f}_1)$, где $\mathfrak{f}_0 \in \mathbb{N}$ и $\mathfrak{f}_1$ есть подгруппа группы $(\mathbb{Z}/2\mathbb{Z})^\nu$. Пусть $\mathfrak{f} \in F$; положим

$$S(\mathfrak{f}) := \{p | p \in \mathcal{P},\ \mathfrak{f}_0 \neq 0\ (p)\}$$

и

$$A_\mathfrak{f} :=$$

$$\{\alpha | \alpha \in T(A),\ \iota(\alpha^{(\infty)}) \in \mathfrak{f}_1,\ \alpha^{(p)} \in \mathcal{T}(\mathbb{Z}_p)\ \text{ и }\ \alpha^{(p)} = 1\ (\mathfrak{f}_0)\ \text{ при }\ p \in \mathcal{P}\}$$

Рассмотрим сврм-конус $\sigma_0(\mathbb{Q})$ под условием

$$\sigma_0(\mathbb{Q})^\perp = \{\sum_{i=1}^{d} a_i e_i | a \in (\mathbb{Q} \cap \mathbb{R}_+)^n\}$$

и заметим, что $\mathfrak{R}(\sigma_0) = \{0\}$. Положим

$$I^{(\mathfrak{f})}(\sigma_0) := \prod_{p \in S(\mathfrak{f})} I^{(p)}(\sigma_0)$$

и определим мономорфизм

$$g_0 : I^{(\mathfrak{f})}(\sigma_0) \to T(A)/A_\mathfrak{f},\ g_0 : \mathfrak{A}_a \mapsto \alpha_a \bmod A_\mathfrak{f},\ \text{ где }\ \mathfrak{A}_a \in I^{(p)}(\sigma_0),\ p \in \mathcal{P},$$

$$\alpha_a \in T(A),\ \alpha_a^{(\infty)} = 1,\ \alpha_a^{(p)} = \pi^a,\ \alpha_a^{(q)} = 1\ \text{ при }\ q \in \mathcal{P} \setminus \{p\}.$$

Положим

$$Gr_\mathfrak{f}(T) := \{\chi | \chi \in Gr(T)),\ A_\mathfrak{f} \subseteq \operatorname{Ker} \chi\},\ Gr_\mathfrak{f}(\sigma_0) := \{\chi \circ g_0 | \chi \in Gr_\mathfrak{f}(T))\}$$

и

$$\mathfrak{g}(\mathfrak{f}, \sigma_0) := \{\chi | \chi \in \Delta(\mathfrak{f}_0, \sigma_0),\ \chi(I_p(\sigma_0)) = \{0\}\ \text{ при }\ p \notin S(\mathfrak{f})$$

$$\text{и }\ (\exists\, \psi \in Gr_\mathfrak{f}(\sigma_0))\ \chi | I_p(\sigma_0) = \psi | I_p(\sigma_0)\ \text{ при }\ p \in S(\mathfrak{f})\}.$$

Ясно, что отображение

$$g(\sigma) : \mathfrak{I}(\sigma_0) \to \mathfrak{I}(\sigma),\ g(\sigma) : \mathfrak{B} \mapsto \mathfrak{B}'\ \text{ с }\ \mathfrak{B}'_j = \prod_{i=1}^{d} \mathfrak{B}_i^{c_{ij}}\ \text{ при }\ 1 \leq j \leq l$$

есть изоморфизм; положим

$$Gr_{\mathfrak{f}}(\sigma) := \{\chi \circ g(\sigma)^{-1} | \chi \in Gr_{\mathfrak{f}}(\sigma_0)\} \text{ и } \mathfrak{g}(\mathfrak{f}, \sigma) := \{\chi \circ g(\sigma)^{-1} | \chi \in \mathfrak{g}(\mathfrak{f}, \sigma_0)\}.$$

Введём бинарные отношения

$$\mathfrak{f}|\mathfrak{f}' := (\mathfrak{f}_0|\mathfrak{f}'_0 \text{ и } \mathfrak{f}_1 \subseteq \mathfrak{f}'_1) \text{ при } \{\mathfrak{f}, \mathfrak{f}'\} \subseteq F$$

и

$$\chi \preceq \chi' := (\mathfrak{f}|\mathfrak{f}' \text{ и } \chi|I^{(\mathfrak{f}')}(\sigma) = \chi') \text{ при } \chi \in \mathfrak{g}(\mathfrak{f}, \sigma) \text{ и } \chi' \in \mathfrak{g}(\mathfrak{f}', \sigma).$$

Наконец, положим

$$\mathfrak{G}(\sigma) := \{\chi | \chi \in \Delta(\sigma),\ (\exists\, \mathfrak{f} \in F, \psi \in \mathfrak{g}(\mathfrak{f}, \sigma))\ \psi \preceq \chi\}.$$

Элементы множества $\mathfrak{G}(\sigma)$ суть гроссенхарактеры конуса σ; по определению, каждый из этих гроссенхарактеров индуцируется одним из элементов группы

$$\bigcup_{\mathfrak{f} \in F} \mathfrak{g}(\mathfrak{f}, \sigma)$$

примитивных характеров этого конуса.

Предложение 2.4.1 . *Пусть*

$$\chi \in \mathfrak{G}(\sigma) \cap \Delta(\mathfrak{f}_0, \sigma) \text{ и } S_0 := \{p | p \in \mathcal{P},\ d_L\mathfrak{f}_0 \neq 0\ (p)\}.$$

Тогда

$$L(\sigma; \chi, s) = H(s) \prod_{i=1}^{B(\kappa)} L(\psi_i, s) \text{ при } s \in \mathbb{C}_{1-\gamma},\ \gamma := (\kappa+1)^{-1}, \tag{2.4.16}$$

где $L(\psi_i, s)$ есть L - ряд Hecke поля k_i с характером ψ_i и $k_i \subseteq L$ при $1 \leq i \leq B(\kappa)$, а

$$H(s) = \prod_{p \in \mathcal{P}} (1 + D_p(s) p^{-s\kappa/(\kappa+1)}) \tag{2.4.17}$$

с

$$D_p(s) = O(1) \text{ при } s \in \mathbb{C}_{1-\gamma} \text{ и } p \in S_0.$$

Более того,

$$\chi = 1 \Rightarrow \psi_i = 1 \text{ при } 1 \leq i \leq B(\kappa).$$

Доказательство. Это теорема Драксла [68, теорема 1] (см. также [128, предложение 4 на стр. 120])tex.

Положим

$$b(\chi) := |\{i | 1 \leq i \leq B(\kappa),\ \psi_i = 1\}|.$$

Замечание. Из равенства $b(\chi) = B(\kappa)$, вообще говоря, не следует, что $\chi = 1$ (см., например, [111]).

Рассмотрим естественный изоморфизм

$$\xi : Y_0(\sigma)(\mathbb{R}) \to (\mathbb{R}_+^*)^{\mu+r} \times S_1^{d_1} \times (\mathbb{Z}/2\mathbb{Z})^{\nu},$$

$$\xi : a \mapsto (\xi_1(a), ..., \xi_{d+\nu}(a)) \ \text{ при } \ a \in Y_0(\sigma)(\mathbb{R}),$$

где

$$\xi_i(a) \in \mathbb{R}_+^* \ \text{ при } \ 1 \leq i \leq \mu + r,\ \xi_i(a) \in S_1 \ \text{ при } \ \mu + r < i \leq d$$

и

$$\xi_i(a) \in \mathbb{Z}/2\mathbb{Z} \ \text{ при } \ d < i \leq d + \nu,$$

и положим

$$\iota_1 = (\xi_{d+1}, ..., \xi_{d+\nu}),\ \iota_1 : Y_0(\sigma)(\mathbb{R}) \to (\mathbb{Z}/2\mathbb{Z})^{\nu};$$

ясно, что $\iota_1 = \iota \circ \lambda_2(\mathbb{R})^{-1}$. Пусть

$$\mathfrak{I}(\sigma)_{pr}^{(\mathfrak{f})} := \{(\alpha) | (\alpha) \in \mathfrak{I}(\sigma)_{pr},\ \alpha = 1\ (\mathfrak{f})\},$$

где

$$\alpha = 1\ (\mathfrak{f}) := (\alpha_i = 1\ (\mathfrak{f}_0) \ \text{ при } \ 1 \leq i \leq l \ \text{ и } \ \iota_1(\alpha) \in \mathfrak{f}_1),$$

и

$$H_{\mathfrak{f}}(\sigma) := \mathfrak{I}(\sigma)/\mathfrak{I}(\sigma)_{pr}^{(\mathfrak{f})}.$$

Лемма 2.4.4. *Группа $H_{\mathfrak{f}}(\sigma)$ конечна.*

Доказательство. Это утверждение следует из предложения 3.3 и конечности группы $\mathfrak{I}(\sigma)_{pr}/\mathfrak{I}(\sigma)_{pr}^{(\mathfrak{f})}$.

Следствие 2.4.3. *Пусть* $\chi \in \Delta(\mathfrak{f}_0, \sigma)$ *и* $\mathfrak{I}(\sigma)_{pr}^{(\mathfrak{f})} \subseteq \operatorname{Ker} \chi$*; тогда* $\chi \in \mathfrak{G}(\sigma)$.

Доказательство. Это утверждение легко следует из леммы 4 и определений.

Положим

$$J(y) := \{\mathfrak{a} | \mathfrak{a} \in \mathfrak{I}_0(\sigma),\ |\mathfrak{a}| < y^{\kappa}\} \ \text{ и } \ \Pi(y) := J(y) \cap \mathcal{P}(\sigma)$$

при $y \in \mathbb{R}_+$.

Предложение 2.4.2. *Пусть* $\chi \in \mathfrak{G}(\sigma),\ y \in \mathbb{R}$ *и* $y > 2$*. Тогда*

$$\sum_{\mathfrak{a} \in J(y)} \chi(\mathfrak{a}) = y\, Q_{\chi}(\log y) + O(y^{1-\gamma}) \ \ c\ \ \gamma \in \mathbb{R}_+^*, \tag{2.4.18}$$

где $Q_{\chi}(\log y) = 0$ *при* $b(\chi) = 0$ *и* $Q_{\chi}(t)$ *есть отличный от нуля полином степени* $b(\chi) - 1$ *с неотрицательными рациональными коэффициентами при* $b(\chi) \in \mathbb{N}$*, и*

$$\sum_{\mathfrak{p} \in \Pi(y)} \chi(\mathfrak{p}) = b(\chi) \int_2^y \frac{du}{\log u} + O(y \exp(-\gamma_1 (\log y)^{1/2}) \ \ c\ \ \gamma_1 \in \mathbb{R}_+^*. \tag{2.4.19}$$

Доказательство. Асимптотические формулы (18) и (19) выводятся из соотношений (12), (16) и (17) с помощью комплексного интегрирования (формула обращения), ср. [128, гл. 1, §4 и §5].

Обозначим через $\mathcal{H}_{\mathfrak{f}}(\sigma)$ группу характеров группы $H_{\mathfrak{f}}(\sigma)$; в силу следствия 3, можно считать, что $\mathcal{H}_{\mathfrak{f}}(\sigma) \subseteq \mathfrak{G}(\sigma)$. Пусть $C \in H_{\mathfrak{f}}(\sigma),\ y \in \mathbb{R}$ и $y > 2$; положим

$$\mathcal{N}(C, y) := |\{\mathfrak{a} | \mathfrak{a} \in J(y) \cap C\}| \ \text{ и } \ \pi(C, y) := |\{\mathfrak{a} | \mathfrak{a} \in \Pi(y) \cap C\}|.$$

Следствие 2.4.4. *Имеют место следующие соотношения:*

$$\mathcal{N}(C, y) = y\, |H_{\mathfrak{f}}(\sigma)|^{-1} \sum_{\chi \in \mathcal{H}_{\mathfrak{f}}(\sigma)} \overline{\chi(C)}\, Q_{\chi}(\log y) + O(y^{1-\gamma}) \ \ c\ \ \gamma \in \mathbb{R}_+^* \tag{2.4.20}$$

и

$$\pi(C, y) = |H_{\mathfrak{f}}(\sigma)|^{-1} \sum_{\chi \in \mathcal{H}_{\mathfrak{f}}(\sigma)} \overline{\chi(C)}\, b(\chi) \int_2^y \frac{du}{\log u} + O(y \exp(-\gamma_1 (\log y)^{1/2}) \ \ c\ \ \gamma_1 \in \mathbb{R}_+^*. \tag{2.4.21}$$

Доказательство. Соотношения (20) и (21) вытекают из формул (18) и (19).

Предложение 2.4.3. *Пусть* $C \in H_{\mathfrak{f}}(\sigma)$, $y \in \mathbb{R}$ *и* $y > 2$*; предположим, что* $\mathfrak{I}_0(\sigma) \cap C \neq \emptyset$. *Тогда*

$$\mathcal{N}(C, y) = y\, q(C, \log y) + O(y^{1-\gamma}) \;\; c \;\; \gamma \in \mathbb{R}_+^* \;\; u \;\; q(C, t) \in \mathbb{R}[t]; \qquad (2.4.22)$$

более того,

$$q(C, t) = \sum_{i=0}^{m} a_i t^i \;\; c \;\; 0 \leq m \leq B(\kappa) - 1 \;\; u \;\; a_m \in \mathbb{R}_+^*.$$

Доказательство. Из соотношения (21) следует, что

$$\pi(1, y) = |H_{\mathfrak{f}}(\sigma)|^{-1} \sum_{\chi \in \mathcal{H}_{\mathfrak{f}}} b(\chi) \int_2^y \frac{du}{\log u} + O(y \exp(-\gamma_1 (\log y)^{1/2}) \gg y(\log y)^{-1}$$

и, значит,

$$\mathcal{N}(1, y) \geq \pi(1, y) \gg y(\log y)^{-1}.$$

Пусть $\mathfrak{a}_0 \in \mathfrak{I}_0(\sigma) \cap C$, тогда

$$\{\mathfrak{a}_0(\alpha) | (\alpha) \in \mathfrak{I}_0(\sigma) \cap \mathfrak{I}_{pr}(\sigma),\ |(\alpha)| < y^{\kappa} |\mathfrak{a}_0|^{-1}\} \subseteq J(y) \cap C$$

и потому

$$\mathcal{N}(C, y) \geq \mathcal{N}(1, y|\mathfrak{a}_0|^{-1/\kappa}) \gg y(\log y)^{-1}. \qquad (2.4.23)$$

Доказываемое утверждение вытекает из соотношений (20) и (23).

Замечание. В работе [111] изучаются множества классов идеалов

$$H^{(0)}(\sigma) := \{C | C \in H(\sigma),\ \mathfrak{I}_0(\sigma) \cap C \neq \emptyset\}$$

норменных торов, рассматриваемых в примере 3, §2 и в примере 2, §3; заметим, что, вообще говоря,

$$H^{(0)}(\sigma) \neq H(\sigma).$$

Пусть $\mathfrak{B} \in \mathfrak{I}(\sigma)$; по определению,

$$\mathcal{X}_{\mathfrak{B}}(\mathbb{Z}) = \{\beta | \beta_j \in \mathfrak{B}_j,$$

$$g\beta_j \prod_{i=1}^{l} \beta_i^{\tilde{r}(g,b)_{ij}^-} = \prod_{i=1}^{l} \beta_i^{\tilde{r}(g,b)_{ij}^+} \text{ при } 1 \le j \le l,\ b \in \mathfrak{C}(\sigma),\ g \in \Gamma\}.$$

Положим

$$Z_{\mathfrak{f}} := \{\beta | \beta \in \mathcal{X}_{\mathfrak{B}}(\mathbb{Z}),\ \beta = 1\ (\mathfrak{f})\};$$

ясно, что

$$Z_{\mathfrak{f}} \subseteq Y_0(\sigma)(\mathbb{Q}) \subseteq Y_0(\sigma)(\mathbb{R}) \subseteq Y(\sigma)(\mathbb{R})$$

и

$$Y(\sigma)(\mathbb{R}) = \{\beta | \beta \in (\mathbb{R} \otimes_{\mathbb{Q}} L)^l,$$
$$g\beta_j \prod_{i=1}^{l} \beta_i^{\tilde{r}(g,b)_{ij}^-} = \prod_{i=1}^{l} \beta_i^{\tilde{r}(g,b)_{ij}^+} \text{ при } 1 \le j \le l,\ b \in \mathfrak{C}(\sigma),\ g \in \Gamma\}.$$

Пусть

$$\alpha \in Y(\sigma)(\mathbb{R}),\ \alpha_j = \sum_{i=1}^{n} a_{ij}\omega_{ij},\ g\alpha_j := \sum_{i=1}^{n} a_{ij} g\omega_{ij} \text{ при } 1 \le j \le l,\ g \in \Gamma,$$

где $\{\omega_{1j}, ..., \omega_{1j}\}$ есть $\mathfrak{o}$ - базис идеала $\mathfrak{B}_j$ при $1 \le j \le l$ и

$$\{a_{ij} | 1 \le i \le n,\ 1 \le j \le l\} \subseteq \mathbb{R};$$

положим

$$N\alpha := \prod_{g \in \Gamma} \prod_{j=1}^{l} g\alpha_j,\ ||\alpha|| := \max\{|N\alpha|^{1/\kappa},\ \xi_j(\alpha),\ \xi_j(\alpha)^{-1} | \mu < j \le \mu + r\}$$

и

$$U(w) := \{\alpha | \alpha \in Y_0(\sigma)(\mathbb{R}),\ ||\alpha|| < w \text{ при } w \in \mathbb{R}_+^*\}.$$

Теорема 2.4.1 . *Пусть $w \in \mathbb{R}$ и $w > 2$; тогда*

$$|Z_{\mathfrak{f}} \cap U(w)| = cw\ (\log w)^b + O(w\ (\log w)^{b-1}),$$

где $c \in \mathbb{R}_+,\ b \in \mathbb{Z}$ и $0 \le b \le B(\kappa) + r - 1$. Более того, если $Z_{\mathfrak{f}} \ne \emptyset$, то $c > 0$.

Доказательство. Пусть $C \in H_{\mathfrak{f}}(\sigma)$ и $\mathfrak{B} \in C^{-1}$. Ясно, что

$$Z_{\mathfrak{f}} = \{\beta | \beta \in (L^*)^l,\ (\beta) = \mathfrak{B}\mathfrak{A},\ \mathfrak{A} \in \mathfrak{I}_0 \cap C\}$$

и потому

$$Z_{\mathfrak{f}} \cap U(w) = \{\beta | \beta \in (L^*)^l,\ (\beta) = \mathfrak{B}\mathfrak{A},$$

$$\mathfrak{A} \in J(w|\mathfrak{B}|^{-1/\kappa}) \cap C,\ w^{-1} < \xi_j(\beta) < w \ \text{ при } \ \mu + 1 \leq j \leq \mu + r\}, \quad (2.4.24)$$

ибо $|(\beta)| = |N\beta|$. Положим

$$A(\beta) := |\{\beta_1 | \beta_1 \in (L^*)^l,$$

$$(\beta_1) = (\beta),\ w^{-1} < \xi_j(\beta_1) < w \ \text{ при } \ \mu + 1 \leq j \leq \mu + r\}|$$

при $\beta \in (L^*)^l$, так что

$$A(\beta) = |\{\varepsilon | \varepsilon \in \mathcal{T}(\mathbb{Z}),$$

$$w^{-1}\xi_j(\beta)^{-1} < \xi_j(\varepsilon) < w\xi_j(\beta)^{-1} \ \text{ при } \ \mu + 1 \leq j \leq \mu + r\}|.$$

Ввиду леммы 3, отсюда следует, что

$$A(\beta) = c_1(\log w)^r(1 + O(1/\log w)). \quad (2.4.25)$$

С другой стороны, из равенства (24) вытекает, что

$$|Z_{\mathfrak{f}} \cap U(w)| = A(\beta)\mathcal{N}(C, w|\mathfrak{B}|^{-1/\kappa}). \quad (2.4.26)$$

Доказываемое утверждение следует из соотношений (25) и (26) и предложения 3.

Глава 3

О представлении простых чисел кубическими полиномами от двух переменных.

3.1 Введение

1. В 1854-ом году В.Я. Буняковский высказал следующее предположение, обобщающее теорему Дирихле о простых числах в арифметических прогрессиях (ср. [65, стр. 333]).

Гипотеза 3.1.1. *Пусть* $f(x) \in \mathbb{Z}[x]$. *Если полином* $f(x)$ *неприводим,* $(\{f(a)|a \in \mathbb{Z}\}) = (1)$ *и старший коэффициент полинома* $f(x)$ *положителен, то множество*

$$\{f(a)|a \in \mathbb{N}\} \cap \mathcal{P}$$

бесконечно.

Эта гипотеза до сих пор не доказана ни для одного нелинейного полинома. Нетрудно показать, что гипотеза 1 эквивалентна следующему утверждению (см., например, [150, лемма 4]).

Гипотеза 3.1.2. *Пусть*

$$f(x) \in \mathbb{Z}[x],\ n \in \mathbb{N}\ \ и\ \ x := (x_1, ...x_n).$$

Если полином $f(x)$ *неприводим и* $(\{f(a)|a \in \mathbb{Z}^n\}) = (1)$, *то множество*

$$\{f(a),\ -f(a)|a \in \mathbb{Z}^n\} \cap \mathcal{P}$$

бесконечно.

С другой стороны, по теореме Матиясевича [22],

$$\{f_1(a)|a \in \mathbb{Z}^n\} \cap \mathbb{N} = \mathcal{P}\ \ \text{и}\ \ \{f_2(a)|a \in \mathbb{Z}^n\} \cap \mathbb{N} = \mathbb{N} \setminus \mathcal{P}$$

для некоторых полиномов $f_1(x)$ и $f_2(x)$ с целыми рациональными коэффициентами. Пусть

$$f(x) \in \mathbb{Z}[x],\ f(x) = \sum_{\alpha \in \mathbb{N}_0^n} b(\alpha) x_1^{\alpha_1} ... x_n^{\alpha_n};$$

следуя [95], положим

$$|f|(x) := \sum_{\alpha \in \mathbb{N}_0^n} |b(\alpha)| x_1^{\alpha_1} ... x_n^{\alpha_n}$$

и

$$\delta(f) := \inf\{\beta | \text{ card } \{a | a \in \mathbb{N}^n,\ |f|(a) \le X\} \le X^\beta\}.$$

Ясно, что чем больше $\delta(f)$, тем вероятнее, что полином f удовлетворяет гипотезе 2. В 1840-ом году Дирихле доказал эту гипотезу для бинарных квадратичных форм (ср. [65, стр. 417 - 418]); много лет спустя Иванец доказал гипотезу 2 для произвольных полиномов второй степени от двух переменных. В конце 1990-ых годов Иванец и Фридландер [80] - [82] доказали, что существует бесконечно много простых вида x^2+y^4, а вскоре после этого Хис-Браун [95] доказал бесконечность множества простых вида $x^3 + 2y^3$. В дальнейшем, развивая идеи работы [95], нам удалось доказать [97], [98], что любая примитивная неприводимая бинарная кубическая форма с целыми рациональными коэффициентами, принимающая хотя бы одно нечётное значение, представляет бесконечно много простых и аналогичную теорему для широкого класса неоднородных полиномов третьей степени от двух переменных.

Заметим, что

$$\delta(f) = 1 \text{ при } f(x,y) = \sum_{\alpha=0}^{2} b(\alpha) x^\alpha y^{2-\alpha},\ \delta(x^2+y^4) = 3/4,$$

$$\delta(f) = 2/3 \text{ при } f(x,y) = \sum_{\alpha=0}^{3} b(\alpha) x^\alpha y^{3-\alpha} \text{ и } \delta(x^2+1) = 1/2.$$

2. Сформулируем полученные в работах [80] - [82], [95], [97] и [98] результаты. Здесь и в дальнейшем

$$X \in \mathbb{R},\ X \ge 3.$$

Теорема 3.1.1 (см. [81]). *Пусть*

$$f(x) := x_1^2 + x_2^4 \text{ и } F(X) := \{a | a \in \mathbb{N}^2,\ f(a) \le X\}.$$

Полином $f(x)$ удовлетворяет гипотезе 2; более того,

$$\sum_{a\in F(X)} \Lambda(f(a)) = 4(\pi)^{-1}\kappa X^{3/4}(1+O(\frac{\log\log X}{\log X})) \ \ при \ \ X\to\infty,$$

где

$$\kappa := \int_0^1 (1-t^4)^{1/2}dt = \Gamma(1/4)^2/(6(2\pi)^{1/2})$$

и $\Lambda : \mathbb{N}\to\mathbb{R}_+$ есть функция Мангольдта.

Теорема 3.1.2 (см. [95]). *Пусть*

$$f(x) := x_1^3 + 2x_2^3.$$

Полином $f(x)$ удовлетворяет гипотезе 2; более того,

$$(\exists\, c\in\mathbb{R}_+^*)\ |\{a_1^3+2a_2^3 | a\in\mathbb{N}^2,\ X\le a_1,a_2\le X(1+\eta(X,c))\}\cap\mathcal{P}| =$$

$$\sigma\ \frac{(\eta(X,c)\log X)^2}{3\log X}\ (1+O((\log\log X)^{-1/6}))\ \ при\ \ X\to\infty,$$

где

$$\eta(X,c) := (\log X)^{-c},\ \sigma := \prod_{p\in\mathcal{P}}(1-\frac{\nu_p-1}{p})\ \ и\ \ \nu_p := |\{a | a\in\mathbb{F}_p,\ a^3=2\}|.$$

Теорема 3.1.3 (см. [97]). *Рассмотрим примитивную неприводимую бинарную кубическую форму $f(x)$ с целыми рациональными коэффициентами. Если множество $f(\mathbb{Z}^2)$ содержит хотя бы одно нечётное число, то множество $f(\mathbb{Z}^2)\cap\mathcal{P}$ бесконечно; в противном случае множество*

$$\{f(a)/2 \mid a\in\mathbb{Z}^2\}\cap\mathcal{P}$$

бесконечно.

Теорема 3.1.4 (см. [98]). *Рассмотрим бинарную кубическую форму $f(x)$ с целыми рациональными коэффициентами и полином*

$$F(x) := a_0^{-1}f(a+dx)\ \ с\ \ d\in\mathbb{Z},\ a\in\mathbb{Z}^2,\ a_0\in\mathbb{N}.$$

Пусть $F(x)\in\mathbb{Z}[x]$, тогда полином $F(x)$ удовлетворяет гипотезе 2.

Гипотеза 3.1.3. *Пусть* $a \in \mathbb{N}$; *обозначим через* $r(a)$ *ранг эллиптической кривой*

$$x^3 + y^3 = az^3$$

и через $R(a)$ *аналитический ранг (т.е. порядок нуля в точке* $s = 1$ *дзета - функции Хассе - Вейля* $L_a(s)$*) этой кривой. Имеет место соотношение*

$$(\forall\ a \in \mathbb{N})\ r(a) = R(a)\ (2).$$

Гипотеза 3 следует из известной гипотезы Бёрча и Свиннертона-Дайера, но пока не доказана.

Следствие 3.1.1. *Пусть* $\{a_i | 0 \leq i \leq 4\} \subseteq \mathbb{Z}$ *и предположим, что*

$$\prod_{i=0}^{4} a_i \neq 0\ (3)\ \ и\ \ (\forall\ p \in \{q | q \in \mathcal{P},\ q = 2\ (3)\})\ a_i \neq 0\ (p^2)\ \ при\ 0 \leq i \leq 4.$$

Тогда из справедливости гипотезы 3 *вытекает, что (проективная) гиперповерхность*

$$H_1 : \sum_{i=0}^{4} a_i x_i^3 = 0$$

удовлетворяет принципу Хассе.

Доказательство. Это утверждение является прямым следствием теоремы 4 и одной теоремы Хис-Брауна [94, теорема 4].

Следствие 3.1.2. *Пусть* $\{a,\ b\} \subseteq \mathbb{Z}$; *рассмотрим (проективную) поверхность*

$$H_2 : x_0^3 + 2x_1^3 + ax_2^3 + bx_3^3 = 0,$$

обозначим через $\bar{x}$ *остаток при делении числа* x, $x \in \mathbb{Z}$, *на* 9 *и предположим, что*

$$(a, b) = (1)\ \ и\ \ \{\overline{a+b},\ \overline{a-b}\} \cap \{0\} \neq \emptyset \tag{3.1.1}$$

или

$$(a, b) = (1)\ \ и\ \ \{\bar{a},\ \bar{b}\} \cap \{2,\ 3,\ 6,\ 7\} \neq \emptyset. \tag{3.1.2}$$

Тогда

$$H_2(\mathbb{Q}) \neq \emptyset. \tag{3.1.3}$$

Доказательство. Если

$$b = 0 \ \text{ или } \ (\exists\, q \in \mathbb{Q})\ a = bq^3, \tag{3.1.4}$$

доказываемое утверждение очевидно. Предположим, что соотношение (4) не имеет место. Рассмотрим семейство эллиптических кривых

$$E_p : x_0^3 + x_1^3 = py^3\ ,\ p \in \mathcal{P};$$

по теореме Сатже [149, предложение 3.3],

$$E_p(\mathbb{Q}) \neq \emptyset \ \text{ при } \ p = 2\ (9),\ p \in \mathcal{P}. \tag{3.1.5}$$

Если имеет место соотношение (1), то

$$(\exists\, d \in \mathbb{N}^2)\ ad_1^3 + bd_2^3 = 54\ (243); \tag{3.1.6}$$

положим в этом случае

$$f_1(y) := \frac{a(d_1 + 3y_1)^3 + b(d_2 + 3y_2)^3}{27}$$

и заметим, что, в силу теоремы 4 и соотношения (6),

$$(\exists\, u \in \mathbb{Z}^2,\ p \in \mathcal{P})\ f_1(u) = p \ \text{ и } \ p = 2\ (9). \tag{3.1.7}$$

Соотношение (3) следует из соотношения (7) и цитированной выше теоремы Сатже. Если соотношение (1) не имеет место, то, по условию, выполняется соотношение (2) и потому

$$(\exists\, d \in \mathbb{N}^2)\ ad_1^3 + bd_2^3 = 2\ (9); \tag{3.1.8}$$

в этом случае положим

$$f_2(y) := a(d_1 + 3y_1)^3 + b(d_2 + 3y_2)^3$$

и заметим, что, в силу теоремы 4 и соотношения (8),

$$(\exists\, u \in \mathbb{Z}^2,\ p \in \mathcal{P})\ f_2(u) = p \ \text{ и } \ p = 2\ (9). \tag{3.1.9}$$

Как и в первом случае, соотношение (3) следует из теоремы Сатже и соотношения (9). Следствие 2 доказано.

Множества рациональных точек $H_1(\mathbb{Q})$ и $H_2(\mathbb{Q})$ изучались также в работе [161].

3. Теоремы 1 - 4 доказываются с помощью метода решета. Рассмотрим последовательность

$$a : \mathbb{N} \to \mathbb{N}_0,\ n \mapsto a_n$$

и попытаемся найти асимптотику суммы

$$\sum_{p\in\mathcal{P},\, p\le X} a_p \ \text{ при } \ X \to \infty$$

или, как в теореме 1, суммы

$$S(X) := \sum_{n\le X} a_n \Lambda(n).$$

Положим

$$A_d(X) := \sum_{n\le X,\, d|n} a_n \ \text{ при } \ d \in \mathbb{N} \ \text{ и } \ A(X) := A_1(X).$$

Ясно, что

$$S(X) = -\sum_{d\le X} (\mu(d)\log d) A_d(X).$$

В работе [82] рассматриваются последовательности a_n, для которых

$$A(X) \gg A(\sqrt{X})(\log X)^2,\ A(X) \gg X^{1/3}(\sum_{n\le X} a_n^2)^{1/2}; \tag{3.1.10}$$

$$A_d(X) = g(d)A(X) + r_d(X), \tag{3.1.11}$$

где $g(d)$ есть мульпликативная функция под условием

$$0 \le g(p^2) \le g(p) < 1,\ g(p) \gg p^{-1},\ g(p^2) \gg p^{-2} \ \text{ при } \ p \in \mathcal{P}$$

и

$$\sum_{p\in P,\, p\le X} g(p) = \log\log X + c_0(g) + O((\log X)^{-c_1}); \tag{3.1.12}$$

$$A_d(X) \ll \frac{\tau(d)^{c_2}}{d} A(X) \ \text{ равномерно в интервале } \ 1 \le d \le X^{1/3}; \tag{3.1.13}$$

$$\sum_{d\le D(X)(\log X)^{c_2}} \mu_3(d)|r_d(t)| \le A(X)(\log X)^{-c_3}$$

$$\text{при } \ t \le x \ \text{ и } \ X^{2/3} < D(X) < X, \tag{3.1.14}$$

где $\mu_3(d)$ есть характеристическая функция множества

$$\{n | n \in \mathbb{N},\ (\forall\, p \in \mathcal{P})\ n \neq 0\ (p^3)\}$$

"свободных от кубов" натуральных чисел, $\tau(d)$ есть число делителей числа d. Условия, аналогичные условиям (10) - (14), суть стандартные ограничения на последовательности, исследуемые методом решета. Хорошо известно, что такие ограничения сами по себе не позволяют получить асимптотику или даже оценить снизу функции $A(X)$ и $S(X)$. Если, например, a_n есть характеристическая функция множества натуральных чисел, содержащих чётное число простых делителей, то $a_p = 0$ при $p \in \mathcal{P}$, хотя последовательность a_n и удовлетворяет условиям (10) - (14) (см. [82, стр. 1045-1046]). Положим

$$\beta(n, C) = \mu(n) \sum_{d|n,\, d\le C} \mu(d) \ \text{ при } \ C \in \mathbb{R}_+^* \ \text{ и } \ n \in \mathbb{N},$$

$$\Pi(l) := \prod_{p\in\mathcal{P},\, p\le l} p \ \text{ при } \ l \in \mathbb{N}$$

и

$$\mathcal{A}(X, N, p_0) :=$$

$$\{(m, n) | (m, n) \in \mathbb{N}^2,\ N \le n \le 2N,\ mn \le X,\ (n, m\Pi(p_0)) = \ (1)\}.$$

В работах [80] - [82] предполагается, что, помимо условий (10) - (14), последовательность a_n удовлетворяет ещё одному условию "второго типа" :

$$\sum_{m\le X} \Big| \sum_{(m,n)\in\mathcal{A}(x,N,p_0)} \beta(n, C)\ a_{mn} \Big| \le A(X)(\log X)^{-c_4} \tag{3.1.15}$$

при

$$\frac{\sqrt{D(X)}}{\Delta(X)} < N < \frac{\sqrt{X}}{\delta(X)} \text{ и } 1 \leq C \leq \frac{X}{D(X)},$$

где

$$\Delta(X) \geq \delta(X) \geq 2,\ 2 \leq p_0 \leq \Delta(x)^{1/c_5 \log\log X}$$

и $c_1, ..., c_5$ суть фиксированные положительные вещественные числа.

Теорема 3.1.5 (см. [82]). *Предположим, что последовательность a_n удовлетворяет условиям* (10) - (15). *Тогда*

$$\sum_{p\in\mathcal{P},\, p\leq X} a_p \log p = HA(X)(1 + O(\frac{\log\delta(X)}{\log\Delta(X)})),$$

где

$$H := \prod_{p\in\mathcal{P}} (1 - g(p))(1 - \frac{1}{p})^{-1}$$

и O - константа зависит лишь от функции g.

Для последовательности Иванца - Фридландера

$$a_n := |\{b | b \in \mathbb{N}^2,\ b_1^2 + b_2^4\}|$$

условия (10) - (13) проверяются сравнительно легко, а условие (14) было проверено в работе [78]. Гораздо труднее доказать для этой последовательности оценку (15); для этой цели применяются довольно тонкие рассуждения в стиле двумерной арифметики Гекке [99] поля $\mathbb{Q}(\sqrt{-1})$.

Последовательности

$$a_n := |\{b | b \in \mathbb{N}^2,\ f(b) = n\}|$$

в теоремах 2 - 4 не удовлетворяют условию (15). Рассмотрим кубическое поле k, т.е. поле алгебраических чисел под условием $[k : \mathbb{Q}] = 3$. Пусть

$$\{\omega_1,\ \omega_2\} \subseteq \mathfrak{o}(k) \setminus \{0\},\ \theta_0 := \omega_2\omega_1^{-1},\ k = \mathbb{Q}(\theta_0) \text{ и } \mathfrak{d} := (\omega_1,\ \omega_2);$$

положим

$$\mathcal{A}(X) :=$$

$$\{(a_1\omega_1 + a_2\omega_2)\mathfrak{d}^{-1} | a \in \mathbb{Z}^2,\ X < a_1, a_2 \leq X(1+\eta(X,c)),\ (a_1,a_2) = (1)\}.$$

Для доказательства теоремы 4 достаточно оценить число $|\mathcal{A}(X) \cap \mathcal{P}(k)|$ простых идеалов в $\mathcal{A}(X)$; при этом роль условий второго типа играют оценки сверху сумм вида

$$\sum_{\mathfrak{a}\mathfrak{b} \in \mathcal{A}_1(X,V)} b_{\mathfrak{a}} g_{\mathfrak{b}} \ \text{ при } \ X^{1+\tau} \ll V \ll X^{3/2-\tau},\ \tau := (\log\log X)^{-1/6},$$

где

$$\mathcal{A}_1(X,V) := \{(\mathfrak{a},\mathfrak{b}) | (\mathfrak{a},\mathfrak{b}) \in I_0(k)^2,\ \mathfrak{a}\mathfrak{b} \in \mathcal{A}(X),\ V < |\mathfrak{b}| \leq 2V\}$$

и

$$b_{\mathfrak{a}} \in \{0,1\},\ g_{\mathfrak{a}} \in \mathbb{R} \ \text{ при } \ \mathfrak{a} \in I_0(k).$$

Такие оценки получены в работах [95] и [97], [98] с помощью трёхмерной арифметики Гекке кубическиих полей.

Цель этой главы - изложить доказательство теоремы 4; следуя нашим совместным работам [97], [98], я предварительно докажу теорему 3. При доказательстве теоремы 3 рассуждения, полностью аналогичные соответствующим рассмотрениям в работе Хис-Брауна [95], иногда опускаются, а при доказательстве теоремы 4 опускаются рассуждения, аналогичные соответствующим расуждением при доказательстве теоремы 3. Круг идей, сделавших возможным доказательство теорем 1 - 4, обсуждается в недавней монографии [89].

Обозначения. Рассмотрим поле алгебраических чисел K и определим две функции

$$\mu : I_0(K) \to \{0,\ \pm 1\},\ \mu(\mathfrak{a}\mathfrak{b}) = \mu(\mathfrak{a})\mu(\mathfrak{b}) \ \text{ при } \ \{\mathfrak{a},\mathfrak{b}\} \subseteq I_0(K),\ (\mathfrak{a},\mathfrak{b}) = (1),$$

$$\mu((1)) = 1,\ \mu(\mathfrak{p}) = -1,\ \mu(\mathfrak{p}^l) = 0 \ \text{ при } \ \mathfrak{p} \in \mathcal{P}(K),\ l \in \mathbb{N} \setminus \{1\}$$

и

$$\tau : I_0(K) \to \mathbb{N},\ \tau(\mathfrak{a}\mathfrak{b}) = \tau(\mathfrak{a})\tau(\mathfrak{b}) \ \text{ при } \ \{\mathfrak{a},\mathfrak{b}\} \subseteq I_0(K),\ (\mathfrak{a},\mathfrak{b}) = (1),$$

$$\tau(\mathfrak{p}^l) = l+1 \text{ при } \mathfrak{p} \in \mathcal{P}(K),\ l \in \mathbb{N}_0;$$

положим, для краткости,

$$\mu(\alpha) := \mu((\alpha)) \text{ и } \tau(\alpha) := \tau((\alpha)) \text{ при } \alpha \in \mathfrak{o}(K) \setminus \{0\}.$$

Обозначим через $\phi(K)$ вычет дзета-функции Дедекинда поля K в точке $s = 1$:

$$\phi(K) := \lim_{s \to 1} (s-1) \sum_{\mathfrak{a} \in I_0(K)} |\mathfrak{a}|^{-s}.$$

При $\mathcal{D} \subseteq I_0(K)$ положим

$$\pi(\mathcal{D}) = |\mathcal{D} \cap \mathcal{P}(K)|.$$

Пусть

$$X \in \mathbb{R},\ X \geq 3,\ \tau := \tau(X) = (\log\log X)^{-1/6},\ \eta := \eta(X, c_0) = (\log X)^{-c_0},$$

где c_0 есть фиксированное вещественное положительное число, зависящее лишь от f и выбираемое по ходу доказательства, и

$$I(X) := \{a | a \in \mathbb{Z}^2,\ X < a_1, a_2 \leq X(1+\eta)\}.$$

В дальнейшем $c,\ c_1,\ c_2, ...,$ а также O - и $\ll$ - константы, вообще говоря, зависят от f. Положим

$$e_q(x) := \exp(2\pi i x/q) \text{ и } \partial_i h(x) := \frac{\partial h(x)}{\partial x_i}\ .$$

3.2 Теорема о представлении простых чисел бинарными кубическими формами (формулировка)

1. Рассмотрим бинарную кубическую форму

$$f(x) = N_{k(x)/\mathbb{Q}(x)}(x_1\omega_1 + x_2\omega_2)|\mathfrak{d}|^{-1}. \tag{3.2.1}$$

Ясно, что $f(x) \in \mathbb{Z}[x]$; положим

$$(\{f(a) | a \in \mathbb{Z}^2\}) = (\varepsilon(f)) \text{ с } \varepsilon(f) \in \mathbb{N} \text{ и } h_f = f(1,1)$$

и предположим, не нарушая общности, что $h_f \in \mathbb{N}$.

Лемма 3.2.1. *Полином $f(x)$ есть неприводимая в $\mathbb{Z}[x]$ примитивная бинарная кубическая форма, причём*

$$\varepsilon(f) \in \{1, 2\} \ \ и$$

$$(N\omega_1,\ N\omega_2,\ N(\omega_1+\omega_2),\ N(\omega_1-\omega_2)) = 0\ (2\ |\mathfrak{d}|) \Longleftrightarrow \varepsilon(f) = 2. \qquad (3.2.2)$$

Любая неприводимая в $\mathbb{Z}[x]$ примитивная бинарная кубическая форма представима в виде (1) .

Доказательство. Положим

$$f(x) = \sum_{i=0}^{3} a_i x_1^i x_2^{3-i} \ \text{ с } \ \{a_i | 0 \le i \le 3\} \subseteq \mathbb{Z}.$$

Так как $k = \mathbb{Q}(\theta_0)$, полином $f(x)$ неприводим в $\mathbb{Z}[x]$. Пусть

$$(a_0, ..., a_3) = 0\ (p) \ \text{ и } \ p \in \mathcal{P},$$

тогда

$$|\mathfrak{d}|^{-1}(N\omega_1,\ N\omega_2,\ N(\omega_1+\omega_2),\ N(\omega_1-\omega_2)) = 0\ (p)$$

и, значит,

$$(\exists\ \{\mathfrak{p}_i | 0 \le i \le 3\} \subseteq \mathcal{P}(k))\ (p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,$$

$$(\omega_1)\mathfrak{d}^{-1} = 0\ (\mathfrak{p}_1),\ (\omega_2)\mathfrak{d}^{-1} = 0\ (\mathfrak{p}_2),\ (\omega_1 \pm \omega_2)\mathfrak{d}^{-1} = 0\ (\mathfrak{p}_3).$$

Из последнего соотношения следует, что $p = 2$ и $a_1 a_2 \neq 0\ (2)$; таким образом, $(a_0, ..., a_3) = (1)$ и, как легко видеть, имеет место соотношение (2). Рассмотрим неприводимую в $\mathbb{Z}[x]$ примитивную бинарную кубическую форму $f(x)$. Ясно, что

$$(\exists\ a \in \mathbb{Z},\ \xi \in k^*)\ f(x) = aN_{k(x)/\mathbb{Q}(x)}(x_1 + \xi x_2).$$

Пусть

$$m\xi \in \mathfrak{o}(k),\ m \in \mathbb{Z},\ \omega := m\xi,\ \mathfrak{d} := (m, \omega)$$

и

$$g(x) := |\mathfrak{d}|^{-1} N_{k(x)/\mathbb{Q}(x)}(x_1 m + x_2 \omega);$$

ясно, что $f(x) = g(x)$. Лемма доказана.

Введём следующие обозначения:

$$\theta := |\mathfrak{d}|^{-1}\theta_0 N(\omega_1), \;\; i(\theta) := (\mathfrak{o}(k) : \mathbb{Z}[\theta]),$$

$$\mathcal{P}_0 := \{p | p \in \mathcal{P}, \; i(\theta) N(\omega_1\omega_2) = 0 \; (p)\}, \;\; \Pi_0 := \prod_{p \in \mathcal{P}_0} p;$$

$$\mathfrak{A}_a := (a_1\omega_1 + a_2\omega_2)\mathfrak{d}^{-1} \;\text{ при }\; a \in \mathbb{Z}^2$$

и

$$\mathcal{A}_0 := \{\mathfrak{A}_a | a \in \mathbb{N}^2, \; (a_1, a_2) = \; (1)\}.$$

Ясно, что $f(a) = |\mathfrak{A}_a|$ при $a \in \mathbb{Z}^2$.

Лемма 3.2.2 . *Пусть*

$$\mathfrak{A}_a \in \mathcal{A}_0, \; p \in \mathcal{P} \setminus \mathcal{P}_0, \; \mathfrak{p}_i \in \mathcal{P}(k) \;\; u \;\; (p, \; \mathfrak{A}_a) = 0 \; (\mathfrak{p}_i) \;\; npu \;\; i \in \{1, 2\}; \quad (3.2.3)$$

тогда $\mathfrak{p}_1 = \mathfrak{p}_2$ *и* $|\mathfrak{p}_1| = p$.

Доказательство. Из соотношения (3) следует, что

$$(a_1 a_2, p) = \; (1), \; i(\theta) \neq 0 \; (\mathfrak{p}_i) \;\text{ и }\; \theta_0 = -a_1 a_2^{-1} \; (\mathfrak{p}_i) \;\text{ при }\; i \in \{1, 2\}.$$

Пусть

$$n \in \mathbb{N} \;\text{ и }\; n = -a_1 a_2^{-1} \; (p),$$

тогда

$$\theta_0 = n \; (\mathfrak{p}_i) \;\text{ при }\; i \in \{1, 2\} \;\text{ и }\; n \in \mathbb{Z}. \quad (3.2.4)$$

Так как $i(\theta) \neq 0 \; (\mathfrak{p}_i)$, из соотношения (4) следует, что

$$|\mathfrak{p}_i| = p \;\text{ при }\; i \in \{1, 2\}.$$

Рассмотрим характеристический многочлен

$$g(u) := N_{k(u)/\mathbb{Q}(u)}(u - \theta_0)$$

элемента θ_0. Имеем

$$g(n) = -a_2^{-3}|\mathfrak{d}\mathfrak{A}_{\vec{a}}|N\omega_1^{-1} = 0\ (p);$$

следовательно, по теореме Дедекинда (см., например, [114, лемма 1]),

$$(p, \theta_0 - n) \in \mathcal{P}(k).$$

Но $\mathfrak{p}_i|(p, \theta_0 - n)$ при $i \in \{1, 2\}$ и, значит,

$$\mathfrak{p}_1 = \mathfrak{p}_2 = (p, \theta_0 - n).$$

Лемма доказана.

Положим

$$\mathcal{A}(X) := \{\mathfrak{A}_a | \mathfrak{A}_a \in \mathcal{A}_0,\ a \in I(X)\}.$$

Лемма 3.2.3. *Пусть* $\{\mathfrak{A}_a, \mathfrak{A}_b\} \subseteq \mathcal{A}(X)$. *Тогда*

$$f(a) = h_f X^3(1 + O(\eta))\ \text{ и }\ \mathfrak{A}_a = \mathfrak{A}_b\ \Rightarrow\ a = b.$$

Доказательство. Пусть $\mathfrak{A}_a \in \mathcal{A}(X)$, тогда

$$f(a) = X^3 f(a/X)\ \text{ и }\ a_i/X = 1 + O(\eta)\ \text{ при }\ i \in \{1, 2\}$$

и потому $f(a) = h_f X^3(1 + O(\eta))$, так как $h_f > 0$. Пусть

$$\{\mathfrak{A}_a, \mathfrak{A}_b\} \subseteq \mathcal{A}(X)\ \text{ и }\ \mathfrak{A}_a = \mathfrak{A}_b;$$

положим

$$\alpha = (a_1\omega_1 + a_2\omega_2)(b_1\omega_1 + b_2\omega_2)^{-1}.$$

Тогда

$$\alpha \in \mathfrak{o}^*\ \text{ и }\ \mathrm{Tr}\ \alpha = (a_1\partial_1 f(b) + a_2\partial_2 f(b))f(b)^{-1},$$

или

$$\mathrm{Tr}\ \alpha = (b_1\partial_1 f(b) + b_2\partial_2 f(b))f(b)^{-1} + O(\eta X f(b)^{-1}(|\partial_1 f(b)| + |\partial_2 f(b)|)).$$

Откуда следует, что $\mathrm{Tr}\ \alpha = 3 + O(\eta)$ и, значит, $\mathrm{Tr}\ \alpha = 3$, ибо $\mathrm{Tr}\ \alpha \in \mathbb{Z}$; аналогично доказывается, что $\mathrm{Tr}\ \alpha^{-1} = 3$. Значит, $\alpha = 1$ и, следовательно, $a = b$. Лемма доказана.

Следствие 3.2.1 . *Пусть* $\mathfrak{A}_a \in \mathcal{A}(X)$, *тогда*

$$f(a) \in \mathcal{P} \Leftrightarrow \mathfrak{A}_a \in \mathcal{P}(k).$$

Доказательство. Это утверждение есть следствие леммы 2 и леммы 3.

2. Положим

$$r := |R|,\ R_0 := (R, \Pi_0)\ \text{ и }\ R = R_0 R_1\ \text{ при }\ R \in I_0(k)$$

и

$$\mathcal{R} := \{R | R \in I_0(k),\ \mu(R)^2 = 1,\ \mu(|R_1|)^2 = 1\}.$$

В силу леммы 2,

$$\{R | R \in \mathcal{A}_0,\ \mu(R)^2 = 1\} \subseteq \mathcal{R}.$$

Положим далее

$$\mathfrak{m}(R) := \{u | u \in \mathbb{Z}^2,\ 1 \leq u_1, u_2 \leq r,\ \mathfrak{A}_u = 0\ (R)\},$$

$$\alpha(R) := r^{-1}\ |\mathfrak{m}(R)|,\ \beta(R) := r^{-2}\ |\mathfrak{m}(R)|, \tag{3.2.5}$$

$$\alpha_1(R) := \prod_{p \in \mathcal{P},\ p|r} (1 - p^{-2})^{-1}(1 - p^{-2}\beta((R,p))^{-1}); \tag{3.2.6}$$

$$\gamma(p) = -\sum_{R \in m(p)} \mu(R)\alpha(R_0)\ \alpha_1(R)\ r^{-1}$$

с

$$m(p) := \{R | R \in \mathcal{R},\ p = 0\ (R),\ R \neq (1)\}$$

и

$$\sigma(f) := \prod_{p \in \mathcal{P}} (1 + p^{-1})(1 - \gamma(p)). \tag{3.2.7}$$

Заметим, что

$$\alpha(R) = \alpha(R_0)\alpha(R_1) = \alpha(R_0)\ \text{ при }\ R \in \mathcal{R}\ \text{ и }\ \alpha((1)) = 1. \tag{3.2.8}$$

Лемма 3.2.4. *Бесконечное произведение в правой части определения* (7) *сходится и имеют место следующие соотношения:*

$$(\forall\, p \in \mathcal{P})\ 0 \leq \gamma(p) \leq 1, \tag{3.2.9}$$

$$(\forall\, p \in \mathcal{P} \setminus (\mathcal{P}_0 \cup \{2\})\ 1 - \gamma(p) \geq 1/4 \tag{3.2.10}$$

и

$$\gamma(2) = 1 \Leftrightarrow \varepsilon(f) = 2. \tag{3.2.11}$$

Доказательство. Пусть $p \notin \mathcal{P}_0$, тогда, в силу определений (5) и (6) и соотношения (8), имеет место равенство:

$$(1 + p^{-1})(1 - \gamma(p)) = 1 - (\nu_p - 1)p^{-1}, \tag{3.2.12}$$

где

$$\nu_p := |\{\mathfrak{p} | \mathfrak{p} \in \mathcal{P}(k),\ |\mathfrak{p}| = p\}|.$$

Из равенства (12) вытекают как соотношение (10), так и следующее соотношение:

$$(\forall\, p \in \mathcal{P} \setminus \mathcal{P}_0)\ 0 \leq \gamma(p) \leq 1, \tag{3.2.13}$$

ибо $0 \leq \nu_p \leq 3$ при $p \in \mathcal{P}$. С другой стороны, из асимптотического закона распределения простых идеалов в полях $\mathbb{Q}$ и k следует, что

$$(\exists\, c(k) \in \mathbb{R}_+^*) \sum_{p \in \mathcal{P},\ p \leq X} (\nu_p - 1) = O(\exp(-c(k)(\log X)^{1/2}) \tag{3.2.14}$$

при $X \to \infty$. Так как множество $\mathcal{P}_0$ конечно, сходимость произведения (7) следует из соотношений (12) и (14). Пусть теперь $p \in \mathcal{P}_0$. Из определений (5) и (6) и равенства (8) следует, что

$$\gamma(p) =$$

$$-\sum_{R \in m(p)} \mu(R)\beta(R)\ \alpha_1(R) = (1 - p^2)^{-1} \sum_{R \in m(p)} \mu(R)(p^2\beta(R) - 1). \tag{3.2.15}$$

Положим

$$b(R) := p^2\beta(R) \text{ и } B(p) := \sum_{R\in I_0(k),\, R|p} \mu(R)b(R);$$

так как

$$\mu(R) \neq 0 \Rightarrow R \in \mathcal{R} \text{ при } R \in I_0(k) \text{ и } p = 0\ (R),$$

равенство (15) переписывается следующим образом:

$$1 - \gamma(p) = (p^2 - 1)^{-1}B(p). \tag{3.2.16}$$

Но

$$b(R) = |\{u|u \in \mathbb{Z}^2,\ 1 \leq u_1, u_2 \leq p,\ \mathfrak{A}_u = 0\ (R)\}| \text{ при } p = 0\ (R);$$

поэтому

$$B(p) = |\{u|u \in \mathbb{Z}^2,\ 1 \leq u_1, u_2 \leq p,\ (\mathfrak{A}_u, p) = (1)\}|,$$

значит, $B(p) \leq p^2 - 1$ и, более того, $B(p) < p^2 - 1$, если $\varepsilon(f) \neq 0\ (p)$. Таким образом, из соотношения (16) следует, что

$$(\forall\, p \in \mathcal{P}_0)\ 0 \leq \gamma(p) \leq 1, \tag{3.2.17}$$

$\gamma(p) < 1$ при $p \neq 2$ и $\gamma(2) < 1$ при $\varepsilon(f) \neq 2$. Соотношение (9) следует из соотношений (13) и (17). Остаётся доказать, что

$$\gamma(2) = 1 \text{ при } \varepsilon(f) = 2;$$

но, в силу леммы 1,

$$2 \in \mathcal{P}_0 \text{ и } B(2) = 3 \text{ при } \varepsilon(f) = 2$$

и потому из равенства (16) следует, что $\gamma(2) = 1$. Лемма доказана.

Положим

$$\pi_f(X) := |\{p|p \in \mathcal{P},\ (\exists\, x \in I(X))\ f(x) = p\}|\ .$$

В силу следствия 1,

$$\pi_f(X) = \pi(\mathcal{A}(X)).$$

Теорема 3.2.1 . *Рассмотрим неприводимую в* $\mathbb{Z}[x]$ *примитивную бинарную кубическую форму* $f(x)$ *с* $\varepsilon(f) = 1$ *и* $h_f \in \mathbb{N}$. *Имеет место следующая асимптотическая формула:*

$$\pi_f(X) = \sigma(f)\,\frac{\eta^2 X^2}{3\log X}\,(1 + O((\log\log X)^{-1/6}))\ \ \textit{при}\ \ X \to \infty. \qquad (3.2.18)$$

Следствие 3.2.2 . *Рассмотрим неприводимую в* $\mathbb{Z}[x]$ *примитивную бинарную кубическую форму* $f(x)$. *Пусть*

$$\varepsilon(f) = 2\ \ и\ \ f(2,1) > 0;$$

положим

$$\pi_{f,1}(X) := |\{p | p \in \mathcal{P},\ p = \frac{f(a)}{2},\ (a_1/2, a_2) \in I(X)\}|.$$

Имеет место следующая асимптотическая формула:

$$\pi_{f,1}(X) = \sigma(g)\,\frac{\eta^2 X^2}{3\log X}\,(1 + O((\log\log X)^{-1/6}))\ \ \textit{при}\ \ X \to \infty, \qquad (3.2.19)$$

где

$$g(y) := \frac{1}{2} f(2y_1, y_2)\ \ и\ \ \varepsilon(g) = 1.$$

Доказательство. Легко видеть, что кубическая форма $g(y)$ удовлетворяет условиям теоремы 1 и, значит, асимптотическая формула (19) вытекает из формулы (18).

Теорема 1 будет доказана в первой части этой главы; теорема 1.3 вытекает из теоремы 1, следствия 2 и леммы 4.

3.3 Несколько вспомогательных утверждений

Положим

$$\sigma(R, X) := |\{a | a \in I(X),\ \mathfrak{A}_a = 0\ (R)\}|,$$

$$\sigma_0(R,a) := \sum_{u\in\mathfrak{m}(R)} e_r(a_1u_1 + a_2u_2);$$

и заметим, что

$$\sigma_0(\mathfrak{ab},a) = \sigma_0(\mathfrak{a},a)\sigma_0(\mathfrak{b},a) \ \text{ при } \ (|\mathfrak{a}|,|\mathfrak{b}|) = (1). \tag{3.3.1}$$

Можно показать (ср. [95, §5]), что

$$\sigma(R,X) = r^{-2} \sum_{(a,x)\in I(X,r)} \sigma_0(R,a)e_r(-a_1x_1 - a_2x_2),$$

где

$$I(X,r) := \{(a,x)|a \in \mathbb{Z}^2,\ 0 \le a_1,a_2 < r,\ x \in I(X)\},$$

и потому

$$\sigma(R,X) = \frac{\eta^2X^2}{r}\,\alpha(R_0) + \rho(R,X), \tag{3.3.2}$$

где

$$\rho(R,X) = \Sigma_0 + O(\frac{X}{r}) \tag{3.3.3}$$

и

$$\Sigma_0 = r^{-2} \sum_{(a,x)\in I(X,r)^*} \sigma_0(R,a)e_r(-a_1x_1 - a_2x_2) \tag{3.3.4}$$

с

$$I(X,r)^* := I(X,r) \setminus \{(0,x)|x \in I(X)\}.$$

Пусть

$$l \in \mathbb{N},\ Q \in \mathbb{R},\ Q \ge 3 \ \text{ и } \ \mathcal{R}(Q) := \{R|R \in \mathcal{R},\ Q < |R| \le 2Q\};$$

положим

$$\Sigma_1 := \sum_{R\in\mathcal{R}(Q)} \tau(R)^l|\rho(R,X)|.$$

Лемма 3.3.1. *Существует вещественное число $c(l)$ под условием*

$$\Sigma_1 \ll (X+Q)(\log Q)^{c(l)}.$$

Доказательство. Из соотношения (3) следует, что

$$\Sigma_1 \le \Sigma_{11} + \Sigma_{12} \ \text{ с } \ \Sigma_{11} \ll X \sum_{R \in \mathcal{R}(Q)} \tau(R)^l |R|^{-1} \ll X (\log Q)^{c_1(l)}$$

и

$$\Sigma_{12} = \sum_{R \in \mathcal{R}(Q)} \tau(R)^l |\Sigma_0|. \tag{3.3.5}$$

Соотношение (4) даёт:

$$\Sigma_0 \le r^{-2} \sum_{a \ne 0 \bmod r} |\sigma_0(R,a)| \, | \sum_{x \in I(X)} e_r(-a_1 x_1 - a_2 x_2)|.$$

Но

$$|\sigma_0(R,a)| = |\sigma_0(R_0,a)| \, |\sigma_0(R_1,a)| \le |R_0|^2 \, |\sigma_0(R_1,a)| \ll |\sigma_0(R_1,a)|$$

и потому

$$|\Sigma_0| \ll \sum_{a \in m_1(r)} \frac{|\sigma_0(R_1,a)|}{r^2} \min\{X, \frac{r}{|a_1|}\} \min\{X, \frac{r}{|a_2|}\} \tag{3.3.6}$$

с

$$m_1(r) := \{a | a \in \mathbb{Z}^2, \ \max\{|a_1|, \ |a_2|\} \le r/2, \ a \ne 0\}.$$

Более того, если

$$|R_1| = p, \ p \in \mathcal{P}, \ a \ne 0 \bmod p \ \text{ и } \ t \ne 0 \ (p),$$

то

$$\sigma_0(R_1,a) = \sum_{tu \in \mathfrak{m}(R_1)} e_p(tua) = \sum_{u \in \mathfrak{m}(R_1)} e_p(tua)$$

и потому

$$(p-1) \, \sigma_0(R_1,a) \sum_{t=1}^{p-1} \sum_{u \in \mathfrak{m}(R_1)} e_p(tua) =$$

$$p \, |\{u | u \in \mathfrak{m}(R_1), u_1 a_1 + u_2 a_2 = 0 \ (p)\}| - |\mathfrak{m}(R_1)|;$$

из этого сотношения вытекает, что

$$(p-1) \, \sigma_0(R_1,a) = p - |\mathfrak{m}(R_1)| = 0 \ \text{ при } \ a_2 \omega_1 \ne a_1 \omega_2 \ (R_1).$$

Значит, в силу соотношения (1),

$$(\forall\ R \in \mathcal{R})\ a_2\omega_1 \neq a_1\omega_2\ (R_1)\ \Rightarrow\ \sigma_0(R_1, a) = 0. \tag{3.3.7}$$

Подставив оценку (6) в соотношение (5) и просуммировав сначала по a с $a_1a_2 = 0$, а затем по a с $a_1a_2 \neq 0$, получим

$$\Sigma_{12} \ll \Sigma_{13} + \Sigma_{14},$$

где

$$\Sigma_{13} \ll X \sum_{0<a\leq Q} \frac{1}{a} \sum_{R\in\mathcal{R}(Q,a)} \tau(R)^l \ll X \sum_{0<a\leq Q} \frac{\tau(a)^{c_1(l)}}{a} \ll X\ (\log Q)^{c_2(l)}$$

с

$$\mathcal{R}(Q, a) := \{R | R \in \mathcal{R}(Q),\ a = 0\ (R_1)\}$$

и

$$\Sigma_{14} := \sum_{R\in\mathcal{R}(Q,a)} \sum_{a\in m_2(r)} \tau(R)^l\ \frac{|\sigma_0(R_1, a)|}{r^2} \min\{X, \frac{r}{|a_1|}\} \min\{X, \frac{r}{|a_2|}\}$$

с

$$m_2(r) := \{a | a \in m_1(r),\ a_1a_2 \neq 0\}.$$

Из определения суммы Σ_{14} следует, что

$$\Sigma_{14} \ll \sum_{R\in\mathcal{R}(Q)} \sum_{a\in\Omega(R)} \tau(R)^l\ \frac{|\sigma_0(R_1, a)|}{|a_1a_2|} \ll Q \sum_{R\in\mathcal{R}(Q)} \sum_{a\in\Omega(R)} \frac{\tau(R)^l}{|a_1a_2|}$$

с

$$\Omega(R) := \{a | a \in \mathbb{Z}^2,\ 1 \leq |a_1|, |a_2| \leq Q,\ a_2\omega_1 = a_1\omega_2\ (R_1)\}$$

и потому

$$\Sigma_{14} \ll Q \sum_{a\in M_0(Q)} \frac{\tau(a_2\omega_1 - a_1\omega_2)^{c_3(l)}}{|a_1a_2|} \ll$$

$$Q \sum_{L\in\mathcal{L}(Q)} \sum_{a\in M_1(L)} (L_1L_2)^{-1} \tau(a_2\omega_1 - a_1\omega_2)^{c_3(l)} \tag{3.3.8}$$

с

$$\mathcal{L}(Q) := \{L | L \in \mathbb{Z}^2,\ \{L_1, L_2\} \subseteq \{2^m | m \in \mathbb{Z},\ 1 \leq 2^m \leq Q\}\},$$

$$M_0(Q) := \{a | a \in \mathbb{Z}^2,\ 1 \le |a_1|, |a_2| \le Q\}$$

и

$$M_1(L) := \{a | a \in \mathbb{Z}^2,\ L_1 \le a_1 \le 2L_1,\ L_2 \le a_2 \le 2L_2\}.$$

Имеет место следующее утверждение (ср. [95, лемма 4.7]):

$$(\exists\, c(l) \in \mathbb{R}) \sum_{a \in M_2(x)} \tau(a_2\omega_1 - a_1\omega_2)^l \ll x_1 x_2\ (\log(x_1 x_2))^{c(l)} \tag{3.3.9}$$

при $x \in \mathbb{R},\ x_1 \ge 2,\ x_2 \ge 2$ с

$$M_2(x) := \{a | a \in \mathbb{Z}^2,\ |a_1| \le x_1,\ |a_2| \le x_2,\ a_1 a_2 \ne 0\}.$$

Из соотношений (8) и (9) вытекает, что

$$\Sigma_{14} \ll Q(\log Q)^{c_4(l)} |\mathcal{L}(Q)| \ll Q(\log Q)^{c_5(l)}.$$

Лемма доказана.

При

$$D \subseteq \mathbb{Z},\ \mathcal{D} \subseteq I_0(k),\ b \in \mathbb{Z} \ \text{ и } \ \mathfrak{b} \in I_0(k)$$

положим

$$D_b := \{a | a \in D,\ a = 0\ (d)\} \ \text{ и } \ \mathcal{D}_{\mathfrak{b}} = \{\mathfrak{a} | \mathfrak{a} \in \mathcal{D}, \mathfrak{a} = 0\ (\mathfrak{b})\}.$$

Пусть $R \in \mathcal{R}$, тогда

$$|\mathcal{A}(X)_R| = \sum_{d=1}^{\infty} \mu(d)\ \sigma(\frac{R}{(R,d)}, \frac{X}{d}) =$$

$$\frac{\eta^2 X^2}{r}\ \alpha(R_0) \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}\ \beta((R,d))^{-1} + \rho_1(R, X), \tag{3.3.10}$$

с

$$\rho_1(R, X) := \sum_{d=1}^{\infty} \mu(d)\ \rho(\frac{R}{(R,d)}, \frac{X}{d}). \tag{3.3.11}$$

Таким образом,

$$|\mathcal{A}(X)_R| = \frac{\eta^2 X^2}{r\zeta(2)}\ \alpha(R_0)\ \alpha_1(R) + \rho_1(R, X), \tag{3.3.12}$$

где $\alpha(R)$ и $\alpha_1(R)$ определены по формулам (2.5) и (2.6). Положим

$$\Sigma_2 := \sum_{R\in\mathcal{R}(Q)} \tau(R)^l |\rho_1(R,X)|.$$

Лемма 3.3.2 . *Пусть $l \in \mathbb{N}$; тогда*

$$(\exists\, c(l)\in\mathbb{R})\ \ \Sigma_2 \ll (Q + XQ^{1/2} + X^{3/2})(\log QX)^{c(l)}.$$

Доказательство. Пусть $\Delta \in \mathbb{R}_+$; в силу определения (11),

$$\Sigma_2 \le \Sigma_{21} + \Sigma_{22} \tag{3.3.13}$$

с

$$\Sigma_{21} := \sum_{d>\Delta} \sum_{R\in\mathcal{R}(Q)} \tau(R)^l |\rho(\frac{R}{(R,d)}, \frac{X}{d})|$$

и

$$\Sigma_{22} := \sum_{d\le\Delta} \sum_{R\in\mathcal{R}(Q)} \tau(R)^l |\rho(\frac{R}{(R,d)}, \frac{X}{d})|.$$

Из соотношения (2) следует, что

$$\Sigma_{21} \le \Sigma_{23} + \Sigma_{24}$$

с

$$\Sigma_{23} := \sum_{d>\Delta} \sum_{R\in\mathcal{R}(Q)} \tau(R)^l |\sigma(\frac{R}{(R,d)}, \frac{X}{d})|,$$

и

$$\Sigma_{24} := \eta^2 X^2 \sum_{d>\Delta} \sum_{R\in\mathcal{R}(Q)} \tau(R)^l\ \frac{|(R,d)|}{d^2\ |R|}\ \alpha(\frac{R_0}{(R_0,d)})$$

$$\ll \eta^2 X^2 \sum_{d>\Delta} \sum_{R\in\mathcal{R}(Q)} \frac{\tau(R)^l}{|R|}\ \frac{|(R,d)|}{d^2} \ll \eta^2 X^2 \sum_{d>\Delta} \sum_{R\in\mathcal{R}(Q)} \frac{\tau(R_1)^l}{|R_1|}\ \frac{|(R_1,d)|}{d^2},$$

ибо

$$\frac{\tau(R_0)^l |(R_0,d)|}{|R_0|}\ \ll 1\ \text{ при }\ R\in\mathcal{R}.$$

Введём новые переменные

$$\mathfrak{A}_1 := (R_1,d),\ \mathfrak{A}_2 := R_1\mathfrak{A}_1^{-1}$$

и заметим, что $d = 0\ (|\mathfrak{A}_1|)$, так как

$$\mu(|(R_1, d)|)^2 = 1 \ \text{ при } \ R \in \mathcal{R}.$$

Положим

$$\mathcal{R}_1(Q) := \{\mathfrak{A} | \mathfrak{A} \in I_0(k)^2,\ \mathfrak{A}_1\mathfrak{A}_2 = R_1,\ R \in \mathcal{R}(Q)\}$$

и

$$D(\mathfrak{A}) := \{d | d \in \mathbb{Z},\ d = 0\ (|\mathfrak{A}|),\ d > \Delta\} \ \text{ при } \ \mathfrak{A} \in I_0(k).$$

Тогда

$$\Sigma_{24} \ll \eta^2 X^2 \sum_{\mathfrak{A} \in \mathcal{R}_1(Q)} \tau(\mathfrak{A}_1)^l \tau(\mathfrak{A}_2)^l |\mathfrak{A}_1|^{-2} |\mathfrak{A}_2|^{-1} \sum_{m > \Delta |\mathfrak{A}_1|^{-1}} m^{-2}$$
$$\ll \eta^2 X^2 \Delta^{-1} (\log X)^{c_1(l)}$$

и

$$\Sigma_{23} \ll \sum_{\mathfrak{A} \in \mathcal{R}_1(Q)} \sum_{d \in D(\mathfrak{A}_1)} \tau(\mathfrak{A}_1)^l \tau(\mathfrak{A}_2)^l |\sigma(\frac{R_0\ \mathfrak{A}_2}{(R_0, d)}, \frac{X}{d})|$$
$$\leq \sum_{d \in D(\mathfrak{A}_1)} \tau(\mathfrak{A}_1)^l \sum_{\mathfrak{A} \in \mathcal{R}_1(Q)} \tau(\mathfrak{A}_2)^l |\sigma(\mathfrak{A}_2, \frac{X}{d})|$$
$$\ll \sum_{d > \Delta} \tau(d)^{c_2(l)} \sum_{a \in I(X/d)} \tau(\mathfrak{A}_a)^{c_2(l)}.$$

Ввиду соотношения (9), отсюда следует, что

$$\Sigma_{23} \ll X^2 \Delta^{-1} (\log X)^{c_3(l)};$$

таким образом,

$$\Sigma_{21} \ll \Delta^{-1}\ X^2 (\log X)^{c_4(l)}. \tag{3.3.14}$$

Аналогичным образом, вводя новые переменные

$$\mathfrak{A} := (R, d),\ \mathfrak{B} := R\ \mathfrak{A}^{-1},$$

получаем

$$\Sigma_{22} \leq \sum_{\mathfrak{A}\mathfrak{B} \in \mathcal{R}(Q)} \sum_{d \in D_1(\mathfrak{A}_1)} \tau(\mathfrak{A})^l \tau(\mathfrak{B})^l |\rho(\mathfrak{B}, \frac{X}{d})|$$

$$= \sum_{\mathfrak{A}\in\mathcal{R}(Q)} \sum_{d\in D_1(\mathfrak{A}_1)} \tau(\mathfrak{A})^l \sum_{\mathfrak{B}\in\mathcal{R}(Q|\mathfrak{A}|^{-1})} \tau(\mathfrak{B})^l |\rho(\mathfrak{B}, \frac{X}{d})|$$

с

$$D_1(\mathfrak{A}) := \{d | d \in \mathbb{Z},\ d = 0\ (|\mathfrak{A}|),\ d \le \Delta\} \ \text{ при } \ \mathfrak{A} \in I_0(k) \ \text{ и } \ \mathfrak{A}_1 := (R_1, d)$$

и, значит, в силу леммы 1,

$$\Sigma_{22} \ll \sum_{d\in D_1(\mathfrak{A}_1)} \tau(\mathfrak{A})^l (\frac{Q}{N\mathfrak{A}} + \frac{X}{d})(\log Q)^{c_5(l)}$$

$$\ll \sum_{d\in D_1(\mathfrak{A}_1)} \tau(\mathfrak{A}_1)^l (\frac{Q}{N\mathfrak{A}_1} + \frac{X}{d})(\log Q)^{c_6(l)}$$

$$\ll \Delta\ (X+Q)(\log Q)^{c_7(l)}(\log X). \tag{3.3.15}$$

Доказываемое утверждение следует из соотношений (13) - (15) при

$$\Delta := 1 + \ \min\{X^{1/2}\,,\, XQ^{-1/2}\}.$$

Пусть

$$A(X) := \{f(a) | a \in I(X),\ (a_1, a_2) = (1)\} = \{|\mathfrak{a}|\ |\mathfrak{a} \in \mathcal{A}(X)\}.$$

При $q \in \mathbb{N}$ и $\mathfrak{A} \in I_0(k)$ положим

$$m_3(q, \mathfrak{A}) := \{R | R \in I_0(k),\ (\mathfrak{A}, q) = 0\ (R),\ |R| = 0\ (q)\}.$$

Предположим теперь, что натуральное число q свободно от квадратов. Из определения функции Мёбиуса $\mu(R)$ можно заключить тогда, что имеет место следующее тождество:

$$\mu(q) \sum_{R\in m_3(q,\mathfrak{A})} \mu(R) = \begin{cases} 1, & |\mathfrak{A}| = 0\ (q), \\ 0, & |\mathfrak{A}| \ne 0\ (q). \end{cases} \tag{3.3.16}$$

Положим

$$m(q) := \{R | R \in \mathcal{R},\ q = 0\ (R),\ |R| = 0\ (q)\};$$

в силу соотношения (16),

$$|A(X)_q| = |\{\mathfrak{A}|\mathfrak{A} \in \mathcal{A}(X),\ |\mathfrak{A}| = 0\ (q)\}| = \mu(q) \sum_{\mathfrak{A}\in\mathcal{A}(X)} \sum_{R\in m_3(q,\mathfrak{A})} \mu(R)$$

$$= \mu(q) \sum_{R\in m(q)} \mu(R)\ |\mathcal{A}(X)_R|. \tag{3.3.17}$$

Из соотношений (17) и (12) следует, что

$$|A(X)_q| = \gamma(q)\ \frac{\eta^2 X^2}{\zeta(2)} + \rho_2(q, X), \tag{3.3.18}$$

с

$$\gamma(q) = \mu(q) \sum_{R\in m(q)} \mu(R)\alpha(R_0)\ \alpha_1(R)\ r^{-1} = \prod_{p\in\mathcal{P},\ p|q} \gamma(p) \tag{3.3.19}$$

и

$$\rho_2(q, X) = \mu(q) \sum_{R\in m(q)} \mu(R)\rho_1(R, X). \tag{3.3.20}$$

Положим

$$\Sigma_3 = \sum_{Q<q\le 2Q} \tau(q)^l |\rho_2(q, X)|.$$

Лемма 3.3.3. *Пусть $l \in \mathbb{N}$; тогда*

$$(\exists\ c(l) \in \mathbb{R})\ \ \Sigma_3 \ll (Q + XQ^{1/2} + X^{3/2})(\log QX)^{c(l)}.$$

Доказательство. Положим

$$\mathcal{R}_1(q) :=$$

$$\{R|R \in \mathcal{R},\ |R_1| = q_1,\ q_0 = (q, \Pi_0),\ q = q_0q_1,\ q_0 = 0\ (R_0),\ |R_0| = 0(q_0)\}.$$

Из равенства (20) следует, что

$$\Sigma_3 \ll$$

$$\sum_{Q<q\le 2Q} \sum_{R\in\mathcal{R}_1(q)} \tau(q)^l \mu(q)^2\ |\rho_1(R, X)| \ll \sum_{R\in\mathcal{R}_2(Q)} \tau(R)^{c_1(l)}\ |\rho_1(R, X)| \tag{3.3.21}$$

с

$$\mathcal{R}_2(Q) := \{R|R \in \mathcal{R},\ Q < |R| \le 2\ \Pi_0^3\ Q\}.$$

Доказываемое утверждение следует из оценки (21) и леммы 2.

Положим

$$\mathcal{B}(X) = \{\mathfrak{A} | \mathfrak{A} \in I_0(k), h_f X^3 < |\mathfrak{A}| \leq h_f X^3(1+\eta)\},$$

$$B(X) = \{N\mathfrak{A} |\ \mathfrak{A} \in \mathcal{B}(X)\};$$

$$m_4(Q) := \{q | q \in \mathbb{Z},\ Q < q \leq 2Q\},$$

$$m_5(q) := \{R | R \in I_0(k),\ q = 0\ (R),\ |R| = 0\ (q)\},$$

$$m_6(q) := \{p | p \in \mathcal{P},\ q = 0\ (p)\} \ \text{ и } \ m_7(p) := \{\mathfrak{p} | \mathfrak{p} \in \mathcal{P}(k),\ p = 0\ (\mathfrak{p})\}.$$

Лемма 3.3.4. *Пусть $l \in \mathbb{N}$, тогда имеет место следующее утверждение:*

$$(\exists\, c(l) \in \mathbb{R}) \sum_{R \in I_0(k),\ |R| \in m_4(Q)} \tau(R)^l\ |card\ \ \mathcal{B}(X)_R - \phi(k)\ h_f \eta X^3 |R|^{-1}|$$

$$\ll X^2 Q^{1/3} (\log Q)^{c(l)}.$$

Доказательство. Это утверждение является обобщением леммы 3.3 работы [95] и доказывается аналогично.

Лемма 3.3.5. *Пусть $l \in \mathbb{N}$, тогда имеет место следующее утверждение:*

$$(\exists\, c(l) \in \mathbb{R}) \sum_{q \in m_4(Q)} \tau(q)^l \mu(q)^2\ |card\ \ B(X)_q - \phi(k)\ h_f \eta X^3\ j(q) q^{-1}|$$

$$\ll X^2 Q^{1/3} (\log Q)^{c(l)}$$

с

$$j(q) := \mu(q)\ q \sum_{R \in m_5(q)} \mu(R) |R|^{-1};$$

более того,

$$j(q) = q \prod_{p \in m_6(q)} (1 - \prod_{\mathfrak{p} \in m_7(p)} (1 - |\mathfrak{p}|^{-1})).$$

Доказательство. Это утверждение является обобщением леммы 2.2 работы [95] и доказывается аналогично.

3.4 Основная конструкция; применение метода решета

1. В силу асимптотического закона распределения простых идеалов (теорема Ландау),

$$\pi(\mathcal{B}(X)) = \frac{h_f \eta X^3}{3 \log X} \, (1 + O(1/\log X));$$

поэтому асимптотическая формула (2.18) эквивалентна следующему утверждению:

$$\pi(\mathcal{A}(X)) = \kappa \pi(\mathcal{B}(X)) + O(\frac{\eta^2 X^2}{\log X} \tau) \tag{3.4.1}$$

с

$$\kappa := \sigma(f) \eta (h_f X)^{-1}, \; \tau := (\log \log X)^{-1/6}.$$

Для доказательства формулы (4.1) используется метод решета (см., например, [88]). Определим на множестве $\mathcal{P}(k)$ отношение линейного порядка " $\prec$ " под условием

$$|\mathfrak{p}_1| < |\mathfrak{p}_2| \; \Rightarrow \mathfrak{p}_1 \prec \mathfrak{p}_2 \;\text{ при }\; \{\mathfrak{p}_1, \mathfrak{p}_2\} \subseteq \mathcal{P}(k).$$

Пусть

$$D \subseteq \mathbb{Z}, \; \mathcal{D} \subseteq I_0(k), \; z \in \mathbb{R}, \; z > 1 \;\text{ и }\; \mathfrak{q} \in \mathcal{P}(k);$$

положим

$$S(D, z) := |\{a | a \in D, \; (\forall \, p \in \mathcal{P}) \; a = 0 \; (p) \Rightarrow p \geq z\}|,$$

$$S(\mathcal{D}, z) := |\{\mathfrak{a} | \mathfrak{a} \in \mathcal{D}, \; (\forall \, \mathfrak{p} \in \mathcal{P}(k)) \; \mathfrak{a} = 0 \; (\mathfrak{p}) \Rightarrow |\mathfrak{p}| \geq z\}|$$

и

$$S(\mathcal{D}, \mathfrak{q}) := |\{\mathfrak{a} | \mathfrak{a} \in \mathcal{D}, \; (\forall \, \mathfrak{p} \in \mathcal{P}(k)) \; \mathfrak{a} = 0 \; (\mathfrak{p}) \Rightarrow \mathfrak{p} \succeq \mathfrak{q}\}|.$$

Предположим теперь, что $\mathcal{D} \in \{\mathcal{A}(X), \; \mathcal{B}(X)\}$ и пусть $h_1 := 2\sqrt{h_f}$; ясно, что

$$\pi(\mathcal{D}) = S(\mathcal{D}, h_1 X^{3/2}) \tag{3.4.2}$$

и (тождество Бухштаба !)

$$S(\mathcal{D}, h_1 X^{3/2}) = S_1(\mathcal{D}) - \sum_{i=2}^{5} S_i(\mathcal{D}), \tag{3.4.3}$$

где

$$S_1(\mathcal{D}) := S(\mathcal{D}, X^\tau),\ S_i(\mathcal{D}) := \sum_{\mathfrak{p}\in m(a_i,b_i)} S(\mathcal{D}_\mathfrak{p}, \mathfrak{p}) \ \text{ при } \ 2 \le i \le 5,$$

$$m(a,b) := \{\mathfrak{p} | \mathfrak{p} \in \mathcal{P}(k),\ a \le |\mathfrak{p}| < b\} \ \text{ при } \ \{a,b\} \subseteq \mathbb{R}\,,$$

$$a_2 = X^\tau,\ a_3 = b_2 = X^{1-\tau},\ a_4 = b_3 = X^{1+\tau},$$

$$a_5 = b_4 = X^{3/2-\tau} \ \text{ и } \ b_5 = h_1 X^{3/2}.$$

Пусть $n \in \mathbb{N}$; положим

$$\lambda(\mathfrak{p}) := \prod_{i=1}^{n} \mathfrak{p}_i \ \text{ при } \ \mathfrak{p} \in \mathcal{P}(k)^n,$$

$$J_n(\mathcal{A}(X)) := \{\mathfrak{p} | \mathfrak{p} \in \mathcal{P}(k)^n,\ X^\tau \le |\mathfrak{p}_n| < ... < |\mathfrak{p}_1| < X^{1-\tau}\},$$

$$J_n(\mathcal{B}(X)) := \{\mathfrak{p} | \mathfrak{p} \in \mathcal{P}(k)^n,\ \mathfrak{p}_n \prec ... \prec \mathfrak{p}_1,\ |\mathfrak{p}_1| < X^{1-\tau},\ |\mathfrak{p}_n| \ge X^\tau\},$$

$$M_1(n,\mathcal{D}) := \{\mathfrak{p} | \mathfrak{p} \in J_{n+1}(\mathcal{D}),\ |\lambda(\mathfrak{p})| < X^{1+\tau}\},$$

$$M_2(n,\mathcal{D}) := \{\mathfrak{p} | \mathfrak{p} \in J_n(\mathcal{D}),\ |\lambda(\mathfrak{p})\mathfrak{p}_{n+1}^{-1})| < X^{1+\tau} \le |\lambda(\mathfrak{p})|\},$$

$$T^{(n)}(\mathcal{D}) := \sum_{\mathfrak{p}\in M_1(n,\mathcal{D})} S(\mathcal{D}_{\lambda(\mathfrak{p})}, X^\tau),\ U^{(n)}(\mathcal{D}) = \sum_{\mathfrak{p}\in M_2(n,\mathcal{D})} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_{n+1})$$

и $T^{(0)}(\mathcal{D}) := S_1(\mathcal{D})$. Воспользовавшись ещё раз тождеством Бухштаба, можно доказать (ср. [95, §2]), что

$$(\exists\, n_0 \in \mathbb{N})\ S_2(\mathcal{D}) = \sum_{1\le n\le n_0} (-1)^{n-1}(T^{(n)}(\mathcal{D}) - U^{(n)}(\mathcal{D})) \ \text{ и } \ n_0 \ll \tau^{-1}. \quad (3.4.4)$$

Положим далее

$$U_1^{(1)}(\mathcal{D}) := \sum_{\mathfrak{p}\in M_3(\mathcal{D})} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_2)$$

с

$$M_3(\mathcal{D}) := \{\mathfrak{p} | \mathfrak{p} \in J_2(\mathcal{D}),\ X^{1+\tau} \le |\lambda(\mathfrak{p})| \le X^{3/2-\tau}\},$$

$$U_2^{(1)}(\mathcal{D}) := \sum_{\mathfrak{p}\in M_4(\mathcal{D})} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_2)$$

с

$$M_4(\mathcal{D}) := \{\mathfrak{p} | \mathfrak{p} \in J_2(\mathcal{D}),\ |\lambda(\mathfrak{p})| \ge X^{3/2+\tau}\},$$

$$U_1^{(2)}(\mathcal{D}) := \sum_{\mathfrak{p}\in M_5(\mathcal{D})} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_3)$$

с

$$M_5(\mathcal{D}) := \{\mathfrak{p}|\mathfrak{p} \in J_3(\mathcal{D}),\ |\lambda(\mathfrak{p})\mathfrak{p}_3^{-1}| \le X^{1+\tau} \le |\lambda(\mathfrak{p})| \le X^{3/2-\tau}\},$$

$$S_6(\mathcal{D}) := \sum_{\mathfrak{p}\in M_6(\mathcal{D})} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_2)$$

с

$$M_6(\mathcal{D}) := \{\mathfrak{p}|\mathfrak{p} \in J_2(\mathcal{D}),\ X^{3/2-\tau} \le |\lambda(\mathfrak{p})| \le X^{3/2+\tau}\}$$

и

$$S_7(\mathcal{D}) := \sum_{\mathfrak{p}\in M_7(\mathcal{D})} S(\mathcal{D}_{\lambda(\mathfrak{p})}, \mathfrak{p}_3)$$

с

$$M_7(\mathcal{D}) := \{\mathfrak{p}|\mathfrak{p} \in J_3(\mathcal{D}),\ |\lambda(\mathfrak{p})\mathfrak{p}_3^{-1}| < X^{1+\tau},\ |\lambda(\mathfrak{p})| > X^{3/2-\tau}\}.$$

Тогда

$$U^{(1)}(\mathcal{D}) = U_1^{(1)}(\mathcal{D}) + S_6(\mathcal{D}) + U_2^{(1)}(\mathcal{D}) \tag{3.4.5}$$

и

$$U^{(2)}(\mathcal{D}) = U_1^{(2)}(\mathcal{D}) + S_7(\mathcal{D}). \tag{3.4.6}$$

Лемма 3.4.1 . *Имеет место следующая оценка:*

$$\pi(\mathcal{A}(X)) - \kappa\pi(\mathcal{B}(X)) \ll \sum_{0\le n\le n_0} |T^{(n)}(\mathcal{A}(X)) - \kappa T^{(n)}(\mathcal{B}(X))|$$

$$+ |U_1^{(1)}(\mathcal{A}(X)) - \kappa U_1^{(1)}(\mathcal{B}(X))| \ + \ |U_2^{(1)}(\mathcal{A}(X)) - \kappa U_2^{(1)}(\mathcal{B}(X))|$$

$$+ |U_1^{(2)}(\mathcal{A}(X)) - \kappa U_1^{(2)}(\mathcal{B}(X))| \ + \sum_{3\le n\le n_0} |U^{(n)}(\mathcal{A}(X)) - \kappa U^{(n)}(\mathcal{B}(X))|$$

$$+ \sum_{j\in\{3,5,6,7\}} (S_j(\mathcal{A}(X)) + \kappa S_j(\mathcal{B}(X))) \ + \ |S_4(\mathcal{A}(X)) - \kappa S_4(\mathcal{B}(X))|.$$

Доказательство. Это неравенство следует из соотношений (2) - (6).

Лемма 3.4.2 . *Имеет место следующая оценка:*

$$\sum_{0\le n\le n_0} |T^{(n)}(\mathcal{A}(X)) - \kappa T^{(n)}(\mathcal{B}(X))| \ll \tau\eta^2 X^2 (\log X)^{-1}. \tag{3.4.7}$$

Доказательство. Предположим, не нарушая общности, что

$$\mathcal{P}_0 \subseteq \{p|p \in \mathcal{P},\ p < X^\tau\},$$

тогда

$$T^{(n)}(\mathcal{A}(X)) = \sum_{p \in M_8(X)} S(A_{p_1 \ldots p_n}, X^\tau) \ \text{ и } \ T^{(0)}(\mathcal{A}(X)) = S(\mathcal{A}(X), X^\tau), \quad (3.4.8)$$

где

$$M_8(X) := \{p|p \in \mathcal{P}^n,\ X^\tau \leq p_n < \ldots < p_1 < X^{1-\tau},\ p_1 \ldots p_n < X^{1+\tau}\},$$

(ср. [95, §2]). С другой стороны, по известной теореме [88, теорема 7.1], из равенства (3.18) следует, что

$$S(A(X)_q, X^\tau) = L(q)\{1 + O(\exp(-1/\tau))\} + O(E(q)), \quad (3.4.9)$$

где

$$L(q) := \frac{\eta^2 X^2}{\zeta(2)} \gamma(q) \prod_{p \in \mathcal{P},\ p < X^\tau} (1 - \gamma(p))$$

и

$$E(q) := \sum_{d \in M_9(X)} \mu(d)^2 \tau(d)^2 |\rho_2(qd, X)|$$

с

$$M_9(X) := \{d|d \in \mathbb{N},\ d < X^{1/3},\ (\forall\, p \in \mathcal{P})\ p|d \Rightarrow p < X^\tau\}.$$

Воспользовавшись соотношением (8), соотношением (9) с $q = p_1 \ldots p_n$ и леммой 3.3, легко находим

$$T^{(n)}(\mathcal{A}(X)) =$$

$$\frac{\eta^2 X^2}{\zeta(2)}\, \Sigma_4 \prod_{p \in \mathcal{P},\ p < X^\tau} (1 - \gamma(p))(1 + O(\exp(-1/\tau))) + O(X^{7/4} (\log X)^c), \quad (3.4.10)$$

где

$$\Sigma_4 := \sum_{p \in M_8(X)} \gamma(p_1 \ldots p_n) \ \text{ и } \ c \in \mathbb{R}.$$

Из леммы 3.5 следует, что (ср. [95, стр. 35 - 37])

$$T^{(n)}(\mathcal{B}(X)) =$$

$$\phi(k)h_f\eta X^3\,\Sigma_5\prod_{p\in\mathcal{P},\,p<X^\tau}(1-\frac{j(p)}{p})(1+O(\exp(-1/\tau)))+O(X^{3-\tau/4}),\quad(3.4.11)$$

где

$$\Sigma_5=\sum_{p\in M_8(X)}\frac{j(p_1\dots p_n)}{p_1\dots p_n}.$$

Доказываемая оценка (7) следует из соотношений (10) и (11) (ср. [95, стр. 37 - 39]). Лемма доказана.

Лемма 3.4.3. *Положим*

$$Q:=\{q|q\in\mathbb{N},\ \mu(q)^2=1,\ N<q\le 2N\}$$

и пусть $z\gg X^\tau,\ N\ll X^{2-\tau}$. *Тогда*

$$\sum_{|\mathfrak{b}|\in Q,\,\mathfrak{b}\in I_0(k)}S(\mathcal{A}(X)_{\mathfrak{b}},z)\ll\sum_{q\in Q}\frac{\eta^2X^2}{q\log^{-1}(z,X^{2-\tau}/N)}+X^{2-\tau/5}$$

и

$$\sum_{|\mathfrak{b}|\in Q,\,\mathfrak{b}\in I_0(k)}S(\mathcal{B}(X)_{\mathfrak{b}},z)\ll\sum_{q\in Q}\frac{\eta^2X^3}{q\log^{-1}(z,X^{2-\tau}/N)}+X^{3-\tau/5}.$$

Доказательство. Это утверждение является обобщением леммы 7.1 работы [95] и доказывается аналогично.

Лемма 3.4.4. *Имеют место следующие оценки:*

$$S_j(\mathcal{A}(X))+\kappa S_j(\mathcal{B}(X))\ll\tau\frac{\eta^2X^2}{\log X}\ \ \textit{при}\ \ j\in\{3,5,6,7\}.$$

Доказательство. Это утверждение является обобщением леммы 3.6 работы [95] и доказывается аналогично.

2. Пусть

$$\xi:=\tau^5\ \text{ и }\ J(l):=\{a|a\in\mathbb{R},\ X^{l\xi}\le a<X^{(l+1)\xi}\}\ \text{ при }\ l\in\mathbb{N}_0;$$

определим функции

$$d_n:I_0(k)\times\mathbb{N}^{n+1}\to\mathbb{R}\ \text{ и }\ b_n:I_0(k)\times\mathbb{N}^{n+1}\to\{0,1\}$$

следующим образом:

$$d_n(\mathfrak{A},m)=\prod_{i=1}^{n+1}\frac{\log p_i}{m_i\xi\log X}\ \text{ при }\ (\mathfrak{A},m)\in M_1(n)$$

и

$$d_n(\mathfrak{A},m)=0\ \text{ при }\ (\mathfrak{A},m)\notin M_1(n),$$

где

$$M_1(n):=\{(\prod_{i=1}^{n+1}\mathfrak{p}_i,m)|m\in\mathbb{N}^{n+1},\ |\mathfrak{p}_i|\in\mathcal{P}(k)\cap J(m_i)\ \text{ при }\ 1\le i\le n+1\};$$

$$b_n(\mathfrak{A},m)=\begin{cases}1 & \text{при } (\mathfrak{A},m)\in M_2(n)\\ 0 & \text{в противном случае,}\end{cases}$$

где

$$M_2(n):=$$

$$\{(\mathfrak{A},m)|\mathfrak{A}\in\mathcal{R},\ m\in\mathbb{N}^{n+1},\ \mathfrak{A}=0\ (\mathfrak{p})\Rightarrow|\mathfrak{p}|\ge X^{m_{n+1}\xi}\ \text{ при }\ \mathfrak{p}\in\mathcal{P}(k)\}.$$

Положим

$$\hat{U}^{(m,n)}(\mathcal{D})=\sum_{\mathfrak{AB}\in\mathcal{D}}b_n(\mathfrak{A},m)d_n(\mathfrak{B},m)\ \text{ при }\ m\in\mathbb{N}^{n+1}\ \text{ и }\ n\in\mathbb{N}_0,\qquad(3.4.12)$$

$$\hat{U}^{(n)}(\mathcal{D})=\sum_{m\in\iota(n)}\hat{U}^{(m,n)}(\mathcal{D})\ \text{ при }\ n\in\mathbb{N}\setminus\{1,2\},\qquad(3.4.13)$$

$$\hat{U}_1^{(n)}(\mathcal{D})=\sum_{m\in\iota(n)}\hat{U}^{(m,n)}(\mathcal{D})\ \text{ при }\ n\in\{1,2\},\qquad(3.4.14)$$

где

$$\iota(n):=\{m|m\in\mathbb{N}^{n+1},\ m_1>...>m_{n+1}\ge\tau\xi^{-1},\ \sum_{i=1}^{n+1}m_i\ge(1+\tau)\xi^{-1},$$

$$\sum_{i=1}^{n+1}(m_i+1)\le(\frac{3}{2}-\tau)\xi^{-1},\ \sum_{i=1}^{n}(m_i+1)\le(1+\tau)\xi^{-1},\ m_1+1\le(1-\tau)\xi^{-1}\}$$

при $n\in\mathbb{N}$, и

$$\hat{S}_4(\mathcal{D})=\sum_{m\in\iota(0)}\hat{U}^{(m,0)}(\mathcal{D}),\qquad(3.4.15)$$

где

$$\iota(0) := \{m | m \in \mathbb{N},\ (1+\tau)\xi^{-1} \le m \le (\frac{3}{2} - \tau)\xi^{-1} - 1\}.$$

Рассмотрим функцию

$$b^{(1)} : I_0(k) \times \mathbb{N}^2 \to \{0, 1\},$$

определяемую соотношением

$$b^{(1)}(\mathfrak{A}, m) = \begin{cases} 1 & \text{при } (\mathfrak{A}, m) \in M_3(n) \\ 0 & \text{в противном случае,} \end{cases}$$

где

$$M_3(n) := \{(\mathfrak{p}_1\mathfrak{p}_2, m) | m \in \mathbb{N}^2,\ |\mathfrak{p}_i| \in \mathcal{P}(k) \cap J(m_i) \ \text{ при } \ i \in \{1, 2\}\};$$

положим

$$\hat{U}^{(\nu,n)}(\mathcal{D}) = \sum_{\mathfrak{A}\mathfrak{B}\in\mathcal{D}} b^{(1)}(\mathfrak{A}, l) d_n(\mathfrak{B}, m) \tag{3.4.16}$$

при

$$\nu := (l, m),\ l \in \mathbb{N}^2,\ m \in \mathbb{N}^{n+1} \ \text{ и } \ n \in \mathbb{N}_0$$

и

$$\hat{U}_2^{(1)}(\mathcal{D}) = \sum_{\nu\in\iota_1(n),\ 0\le n\le n_0} \hat{U}^{(\nu,n)}(\mathcal{D}), \tag{3.4.17}$$

где

$$\iota_1(n) = \{(l, m) | (l, m) \in \mathbb{N}^2 \times \mathbb{N}^{n+1},\ m_1 > ... > m_{n+1} \ge l_2 \ \text{ при } \ n \in \mathbb{N}_0,$$

$$\tau \le l_2\xi < l_1\xi \le 1 - \tau - \xi,\ (l_1 + l_2)\xi \ge 3/2 + \tau\}.$$

Лемма 3.4.5 . *Имеют место следующие соотношения:*

$$\sum_{n\ge 3} |U^{(n)}(\mathcal{D}) - \hat{U}^{(n)}(\mathcal{D})| \ll \frac{\eta^2 X^2}{\log X}\, \xi\tau^{-4}$$

и

$$|U_1^{(n)}(\mathcal{D}) - \hat{U}_1^{(n)}(\mathcal{D})| \ll \frac{\eta^2 X^2}{\log X}\, \xi\tau^{-3}$$

при $n \in \{1,2\}$ *;*

$$|S_4(\mathcal{D}) - \hat{S}_4(\mathcal{D})| \ll \frac{\eta^2 X^2}{\log X}\,\xi\tau^{-3}$$

и

$$|U_2^{(1)}(\mathcal{D}) - \hat{U}_2^{(1)}(\mathcal{D})| \ll \frac{\eta^2 X^2}{\log X}\,\xi\tau^{-4},$$

где $\mathcal{D} \in \{\mathcal{A}(X), \mathcal{B}(X)\}$ *.*

Доказательство. Это утверждение является обобщением леммы 3.7 работы [95] и доказывается аналогично.

Пусть $t \in \mathbb{R}_+$ и $m \in \mathbb{N}^{n+1}$; положим

$$G(m,t) = \{x | x \in \mathbb{R}^{n+1},\ x_i \in J(m_i)\ \text{ при }\ 1 \le i \le n+1,\ \prod_{i=1}^{n+1} x_i \le t\}$$

и рассмотрим функцию

$$w : \mathbb{R}_+ \to \mathbb{R}_+,\ w : t \mapsto \int_{G(m,t)} dx.$$

Лемма 3.4.6 . *При* $\{t,h\} \subseteq \mathbb{R}_+$ *имеют место следующие соотношения:*

$$0 \le w'(t) \le (\xi \log X)^n \tag{3.4.18}$$

и

$$|w'(t+h) - w'(t)| \le ht^{-1} \prod_{i=1}^{n-1} \int_{u \in J(m_i)} \frac{du}{u} \le ht^{-1}(\xi \log X)^{n-1}. \tag{3.4.19}$$

Доказательство. См. [95, стр. 48].

Положим

$$d_n = e_n + g_n \tag{3.4.20}$$

с

$$e_n(\mathfrak{A}, m) := w'(|\mathfrak{A}|) \prod_{i=1}^{n+1} (m_i \xi \log X)^{-1} \sum_{\mathfrak{B} \in M_4(\mathfrak{A})} \mu(\mathfrak{B}) \log(L|\mathfrak{B}|^{-1}) \tag{3.4.21}$$

при $n \in \mathbb{N}_0$, где

$$L := X^{\tau/2} \text{ и } M_4(\mathfrak{A}) := \{\mathfrak{B} | \mathfrak{B} \in I_0(k),\ |\mathfrak{B}| < L,\ \mathfrak{A} = 0\ (\mathfrak{B})\}.$$

Пусть

$$U_e(\mathcal{A}(X)) := \sum_{(\mathfrak{A},\mathfrak{B}) \in M_5} b_{\mathfrak{A}} e_n(\mathfrak{B}, m), \tag{3.4.22}$$

где

$$M_5 := \{(\mathfrak{A}, \mathfrak{B}) | (\mathfrak{A}, \mathfrak{B}) \in I_0(k)^2,\ \mathfrak{A}\mathfrak{B} \in \mathcal{A}(X)\}$$

и

$$b_{\mathfrak{A}} \in \{b^{(1)}(\mathfrak{A}, l),\ b_n(\mathfrak{A}, m)\}.$$

Из соотношений (20), (12) и (16) получим:

$$U(\mathcal{A}(X)) = U_e(\mathcal{A}(X)) + U_g(\mathcal{A}(X)) \tag{3.4.23}$$

с

$$U \in \{\hat{U}^{(m,n)},\ \hat{U}^{(\nu,n)}\};$$

более того, соотношения (23), (13) - (15) и (17) дают:

$$V(\mathcal{A}(X)) = V_e(\mathcal{A}(X)) + V_g(\mathcal{A}(X))$$

с

$$V \in \{\hat{U}^{(n)},\ \hat{U}_1^{(n)},\ \hat{U}_2^{(1)},\ \hat{S}_4\}.$$

Лемма 3.4.7. *Имеют место следующие соотношения:*

$$U_e(\mathcal{A}(X)) - \kappa U(\mathcal{B}(X)) \ll N^{-1}\eta^{5/2}X^2(\log X)^{c(f)}, \tag{3.4.24}$$

где $N := \prod_{i=1}^{n+1} m_i$,

$$V_e(\mathcal{A}(X)) - \kappa V(\mathcal{B}(X)) = O(\eta^{5/2}X^2(\log X)^{c(f)}), \tag{3.4.25}$$

и

$$\sum_{n=3}^{\infty} |\hat{U}_e^{(n)}(\mathcal{A}(X)) - \kappa \hat{U}^{(n)}(\mathcal{B}(X))| = O(\eta^{5/2}X^2(\log X)^{c(f)}) \tag{3.4.26}$$

с $c(f) \in \mathbb{R}$.

Доказательство. Из соотношений (22) и (21) следует, что

$$U_e(\mathcal{A}(X)) := \frac{1}{N(\xi \log X)^{n+1}} \sum_{(\mathfrak{A},\mathfrak{B})\in M_5} \sum_{\mathfrak{D}\in M_4(\mathfrak{B})} b_{\mathfrak{A}} w'(|\mathfrak{B}|)\mu(\mathfrak{D}) \log(L|\mathfrak{D}|^{-1}).$$

Как можно показать (ср. [95, стр. 61 - 62]), из неравенства (19) и соотношения (3.9) при $n \in \mathbb{N}$ и соотношения (3.10) и леммы 3.2 при $n = 0$ вытекает, что

$$U_e(\mathcal{A}(X)) = \sum_{(\mathfrak{A},\mathfrak{D})\in M_6} a(\mathfrak{A},\mathfrak{D})|\mathcal{A}(X)_{\mathfrak{A}\mathfrak{D}}| + O(N^{-1}\eta^{5/2}X^2(\log X)^{c_1(f)}) \quad (3.4.27)$$

$$\text{с } \ c_1(f) \in \mathbb{R}, \ \ a(\mathfrak{A},\mathfrak{D}) := b_{\mathfrak{A}} \frac{w'(h_f X^3 |\mathfrak{A}|^{-1})}{N(\xi \log X)^{n+1}} \, \mu(\mathfrak{D}) \log(L|\mathfrak{D}|^{-1}) \ \text{ и}$$

$$M_6 := \{(\mathfrak{A},\mathfrak{D})|(\mathfrak{A},\mathfrak{D}) \in I_0(k)^2, \ \mathfrak{A}\mathfrak{D} \in \mathcal{R}, \ |\mathfrak{D}| < L\}.$$

Из соотношений (3.12), (18), (27) и леммы 3.2 следует (ср. [95, стр. 62]), что

$$U_e(\mathcal{A}(X)) = \frac{\eta^2 X^2 \, \Sigma_6}{\zeta(2) N(\xi \log X)^{n+1}} \sum_{\mathfrak{A}\in\mathcal{R}} b_{\mathfrak{A}} w'(h_f X^3 |\mathfrak{A}|^{-1}) |\mathfrak{A}|^{-1} \, \alpha_1(\mathfrak{A})$$

$$+ O(\eta^{5/2} X^2 N^{-1} (\log X)^{c_2(f)}) \quad (3.4.28)$$

$$\text{с } \quad c_2(f) \in \mathbb{R} \ \text{ и } \ \Sigma_6 := \sum_{\mathfrak{D}\in\mathcal{R}, |\mathfrak{D}|<L} \frac{\mu(\mathfrak{D}) \, \alpha(\mathfrak{D}_0) \, \alpha_1(\mathfrak{D})}{|\mathfrak{D}|} \log(L|\mathfrak{D}|^{-1}).$$

По теореме Коши,

$$\Sigma_6 = \frac{1}{2\pi i} \int_{1-i\infty}^{1+i\infty} l(s+1) L^s \frac{ds}{s^2} \ \text{ с } \ l(s) := \sum_{\mathfrak{D}\in\mathcal{R}} \frac{\mu(\mathfrak{D}) \, \alpha(\mathfrak{D}_0) \, \alpha_1(\mathfrak{D})}{|\mathfrak{D}|^s} \, .$$

Разлагая функцию

$$s \mapsto s^{-2} L^s l(s+1)$$

в ряд Лорана в окрестности точки $s = 0$ и вспоминая соотношения (2.5) - (2.8), легко находим

$$\Sigma_6 = \sigma(f)\zeta(2) + O(\exp(-c_3(f)(\log L)^{1/2})) \ \text{ с } \ c_3(f) \in \mathbb{R}_+^*. \quad (3.4.29)$$

Из соотношений (28) и (29) следует, что

$$U_e(\mathcal{A}(X)) = \sigma(f)\eta^2 X^2 \Sigma_7 (1 + O(\exp(-c_4(f)(\log L)^{1/2})))$$

$$+ O(N^{-1}\eta^{5/2}X^2(\log X)^{c_5(f)}) \ \text{ с } \ c_4(f) \in \mathbb{R}_+^*, \ c_5(f) \in \mathbb{R}, \tag{3.4.30}$$

где

$$\Sigma_7 := \sum_{\mathfrak{A}\in\mathcal{R}} b_{\mathfrak{A}} w'(h_f X^3 |\mathfrak{A}|^{-1}) \alpha_1(\mathfrak{A}) (N(\xi \log X)^{n+1} |\mathfrak{A}|)^{-1}.$$

Легко видеть, что

$$\alpha_1(\mathfrak{A}) = 1 + O(\exp(-c_6(f)(\log L)^{1/2})) \ \text{ с } \ c_6(f) \in \mathbb{R}_+^*$$

при $b_{\mathfrak{A}} \neq 0$; поэтому соотношение (30) переписывается следующим образом:

$$U_e(\mathcal{A}(X)) = \sigma(f)\eta^2 X^2 \Sigma_8 + O(N^{-1}\eta^{5/2}X^2(\log X)^{c_7(f)}) \ \text{ с } \ c_7(f) \in \mathbb{R}, \tag{3.4.31}$$

где

$$\Sigma_8 := \sum_{\mathfrak{A}\in\mathcal{R}} b_{\mathfrak{A}} w'(h_f X^3 |\mathfrak{A}|^{-1}) (N(\xi \log X)^{n+1} |\mathfrak{A}|)^{-1}.$$

Доказателство асимптотической формулы

$$U(\mathcal{B}(X)) = h_f \eta X^3 \Sigma_8 + O(N^{-1}\eta^2 X^3). \tag{3.4.32}$$

аналогично доказательству частного случая этой формулы, приведённому на стр. 64 - 66 работы [95]. Оценка (24) следует из соотношений (31) и (32). В силу определений (13) - (17), для доказательства оценок (25) и (26) достаточно заметить, что

$$\max\{ \sum_{m\in\iota(n)} (\prod_{i=1}^{n+1} m_i)^{-1}, \ \sum_{m\in\iota(0)} m^{-1} | n \in \mathbb{N}\} \ll \log X$$

(ср. [95, стр. 66]).

Предложение 3.4.1 . *Имеет место следующее соотношение:*

$$\pi(\mathcal{A}(X)) - \kappa\pi(\mathcal{B}(X)) \ll \tau\eta^2 X^2 (\log X)^{-1} + \eta^{5/2} X^2 (\log X)^{c(f)} + \Sigma_9 \tag{3.4.33}$$

с

$$\Sigma_9 := \sum_{n=3}^{\infty} |\hat{U}_g^{(n)}(\mathcal{A}(X))| + \sum_{n\in\{1,2\}} |\hat{U}_{1,g}^{(n)}(\mathcal{A}(X))| + |\hat{S}_{4,g}(\mathcal{A}(X)| + |\hat{U}_{2,g}^{(1)}(\mathcal{A}(X))|$$

и $c(f) \in \mathbb{R}$.

Доказательство. Оценка (33) следует из леммы 1, леммы 2, леммы 4, леммы 5 и леммы 7 .

Для завершения доказательства соотношения (1) необходимо оценить сверху сумму Σ_9 .

3.5 Идеальные числа Гекке, большое решето Линника и сумма Σ_9

1. Рассмотрим поле алгебраических чисел K; обозначим через $H(K)$ группу классов идеалов этого поля и через

$$\mathfrak{c} : I(K) \to H(K)$$

естественный эпиморфизм группы дробных идеалов $I(K)$ на группу $H(K)$. Пусть

$$H(K) \cong \mathbb{Z}/h_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/h_t\mathbb{Z} \text{ с } \prod_{i=1}^{t} h_i = h_K.$$

Следуя Гекке [99], зафиксируем последовательность идеалов $\mathfrak{a}$ кольца $\mathfrak{o}(K)$ и последовательность α элементов группы K^* под условием

$$\mathfrak{a} \in I_0(K)^t,\ \alpha \in (K^*)^t,\ \mathfrak{a}_i^{h_i} = (\alpha_i) \text{ при } 0 \le i \le t$$

и

$$H(K) = \{\prod_{i=1}^{t} \mathfrak{c}(\mathfrak{a}_i)^{l_i} | l \in \mathbb{Z}^t,\ 0 \le l_i \le h_i \text{ при } 1 \le i \le t\}.$$

Положим $n := [K : \mathbb{Q}]$, рассмотрим естественные вложения

$$\sigma_i : K \hookrightarrow \mathbb{C} \text{ при } 1 \le i \le n$$

и предположим, как обычно, что

$$n = r_1 + 2\,r_2,\ r(K) := r_1 + r_2 - 1,\ \sigma_i(K) \subseteq \mathbb{R} \Leftrightarrow 1 \le i \le r_1$$

и

$$\sigma_{i+r_2}\gamma = \overline{\sigma_i\gamma} \ \text{ при } \ r_1+1 \le i \le r_1+r_2 \ \text{ и } \ \gamma \in K.$$

Рассмотрим поле

$$K_1 := K(\beta_1, ..., \beta_t) \ \text{ с } \ \beta_j^{h_j} = \alpha_j \ \text{ при } \ 1 \le j \le t$$

и продолжим вложения σ_j до вложений

$$\sigma_j : K_1 \hookrightarrow \mathbb{C}, \ 1 \le j \le n,$$

под условием

$$\sigma_{i+r_2}\beta_j = \overline{\sigma_i\beta_j} \ \text{ при } \ r_1+1 \le i \le r_1+r_2 \ \text{ и } \ 1 \le j \le t.$$

Обозначим через $\mathfrak{I}(K)^*$ подгруппу группы K_1^*, порождённую множеством

$$K^* \cup \{\beta_j | 1 \le j \le t\}.$$

Положим

$$\mathfrak{I}(K) := \{0\} \cup \mathfrak{I}(K)^*, \ \mathfrak{I}_0(K) := \mathfrak{I}(K) \cap \mathfrak{o}(L) \ \text{ и } \ \mathfrak{I}_0(K)^* := \mathfrak{I}_0(K) \setminus \{0\};$$

элементы множества $\mathfrak{I}(K)$ суть *идеальные числа*, а элементы множества $\mathfrak{I}_0(K)$ суть *целые идеальные числа* поля K. Обозначим через

$$\psi : \mathfrak{I}(K)^* \to I(K), \ \psi : \beta \mapsto (\beta) \ \text{ при } \ \beta \in \mathfrak{I}(K)^*,$$

эпиморфзм с $\operatorname{Ker}\psi = \mathfrak{o}(K)^*$. По построению, $\psi(\mathfrak{I}_0(K)^*) = I_0(K)$. Положим

$$N\beta := \prod_{i=1}^{n} \sigma_i\beta \ \text{ и } \ \operatorname{tr}\beta := \sum_{i=1}^{n} \sigma_i\beta \ \text{ при } \ \beta \in \mathfrak{I}(K)^*$$

и заметим, что $|N\beta| = |(\beta)|$ при $\beta \in \mathfrak{I}(K)^*$ (следует отметить, что, вообще говоря,

$$N\beta \ne N_{K_1/\mathbb{Q}}\,\beta \ \text{ и } \ \operatorname{tr}\beta \ne \operatorname{tr}_{K_1/\mathbb{Q}}\,\beta \ \text{ при } \ \beta \in \mathfrak{I}(K),$$

но, разумеется,

$$N\beta = N_{K/\mathbb{Q}}\,\beta \ \text{ и } \ \mathrm{tr}\,\beta = \mathrm{tr}_{\,K/\mathbb{Q}}\,\beta \ \text{ при } \ \beta \in K\ ).$$

Положим $\mathfrak{c}\,(\beta) := \mathfrak{c}\,((\beta))$ при $\beta \in \mathfrak{I}(K)^*$. Рассмотрим эпиморфизм

$$\mathfrak{c} : \mathfrak{I}(K)^* \to H(K)$$

и обозначим через

$$\mathcal{T} := \{T | T \subseteq \mathfrak{I}(K)^*,\ |\mathfrak{c}\,(T)| = 1\}$$

изоморфную $H(K)$ группу классов идеальных чисел. Положим

$$\mathrm{cl}\,\beta := T \cup \{0\} \ \text{ при } \ T \in \mathcal{T} \ \text{ и } \ \beta \in T;$$

ясно, что

$$(\forall\ \beta \in \mathfrak{I}(K)^*)\ \mathrm{cl}\,\beta = \{\beta\alpha | \alpha \in K\}. \tag{3.5.1}$$

Из соотношения (1), в частности, следует, что при $T \in \mathcal{T}$ для любого $\mathbb{Q}$ - базиса $\{w_1, ..., w_n\}$ векторного пространства $T \cup \{0\}$ найдётся однозначно определённый ("дуальный") базис $\{\tilde{w}_1, ..., \tilde{w}_n\}$ векторного пространства $T^{-1} \cup \{0\}$ под условием

$$\mathrm{tr}\,(w_i\tilde{w}_j) = \begin{cases} 1, & \text{при } i = j,\ 1 \le i \le n \\ 0, & \text{при } 1 \le i < j \le n. \end{cases}$$

Положим

$$T^{(0)} := (T \cup \{0\}) \cap \mathfrak{o}(L) \ \text{ при } \ T \in \mathcal{T};$$

ясно, что $T^{(0)}$ есть $\mathfrak{o}(K)$ - модуль. Будем называть $\mathbb{Z}$ - базис модуля $T^{(0)}$ *целым базисом* класса T; из соотношения (1) легко следует, что дискриминант целого базиса любого класса идеальных чисел равен d_K, дискриминанту поля K. Положим, для краткости,

$$\varphi_K(\beta) := |(\mathfrak{o}(K)/(\beta))^*| \ \text{ и } \ \tau(\beta) := \tau((\beta)) \ \text{ при } \ \beta \in \mathfrak{I}_0(K)^*$$

и

$$(\alpha,\beta):=((\alpha),(\beta))\ \text{ при }\ \{\alpha,\beta\}\subseteq\mathfrak{I}_0(K)^*.$$

Лемма 3.5.1 . *Пусть*

$$\{x,y\}\subseteq\mathbb{R},\ x\geq y\geq 2,\ l\in\mathbb{N},\ r\in\mathbb{Z},$$

$$\{\alpha,\beta\}\subseteq\mathfrak{I}_0(K)^*,\ \mathfrak{c}(\alpha)=\mathfrak{c}(\beta),\ (\alpha,\beta)=(1)$$

и предположим, что

$$\max\{|\sigma_i\alpha|,\ |\sigma_i\beta|\ |1\leq i\leq n\}\leq x^r.$$

Тогда

$$\sum_{m\in M_1(x,y)}\tau(m_1\alpha+m_2\beta)^l\ll xy(\log x)^{c(l,r)}$$

с

$$M_1(x,y):=\{m|m\in\mathbb{Z}^2,\ |m_1|\leq x,\ |m_2|\leq y,\ m_2\neq 0\}\ \ u\ \ c(l,r)\in\mathbb{R}.$$

Доказательство. Это утверждение является обобщением леммы 4.6 работы [95] и доказывается аналогично.

2. Пусть теперь

$$K=k,\ \delta\in\mathfrak{I}_0(k)\ \text{ и }\ \mathfrak{d}=(\delta).$$

В этом случае, не нарушая общности, можно считать, что $\sigma_1(K_1)\subseteq\mathbb{R}$ и, в частности, $\sigma_1(\mathfrak{I}(k))\subseteq\mathbb{R}$. Положим

$$\mathfrak{o}(k)^*=\{(-1)^a\varepsilon_0^l\ |a\in\{0,1\},\ l\in\mathbb{Z}\}\ \text{ при }\ r(k)=1$$

и

$$\mathfrak{o}(k)^*=\{(-1)^a\varepsilon_1^{l_1}\varepsilon_2^{l_2}\ |a\in\{0,1\},\ l\in\mathbb{Z}^2\}\ \text{ при }\ r(k)=2.$$

Выберем и зафиксируем целый базис в каждом из классов идеальных чисел поля k, предполагая при этом, что зафиксированный целый базис $\{w_1,w_2,w_3\}$ модуля $\mathrm{cl}\ \delta^{-1}$ удовлетворяет следующему условию:

$$w_1=\omega_1\delta^{-1},\ lw_2=\omega_2\delta^{-1}\ \text{ с }\ l\in\mathbb{Z}.$$

При $\beta \in \mathfrak{I}(k)$ положим

$$\hat{\beta} := b \ \text{ с } \ b \in \mathbb{Q}^3, \ b_i = \operatorname{tr}(\beta v_i \tilde{w}_3) \ \text{ при } \ 1 \le i \le 3,$$

где $\{v_1, \ v_2, \ v_3\}$ есть зафиксированный целый базис класса cl $(\beta\delta)^{-1}$. Пусть $T \in \mathcal{T}$; определим линейное отображение

$$h_T : T \cup \{0\} \to \mathbb{Q}^3, \ h_T : \beta \mapsto \hat{\beta} \ \text{ при } \ \beta \in T$$

трёхмерного векторного пространства $T \cup \{0\}$ над полем $\mathbb{Q}$ на $\mathbb{Q}^3$ и заметим, что $h_T(T^{(0)})$ есть подрешётка решётки $\mathbb{Z}^3$ индекса $|\det h_T|$. Положим

$$T_{\mathbb{R}} := (T \cup \{0\}) \otimes_{\mathbb{Q}} \mathbb{R}$$

и продолжим отображение h_T до $\mathbb{R}$ - линейного отображения

$$h_T : T_{\mathbb{R}} \to \mathbb{R}^3, \ h_T : \sum_{i=1}^{3} a_i \bar{w}_i \mapsto \sum_{i=1}^{3} a_i h_T(\bar{w}_i) \ \text{ при } \ a \in \mathbb{R}^3,$$

где $\{\bar{w}_1, \bar{w}_2, \bar{w}_3\}$ есть зафиксированный базис $\mathbb{Z}$ - модуля $T^{(0)}$. Введём следующие обозначения:

$$\sigma_j \sum_{i=1}^{3} a_i \bar{w}_i := \sum_{i=1}^{3} a_i \sigma_j \bar{w}_i \ \text{ при } \ a \in \mathbb{R}^3 \ \text{ и } \ 1 \le j \le 3 \ ,$$

$$N\alpha := \prod_{j=1}^{3} \sigma_j \alpha \ \text{ и } \ \operatorname{tr} \alpha := \sum_{j=1}^{3} \sigma_j \alpha \ \text{ при } \ \alpha \in T_{\mathbb{R}} \ ,$$

$$\hat{x} := h_T(x) \ \text{ при } \ x \in T_{\mathbb{R}} \ \text{ и } \ \check{x} := h_T^{-1}(x) \ \text{ при } \ x \in \mathbb{R}^3 \ ;$$

$$\mathcal{C}(v, s) := \{x | x \in \mathbb{R}^3, \ v_i \le x_i \le v_i + s \ \text{ при } \ 1 \le i \le 3\}$$

при $v \in \mathbb{R}^3$ и $s \in \mathbb{R}_+^*$.

Определение 3.5.1 . *Пусть* $V \in \mathbb{R}_+^*$. *Куб* $\mathcal{C}(v, s)$ *есть* V *- куб, если*

$$(\forall \, \varepsilon \in \mathfrak{o}(k)^* \setminus \{1\}, \ \{x, y\} \subseteq \mathcal{C}(v, s)) \ \varepsilon\check{x} \ne \check{y}$$

и

$$s \ge L^2, \ N\check{x} \gg V \ \ и \ \ x_i \ll V^{1/3} \ \ при \ \ x \in \mathcal{C}(v, s) \ \ и \ \ 1 \le i \le 3. \qquad (3.5.2)$$

Пусть $T \in \mathcal{T},\ \alpha \in T^{(0)}$ и $q \in \mathbb{N}$; положим

$$I := |\det\, h_T|^{-1} \int_{\mathcal{C}(v,s)} w'(N\check{x}),\ dx,$$

$$\varepsilon(\alpha, q) = \begin{cases} 1 & \text{при } (\alpha, q) = (1), \\ 0 & \text{при } (\alpha, q) \neq (1) \end{cases}$$

и

$$M_2(q, T, \alpha) := \{\beta | \beta \in T^{(0)},\ \beta = \alpha\ (q),\ \hat{\beta} \in \mathcal{C}(v, s)\}.$$

Лемма 3.5.2. *Пусть $T \in \mathcal{T},\ \alpha \in T^{(0)},\ q \in \mathbb{N}$ и $1 \leq q \leq L^{1/6}$. Если куб $\mathcal{C}(v, s)$ есть V - куб, то*

$$(\exists\, \{c_1, c_2\} \subseteq \mathbb{R}_+^*) \sum_{\beta \in M_2(q,T,\alpha)} e_n((\beta), m) =$$

$$\phi(k)^{-1} N^{-1} (\xi \log X)^{-n-1}\, \frac{\varepsilon(\alpha, q)}{\varphi_k(q)}\, I + O(s^3 N^{-1} \tau(q)^{c_1} \exp(-c_2 \sqrt{\log L})), \quad (3.5.3)$$

где $N := \prod_{i=1}^{n+1} m_i$.

Доказательство. Это утверждение является обобщением леммы 8.1 работы [95] и доказывается аналогично.

Предложение 3.5.1. *Пусть*

$$N := \prod_{i=1}^{n+1} m_i;\ T \in \mathcal{T},\ \alpha \in T^{(0)},\ \{l, q\} \subseteq \mathbb{N}\ \text{ и }\ 1 \leq q \leq (\log X)^l.$$

Если куб $\mathcal{C}(v, s)$ есть V - куб, то

$$(\exists\, c \in \mathbb{R}_+^*) \sum_{\beta \in M_2(q,T,\alpha)} d_n((\beta), m) =$$

$$\phi(k)^{-1} N^{-1} (\xi \log X)^{-n-1}\, \frac{\varepsilon(\alpha, q)}{\varphi_k(q)}\, I + \ O(V \exp(-c\sqrt{\log L})). \quad (3.5.4)$$

Доказательство. Заметим прежде всего, что, по определению, если

$$d_n((\beta), m) \neq 0\ \text{ и }\ q \leq L^{1/6},$$

то

$$(\forall\, \mathfrak{p} \in \mathcal{P}(k))\ (\beta) = 0\ (\mathfrak{p}) \Rightarrow \mathfrak{p} \geq X^{\tau} \geq L > N_{k/\mathbb{Q}}(q)$$

и потому

$$(\beta, q) = (1) \ \text{ при } \ d_n((\beta), m) \neq 0 \ \text{ и } \ q \leq L^{1/6}.$$

Таким образом, соотношение (4) очевидным образом выполняется при $\varepsilon(\alpha, q) = 0$. Пусть

$$\varepsilon(\alpha, q) = 1, \ \text{ то есть } \ (\alpha, q) = (1).$$

Положим

$$\mathfrak{I}_1(k, q) := \{\alpha | \alpha \in \mathfrak{I}^*(k), \ (\alpha) = \prod_{\mathfrak{p} \in M_3(q)} \mathfrak{p}^{n(\mathfrak{p})}, \ n(\mathfrak{p}) \in \mathbb{Z}\},$$

где

$$M_3(q) := \{\mathfrak{p} | \mathfrak{p} \in \mathcal{P}(k), \ (\mathfrak{p}, q) = (1)\},$$

$$I_1(k, q) := \mathfrak{I}_1(k, q) \cap k, \ I_2(k, q) := \{\alpha | \alpha \in k^*, \ \alpha = 1 \ (q)\}$$

и обозначим через

$$\mathfrak{h} := \{\chi | \chi : I_1(k, q) \to S^1 \ \text{ с } \ I_2(k, q) \subseteq \operatorname{Ker} \chi\}$$

группу тривиальных на подгруппе $I_2(k, q)$ характеров группы $I_1(k, q)$. Положим, для краткости,

$$d_{\mathfrak{A}} := d_n(\mathfrak{A}, m) \ \text{ при } \ \mathfrak{A} \in I_0(k), \ n \in \mathbb{N}_0 \ \text{ и } \ m \in \mathbb{N}^{n+1};$$

ясно, что

$$\sum_{\beta \in M_2(q, T, \alpha)} d_n((\beta), m) = \varphi_k(q)^{-1} \sum_{\chi \in \mathfrak{h}} \overline{\chi}(\alpha) \sum_{\beta \in M_4} \chi(\beta) \, d_{(\beta)}, \tag{3.5.5}$$

где

$$M_4 := \{\beta | \beta \in T^{(0)}, \ \hat{\beta} \in \mathcal{C}(v, s)\}$$

и каждый из характеров группы $I_1(k, q)$ каким-либо образом продолжен до характера группы $\mathfrak{I}_1(k, q)$ (сумма в правой части раенства (5) не зависит от выбранного продолжения, так как $\beta\alpha^{-1} \in k^*$). Определим функции

$$\psi_1 : T_{\mathbb{R}} \setminus \{0\} \to \mathbb{R}_+^*, \ \ \psi_2 : T_{\mathbb{R}} \setminus \{0\} \to \mathbb{R}_+^*$$

и функции

$$\nu_0 : \mathfrak{h} \times T_{\mathbb{R}} \setminus \{0\} \to \mathbb{R}_+^*, \;\; \nu : \mathfrak{h} \times T_{\mathbb{R}} \setminus \{0\} \to \mathbb{R}_+^*$$

следующим образом. Пусть $\beta \in T_{\mathbb{R}} \setminus \{0\}$ и $\chi \in \mathfrak{h}$. При $r(k) = 1$ (и, значит, $r_1 = r_2 = 1$) положим

$$\psi_1(\beta) = \frac{\log|\sigma_1\beta|}{\log|\sigma_1\varepsilon_0|} \;\text{ и }\; \psi_2(\beta) = \psi_0(\beta) - \theta\psi_1(\beta),$$

где

$$\frac{\sigma_2\beta}{|\sigma_2\beta|} = \exp(2\pi i\psi_0(\beta)) \;\text{ с }\; 0 \le \psi_0(\beta) < 1$$

и

$$\frac{\sigma_2\varepsilon_0}{|\sigma_2\varepsilon_0|} = \exp(2\pi i\theta) \;\text{ с }\; 0 \le \theta < 1,$$
$$\nu_0(\chi, \beta) = \exp(-2\pi i t_0\psi_1(\beta)),$$

где

$$\chi(\varepsilon_0) = \exp(2\pi i t_0) \;\text{ с }\; 0 \le t_0 < 1.$$

При $r(k) = 2$ (и, значит, $r_1 = 3,\ r_2 = 1$) положим

$$R(k) := (a_{ij})_{1\le i,j\le 3}$$

с

$$a_{1j} = 1/3 \;\text{ и }\; a_{ij} = \log|\sigma_j\varepsilon_{i-1}| \;\text{ при }\; 1 \le j \le 3,\ i \in \{2,3\};$$

положим

$$(\log|N\beta|, \psi_1(\beta), \psi_2(\beta)) = R(k)^{-1}l(\beta)$$

с

$$l(\beta) := (\log|\sigma_1\beta|, \log|\sigma_2\beta|, \log|\sigma_3\beta|)$$

и

$$\nu_0(\chi, \beta) = \exp(-2\pi i(t_1\psi_1(\beta) + t_2\psi_2(\beta))),$$

где

$$\chi(\varepsilon_j) = \exp(2\pi i t_j) \;\text{ с }\; 0 \le t_j < 1 \;\text{ при }\; j \in \{1,2\}.$$

В обоих случаях положим

$$\nu(\chi,\beta)=\chi(\beta)(\frac{\beta}{|\beta|})^a\,\nu_0(\chi,\beta)\ \text{ при }\ \chi(-1)=(-1)^a\ \text{ с }\ a\in\{0,1\}.$$

Важно отметить, что характеры λ_1 и λ_2, определяемые соотношением

$$\lambda_j(\beta):=\exp(-2\pi i\psi_j(\beta))\ \text{ при }\ \beta\in T_{\mathbb{R}}\setminus\{0\}\ \text{ и }\ j\in\{1,2\}\ ,$$

порождают группу неразветвлённых гроссенхарактеров поля k. Определим функции

$$H:\mathbb{R}\to[0,1]\ \text{ и }\ W:\mathfrak{I}^*(k)\times(0,1/2)\times\mathbb{R}^3\to[0,1],$$

положив

$$H(u)=\begin{cases}1-\Delta^{-1}||u||, & ||u||\le\Delta,\\ 0, & ||u||\ge\Delta,\end{cases}$$

где $||u||:=\min\{|u-n|\ |n\in\mathbb{Z}\}$ при $u\in\mathbb{R}$, и

$$W(\beta;\Delta,x)=H(\psi_1(\beta)-\psi_1(\check{x}))H(\psi_2(\beta)-\psi_2(\check{x}))$$

при $\Delta\in(0,1/2),\ x\in\mathbb{R}^3$ и $\beta\in\mathfrak{I}^*(k)$. Рассмотрим следующую сумму:

$$\Sigma(\chi,x):=\sum_{\beta\in M_5(x,\Delta)}d_{(\beta)}\,\nu(\chi,\beta)W(\beta;\Delta,x)\ \text{ при }\ x\in\mathcal{C}(v,s)\ \text{ и }\ \chi\in\mathfrak{h},$$

где

$$M_5(x,\Delta):=\{\beta|\beta\in T^{(0)},\ N\check{x}<|(\beta)|\le N\check{x}+\Delta V\};$$

ясно, что

$$\Sigma(\chi,x)=$$

$$h_k^{-1}\sum_{\nu_1\in\hat{H}(k)}\overline{\nu_1(\mathfrak{c}(T))}\sum_{\beta\in M_6(x,\Delta)}d_{(\beta)}\nu_1(\mathfrak{c}(\beta))\nu(\chi,\beta)W(\beta;\Delta,x),\qquad(3.5.6)$$

где $\hat{H}(k)$ есть группа характеров группы $H(k)$ и

$$M_6(x,\Delta):=\{\beta|\beta\in\mathfrak{I}_0^*(k),\ N\check{x}<|(\beta)|\le N\check{x}+\Delta V\}.$$

Воспользовавшись равенством (6) и обобщая доказательство леммы 9.3 работы [95], можно показать, что

$$\Sigma(\chi,x)=\varepsilon(\chi)(w(N\check{x}+\Delta V)-w(N\check{x}))\Delta^2N^{-1}(\xi\log X)^{-n-1}$$

$$+O_l(\Delta^{-2}N^{-1}V\exp(-c_1\sqrt{\log L}))\ \text{ с }\ c_1\in\mathbb{R}_+^*\,, \tag{3.5.7}$$

$\varepsilon(\chi)=1$ при $\chi=1$ и $\varepsilon(\chi)=0$ при $\chi\neq 1$. Положим

$$\Sigma_1(\chi,x)=\nu_0(\chi,\beta)^{-1}\Sigma(\chi,x)\ \text{ и }\ \mathfrak{j}=\int_{\mathcal{C}(a,s)}\Sigma_1(\chi,x)dx. \tag{3.5.8}$$

Из соотношений (7), (8) и неравенства (4.19) следует, что (ср. [95, стр. 58 - 59])

$$\mathfrak{j}=\varepsilon(\chi)\Delta^3VN^{-1}(\xi\log X)^{-n-1}|\det h_T|I+$$

$$O(\Delta^4V^2N^{-1})\ +\ O_l(\Delta^{-2}N^{-1}Vs^3\exp(-c_2\sqrt{\log L}))\ \text{ с }\ c_2\in\mathbb{R}_+^*\,. \tag{3.5.9}$$

Лемма 3.5.3 *Пусть*

$$\alpha\in\mathfrak{I}^*(k),\ W(\alpha;\Delta,x)\neq 0,\ N\check{x}<N(\alpha)\leq N\check{x}+\Delta V\ \ u\ \ V\ll N(\alpha)\ll V.$$

Тогда

$$(\ \exists\,\beta\in\mathfrak{I}^*(k),\ y\in\mathbb{R}^3,\ \varepsilon\in\mathfrak{o}^*(k),\ c_3\in\mathbb{R}_+^*)\ (\alpha)=(\beta),\ |\hat{\beta}-x|\leq c_3\,\Delta x;$$

$$\check{x}=\check{y}\varepsilon\ \ u\ \ |\hat{\alpha}-y|\leq c_3\,\Delta y.$$

Доказательство. Это утверждение следует из общей теории (см., например, [125] или [128, гл. I, §7]), но может быть доказано и прямым вычислением (ср. [95, стр. 56 - 57]).

Положим

$$\mathcal{C}_1(v,s)=\{t|t\in\mathbb{R}^3,\ (\ \exists\,x\in\mathcal{C}(v,s))\ |t-x|\leq c_3V^{1/3}\Delta\};$$

из леммы 3 и определения (8) следует, что

$$\Sigma_1(x)=\sum_{\beta\in M_7(x,\Delta)}\chi(\beta)W(\beta;\Delta,x)(1+O(\Delta)),$$

где

$$M_7(x,\Delta) := \{\beta | \beta \in T^{(0)},\ \hat{\beta} \in \mathcal{C}_1(v,s),\ N\check{x} < |(\beta)| \leq N\check{x} + \Delta V\},$$

и потому

$$\mathfrak{j} = \sum_{\beta \in M_8} d_{(\beta)}\chi(\beta)(1+O(\Delta)) \int_{M_9(\beta,\Delta)} W(\beta;\Delta,x)dx \tag{3.5.10}$$

с

$$M_8 := \{\beta | \beta \in T^{(0)},\ \hat{\beta} \in \mathcal{C}_1(v,s)\}$$

и

$$M_9(\beta,\Delta) := \{x | x \in \mathcal{C}(v,s),\ N\check{x} < |(\beta)| \leq N\check{x} + \Delta V\}.$$

Определение 3.5.2. *Пусть $T \in \mathcal{T}$; будем говорить, что односвязное подмножество F пространства $\mathbb{R}^3$ есть $\mathfrak{o}^*(k)$ - фундаментальная область, если*

$$(\forall\, \varepsilon \in \mathfrak{o}(k)^* \setminus \{1\},\ \{x,y\} \subseteq F)\ \varepsilon\check{x} \neq \check{y} \ \ u\ \ h_T(\{\varepsilon\check{x} | x \in F,\ \varepsilon \in \mathfrak{o}(k)^*\}) = \mathbb{R}^3.$$

Как можно показать (ср. [95, стр. 59 - 60]), из соотношения (10) следует, что

$$\mathfrak{j} = \sum_{\beta \in M_{10}} d_{(\beta)}\chi(\beta)(1+O(\Delta))I_0(\beta) + O(\Delta^4 V^2 \log X),$$

с

$$I_0(\beta) := \int_{x \in M_{11}(\beta,\Delta)} W(\beta;\Delta,x)dx,$$
$$M_{10} := \{\beta | \beta \in T^{(0)},\ \hat{\beta} \in \mathcal{C}(v,s)\}$$

и

$$M_{11}(\beta,\Delta) := \{x | x \in F,\ N\check{x} < |(\beta)| \leq N\check{x} + \Delta V\},$$

где F есть некоторая $\mathfrak{o}^*(k)$ - фундаментальная область (значение интеграла $I_0(\beta)$ от выбора фундаментальной области не зависит). Легко видеть, что

$$I_0(\beta) = \Delta^3 V \phi(k) h(k)^{-1} |\det h_T|$$

и потому

$$\mathfrak{j} = \Delta^3 V\phi(k)h(k)^{-1}|\det\ h_T| \sum_{\beta\in M_{10}} d_{(\beta)}\chi(\beta)(1+O(\Delta))$$

$$+ O(\Delta^4 V^2 \log X). \tag{3.5.11}$$

При $\varepsilon(\alpha,q)=1$ доказываемое соотношение (4) вытекает из соотношений (5), (9) и (11) при подходящем выборе параметра Δ. Тем самым, предложение 1 доказано.

Следствие 3.5.1. *Предположим, что куб* $\mathcal{C}(v,s)$ *есть* V *- куб. Тогда*

$$(\exists\, c(f)\in\mathbb{R}_+^*) \sum_{\beta\in M_2(q,T,\alpha)} g_{(\beta)} \ll V\exp(-c(f)\sqrt{\log L}) \tag{3.5.12}$$

при $1<q\le(\log X)^l,\ T\in\mathcal{T}$ *и* $\alpha\in T^{(0)}$.

Доказательство. Так как, по определению (см. (4.20)),

$$g_{(\beta)} = d_n((\beta),m) - e_n((\beta),m),$$

соотношение (12) вытекает из соотношений (3) и (4).

3. Положим

$$g_{\mathfrak{A}} := g_n(\mathfrak{A},m) \ \text{ при } \ \mathfrak{A}\in I_0(k),\ n\in\mathbb{N}_0 \ \text{ и } \ m\in\mathbb{N}^{n+1}$$

и

$$\mathbb{Z}_n := \{a|a\in\mathbb{Z}^n,\ \text{н.о.д. } (a_1,...,a_n)=1\}.$$

Пусть $V\in\mathbb{R}_+^*$; положим

$$\mathcal{A}_1(X,V) := \{(\mathfrak{a},\mathfrak{b})|(\mathfrak{a},\mathfrak{b})\in I_0(k)^2,\ \mathfrak{ab}\in\mathcal{A}(X),\ V<|\mathfrak{b}|\le 2V\}.$$

Предложение 3.5.2. *Рассмотрим* V *- куб* $\mathcal{C}(v,s)$*; пусть*

$$Q_1\in\mathbb{R}_+^*,\ Q_1\le\exp((\log X)^{1/3})$$

и предположим, что

$$(\exists\, c(f) \in \mathbb{R}_+^*) \sum_{\beta \in M_2(q,T,\alpha)} g_{(\beta)} \ll V \exp(-c(f)\sqrt{\log L}) \tag{3.5.13}$$

при $1 < q \le Q_1$, $T \in \mathcal{T}$ *и* $\alpha \in T^{(0)}$. *Тогда*

$$(\exists\, c(f) \in \mathbb{R}) \sum_{(\mathfrak{a},\mathfrak{b}) \in \mathcal{A}_1(X,V)} b_{\mathfrak{a}} g_{\mathfrak{b}} \ll X^2 Q_1^{-1/160} (\log X)^{c(f)}$$

при $X^{1+\tau} \ll V \ll X^{3/2-\tau}$.

Доказательство. Пусть $X^{1+\tau} \ll V \ll X^{3/2-\tau}$. Положим

$$\Sigma_{10}(V) := \sum_{(\mathfrak{a},\mathfrak{b}) \in \mathcal{A}_1(X,V)} b_{\mathfrak{a}} g_{\mathfrak{b}};$$

$$M_{12}(u,V) := \{(\mathfrak{a},\mathfrak{b}) | (\mathfrak{a},\mathfrak{b}) \in I_0(k)^2,\ \mathfrak{a}\mathfrak{b} = \mathfrak{A}_u,\ V < |\mathfrak{b}| \le 2V\},$$

$$\text{где } \mathfrak{A}_u := (u_1\omega_1 + u_2\omega_2)\mathfrak{d}^{-1} \text{ при } u \in \mathbb{Z}^2$$

и обозначим через

$$\Psi : \mathbb{R}^2 \to \{0,1\},\ \ \Psi : x \mapsto \begin{cases} 1 & \text{при } x \in I_{\mathbb{R}}(X) \\ 0 & \text{в противном случае}, \end{cases}$$

характеристическую функцию квадрата

$$I_{\mathbb{R}}(X) := \{x | x \in \mathbb{R}^2,\ X < x_1, x_2 \le X(1+\eta)\}.$$

Из определения множества $\mathcal{A}(X)$ следует, что

$$\Sigma_{10}(V) = \sum_{u \in \mathbb{Z}_2} \sum_{(\mathfrak{a},\mathfrak{b}) \in M_{12}(u,V)} \Psi(a) b_{\mathfrak{a}} g_{\mathfrak{b}}\ . \tag{3.5.14}$$

Положим

$$I_2(k) := \{\mathfrak{a} | \mathfrak{a} \in I_0(k),\ (\forall\, p \in \mathcal{P})\ p^{-1}\mathfrak{a} \notin I_0(k)\}.$$

Как можно показать (ср. [95, стр. 67 - 68]), из соотношения (14) следует, что

$$\Sigma_{10}(V) = \sum_{u \in \mathbb{Z}^2} \sum_{(\mathfrak{a},\mathfrak{b}) \in M_{13}(u,V)} \Psi(a) b_{\mathfrak{a}} g_{\mathfrak{b}} \ +\ O(X^{2-\tau/2} (\log X)^{c_3}) \tag{3.5.15}$$

с $c_3 \in \mathbb{R}$, где

$$M_{13}(u,V) := \{(\mathfrak{a},\mathfrak{b})|(\mathfrak{a},\mathfrak{b}) \in I_2(k)^2,\ \mathfrak{ab} = \mathfrak{A}_u,\ V < |\mathfrak{b}| \le 2V\}.$$

Положим

$$\mathfrak{I}_2(k) := \{\beta|\beta \in \mathfrak{I}^*(k),\ (\beta) \in I_2(k)\};$$

$$\mathfrak{I}_3(k) := \{\beta|\beta \in \mathfrak{I}_2(k),\ |(\beta)|^{1/3}(\sigma_1\varepsilon_0)^{-1/2} < \sigma_1\beta \le |(\beta)|^{1/3}(\sigma_1\varepsilon_0)^{1/2}\}$$

при $r(k) = 1$, где ε_0 есть фундаментальная единица поля k под условием $\sigma_1\varepsilon_0 > 1$, и

$$\mathfrak{I}_3(k) := \{\beta|\beta \in \mathfrak{I}_2(k),\ N\beta > 0,$$

$$(\exists\, x \in M_0)\ |\sigma_j\beta| = |(\beta)|^{1/3}|\sigma_j\varepsilon_1|^{x_1}|\sigma_j\varepsilon_2|^{x_2} \text{ при } 1 \le j \le 3\}$$

при $r(k) = 2$, где $\varepsilon_1,\ \varepsilon_2$ суть две мультипликативно независимые фундаментальные единица поля k под условием $N\varepsilon_1 = N\varepsilon_2 = 1$ и

$$M_0 := \{x|x \in \mathbb{R}^2,\ -1/2 < x_i \le 1/2 \text{ при } i \in \{1,2\}\}.$$

Определим функцию

$$G : \mathfrak{I}^*(k) \to \mathbb{R},\ \ G : \beta \mapsto \begin{cases} g_{(\beta)} & \text{при } \beta \in \mathfrak{I}_3(k), \\ 0 & \text{в противном случае .} \end{cases}$$

В этих обозначениях соотношение (15) переписывается следующим образом:

$$\Sigma_{10}(V) = \sum_{u\in\mathbb{Z}^2} \sum_{(\alpha,\beta)\in M_{14}(u,V)} b_{(\alpha)}G(\beta)\Psi(u) \ +\ O(X^{2-\tau/2}(\log X)^{c_3}) \qquad (3.5.16)$$

с

$$M_{14}(u,V) :=$$

$$\{(\alpha,\beta)|(\alpha) \in I_2(k),\ \beta \in \mathfrak{I}_0^*(k),\ \delta\alpha\beta = u_1\omega_1 + u_2\omega_2,\ V < |(\beta)| \le 2V\}.$$

Поскольку $|(\alpha)| \ll X^3V^{-1}$, из соотношения (15) и неравенства Коши - Буняковского следует, что

$$\Sigma_{10}(V) \ll X^{2-\tau/2}(\log X)^{c_3} + X^{3/2}V^{-1/2}\Sigma_{11}(V)^{1/2} \qquad (3.5.17)$$

с

$$\Sigma_{11}(V) := \sum_{(\alpha)\in I_2(k)} |\sum_{u\in\mathbb{Z}^2} \sum_{\beta\in M_{15}(u,\alpha,V)} \Psi(u)G(\beta)|^2,$$

где

$$M_{15}(u,\alpha,V) := \{\beta|\beta\in\mathfrak{J}_0^*(k),\ V<|(\beta)|\le 2V,\ \delta\alpha\beta = u_1\omega_1+u_2\omega_2\}.$$

Рассмотрим функцию

$$\psi : \mathbb{Z}^4\times\mathfrak{J}_0^*(k)^2\to\{0,1\},$$

$$\psi : (u,\beta)\mapsto |\{\alpha|(\alpha)\in I_2(k),\ \delta\alpha\beta_i = u_{i1}\omega_1+u_{i2}\omega_2 \text{ при } i\in\{1,2\}\}|$$

(здесь $\mathbb{Z}^4 = \{(u_1,u_2)|\{u_1,u_2\}\subseteq\mathbb{Z}^2\}$); ясно, что

$$\Sigma_{11}(V) = \sum_{u\in\mathbb{Z}^4}\sum_{\beta\in M_{16}(V)} \Psi(u_1)\Psi(u_2)G(\beta_1)G(\beta_2)\psi(u,\beta) \tag{3.5.18}$$

с

$$M_{16}(V) := \{\beta|\beta\in\mathfrak{J}_0^*(k)^2,\ V<|(\beta_i)|\le 2V \text{ при } i\in\{1,2\}\}.$$

Из соотношения (18) легко следует (ср. [95, стр. 68]), что

$$\Sigma_{11}(V) = \Sigma_{12}(V) + O(X^2(\log X)^{c_4}) \text{ с } c_4\in\mathbb{R}, \tag{3.5.19}$$

где

$$\Sigma_{12}(V) := \sum_{u\in\mathbb{Z}^4}\sum_{\beta\in M_{17}(V)} \Psi(u_1)\Psi(u_2)G(\beta_1)G(\beta_2)\psi(u,\beta) \tag{3.5.20}$$

с

$$M_{17}(V) := \{\beta|\beta\in M_{16}(V),\ \beta_1\ne\beta_2\}.$$

Обозначения. При $b\in\mathbb{Z}^3\setminus\{0\}$ положим

$$\text{н.о.д. } (b_1,b_2,b_3) = d(b) \text{ с } d(b)\in\mathbb{N},\ [b] := d(b)^{-1}b \text{ и } [0] := 0.$$

При $\{x,y\}\subseteq\mathbb{R}^3$ положим

$$x\wedge y := (x_2y_3-x_3y_2, x_3y_1-x_1y_3, x_1y_2-x_2y_1).$$

Пусть $\psi(u,\beta)=1$ и $i\in\{1,2\}$, тогда

$$\delta\alpha\beta_i=u_{i1}\omega_1+u_{i2}\omega_2=\delta(u_{i1}w_1+u_{i2}(lw_2))$$

и, значит,

$$\text{cl }\beta_1=\text{cl }\beta_2,\ \alpha\in\text{cl}(\delta\beta_i)^{-1}\ \text{ и }\ \alpha\beta_i=u_{i1}w_1+u_{i2}(lw_2). \tag{3.5.21}$$

Обозначим через $\{v_1^{(i)},v_2^{(i)},v_3^{(i)}\}$ выбранный базис $\mathbb{Z}$ - модуля $\text{cl}(\beta_i\delta)^{-1}$ и положим

$$b_j^{(i)}:=\text{tr }(v_j^{(i)}\beta_i\bar{w}_3)$$

при $i\in\{1,2\}$; пусть

$$\alpha=\alpha_1v_1+\alpha_2v_2+\alpha_3v_3.$$

Из соотношения (21) следует, что

$$\sum_{j=1}^{3}\alpha_jb_j^{(i)}=0\ \text{ при }\ i\in\{1,2\}$$

и потому

$$(\exists\, c\in\mathbb{Z})\ \hat{\alpha}=c\,[\hat{\beta}_1\wedge\hat{\beta}_2];$$

но $(\alpha)\in I_2(k)$, следовательно, $c\in\{1,-1\}$. Таким образом,

$$\hat{\alpha}=\pm[\hat{\beta}_1\wedge\hat{\beta}_2]. \tag{3.5.22}$$

Лемма 3.5.4 *Пусть* $1\ll Y\ll X^{\tau/3}$. *Тогда*

$$(\exists\, c(f)\in\mathbb{R},\ T\in\mathcal{T})\ \Sigma_{10}(V)\ll X^2Y^{-1/2}(\log X)^c+X^{3/2}V^{-1/2}\Sigma_{13}^{1/2},$$

где

$$\Sigma_{13}=\sum_{(u,\beta)\in M_{18}}G(\beta_1)G(\beta_2)\Psi(u_1)\Psi(u_2)\psi(u,\beta)$$

с

$$M_{18}:=\{(u,\beta)|u\in\mathbb{Z}^4,\ \beta_i\in T^{(0)},$$

$$V<|(\beta_i)|\le 2V\ \ npu\ \ i\in\{1,2\},\ d(\hat{\beta}_1\wedge\hat{\beta}_2)>VX^{-1}Y^{-1}\}.$$

Доказательство. Можно доказать (ср. [95, стр. 69 - 71]), что это утверждение следует из соотношений (17) и (19) - (22).

Положим

$$\beta_{12} = \sum_{j=1}^{3} (\hat{\beta}_1 \wedge \hat{\beta}_2)_j v_j,\ h_{i1}(\beta) = \mathrm{tr}\ (\beta_i \beta_{12} \bar{w}_1)\ \text{ и }\ h_{i2}(\beta) = \mathrm{tr}\ (\beta_i \beta_{12} \bar{w}_2)$$

при $i \in \{1, 2\}$. Нетрудно показать, что

$$\Sigma_{13} = \sum_{\beta \in M_{19}} G(\beta_1) G(\beta_2) \Psi(d(\hat{\beta}_1 \wedge \hat{\beta}_2)^{-1} h_{i1}(\beta)) \Psi(d(\hat{\beta}_1 \wedge \hat{\beta}_2)^{-1} h_{i2}(\beta))$$

с

$$M_{19} := \{\beta | \beta_i \in T^{(0)},$$

$$V < |(\beta_i)| \le 2V \ \text{ при } \ i \in \{1, 2\},\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) > V X^{-1} Y^{-1}\}.$$

Положим

$$U(y) := \{(\hat{\beta}_1, \hat{\beta}_2) | \beta_i \in T^{(0)},$$

$$V < N\beta_i \le 2V,\ yX < h_{ij}(\beta) \le yX(1 + \eta) \ \text{ при } \ \{i, j\} \subseteq \{1, 2\}\};$$

в этих обозначениях,

$$\Sigma_{13} = \sum_{\beta \in M_{20}} G(\beta_1) G(\beta_2) \tag{3.5.23}$$

с

$$M_{20} := \{\beta | (\hat{\beta}_1, \hat{\beta}_2) \in U(d(\hat{\beta}_1 \wedge \hat{\beta}_2)),\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) > V X^{-1} Y^{-1}\}.$$

Положим

$$I_m := (\frac{m-1}{S}\Delta,\ \frac{m}{S}\Delta] \ \text{ при } \ m \in \mathbb{N} \ \text{ и } \ \{S, \Delta\} \subseteq \mathbb{R}_+^*\ ,$$

$$M_{21}(d_1) := \{\beta | (\hat{\beta}_1, \hat{\beta}_2) \in U(d_1),\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) = d_1\} \ \text{ при } \ d_1 \in \mathbb{N}$$

и

$$\Sigma_{14}(m, \Delta) := \sum_{d_1 \in I_m \cap \mathbb{N}} \Big| \sum_{\beta \in M_{21}(d_1)} G(\beta_1) G(\beta_2) \Big|. \tag{3.5.24}$$

Из соотношений (23) и (24) следует, что

$$(\exists\ m \in \mathbb{N},\ \{S, \Delta\} \subseteq \mathbb{R}_+^*)\ S \ll X^{2\tau/3},\ S < m \le 2S,$$

$$VX^{-1}Y^{-1} < \Delta \ll VX^{-1} \text{ и } \Sigma_{13} \ll (\log X)\, S\, \Sigma_{14}(m, \Delta). \tag{3.5.25}$$

Положим

$$U_{\mathbb{R}}(y) := \{(\hat{\beta}_1, \hat{\beta}_2) | \beta_i \in T_{\mathbb{R}},\ V < N\beta_i \le 2V,\ yX < h_{ij}(\beta) \le yX(1+\eta),$$

$$N\beta_i^{1/3}(\sigma_1\varepsilon_0)^{-1/2} < \sigma_1\beta_i \le N\beta_i^{1/3}(\sigma_1\varepsilon_0)^{1/2} \text{ при } \{i,j\} \subseteq \{1,2\}\}$$

при $r(k) = 1$ и

$$U_{\mathbb{R}}(y) := \{(\hat{\beta}_1, \hat{\beta}_2) | \beta_i \in T_{\mathbb{R}},\ V < N\beta_i \le 2V,\ yX < h_{ij}(\beta) \le yX(1+\eta),$$

$$(\exists\, x \in M_0)\ |\sigma_j\beta_i| = N\beta_i^{1/3}|\sigma_j\varepsilon_1|^{x_1}|\sigma_j\varepsilon_2|^{x_2} \text{ при } \{i,j\} \subseteq \{1,2\}\}$$

при $r(k) = 2$. Заметим, что

$$\hat{\beta}_1 \ne \pm\hat{\beta}_2 \text{ при } (\hat{\beta}_1, \hat{\beta}_2) \in U_{\mathbb{R}}(y) \text{ и } y \in \mathbb{R}_+^*\,, \tag{3.5.26}$$

ибо $\beta_{12} = 0$ и, значит, $h_{ij}(\beta) = 0$ при $\beta_1 = \pm\beta_2$ и $\{i,j\} \subseteq \{1,2\}$. Положим далее

$$\mathcal{K}(n) := \{x | x \in \mathbb{R}^6,\ V^{1/3}(n_i - 1)S^{-1} < x_i \le V^{1/3}n_iS^{-1} \text{ при } 1 \le i \le 6\}$$

при $n \in \mathbb{Z}^6$ и пусть

$$\mathfrak{K}_1 := \{\mathcal{K}(n) | n \in \mathbb{Z}^6,\ (\exists\, d_1 \in I_m \cap \mathbb{N})\ \mathcal{K}(n) \subseteq U_{\mathbb{R}}(d_1)\},$$

$$\mathfrak{K}_2 :=$$

$$\{\mathcal{K}(n) | n \in \mathbb{Z}^6,\ \mathcal{K}(n) \notin \mathfrak{K}_1 \text{ и } (\exists\, d_1 \in I_m \cap \mathbb{N})\ \mathcal{K}(n) \cap U_{\mathbb{R}}(d_1) \ne \emptyset\}.$$

Из соотношения (26) следует, что

$$(n_1, n_2, n_3) \ne \pm(n_4, n_5, n_6) \text{ при } \mathcal{K}(n) \in \mathfrak{K}_1\,. \tag{3.5.27}$$

В этих обозначениях,

$$\Sigma_{14}(m, \Delta) = \Sigma_{14}^{(1)}(m, \Delta) + \Sigma_{14}^{(2)}(m, \Delta), \tag{3.5.28}$$

где

$$\Sigma_{14}^{(i)}(m,\Delta) := \sum_{d_1 \in I_m \cap \mathbb{N}} \Big| \sum_{\beta \in M_{22}(d_1,i)} G(\beta_1)G(\beta_2)\Big|$$

и

$$M_{22}(d_1,i) := \{\beta | (\exists\, n \in \mathbb{Z}^6)\ (\hat{\beta}_1, \hat{\beta}_2) \in \mathcal{K}(n),\ \mathcal{K}(n) \in \mathfrak{K}_i,\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) = d_1\}$$

при $d_1 \in \mathbb{N}$ и $i \in \{1,2\}$. Можно показать (ср. [95, стр. 73 - 74] и [97, стр. 281 - 282]), что

$$|\mathfrak{K}_2| \ll S^5.$$

Из этой оценки, соотношений (24), (25), (28) и леммы 4 следует тогда (ср. [95, стр. 75]), что

$$(\exists\, \mathcal{K} \in \mathfrak{K}_1,\ c \in \mathbb{R})\ \Sigma_{10}(V) \ll$$

$$(X^2Y^{-1/2}\ +\ X^{3/2}V^{-1/2}Y^7\Sigma_{15}(\mathcal{K})^{1/2})(\log X)^c, \tag{3.5.29}$$

где

$$\Sigma_{15}(\mathcal{K}) := \sum_{d_1 \in I_m \cap \mathbb{N}} \Big| \sum_{\beta \in M_{23}(d_1)} G(\beta_1)G(\beta_2)\Big|$$

с

$$M_{23}(d_1) := \{\beta | (\hat{\beta}_1, \hat{\beta}_2) \in \mathcal{K},\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) = d_1\}.$$

Положим, для краткости,

$$d_0 := X^{-1}VY^{15} + V^{1/6};$$

воспользовавшись леммой 1, одной леммой из геометрии чисел [95, лемма 4.8], соотношением (27) и оценкой (29), можно доказать (ср. [95, стр. 75 - 77]), что

$$(\exists\, \mathcal{K} \in \mathfrak{K}_1,\ c \in \mathbb{R})\ \Sigma_{10}(V) \ll$$

$$(X^2Y^{-1/2}\ +\ X^{3/2}V^{-1/2}Y^7\Sigma_{16}^{1/2})(\log X)^c, \tag{3.5.30}$$

где

$$\Sigma_{16}(\mathcal{K}) := \sum_{d \in M_{25}} \Big| \sum_{\beta \in M_{24}(d_1 d_2)} G(\beta_1)G(\beta_2)\Big|$$

с

$$M_{24}(a) := \{\beta | (\hat{\beta}_1, \hat{\beta}_2) \in \mathcal{K},\ d(\hat{\beta}_1 \wedge \hat{\beta}_2) = 0\ (a)\}\ \text{ при }\ a \in \mathbb{N}$$

и

$$M_{25} := \{d | d \subseteq \mathbb{N}^2,\ d_1 \in I_m,\ d_1 d_2 < d_0\}.$$

Сумма $\Sigma_{16}(\mathcal{K})$ оценивается методом большого решета. Пусть R - коммутативное кольцо и $m \in \mathbb{N}$; положим, для краткости,

$$ab := \sum_{i=1}^{m} a_i b_i\ \text{ при }\ \{a, b\} \subseteq R^m.$$

Представим куб $\mathcal{K}$ в качестве произведения двух трёхмерных кубов:

$$\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2\ \text{ с }\ \mathcal{K}_j \subseteq \mathbb{R}^3\ \text{ при }\ j \in \{1, 2\}$$

и положим

$$\sigma(a; G, \mathcal{D}) = \sum_{\hat{\beta} \in \mathcal{D} \cap \mathbb{Z}^3} \exp(2\pi i a\hat{\beta}) G(\beta)\ \text{ при }\ a \in \mathbb{Z}^3\ \text{ и }\ \mathcal{D} \subseteq \mathbb{R}^3.$$

Можно показать (ср. [95, стр. 78]), что

$$\Sigma_{16}(\mathcal{K}) \ll XY \frac{\log V}{V} \sum_{q \le d_0} \frac{\tau(q)}{q} \sum_{b \in M_{26}(q)} \sum_{j \in \{1,2\}} |\sigma(q^{-1}b; G, \mathcal{K}_j)|^2 \qquad (3.5.31)$$

с

$$M_{26}(q) := \{b | b \in \mathbb{Z}^3,\ 1 \le b_j \le q\ \text{ при }\ 1 \le j \le 3,\ (q, b_1, b_2, b_3) = (1)\}.$$

Из соотношения (31) и леммы 13.1 ("большое решето" !) работы [95] следует (ср. [95, стр. 81]), что

$$(\exists\, c \in \mathbb{R})\ \Sigma_{16}(\mathcal{K}) \ll \Sigma_{17}(\mathcal{K}) + XV(YQ_0^{-1/2} + Y^{46}X^{-\tau/2})(\log X)^c \qquad (3.5.32)$$

при $1 \le Q_0 < d_0$, где

$$\Sigma_{17}(\mathcal{K}) := XY \frac{\log V}{V} \sum_{q \le Q_0} \frac{\tau(q)}{q} \sum_{b \in M_{26}(q)} \sum_{j \in \{1,2\}} |\sigma(q^{-1}b; G, \mathcal{K}_j)|^2. \qquad (3.5.33)$$

Но

$$\sigma(q^{-1}b; G, \mathcal{K}_j) = \sum_{c \in (\mathbb{Z}/q\mathbb{Z})^3} \exp(\frac{2\pi i bc}{q}) \sum_{\hat{\beta} \in M_{27}(q)} G(\beta)$$

с

$$M_{27}(q) := \{b | b \in \mathcal{K}_j \cap \mathbb{Z}^3,\ b = c\ (q)\},$$

а

$$\sum_{\hat{\beta} \in M_{27}(q)} G(\beta) = \sum_{\beta \in M_{28}(q)} g_{(\beta)} \sum_{d|\beta} \mu(d)$$

с

$$M_{28}(q) := \{\beta | \beta \in \mathfrak{I}_0^*(k),\ \hat{\beta} \in \mathcal{K}_j \cap \mathbb{Z}^3,\ \hat{\beta} = c\ (q)\};$$

поэтому

$$\sigma(q^{-1}b; G, \mathcal{K}_j) \ll \sum_{d=1}^{\infty} \sum_{c \in (\mathbb{Z}/q\mathbb{Z})^3} | \sum_{\hat{\beta} \in M_{29}(q,d)} g_{(\beta)}|, \tag{3.5.34}$$

где

$$M_{29}(q, d) := \{\beta | \beta \in M_{28}(q),\ \beta = 0\ (d)\},$$

при $j \in \{1, 2\}$. Условия $\beta = 0\ (d)$ и $\hat{\beta} = c\ (q)$ эквивалентны сравнению по модулю $[q, d] :=$ н.о.к. (q, d); в силу предположения (13), отсюда и из соотношеня (34) следует, что

$$(\exists\, c \in \mathbb{R}_+^*) \sum_{\hat{\beta} \in M_{29}(q,d)} g_{(\beta)} \ll V \exp(-c\sqrt{\log L}) \text{ при } 1 < [q, d] \leq Q_1$$

и потому (ср. [95, стр. 82])

$$(\exists\, c \in \mathbb{R}_+^*)\ \sigma(q^{-1}b; G, \mathcal{K}_j) \ll Q_1^2 V \exp(-c\sqrt{\log L}) \ +\ Q_1^{-1} V (\log X)^c \tag{3.5.35}$$

при $j \in \{1, 2\}$. Положив, как и в работе [95] на стр. 83,

$$Q_0 = Q_1^{1/2} \text{ и } Y = Q_1^{1/80}$$

и воспользовавшись соотношениями (30), (32), (33) и (35), получим

$$(\exists\, c \in \mathbb{R})\ \Sigma_{10}(V) \ll X^2 Q_1^{-1/160} (\log X)^c.$$

Тем самым, предложение 2 доказано.

Для завершения доказательства теоремы 2.1 достаточно заметить, что слагаемые суммы Σ_9 имеют вид $\Sigma_{10}(V)$, воспользоваться следствием 1 и положить $Q_1 = (\log X)^{300c_0}$ (ср. [95, стр. 21]).

3.6 Теорема о представлении простых чисел кубическими полиномами от двух переменных

1. Пусть

$$d \in \mathbb{N},\ a \in \mathbb{Z}^2,\ 0 \le a_1, a_2 < d \ \text{ и } \ (a_1,\ a_2,\ d) = (1).$$

Положим

$$F(x) := N_{k(x)/\mathbb{Q}(x)}((a_1 + dx_1)\omega_1 + (a_2 + dx_2)\omega_2)|\mathfrak{d}(a)|^{-1}, \tag{3.6.1}$$

где

$$\mathfrak{d}(a) := (a_1\omega_1 + a_2\omega_2,\ d\omega_1,\ d\omega_2).$$

Ясно, что $F(x) \in \mathbb{Z}[x]$; положим

$$h_F := d^3|(\omega_1 + \omega_2)\mathfrak{d}(a)^{-1}|$$

и заметим, что

$$F(x) = h_F X^3(1 + O(\eta)) \ \text{ при } \ x \in I(X).$$

По определению, $h_F = d^3|\mathfrak{d}|\ |\mathfrak{d}(a)|^{-1}h_f$ и потому $h_F \in \mathbb{N}$. Положим далее

$$\mathfrak{A}_u(a) := ((a_1 + du_1)\omega_1 + (a_2 + du_2)\omega_2)|\mathfrak{d}(a)|^{-1} \ \text{ при } \ u \in \mathbb{Z}^2$$

и

$$\mathfrak{m}(R, a) := \{u | u \in \mathbb{Z}^2,\ 1 \le u_1, u_2 \le r,\ \mathfrak{A}_u(a) = 0\ (R)\} \ \text{ при } \ R \in I_0(k).$$

Из сказанного следует, что

$$F(x) = |\mathfrak{A}_x(a)| \text{ при } x \in I(X) \cap \mathbb{Z}^2. \tag{3.6.2}$$

Пусть

$$\mathcal{P}_0(d) := \{p | p \in \mathcal{P},\ di(\theta) N(\omega_1\omega_2) = 0\ (p)\} \text{ и } \Pi_0(d) := \prod_{p \in \mathcal{P}_0(d)} p.$$

Положим

$$R_0(d) := (R, \Pi_0(d)) \text{ и } R_1(d) := R \cdot R_0(d)^{-1} \text{ при } R \in I_0(k),$$

$$\mathcal{R}(d) := \{R | R \in I_0(k),\ \mu(R)^2 = 1,\ \mu(|R_1(d)|)^2 = 1\},$$

$$m_d(q) := \{R | R \in \mathcal{R}(d),\ q = 0\ (R),\ |R| = 0\ (q)\} \text{ при } q \in \mathbb{N}$$

и

$$\Gamma(p) := \sum_{R \in m_d(p)} \mu(R)\ |\mathfrak{m}(R_0(d), a)|\ b(R)\ r^{-2} \text{ при } p \in \mathcal{P},$$

где

$$b(R) := \prod_{p \in M_1(R)} (1 - p^{-2})^{-1}(1 - p^{-2}\ |(R,p)|^2\ |\mathfrak{m}((R,p),a)|)$$

и

$$M_1(R) := \{p | p \in \mathcal{P},\ r = 0\ (p),\ d \neq 0\ (p)\}.$$

Заметим, что

$$\Gamma(p) = \frac{\nu_p}{p+1} \text{ при } p \in \mathcal{P} \setminus \mathcal{P}_0(d) \tag{3.6.3}$$

и $\Gamma(p) = \gamma(p)$ при $d = 1$. Положим

$$\sigma(F) := \prod_{p \in \mathcal{P}} (1 + p^{-1})^{-1}(1 - \Gamma(p)) \cdot \prod_{p \in \mathcal{P},\ p|d} (1 - p^{-2})^{-1};$$

как было отмечено в §2 (см. доказательство леммы 2.4), из соотношения (3) следует, что бесконечное произведение

$$\prod_{p \in \mathcal{P}} (1 + p^{-1})^{-1}(1 - \Gamma(p))$$

есть (условно) сходящееся произведение. Как и в §2 (при $d = 1$), положим

$$(\{F(a)|a \in \mathbb{Z}^2\}) = (\varepsilon(F)) \text{ с } \varepsilon(F) \in \mathbb{N}$$

и

$$\pi_F(X) := |\{p|p \in \mathcal{P},\ (\exists\, x \in I(X))\ F(x) = p\}|\ .$$

Теорема 3.6.1 . *Имеет место следующая асимптотическая формула:*

$$\pi_F(X) = \sigma(F)\,\frac{\eta^2 X^2}{3\log X}\,(1 + O((\log\log X)^{-1/6})) \quad \textit{при} \quad X \to \infty \tag{3.6.4}$$

и, более того,

$$\varepsilon(F) = 1 \Leftrightarrow \sigma(F) \in \mathbb{R}_+^*\ . \tag{3.6.5}$$

Ясно, что теорема 1.4 следует из теоремы 1.

Лемма 3.6.1 . *Имеют место следующие соотношения:*

$$\varepsilon(F) \in \{1, 2, 3, 6\},$$

$$\Gamma(p) = 1 \Leftrightarrow \varepsilon(F) = 0\ (p) \quad \textit{при} \quad p \in \{2, 3\}$$

и

$$(\exists\, c_1 \in \mathbb{R}_+^*)\ (\forall\, p \in \mathcal{P} \setminus \{2, 3\})\ 0 \le \Gamma(p) \le 1 - c_1.$$

Доказательство. Это утверждение вытекает из законов арифметики кубических полей [114] (см. [98, лемма 2.4]).

Положим

$$\mathcal{A}(a, X) := \{\mathfrak{A}_u(a)|u \in I(X) \cap \mathbb{Z}^2,\ (a_1 + du_1,\ a_2 + du_2) = (1)\}$$

и заметим, что

$$\pi(\mathcal{A}(a, X)) = \pi_F(X), \tag{3.6.6}$$

в силу соотношения (2) и леммы 2.2 (ср. следствие 2.1). Пусть

$$\mathcal{B}(a, X) := \{\mathfrak{A}|\mathfrak{A} \in I_0(k), h_F X^3 < |\mathfrak{A}| \le h_F X^3(1 + \eta)\}$$

и

$$\kappa(F) := \sigma(F)\eta(h_F X)^{-1}.$$

Предложение 3.6.1 . *Имеет место следующее соотношение:*

$$\pi(\mathcal{A}(a,X)) = \kappa(F)\pi(\mathcal{B}(a,X)) + O(\frac{\eta^2 X^2 \tau}{\log X}). \tag{3.6.7}$$

Ввиду тождества (6), теорема 1 следует из предложения 1 и леммы 1 (ср. начало §2).

2. Доказательство предложениия 1 есть обобщение доказательства соотношения (4.1). При $R \in \mathcal{R}(d))$ положим

$$< \mathcal{A}(a,X)_R > :=$$

$$\eta^2 X^2 |\mathfrak{m}(R,a)| r^{-2} \sum_{\delta \in \mathbb{N},\ (\delta,d)=(1)} \mu(\delta) N((R,\delta))^2 |\mathfrak{m}((R,\delta),a)|^{-1} \delta^{-2}$$

и

$$\rho_1(a,R,X) := |\mathcal{A}(a,X)_R| - < \mathcal{A}(a,X)_R > \ .$$

Лемма 3.6.2 . *Пусть $l \in \mathbb{N}$; тогда*

$$(\exists\, c(l) \in \mathbb{R}) \sum_{R \in M_2(Q)} \tau(R)^l |\rho_1(a,R,X)| \ll (Q + XQ^{1/2} + X^{3/2})(\log QX)^{c(l)},$$

где

$$M_2(Q) := \{R | R \in \mathcal{R}(d),\ Q < |R| \le 2Q\}.$$

Доказательство. Это утверждение является обобщением леммы 3.2 и доказывается аналогично (см. [98, лемма 2.2]).

Положим

$$A(a,X) := \{|\mathfrak{A}|\ |\mathfrak{A} \in \mathcal{A}(a,X)\},$$

$$< A(a,X)_q > := \mu(q) \sum_{R \in m_d(q)} \mu(R)\ < \mathcal{A}(a,X)_R >$$

и

$$\rho_2(a,q,X) := \mu(q) \sum_{R \in m_d(q)} \mu(R) \rho_1(a,R,X)$$

при $q \in \mathbb{N}$. Из соотношения (2) следует, что

$$A(a,X) := \{F(x) | x \in I(X) \cap \mathbb{Z}^2,\ (a_1 + du_1,\ a_2 + du_2) = (1)\}.$$

Лемма 3.6.3. *Пусть* $l \in \mathbb{N}$; *тогда*

$$(\exists\, c(l) \in \mathbb{R}) \sum_{q \in M_3(Q)} \mu(q)^2 \tau(q)^l |\rho_2(a,q,X)| \ll$$

$$(Q + XQ^{1/2} + X^{3/2})(\log QX)^{c(l)},$$

где

$$M_3(Q) := \{q | q \in \mathbb{N},\ Q < q \leq 2Q\}.$$

Более того, если $q \in \mathbb{N}$ *и* $\mu(q)^2 = 1$, *то*

$$< A(a,X)_q > = (\eta X)^2\, \Gamma(q)\, \zeta_d(2)^{-1},$$

где

$$\zeta_d(s) := \zeta(s) \prod_{p \in \mathcal{P},\, p|d} (1 - p^{-s}) \quad u \quad \Gamma(q) := \prod_{p \in \mathcal{P},\, p|q} \Gamma(p),$$

и

$$|A(a,X)_q| =< A(a,X)_q > \ + \rho_2(a,q,X).$$

Доказательство. Эта лемма есть обобщение леммы 3.3 и соотношений (3.17) - (3.20). Доказательство леммы проводится аналогично доказательству цитируемых утверждений из §3.

Лемма 3.6.4. *В обозначениях* §4, *имеет место следующее обобщение соотношения* (4.33)*:*

$$\pi(\mathcal{A}(a,X)) - \kappa(F)\pi(\mathcal{B}(a,X)) \ll$$

$$\tau\eta^2 X^2 (\log X)^{-1} + \eta^{5/2} X^2 (\log X)^{c(F)} + \Sigma_{18} \tag{3.6.8}$$

с

$$\Sigma_{18} := \sum_{n=3}^{\infty} |\hat{U}_g^{(n)}(\mathcal{A}(a,X))| +$$

$$\sum_{n \in \{1,2\}} |\hat{U}_{1,g}^{(n)}(\mathcal{A}(a,X))| + |\hat{S}_{4,g}(\mathcal{A}(a,X)| + |\hat{U}_{2,g}^{(1)}(\mathcal{A}(a,X))|$$

и $c(F) \in \mathbb{R}$.

Доказательство. Эта лемма выводится из леммы 2 и леммы 3 методом решета (ср. §4).

3. Для завершения доказательства предложения 1 необходимо оценить сверху сумму Σ_{18} . Как и в §5, требуемая оценка вытекает из следствия 5.1 и следующего аналога предложения 5.2.

Предложение 3.6.2 . *Рассмотрим V - куб $\mathcal{C}(v,s)$; пусть*

$$Q_1 \in \mathbb{R}_+^*,\ Q_1 \le \exp((\log X)^{1/3})$$

и предположим, что

$$(\exists\, c(f) \in \mathbb{R}_+^*) \sum_{\beta \in M_2(q,T,\alpha)} g_{(\beta)} \ll V \exp(-c(f)\sqrt{\log L}) \tag{3.6.9}$$

при $1 < q \le Q_1$, $T \in \mathcal{T}$ и $\alpha \in T^{(0)}$. Тогда

$$(\exists\, c(f) \in \mathbb{R}) \sum_{(\mathfrak{a},\mathfrak{b}) \in \mathcal{A}_2(a,X,V)} b_{\mathfrak{a}} g_{\mathfrak{b}} \ll X^2 Q_1^{-1/160} (\log X)^{c(f)}$$

при $X^{1+\tau} \ll V \ll X^{3/2-\tau}$, где

$$\mathcal{A}_2(a,X,V) := \{(\mathfrak{a},\mathfrak{b}) | (\mathfrak{a},\mathfrak{b}) \in I_0(k)^2,\ \mathfrak{ab} \in \mathcal{A}(a,X),\ V < |\mathfrak{b}| \le 2V\}.$$

Доказательство. Описанное в §5 доказательство предложения 5.2 обобщается на рассматриваемую в этом параграфе ситуацию; тем самым удаётся доказать и это предложение (ср. [98, стр. 306 - 311]).

Глава 4

Приложение: семь коротких заметок

4.1 О распределении степенных вычетов и невычетов

1. В этом параграфе известные оценки А. Вейля [165] применяются к изучению степенных характеров [25]. Пусть p - нечётное простое число; $l|p-1$; χ - мультипликативный характер степени l; $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ - корни l-ой степени из единицы; $\Phi(t)$ - неприводимый полином степени f с коэффициентами в $\mathbb{F}_p$. Положим

$$\mathcal{E}(\varepsilon, \Phi) := \{x | x \in \mathbb{F}_p,\ \chi(\Phi(x+i)) = \varepsilon_i \text{ при } 1 \le i \le s\},$$

$$E(\varepsilon, \Phi) := |\mathcal{E}(\varepsilon, \Phi)|$$

и, отожествив $\mathbb{F}_p$ с множеством $\{n | n \in \mathbb{Z},\ 0 \le n \le p-1\}$,

$$\mathcal{E}_0(\varepsilon, \Phi) := \{x | x \in \mathbb{F}_p,\ 0 \le x \le p/s,\ \chi(\Phi(xs+i)) = \varepsilon_i \text{ при } 1 \le i \le s\},$$

$$E_0(\varepsilon, \Phi) := |\mathcal{E}_0(\varepsilon, \Phi)|;$$

$$\mathcal{E}(\varepsilon, p_1, p_2, \Phi) := \{x |\ x \in \mathbb{F}_p,\ p_1 \le x \le p_2,\ \chi(\Phi(x+i)) = \varepsilon_i \text{ при } 1 \le i \le s\},$$

$$E(\varepsilon, p_1, p_2, \Phi) := |\mathcal{E}(\varepsilon, p_1, p_2, \Phi)|$$

в предположении $0 \le p_1 \le p_2 \le p-1$.

Теорема 4.1.1. *Имеет место следующее неравенство:*

$$|E(\varepsilon, \Phi) - \frac{p}{l^s}| < sflp^{1/2}.$$

Теорема 4.1.2. *Имеет место следующее неравенство:*

$$|E(\varepsilon, p_1, p_2, \Phi) - \frac{p_2 - p_1}{l^s}| < 2sflp^{1/2} \log p.$$

Теорема 4.1.3. *Имеет место следующее неравенство:*

$$|E_0(\varepsilon, \Phi) - \frac{p}{sl^s}| < 2sflp^{1/2} \log p.$$

Эти теоремы обобщают и усиливают результаты Дэвенпорта [61].

2. Докажем сформулированные утверждения.

Лемма 4.1.1. *Пусть χ - неединичный мультипликативный характер по* $\bmod p$ *степени l; $\Phi(t)$ - полином степени f с коэффициентами в $\mathbb{F}_p$, причём $\Phi(t) \neq \Psi(t)^l$ ни для какого полинома $\Psi(t)$ в $\mathbb{F}_p[t]$, и пусть $a \in \mathbb{F}_p$. Тогда*

$$|\sum_{x\in\mathbb{F}_p} \chi(\Phi(x))| \leq (f-1)p^{1/2}. \tag{4.1.1}$$

и

$$|\sum_{x\in\mathbb{F}_p} \chi(\Phi(x)) \exp\frac{2\pi iax}{p}| \leq fp^{1/2}. \tag{4.1.2}$$

Доказательство. Неравенства (1) и (2) вытекают из результатов Вейля [165], см. также [105, гл.11-12].

В условиях предыдущей леммы имеет место следующая лемма 2.

Лемма 4.1.2. *Пусть $1 \leq p_1 \leq p_2 \leq p$, тогда*

$$|\sum_{x=p_1}^{p_2} \chi(\Phi(x))| \leq 2fp^{1/2}\log p.$$

Доказательство. Пусть $T \subseteq \{x \mid x \in \mathbb{Z},\ 0 \leq x \leq p-1\}$, тогда

$$\sum_{t\in T} \chi(\Phi(t)) = \frac{1}{p}\sum_{t\in T}\sum_{s=0}^{p-1}\sum_{a=0}^{p-1} \chi(\Phi(s)) \exp\frac{2\pi ia(s-t)}{p}.$$

В частности, при $T = [p_1, p_2]$, полагая

$$S := \sum_{x=p_1}^{p_2} \chi(\Phi(x)) \ \text{ и } \ F_a := \sum_{s=0}^{p-1} \chi(\Phi(s)) \exp\frac{2\pi ias}{p},$$

получим

$$|S| \leq \frac{1}{p}\sum_{a=0}^{p-1} |F_a| \cdot |\sum_{t=p_1}^{p_2} \exp(-\frac{2\pi iat}{p})| \tag{4.1.3}$$

В силу неравенств (1) и (2) леммы 1, из (3) следует, что

$$|S| < (f-1)p^{1/2} + fp^{-1/2}\sum_{a=1}^{p-1} \frac{|\sin(\pi a(p_1-p_2+1)p^{-1}|}{|\sin(\pi ap^{-1})|}$$

$$\leq (f-1)p^{1/2} + 2fp^{-1/2} \sum_{1\leq a\leq (p-1)/2} |\sin(\pi a p^{-1})|^{-1} \leq 2fp^{1/2}\log p,$$

так как $\sin x > 2x\pi^{-1}$ при $0 < x < \pi/2$.

Метод доказательства леммы 2 восходит к классическим работам И.М. Виноградова и Г. Полиа, ср. [105, гл. 12].

Переходя к доказательству теорем, положим

$$\zeta := \exp(\frac{2\pi i}{l}),\ \mu := \{\zeta^k | 1 \leq k < l\}$$

и

$$\mathfrak{m}_i := \{x | x \in \mathbb{F}_p,\ \Phi(x+i) = 0\},\ \mathfrak{m} := \bigcup_{1\leq i\leq s} \mathfrak{m}_i.$$

Пусть

$$f(y,\lambda) := \frac{1}{l}\prod_{k=1}^{l-1}(1 - \zeta^k\lambda^{-1}\chi(y))$$

при $y \in \mathbb{F}_p,\ \lambda \in \mu$ и

$$g(x,\varepsilon,\Phi) := \prod_{i=1}^{s} f(\Phi(x+i),\varepsilon_i).$$

Ясно, что

$$f(0,\lambda) = l^{-1},\ f(y,\lambda) = 1 \text{ при } \chi(y) = \lambda \text{ и } f(y,\lambda) = 0 \text{ при } \chi(y) \notin \{0,\lambda\}.$$

Поэтому $g(x,\varepsilon,\Phi) = 1$, если $\chi(\Phi(x+i)) = \varepsilon_i$ при $1 \leq i \leq s$; $g(x,\varepsilon,\Phi) = 0$, если $\chi(\Phi(x+i)) \notin \{0,\varepsilon_i\}$ для некоторого i в интервале $1 \leq i \leq s$; наконец, $0 \leq g(x,\varepsilon,\Phi) \leq 1$, если $\chi(\Phi(x+i)) = 0$ для некоторого i в интервале $1 \leq i \leq s$. Отсюда следует, что

$$E(\varepsilon,p_1,p_2,\Phi) = \sum_{x=p_1}^{p_2} g(x;\varepsilon,\Phi) - R$$

и потому

$$E(\varepsilon,p_1,p_2,\Phi) = \frac{p_2-p_1}{l^s} + \sum_{\beta\in B}\sum_{x=p_1}^{p_2} K(\beta)\chi(\prod_{i=1}^{s}\Phi(x+i)^{\beta_i}) - R \qquad (4.1.4)$$

с остаточным членом R, удовлетворяющим неравенству
$0 \leq R \leq | \mathfrak{m} | \leq fs$, где

$$B := \{\beta | \beta \in \mathbb{Z}^s \setminus \{0\},\ 0 \leq \beta_i \leq l-1 \text{ при } 1 \leq i \leq s\}$$

и $|K(\beta)| = l^{-s}$. Асимптотические формулы теорем 1 и 2 вытекают из формулы (4), оценки (1) леммы 1 и леммы 2.

4.2 О целых точках на плоскости с взаимно простыми координатами

Назовём подмножество точек T эвклидовой плоскости $\mathbb{R}^2$, удовлетворяющее условию

$$a \in T \Rightarrow \{ta | t \in \mathbb{R},\ 0 \leq t \leq 1\} \subseteq T,$$

звёздообразным. Ясно, что выпуклое множество, содержащее начало координат, звёздообразно (но обратное утверждение, разумеется, неверно). Зафиксируем звёздообразное множество T, $T \subseteq \mathbb{R}^2$; пусть $x \in \mathbb{R}_+$, положим

$$T(x) := \{x^{1/2} a | a \in T\},\ L(x) := (T(x) \cap \mathbb{Z}^2) \setminus \{0\},\ N(x) := |L(x)|$$

и

$$L_0(x) := \{a | a \in L(x),\ (a_1, a_2) = (1)\},\ N_0(x) := |L_0(x)|.$$

Обозначим, как обычно, дзета-функцию Римана через $\zeta(s)$.

Теорема 4.2.1. *В предположении гипотезы Римана, из асимптотической формулы*

$$N(x) = \lambda x + O(x^\alpha) \ \ при \ \ x \to \infty, \tag{4.2.1}$$

в которой $\{\lambda, \alpha\} \subseteq \mathbb{R}, \lambda > 0$ *и* $0 \leq \alpha \leq 1/2$, *следует асимптотическая формула*

$$N_0(x) = \frac{\lambda x}{\zeta(2)} + O_\gamma(x^\gamma) \ \ при \ \ x \to \infty \tag{4.2.2}$$

для любого γ *под условием* $\gamma > (2-\alpha)(5-4\alpha)^{-1}$.

Доказательство. Ясно, что

$$N(x) = \sum_{d=1}^{\infty} N_0(\frac{x}{d^2}),$$

и потому

$$N_0(x) = \sum_{d=1}^{\infty} \mu(d) N(\frac{x}{d^2}). \tag{4.2.3}$$

Пусть

$$N_y(x) := \sum_{d \le y} \mu(d) N(\frac{x}{d^2}) \ \text{ и } \ N^y(x) := \sum_{d > y} \mu(d) N(\frac{x}{d^2}) \ \text{ при } \ y > 0. \tag{4.2.4}$$

Тогда

$$N_0(x) = N_y(x) + N^y(x). \tag{4.2.5}$$

Из соотношений (1) и (4) следует, что

$$N_y(x) = \lambda x \sum_{d \le y} \mu(d) d^{-2} + O_\varepsilon(x^\alpha y^{1-2\alpha+\varepsilon}) \tag{4.2.6}$$

при $\varepsilon > 0$. Положим $B(k) := \sum\limits_{d \le k} \mu(d), \ k \in \mathbb{N}$. Как известно (см.,например, [163, гл. 14]), из гипотезы Римана следует, что

$$B(k) = O_\varepsilon(k^{1/2+\varepsilon}) \tag{4.2.7}$$

при $\varepsilon > 0$, и потому

$$\sum_{d > y} \mu(d) d^{-2} = O_\varepsilon(y^{-3/2+\varepsilon}). \tag{4.2.8}$$

С другой стороны,

$$N^y(x) = \sum_{d>y} (B(d) - B(d-1)) N(\frac{x}{d^2}) = -B([y]) N(\frac{x}{([y]+1)^2})$$

$$+ \sum_{d>y} B(d)(N(\frac{x}{d^2}) - N(\frac{x}{(d+1)^2})).$$

Ввиду неравенства

$$N(\frac{x}{d^2}) \ge N(\frac{x}{(d+1)^2}),$$

оценки (7) и формулы (1) отсюда следует, что

$$N^y(x) = O_\varepsilon(xy^{-3/2+\varepsilon}) + O_\varepsilon(\sum_{d>y} d^{1/2+\varepsilon}(N(\frac{x}{d^2}) - N(\frac{x}{(d+1)^2}))).$$

Но

$$\sum_{d>y} d^{1/2+\varepsilon}(N(\frac{x}{d^2}) - N(\frac{x}{(d+1)^2})) = \sum_{d>y} N(\frac{x}{d^2})(d^{1/2+\varepsilon} - (d-1)^{1/2+\varepsilon})$$

$$+[y]^{1/2+\varepsilon} N(\frac{x}{([y]+1)^2}) = O_\varepsilon(xy^{-3/2+\varepsilon})$$

и потому

$$N^y(x) = O_\varepsilon(xy^{-3/2+\varepsilon}). \tag{4.2.9}$$

Теорема 4 вытекает из соотношений (5), (6) и (9) при

$$y = x^{2(1-\alpha)/(5-4\alpha)}.$$

Замечание 1. Идея доказательства теоремы 4 восходит к [45]. Я доказал эту теорему в 1982-ом году [126], отвечая на вопрос Цагера, ср. [171], [141]. Мой результат был обобщён и усилен в работе [142].

Замечание 2. Предположим, что T - выпуклая область, ограниченная гладкой кривой с нигде не обращающейся в нуль кривизной, и $0 \in T$. Тогда, по теореме Хаксли [100], в формуле (1) можно взять $\alpha = 23/73$ и, следовательно, при $\gamma > 41/91$ имеет место формула (2) (теорема 4). В работе [101] показано, что для таких областей формула (2) имеет место уже при $\gamma > 5/12$.

4.3 О числе рациональных точек ограниченной высоты на одной кубической поверхности

В этом параграфе излагаются результаты, полученные в работе [96] в соавторстве с Хис-Брауном.

1. Рассмотрим открытое множество

$$U : X_0 \neq 0$$

на проективной кубической поверхности

$$S : X_0^3 = X_1X_2X_3.$$

Ясно, что

$$U(\mathbb{Q}) = \{[x] | x \in \mathbb{Z}^4,\ x_0 > 0,\ x_0^3 = x_1x_2x_3,\ \text{н.о.д.}\ (x_0, ..., x_3) = 1\},$$

где $[x] := \{tx | t \in \mathbb{Q}\}$ есть прямая в $\mathbb{Q}^4$, проходящая через точки 0 и x. Рассмотрим функцию

$$h\colon \mathbb{R}^n \to \mathbb{Z},\ h\colon x \mapsto \max\{|x_i|\ |1 \le i \le n\}.$$

Положим $h([x]) = h(x)$ при $[x] \in U(\mathbb{Q})$ и пусть

$$\mathcal{N}(H) := \text{card}\ \{y | y \in U(\mathbb{Q}),\ h(y) < H\}.$$

Теорема 4.3.1. *При $H \to \infty$ имеет место следующая асимптотическая формула:*

$$\mathcal{N}(H) = \frac{H(\log H)^6}{6!} \prod_{p \in P} l_p + O(H(\log H)^5), \tag{4.3.1}$$

где

$$l_p := (1 - \frac{1}{p})^7 (1 + \frac{7}{p} + \frac{1}{p^2}).$$

Теорема 1 показывает, что поверхность S удовлетворяет гипотезе В.В.Батырева и Ю.И.Манина [46], [145]. В этом параграфе приведёно элементарное доказательство теоремы 1, полученное в работе [96]. Более сильный результат получен в работе [53] аналитическими методами.

2. Докажем несколько вспомогательных утверждений. Пусть

$$w \in \mathbb{N}^3,\ \text{н.о.д.}\ (w_i, w_j) = 1 \text{ при } i \ne j \ \text{ и } \ Z \in (\mathbb{R}_+^*)^3;$$

положим

$$w_0 := w_1w_2w_3,\ Z_0 := Z_1Z_2Z_3,\ z_0 := \max\{Z_i^{-1/2} | 0 \le i \le 3\}$$

и

$$\mathfrak{m} := \{x | x \in \mathbb{N}^3, \text{ н.о.д. } (x_1, x_2, x_3) = 1,$$

$$x_i \leq Z_i \text{ и н.о.д. } (x_i, w_i) = 1 \text{ при } 1 \leq i \leq 3\}.$$

Определим три мультипликативные функции e, f и g по формулам:

$$f(n) = \prod_{p \in P, p|n} (1 - p^{-1})(1 - p^{-3})^{-1}, \; g(n) = \sum_{d|n} \mu(d)^2 d^{-1/2},$$

$$e(n) := \sum_{d|n} f(d)\mu(d)^2 \mu(\frac{n}{d}) \text{ при } n \in \mathbb{N}.$$

Ясно, что

$$f(p^n) = p^2(p^2 + p + 1)^{-1}, \; g(p^n) = 1 + p^{-1/2} \text{ при } p \in P, \; n \in \mathbb{N} \tag{4.3.2}$$

и

$$e(p) = f(p) - 1, \; e(p^2) = f(p), \; e(p^n) = 0 \text{ при } p \in P, \; n \in \mathbb{N} \setminus \{1, 2\}. \tag{4.3.3}$$

Лемма 4.3.1. *Имеет место следующая оценка*

$$|\mathfrak{m}| = \frac{Z_0}{\zeta(3)}(f(w_0) + O(g(w_0)z_0)).$$

Доказательство. Не нарушая общности, предположим, что $Z_i \geq 1$ при $1 \leq i \leq 3$. Положим

$$\mathfrak{m}_1(Z, w) := \{x | x \in \mathbb{N}^3, \; x_i \leq Z_i, \text{ н.о.д. } (x_i, w_i) = 1 \text{ при } 1 \leq i \leq 3\}$$

и

$$\mathfrak{a}(V, n) := \{v | v \in \mathbb{N}, \; v \leq V, \text{ н.о.д. } (v, n) = 1\},$$

так что

$$|\mathfrak{m}_1(Z, w)| = \prod_{i=1}^{3} |\mathfrak{a}(Z_i, w_i)|. \tag{4.3.4}$$

Но

$$|\mathfrak{a}(V, n)| = \sum_{1 \leq v \leq V, d|v, d|n} \mu(d) = \sum_{d|n} \mu(d)[\frac{V}{d}] = \sum_{d|n} \mu(d)(\frac{V}{d} + O(\frac{V^{1/2}}{d^{1/2}})),$$

ибо $[\theta] = \theta + O(\theta^{1/2})$ при $\theta \in \mathbb{R}_+$; следовательно,

$$|\mathfrak{a}(V,n)| = \frac{V\varphi(n)}{n} + O(V^{1/2}g(n)), \tag{4.3.5}$$

где $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|$ есть функция Эйлера. Пусть $0 \le a_i, b_i \le c_i$ при $1 \le i \le N,\ N \in \mathbb{N}$ и

$$c_0 := \max\{b_i^{1/2}c_i^{-1/2} | 1 \le i \le N\},$$

тогда

$$\prod_{i=1}^{N}(a_i + O(b_i)) = \prod_{i=1}^{N} a_i + O(c_0 \prod_{i=1}^{N} c_i). \tag{4.3.6}$$

Подставив (4) в (5) и воспользовавшись соотношением (6) с

$$a_i = Z_i\varphi(w_i)w_i^{-1},\ b_i = Z_i^{1/2}g(w_i),\ c_i = Z_i g(w_i),$$

получим

$$|\mathfrak{m}_1(Z,w)| = \prod_{i=1}^{3}(Z_i\varphi(w_i)w_i^{-1} + O(Z_i^{1/2}g(w_i)) = Z_0(\frac{\varphi(w_0)}{w_0} + O(g(w_0)z_0)).$$

Остаётся заметить, что

$$|\mathfrak{m}| = \sum_{d\in\mathbb{N}(w_0)} \mu(d)|\mathfrak{m}_1(\frac{Z}{d}, w)| =$$

$$Z_0(\frac{\varphi(w_0)}{w_0} \sum_{d\in\mathbb{N}(w_0)} \mu(d)d^{-3} + O(g(w_0)z_0 \sum_{d=1}^{\infty} d^{-5/2}))$$

и что

$$\frac{\varphi(w_0)}{w_0} \sum_{d\in\mathbb{N}(w_0)} \mu(d)d^{-3} = \frac{f(w_0)}{\zeta(3)},$$

где $\mathbb{N}(n) := \{v | v \in \mathbb{N},\ \text{н.о.д. } (v,n) = 1\}$ при $n \in \mathbb{N}$. Лемма доказана.

Введём следующие обоозначения. Пусть

$$J := \{(i,j) | (i,j) \in \mathbb{N}^2,\ i \le 3,\ j \le 3,\ i \ne j\}$$

и

$$J_1 := \{(i,j,k,l)|\{(i,j),(k,l)\} \subseteq J,\ (i,j) \neq (k,l)\};$$

ясно, что $|J| = 6$ и $|J_1| = 30$. Положим

$$y := (y_{12}, y_{13}, y_{21}, y_{23}, y_{31}, y_{32}),\ |y| := \prod_{(i,j)\in J} y_{ij} \text{ при } y \in \mathbb{R}^6$$

и $y := (..., y_{ijkl}, ...)$ при $y \in \mathbb{R}^{30}$, где (i,j,k,l) пробегает множество индексов J_1. Обозначим через $v(P)$ объём шестимерного полиэдра P, задаваемого следующими неравенствами:

$$y_{ij} \geq 0 \text{ при } (i,j) \in J;\ y_{12} + y_{13} + 2(y_{21} + y_{31}) \leq 1;$$

$$y_{21} + y_{23} + 2(y_{12} + y_{32}) \leq 1;\ y_{31} + y_{32} + 2(y_{13} + y_{23}) \leq 1.$$

Лемма 4.3.2. *Имеет место следующее равенство:*

$$v(P) = \frac{1}{4 \cdot 6!}.$$

Доказательство. См., например, [77].

Пусть $d \in \mathbb{N}^6,\ \delta \in \mathbb{N}^{30}$ и $(i,j) \in J$; положим

$$r_{ij}(d,\delta) := \min\{n|n \in \mathbb{N},\ d_{ij}|n,\ \delta_{ijkl}|n \text{ при } (i,j,k,l) \in J_1\}$$

и пусть $r(d,\delta) := \prod_{(i,j)\in J} r_{ij}(d,\delta)$. При $R \in \mathbb{N}$ положим

$$Q(R) := \{(d,\delta)|d \in \mathbb{N}^6,\ \delta \in \mathbb{N}^{30},\ r(d,\delta) = R\}$$

и

$$b(R) := \sum_{(d,\delta)\in Q(R)} \prod_{(i,j)\in J} e(d_{ij}) \prod_{(k,l,m,n)\in J_1} \mu(\delta_{klmn}).$$

Рассмотрим ряд Дирихле

$$\lambda(s) := \sum_{n=1}^{\infty} b(n) n^{-s}.$$

Лемма 4.3.3. *При $s \in \mathbb{C}_{1/2}$ ряд $\lambda(s)$ сходится абсолютно и*

$$\lambda(1) = \zeta(3) \prod_{p \in P} l_p. \tag{4.3.7}$$

Доказательство. Так как функция $b\colon \mathbb{N} \to \mathbb{Z}$ мультипликативна, рассматриваемый ряд разлагается в эйлерово произведение:

$$\lambda(s) := \prod_{p \in P} \lambda_p(s),\ \lambda_p(s) := \sum_{n=0}^{\infty} b(p^n) p^{-ns}.$$

Пусть $p \in P,\ n \in \mathbb{N},\ (d, \delta) \in Q(p^n),\ e(d_{ij}) \neq 0,\ \mu(\delta_{ijkl}) \neq 0,\ (i, j, k, l) \in J_1$, тогда

$$d_{ij} \in \{1, p, p^2\},\ \delta_{ijkl} \in \{1, p\},$$

и потому

$$r_{ij}(d, \delta) \in \{1, p, p^2\},\ r(d, \delta) \in \{p^n | 0 \leq n \leq 12\}.$$

Таким образом, $b(p^n) = 0$ при $n \geq 13$ и, значит,

$$\lambda_p(s) := \sum_{n=0}^{12} b(p^n) p^{-ns}. \tag{4.3.8}$$

С другой стороны, $b(p^n) = O(1)$ при $p \in P$ и $0 \leq n \leq 12$; поэтому из соотношения (8) следует, что

$$\lambda_p(s) = 1 + b(p) p^{-s} + O(p^{-2\sigma}),\ \sigma := Re\ s.$$

Пусть $(d, \delta) \in Q(p)$, тогда найдётся пара (i, j) под условием

$$(i, j) \in J,\ r_{ij}(d, \delta) = p,\ r_{kl}(d, \delta) = 1 \text{ при } (i, j, k, l) \in J_1.$$

Из этого условия следует, что $\delta_{klmn} = 1$ при $(i, j, k, l) \in J_1$ (так как $p | r_{kl}(d, \delta)$ и $p | r_{mn}(d, \delta)$ при $\delta_{klmn} = p$), следовательно, $d_{ij} = p$ и, значит, $|e(d_{ij})| = |e(p)| \leq p^{-1}$. Таким образом,

$$|b(p)| \leq \sum_{(d,\delta) \in Q(p)} \prod_{(i,j) \in J} |e(d_{ij})| = O(p^{-1}),$$

так что $\lambda_p(s) = 1 + O(p^{-1-\sigma} + p^{-2\sigma})$ и, значит, ряд $\lambda(s)$ абсолютно сходится при $s \in \mathbb{C}_{1/2}$.

Докажем тождество (7). Пусть $p \in P$; положим

$$I(p) := \bigcup_{0 \le n \le 12} Q(p^n),\ I_1(p) := \{x | x \in \mathbb{N}^6,\ 1 \le x_{ij} \le p^2 \text{ при } (i,j) \in J\}$$

и

$$I_2(d,\delta) := \{x | x \in I_1(p),\ r_{ij}(d,\delta) | x_{ij} \text{ при } (i,j) \in J\}.$$

Ясно, что

$$\text{card } \{x | x \in \mathbb{Z}/p^2\mathbb{Z},\ l | x\} = l^{-1}p^2 \text{ при } l \in \{1, p, p^2\};$$

поэтому

$$\lambda_p(1) = \sum_{(d,\delta) \in I(p)} \prod_{(i,j) \in J} e(d_{ij}) \prod_{(k,l,m,n) \in J_1} \mu(\delta_{klmn}) r(d,\delta)^{-1} =$$

$$p^{-12} \sum_{(d,\delta) \in I(p)} \prod_{(i,j) \in J} e(d_{ij}) \prod_{(k,l,m,n) \in J_1} \mu(\delta_{klmn}) |I_2(d,\delta)|,$$

или

$$p^{12}\lambda_p(1) = \sum_{x \in I_1(p)} \sum_{(d,\delta) \in I_4(p,x)} \prod_{(i,j) \in J} e(d_{ij}) \prod_{(k,l,m,n) \in J_1} \mu(\delta_{klmn}), \tag{4.3.9}$$

где

$$I_3(p) := \{y | y \in \mathbb{N}^{12},\ y_{ijkl} \in \{1, p\} \text{ при } (i,j,k,l) \in J_1\}$$

и

$$I_4(p,x) := \{(d,\delta) | d \in I_1(p),\ \delta \in I_3(p),\ d_{ij} | x_{ij},\ \delta_{ijkl} | x_{ij} \text{ при } (i,j,k,l) \in J_1\}.$$

Положим

$$I_5(p) := \{x | x \in I_1(p),\ \text{н.о.д. } (p, x_{ij}, x_{kl}) = 1 \text{ при } (i,j,k,l) \in J_1\}.$$

и

$$I_6(p,x) := \{d | d \in I_1(p),\ d_{ij} | x_{ij} \text{ при } (i,j) \in J\}.$$

Так как

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{при } n=1,\\ 0 & \text{при } n\neq 1\end{cases}$$

и

$$\sum_{d|p^l}e(d)=\begin{cases}1 & \text{при } l=0\\ f(p) & \text{при } l=1\\ 0 & \text{при } l\geq 2,\end{cases}$$

из условий суммирования в (9) следует, что

$$p^{12}\lambda_p(1)=\sum_{x\in I_5(p)}\sum_{d\in I_6(p,x)}\prod_{(i,j)\in J}e(d_{ij})=|I_7(p)|+|I_8(p)|f(p),$$

где

$$I_7(p):=\{x|x\in I_1(p),\ x_{ij}\neq 0 \bmod p \text{ при } (i,j)\in J\}$$

и

$$I_8(p):=\{x|x\in I_5(p),\ (\exists\ (i,j)\in J)\ p|x_{ij}\}.$$

Остаётся заметить, что $|I_7(p)|=(p^2-p)^6,\ |I_8(p)|=6(p^2-p)^5(p-1)$ и потому

$$\lambda_p(1)=p^{-12}((p^2-p)^6+6(p^2-p)^5(p-1)p^2(p^2+p+1)^{-1})=(1-p^{-3})^{-1}l_p,$$

откуда немедленно следует равенство (7). Лемма доказана.

Пусть $H>0$ и $r\in\mathbb{N}^6$. Рассмотрим подмножества $T_k(H),\ k\in\{0,1\}$, пространства $\mathbb{R}^6$, задаваемые неравенствами:

$$y_{ij}\geq 1+k \text{ при } (i,j)\in J;\ y_{12}y_{13}(y_{21}y_{31})^2\leq H;$$

$$y_{21}y_{23}(y_{12}y_{32})^2\leq H;\ y_{31}y_{32}(y_{13}y_{23})^2\leq H,$$

и положим

$$Q_k(H):=T_k(H)\cap\mathbb{Z}^6,\ S_k(H):=\sum_{y\in Q_k(H)}\frac{1}{|y|}.$$

Положим далее

$$Q_0(H,r):=\{y|y\in Q_0(H),\ r_{ij}|y_{ij} \text{ при } (i,j)\in J\}$$

и

$$S(H,r) := \sum_{y \in Q_0(H,r)} \frac{1}{|y|}.$$

Лемма 4.3.4. *При $H \to \infty$ имеет место следующая асимптотическая формула:*

$$S(H,r) = \frac{(\log H)^6}{4 \cdot 6! R} + O(R^{-3/4}(\log H)^5), \tag{4.3.10}$$

где $R := |r|$.

Доказательство. Положим

$$K_1(y) := \{x | x \in \mathbb{R}^6,\ y_{ij} \le x_{ij} \le y_{ij} + 1 \text{ при } (i,j) \in J\},$$

$$K_2(y) := \{x | x \in \mathbb{R}^6,\ y_{ij} - 1 \le x_{ij} \le y_{ij} \text{ при } (i,j) \in J\}$$

и

$$I(H) := \int\limits_{T_0(H)} \frac{dx}{|x|}.$$

Ясно, что

$$\int\limits_{K_1(y)} \frac{dx}{|x|} \le \frac{1}{|y|} \le \int\limits_{K_2(y)} \frac{dx}{|x|}$$

и потому

$$S_0(H) \le I(H) \le S_1(H).$$

Но

$$S_0(H) = S_1(H) + \sum_{(i,j) \in J} \sum_{y \in Q_{ij}(H)} \frac{1}{|y|},$$

где

$$Q_{ij}(H) := \{y | y \in Q_0(H),\ y_{ij} = 1\}$$

при $(i,j) \in J$, так что

$$S_0(H) \le S_1(H) + 6(\sum_{1 \le u \le H} \frac{1}{u})^5 = S_1(H) + O((\log H)^5)$$

и потому

$$S_0(H) = I(H) + O((\log H)^5).$$

Из равенства

$$I(H) = (\log H)^6 v(P)$$

и леммы 2 следует, что

$$S_0(H) = \frac{(\log H)^6}{4 \cdot 6!} + O((\log H)^5). \tag{4.3.11}$$

С другой стороны,

$$\{y | y_{ij} = r_{ij} z_{ij} \text{ при } (i,j) \in J,\ z \in Q_0(HR^{-2})\} \subseteq Q(H,r)$$

$$\subseteq \{y | y_{ij} = r_{ij} z_{ij} \text{ при } (i,j) \in J,\ z \in Q_0(H)\}$$

и потому

$$R^{-1} S_0(HR^{-2}) \leq S(H,r) \leq R^{-1} S_0(H). \tag{4.3.12}$$

Формула (10) следует из соотношений (11) и (12) при $\log R \ll \log H$; если же $r_{ij} > H$ для каких-либо i и j, то

$$S(H,r) = 0,\ R^{-1}(\log H)^6 \ll R^{-3/4}(\log H)^5$$

и формула (10) выполняется автоматически. Лемма доказана.

3. Переходя к доказательству теоремы 1, положим

$$A = \{x | x \in \mathbb{N}^4,\ \text{н.о.д. } (x_0, ..., x_3) = 1,\ x_0^3 = x_1 x_2 x_3\},$$

и

$$\mathcal{N}_0(H) := \text{card } \{x | x \in A,\ h(x) \leq H\}.$$

Ясно, что

$$\mathcal{N}(H) = 4\mathcal{N}_0(H). \tag{4.3.13}$$

Пусть $\{u, v\} \subseteq \mathbb{N}$; положим далее

$$B(u) := \{y | y \in \mathbb{N}^3,\ \text{н.о.д. } (y_1, y_2, y_3) = 1,\ y_1 y_2 y_3 = u^3,$$

$$(\forall\, p \in P) y_i \neq 0 \bmod p^3 \text{ при } 1 \leq i \leq 3\}$$

$$C(u,v) := \{(y,z)|y \in B(u),\ z \in \mathbb{N}^3,\ \text{н.о.д. } (z_1,z_2,z_3) = 1,\ z_1z_2z_3 = v,$$

$$\text{н.о.д. } (z_i,y_j,y_k) = 1 \text{ при } \{i,j,k\} = \{1,2,3\}\}$$

и заметим, что

$$C(u,v) \cap C(u',v') = \emptyset$$

при

$$\{u,v,u',v'\} \subseteq \mathbb{N},\ (u,v) \neq (u',v').$$

Пусть

$$C_0 := \bigcup_{\{u,v\}\subseteq\mathbb{N}} C(u,v);$$

определим биекцию $\alpha\colon C_0 \to A$ множеств C_0 и A, положив

$$\alpha(y,z) := (uv, y_1z_1^3, y_2z_2^3, y_3z_3^3) \text{ при } (y,z) \in C(u,v).$$

По построению,

$$\mathcal{N}_0(H) = \sum_{\{u,v\}\subseteq\mathbb{N}} \text{card } \{(y,z)|(y,z) \in C(u,v),\ h(\alpha(y,z)) \leq H\}. \tag{4.3.14}$$

Положим

$$B(u,H) := \{y|y \in B(u),\ h(y) \leq H\}$$

Соотношение (14) и лемма 1 с

$$Z_i := (H/y_i)^{1/3} \text{ при } 1 \leq i \leq 3,$$

дают

$$\mathcal{N}_0(H) = \mathcal{M}(H) + \mathcal{R}(H), \tag{4.3.15}$$

где

$$\mathcal{M}(H) := \frac{H}{\zeta(3)} \sum_{1\leq u\leq H} \frac{1}{u} \sum_{y\in B(u,H)} f(w_0(y)), \tag{4.3.16}$$

$$\mathcal{R}(H) \ll \sum_{i=1}^{3} \mathcal{R}_i(H),$$

$$\mathcal{R}_i(H) := H^{5/6} \sum_{1\le u\le H} \frac{1}{u} \sum_{y\in B(u,H)} g(w_0(y)) y_i^{1/6} \text{ при } 1 \le i \le 3 \qquad (4.3.17)$$

и

$$w_1(y) := \text{ н.о.д. } (y_2, y_3),\ w_2(y) := \text{ н.о.д. } (y_1, y_3),$$

$$w_3(y) := \text{ н.о.д. } (y_1, y_2),\ w_0(y) := \prod_{i=1}^{3} w_i(y) \text{ при } y \in \mathbb{N}^3.$$

Для каждого y из $B(u)$ найдётся 6 попарно взаимно простых свободных от квадратов чисел $y_{ij},\ (i,j) \in J$, под условием:

$$y_1 = y_{12}y_{13}(y_{21}y_{31})^2,\ y_2 = y_{21}y_{23}(y_{12}y_{32})^2,\ y_3 = y_{31}y_{32}(y_{13}y_{23})^2,$$

так что

$$w_0(y) := \prod_{(i,j)\in J} y_{ij}.$$

Положим

$$J_2 := \{(1,2),\ (1,3),\ (2,1),\ (2,3)\},$$

$$g_1(y) := \prod_{(i,j)\in J_2} g(y_{ij}),\ g_2(y) := g_1(y)g(y_{31}y_{32})$$

и

$$Q_2(H) := \{(y_{12}, y_{13}, y_{21}, y_{23}) | y_{ij} \in \mathbb{N},\ y_{ij} \le H \text{ при } (i,j) \in J_2\ \}.$$

Из (17), в частности, следует, что

$$\mathcal{R}_3(H) \ll H^{5/6} \sum_{y\in Q_0(H)} \frac{g_2(y)}{y_{12}y_{21}(y_{13}y_{23})^{2/3}(y_{31}y_{32})^{5/6}} =$$

$$H^{5/6} \sum_{y\in Q_2(H)} \frac{g_1(y)}{y_{12}y_{21}(y_{13}y_{23})^{2/3}} S_2(H(y_{13}y_{23})^{-2}),$$

где

$$S_2(Y) := \sum_{n\le Y} g(n)\tau(n)n^{-5/6} \text{ и } \tau(n) := \sum_{d|n} 1.$$

Легко видеть, что

$$S_2(Y) \ll Y^{1/6} \log Y$$

и потому

$$\mathcal{R}_3(H) \ll H\log H \sum_{y\in Q_2(H)} \frac{g_1(y)}{y_{12}y_{21}y_{13}y_{23}} =$$

$$H\log H(\sum_{n\le H} g(n)/n)^4 \ll H(\log H)^5.$$

Точно также доказываются оценки

$$\mathcal{R}_1(H) \ll H(\log H)^5,\ \mathcal{R}_2(H) \ll H(\log H)^5.$$

Таким образом, равенство (15) принимает следующий вид:

$$\mathcal{N}_0(H) = \mathcal{M}(H) + O(H(\log H)^5). \tag{4.3.18}$$

Остаётся вычислить $\mathcal{M}(H)$. Положим

$$Q_3(H) := \{y|y \in Q_0(H),\ \text{н.о.д. } (y_{ij}, y_{kl}) = 1 \text{ при } (i,j,k,l) \in J_1\ \}$$

и пусть

$$Q_3(H,d) := Q_3(H) \cap Q_0(H,d) \ \text{ при } \ d \in \mathbb{N}^6.$$

В новых переменных $\{y_{ij}|(i,j) \in J\}$ определение (16) переписывается следующим образом:

$$\mathcal{M}(H) = H\zeta(3)^{-1} \sum_{y\in Q_3(H)} \frac{1}{|y|} \prod_{(i,j)\in J} \mu(y_{ij})^2 f(y_{ij}),$$

или

$$\mathcal{M}(H) = H\zeta(3)^{-1} \sum_{y\in Q_3(H)} \frac{1}{|y|} \prod_{(i,j)\in J} \sum_{d|y_{ij}} e(d),$$

так как

$$\mu(n)^2 f(n) = \sum_{d|n} e(d) \text{ при } n \in \mathbb{N}.$$

Таким образом,

$$\mathcal{M}(H) = H\zeta(3)^{-1} \sum_{d\in\mathbb{N}^6} \frac{1}{|y|} \prod_{(i,j)\in J} e(d_{ij}) S_3(H,d)$$

с

$$S_3(H,d) := \sum_{y\in Q_3(H,d)} \frac{1}{|y|} = \sum_{\delta\in\mathbb{N}^{30}} \prod_{(k,l,m,n)\in J_1} \mu(\delta_{klmn}) \sum_{y\in Q_0(H,r(d,\delta))} \frac{1}{|y|},$$

так что

$$\mathcal{M}(H) = H\zeta(3)^{-1} \sum_{d\in\mathbb{N}^6} \sum_{\delta\in\mathbb{N}^{30}} S(H, r(d,\delta)) \prod_{(i,j)\in J} \prod_{(k,l,m,n)\in J_1} e(d_{ij})\delta_{klmn}.$$

Из этого соотношения и леммы 4 следует, что

$$\mathcal{M}(H) = \frac{\lambda(1)H(\log H)^6}{4\cdot 6!\zeta(3)} + O(|\lambda(3/4)|H(\log H)^5)$$

и потому, в силу леммы 3,

$$\mathcal{M}(H) = \frac{H(\log H)^6}{4\cdot 6!} \prod_{p\in P} l_p + O(H(\log H)^5). \tag{4.3.19}$$

Асимптотическая формула (1) является простым следствием соотношений (13), (18) и (19). Теорема доказана.

4.4 О представлении больших целых чисел положительно определёнными квадратичными формами

1. Пусть $f(x)$ - невырожденная целочисленная примитивная квадратичная форма от $k \geq 2$ переменных. Вопрос о разрешимости уравнения

$$f(x) = m,\ m \in \mathbb{Z}, \tag{4.4.1}$$

в целых числах - одна из старейших классических проблем теории чисел. Арифметика бинарных квадратичных форм изучается методами алгебраической теории чисел (квадратичные поля). При $k \geq 4$ распределение целых точек на квадриках вида (1) можно исследовать как круговым методом (см., например, [19, гл. I-III], [20], [31], [93]), так и методами теории модулярных форм [42], [104, гл. 11]. При $k = 3$ решить рассматриваемую задачу круговым методом пока не удаётся. Много интересных результатов о представлении целых чисел тернарными квадратичными формами было получено в работах

Ю.В. Линника и его учеников, см., например, [18], [17], [19, гл. IV-V], [21]. В середине 1980-ых годов Х. Иванец [103] (ср. [3]) получил новые оценки коэффициентов Фурье параболических форм полуцелого веса, позволяющие полностью решить поставленную задачу для положительно определённых тернарных квадратичных форм [69], [9], [71], [10]. В последние годы интересные результаты получены и в исследованной Ю.В. Линником и Б.Ф. Скубенко [17, гл. V-VI] задаче о распределении целых точек на двумерных гиперболоидах, см., например, [69], [55], [70].

Прочитав работы [103], [69], [9], [42], я написал небольшой обзор [134], задуманный как введение в современную аналитическую теорию квадратичных форм, и короткую заметку [135], в которой мне удалось дать простое доказательство одной теоремы Д.Р. Хис-Брауна [92] (см. следствие 2 в no. 2). Слегка отредактированный вариант обзора [134] и составляет содержание этого параграфа.

2. Рассмотрим множество

$$\mathcal{A}_k := \{A | A \in M_k(\mathbb{Z}),\ A^t = A,\ 2|a_{ii} \text{ при } 1 \leq i \leq k,\ |A| > 0\}$$

симметричных положительных целочисленных матриц с чётной главной диагональю, положим

$$f_A(x) := \frac{1}{2} x^t A x,\ d(f_A) := |A|,\ N(f_A) := \min\{n | n \in \mathbb{N},\ nA^{-1} \in \mathcal{A}_k\}$$

и

$$\nu(f_A) := \text{ card } \{C | C \in \mathrm{GL}_k(\mathbb{Z}),\ C^t A C = A\}$$

при $A \in \mathcal{A}_k$. Ясно, что $f_A(x) \in \mathbb{Z}[x]$ и f_A есть положительно определённая квадратичная форма ранга k. Числа $d(f_A)$ и $N(f_A)$ суть дискриминант и ступень квадратичной формы f_A. Заметим, что $2|d(f_A)$ и $4|N(f_A)$ при нечётном k (пользуюсь случаем поблагодарить В.А. Гриценко [11] за простое доказательство этого утверждения).

При $n \in \mathbb{N},\ A \in \mathcal{A}_k$ и $f := f_A$ квадрика

$$E_{f,n} : f(x) = n$$

определена над $\mathbb{Z}$; положим

$$r_f(n) := |E_{f,n}(\mathbb{Z})|.$$

Пусть $l := (k-1)$ и $\omega \subseteq S_l$; определим проекцию

$$\pi \colon \mathbb{R}^k \setminus \{0\} \to S_l,\ \pi \colon x \mapsto (2f(x))^{-1/2} A^{1/2} x$$

и положим

$$r_f(n, \omega) := |E_{f,n}(\mathbb{Z}) \cap \pi^{-1}(\omega)|.$$

Ясно, что $r_f(n, S_l) = r_f(n)$; по определению, $r_f(n)$ есть число целых точек на l - мерном эллипсоиде $E_{f,n}(\mathbb{R})$. Пусть

$$\mathcal{A}_k^{(0)} := \{A | A \in \mathcal{A}_k,\ (\{a_{ij}, \frac{1}{2}a_{ii} |\ 1 \leq i, j \leq k\}) = (1)\};$$

обозначим через

$$\mathcal{F}_k := \{f_A | A \in \mathcal{A}_k^{(0)}\}$$

множество положительно определённых примитивных квадратичных форм ранга k. Пусть $\{f_A, f_B\} \subseteq \mathcal{F}_k$; говорят, что квадратичные формы f_A и f_B принадлежат одному классу (являются эквивалентными), если

$$(\exists\, C \in \mathrm{GL}_k(\mathbb{Z}))\ C^t A C = B,$$

и что f_A и f_B принадлежат одному роду, если

$$(\forall\, p \in \mathcal{P})\ (\exists\, C \in \mathrm{GL}_k(\mathbb{Z}_p))\ C^t A C = B.$$

Обозначим через $\mathcal{K}_k$ множество классов и через $\mathcal{G}_k$ множество родов квадратичных форм $f,\ f \in \mathcal{F}_k$. Пусть $G \in \mathcal{G}_k$; как известно,

$$(\exists\, h \in \mathbb{N})\ G = \bigcup_{1 \leq i \leq h} K_i \text{ с } \{K_i | 1 \leq i \leq h\} \subseteq \mathcal{K}_k.$$

Ясно, что

$$r_f(n) = r_g(n) \text{ и } \nu(f) = \nu(g) \text{ при } \{f, g\} \subseteq K,\ K \in \mathcal{K}_k,\ n \in \mathbb{N}.$$

Более того,

$$d(f) = d(g) \text{ и } N(f) = N(g) \text{ при } \{f, g\} \subseteq G,\ G \in \mathcal{G}_k.$$

При $f \in K,\ K \in \mathcal{K}_k,\ n \in \mathbb{N}$ положим $r(K, n) := r_f(n)$ и $\nu(K, n) := \nu_f(n)$. Пусть

$$G \in \mathcal{G}_k \text{ и } G = \bigcup_{1 \le i \le h} K_i \text{ с } \{K_i | 1 \le i \le h\} \subseteq \mathcal{K}_k;$$

следуя Зигелю [159], положим

$$r(G, n) := (\sum_{i=1}^{h} \frac{r(K_i, n)}{\nu(K_i, n)})(\sum_{i=1}^{h} \frac{1}{\nu(K_i, n)})^{-1}.$$

Пусть $f \in \mathcal{F}_k,\ k \ge 3,\ n \in \mathbb{N}$ и $p \in \mathcal{P}$. Положим далее

$$\alpha(p, n) := \lim_{a \to \infty} p^{-a(k-1)}\ |E_{f,n}(\mathbb{Z}/p^a\mathbb{Z})|,$$

$$\alpha_0(f, n) := \prod_{p \in \mathcal{P}} \alpha(p, n) \text{ и } \alpha_\infty(f) := \frac{(2\pi)^{k/2}}{d(f)^{1/2}\Gamma(k/2)}.$$

При $f \in G,\ G \in \mathcal{G}_k$ положим $\text{gen } f := G$.

Теорема 4.4.1. *Пусть $k \ge 3,\ f \in \mathcal{F}_k$ и $n \in \mathbb{N}$. Тогда*

$$r(gen\ f, n) = n^{k/2-1}\alpha_\infty(f)\alpha_0(f, n). \tag{4.4.2}$$

Более того,

(i) если $k \ge 5$ и $(\forall\ p \in \mathcal{P})\ E_{f,n}(\mathbb{Z}_p) \ne \emptyset$, то $1 \ll_f \alpha_0(f, n) \ll_f 1$;

(ii) если $k = 4$ и

$$(\forall\ p \in \mathcal{P})\ (\exists\ x \in E_{f,n}(\mathbb{Z}_p))\ \nabla f(x) \ne 0\ (mod\ p),$$

где $\nabla f := (\frac{\partial f}{\partial x_1}, ..., \frac{\partial f)}{\partial x_k})$, то

$$n^{-\varepsilon} \ll_{\varepsilon,f} \alpha_0(f, n) \ll_{\varepsilon,f} n^{\varepsilon} \text{ при } \varepsilon > 0;$$

(iii) если $k = 3$, $(n, d(f)) = (1)$ *и* $(\forall\, p \in \mathcal{P})\ E_{f,n}(\mathbb{Z}_p) \neq \emptyset$, *то*

$$n^{-\varepsilon} \ll_{\varepsilon,f} \alpha_0(f,n) \ll_{\varepsilon,f} n^{\varepsilon} \text{ при } \varepsilon > 0.$$

Доказательство. Равенство (2) есть известная теорема Зигеля [159] (см. также [71]). Утверждения (i) и (ii) доказаны, например, в работе Хис-Брауна [93] (см. также [19]); заметим, что в работах по круговому методу функция $\alpha_0(f,n)$ называется сингулярным рядом, а функция $\alpha_\infty(f)$ - сингулярным интегралом задачи. Утверждение (iii) доказано, например, в работе [71]; заметим, что константа в оценке $\alpha_0(f,n) \gg_{\varepsilon,f} n^{-\varepsilon}$ не является эффективно вычислимой, так как при доказательстве этой оценки используется теорема Зигеля о числе классов мнимых квадратичных полей.

Теорема 4.4.2. *Пусть* $k \geq 4$, $f \in \mathcal{F}_k$, $n \in \mathbb{N}$, $(n, N(f)) = (1)$ *и*

$$\delta < \begin{cases} 1/2, & \text{если } 2|k \\ 2/7, & \text{если } (2,k) = (1). \end{cases}$$

Тогда

$$r_f(n) = r(gen\ f, n) + O_{\delta,f}(n^{k/4-\delta}).$$

Более слабую оценку

$$r_f(n) = r(\text{gen } f, n) + O_{\varepsilon,f}(n^{k/4-1/4+\varepsilon}),$$

при $k \geq 4$ и $\varepsilon > 0$, можно доказать для произвольного n, без ограничения $(n, N(f)) = (1)$ (см., например, [19], [93], [104, гл. 11]).

Обозначим через

$$\mathbb{N}_{sf} := \{n | n \in \mathbb{N},\ \forall\, (p \in \mathcal{P})\ n \neq 0(p^2)\}$$

множество всех свободных от квадратов натуральных чисел.

Теорема 4.4.3. *Пусть* $f \in \mathcal{F}_3$, $n \in \mathbb{N}$ *и* $\varepsilon > 0$. *Предположим, что* $(n, N(f)) = (1)$ *и выполнено одно из двух условий:*

$$(\forall\, m \in \mathbb{N})\ n \neq m^2$$

или

$$N(f)/4 \in \mathbb{N}_{sf}.$$

Тогда

$$r_f(n) = r(gen\ f, n) + O_{\varepsilon,f}(n^{1/2-1/28+\varepsilon}).$$

Следствие 4.4.1. *Пусть* $f(x) = x_1^2 + x_2^2 + p^3x_3^2,\ p \in \mathcal{P},\ n \in \mathbb{N}$ *и* $\varepsilon > 0$. *Предположим, что* $p = 5\ (8)$ *и* $n = 7\ (8)$. *Тогда*

$$r_f(n) \gg_{\varepsilon,p} n^{1/2-\varepsilon}.$$

Будем называть натуральное число n квадратично полным, если

$$(\forall\ p \in \mathcal{P})\ p|n\ \Rightarrow\ p^2|n.$$

Следствие 4.4.2. *Любое достаточно большое натуральное число есть сумма двух квадратов и квадратично полного числа.*

Доказательство. Положим

$$\mathbb{N}_7 := \{4^{l-1}(8m-1)|\{l,m\} \subseteq \mathbb{N}\}.$$

По теореме Гаусса, любое натуральное число, не принадлежащее множеству $\mathbb{N}_7$, есть сумма трёх квадратов. Пусть $n \in \mathbb{N}_7$. Если $4|n$ и $n > 7^3$, то $n-7^3$ есть сумма двух квадратов; с другой стороны, из следствия 1 вытекает, что число $8m-1$ представимо квадратичной формой $x_1^2 + x_2^2 + 125x_3^2$ при достаточно большом m.

Следствие 2 есть теорема Хис-Брауна [92]; в той же работе [92] формулируется гипотеза о представимости всех достаточно больших чисел вида $8m+7,\ m \in \mathbb{N}$, квадратичной формой

$$f(x) = x_1^2 + x_2^2 + 125x_3^2$$

и отмечается, что из этой гипотезы легко вывести следствие 2. Впоследствии эта проблема подробно обсуждалась в одной работе Бломера [47].

Обозначим через λ_l меру Лебега на сфере S_l, $l \in \mathbb{N}$, под условием $\lambda_l(S_l) = 1$ и пусть

$$\Omega := \{\omega | \omega \subseteq S_l,\ \partial\omega \text{ есть гладкое } (l-1) - \text{мерное многообразие}\}.$$

Теорема 4.4.4. *Пусть*

$$k \geq 3,\ f \in \mathcal{F}_k,\ n \in \mathbb{N},\ (n, 2d(f)) = (1),\ l := (k-1),\ \omega \in \Omega,\ \varepsilon > 0$$

и

$$\alpha(k) = \begin{cases} (k-2)(3k+2)^{-1} & \text{при } 2|k, \\ |k - 73/24|(3k+3)^{-1} & \text{при } (2,k) = (1). \end{cases}$$

Тогда

$$r_f(n, \omega) = \lambda_l(\omega) r_f(n) + O_{\varepsilon, f}(n^{k/2-1-\alpha(k)+\varepsilon}).$$

Теоремы 2 и 3 и вытекающее из теоремы 3 следствие 1 будут доказаны в no. 3; теорема 4 доказывается в no. 4.

3. Пусть $N \in \mathbb{N}$. Положим, как обычно,

$$\Gamma_0(N) := \{\gamma | \gamma \in \mathrm{SL}_2(\mathbb{Z}),\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ c = 0 \pmod N\},$$

$$H := \{x + iy | x \in \mathbb{R},\ y \in \mathbb{R}_+^*\}$$

и

$$\gamma z := (az+b)(cz+d)^{-1} \text{ при } z \in \mathbb{C} \cup \{i\infty\},\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Введём в рассмотрение обобщённый символ Якоби:

$$\mathbb{Z}^2 \to \{0, \pm 1\},\ (c, d) \mapsto (\frac{c}{d})$$

(см., например, [157]) и положим

$$\varepsilon_d = \begin{cases} 1 & \text{при } d = 1(4), \\ i & \text{при } d = -1(4). \end{cases}$$

Пусть $4|N$ при нечётном k и χ - характер Дирихле по модулю N. Положим

$$v_k(\chi,\gamma)=\begin{cases}\chi(d), & \text{если } 2|k\\ \chi(d)\,\varepsilon_d^{-k}\,(\frac{c}{d})^k, & \text{если } (2,k)=(1)\end{cases}$$

при $\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $\gamma\in\Gamma_0(N)$. Функция $\varphi\colon H\to\mathbb{C}$, регулярная в полуплоскости H и в параболических вершинах группы $\Gamma_0(N)$ и удовлетворяющая условию

$$\varphi(\gamma z)=v_k(\chi,\gamma)(cz+d)^{k/2}\varphi(z)$$

при $\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $\gamma\in\Gamma_0(N)$ и $z\in H$, называется $\Gamma_0(N)$ - модулярной формой веса $k/2$ с характером χ. Обозначим через $M_{k/2}(N,\chi)$ множество всех таких форм; как известно, $M_{k/2}(N,\chi)$ есть конечномерное векторное пространство над полем $\mathbb{C}$. Обозначим через $S_{k/2}(N,\chi)$ подпространство параболических форм пространства $M_{k/2}(N,\chi)$ и положим

$$\varphi(z)=\sum_{n=1}^{\infty}a(\varphi,n)e^{2\pi inz}\ \text{ при }\ \varphi(z)\in S_{k/2}(N,\chi);$$

пространство $S_{k/2}(N,\chi)$ является унитарным векторным пространством со скалярным произведением, определяемым по формуле

$$<\varphi_1|\varphi_2>:=\int\limits_{\Gamma_0(N)\backslash H}y^{k-2}\varphi_1(z)\overline{\varphi_2(z)}dxdy$$

при $\{\varphi_1,\varphi_2\}\subseteq S_{k/2}(N,\chi)$ и $||\varphi||:=<\varphi|\varphi>^{1/2}$. Положим

$$g(k):=\dim\,S_{k/2}(N,\chi).$$

Пусть $f\in\mathcal{F}_k$. Положим $D(f):=d(f)$ при $4|k$, $D(f):=-d(f)$ при $k=2$ (4) и $D(f)=d(f)/2$ при нечётном k; пусть

$$\chi_f(n)=(\frac{D(f)}{n}).$$

Положим далее

$$\theta(f,z) := \sum_{n=1}^{\infty} r_f(n) e^{2\pi i n z} \text{ и } \theta(G,z) := \sum_{n=1}^{\infty} r(G,n) e^{2\pi i n z}$$

при $G \in \mathcal{G}_k$ и $z \in H$.

Лемма 4.4.1. *Пусть $k \geq 3$ и $f \in \mathcal{F}_k$. Тогда*

$$\theta(f,z) \in M_{k/2}(N(f), \chi_f)$$

и, более того,

$$\theta(f,z) - \theta(gen\ f, z) \in S_{k/2}(N(f), \chi_f).$$

Доказательство. Это хорошо известное утверждение, восходящее к работам Гекке, Шёнеберга, Пфетцера [146] и Зигеля [159].

При $n \in \mathbb{N}$ положим

$$\tau(n) := \sum_{\delta | c} 1.$$

Лемма 4.4.2. *Пусть $\{k, N\} \subseteq \mathbb{N}$, χ - характер Дирихле по модулю N и $\varphi(z) \in S_k(N, \chi)$. Если параболическая форма $\varphi(z)$ является общей собственной функцией семейства операторов Гекке*

$$\{T_p | p \in \mathcal{P},\ (p, N) = (1)\},$$

то

$$|a(\varphi, n)| \leq |a(\varphi, 1)| \tau(n) n^{(k-1)/2} \text{ при } (n, N) = (1).$$

Доказательство. Это утверждение следует из теоремы Делиня [63, теорема (8.2)] при $k \geq 2$ и из теоремы Делиня и Серра при $k = 1$ [64].

Введём в рассмотрение суммы Клостермана

$$K_k(\chi; n, c) := \sum_{d \in (\mathbb{Z}/c\mathbb{Z})^*} v_k(\chi, \gamma) \exp(\frac{2\pi i n (d + d^{-1})}{c}),$$

где $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\gamma \in \Gamma_0(N)$.

Лемма 4.4.3. *Пусть* $\{k, N\} \subseteq \mathbb{N}$, χ - *характер Дирихле по модулю* N *и* $k > 4$. *Тогда для любого ортонормированного базиса*

$$\{\varphi_j | \varphi_j(z) = \sum_{n=1}^{\infty} a_j(n) e^{2\pi i n z},\ 1 \leq j \leq g(k)\}$$

пространства $S_{k/2}(N, \chi)$ *имеет место равенство*

$$\sum_{j=1}^{g(k)} |a_j(n)|^2 = \frac{(4\pi n)^{k/2-1}}{\Gamma(k/2-1)}(1 + 2\pi(-i)^k \sum_{c \in \mathbb{N}, N|c} \frac{K_k(\chi; n, c)}{c} J_{k/2-1}(\frac{4\pi n}{c})), \quad (4.4.3)$$

где $J_\nu(z)$ *есть функция Бесселя.*

Доказательство. Следуя [148, уравнение (5.1.9)], положим

$$G_{k,m}(z) := \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} v_k(\chi, \gamma)(cz + d)^{-k/2} e^{2\pi i m \gamma z},\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

где $\Gamma_\infty := \{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} | n \in \mathbb{Z}\}$. Пусть $m \in \mathbb{N}$, тогда

$$G_{k,m} \in S_{k/2}(N, \chi) \text{ и } G_{k,m}(z) = \sum_{n=1}^{\infty} A_m(n) e^{2\pi i n z},$$

где

$$A_m(n) := \delta_{mn} + 2\pi e^{-ik\pi/4} (\frac{n}{m})^{k/2-1} \sum_{c \in \mathbb{N}, N|c} \frac{W(n, m; c)}{c} J_{k/2-1}(\frac{4\pi (mn)^{1/2}}{c}) \quad (4.4.4)$$

и

$$W(n, m; c) := \sum_{\gamma \in \Gamma_0(N)} v_k(\chi, \gamma) \exp(\frac{2\pi i (ma + nd)}{c}),\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad (4.4.5)$$

см. [148, теорема 5.1.2 и равенство (5.3.32)]. Более того, при

$$\varphi(z) = \sum_{n=1}^{\infty} a(\varphi, n) e^{2\pi i n z},\ \varphi \in S_k(N, \chi)$$

из теоремы 5.3.2 в [148] следует, что

$$< \varphi | G_{k,m} >= \frac{\Gamma(k/2-1)}{(4\pi m)^{k/2-1}} a(\varphi, m).$$

Таким образом,

$$G_{k,m} = \sum_{j=1}^{g(k)} < G_{k,m}|\varphi_j > \varphi_j = \frac{\Gamma(k/2-1)}{(4\pi m)^{k/2-1}} \sum_{j=1}^{g(k)} \overline{a_j(m)}\varphi_j$$

и, значит,

$$A_m(n) = \frac{\Gamma(k/2-1)}{(4\pi m)^{k/2-1}} \sum_{j=1}^{g(k)} \overline{a_j(m)}a_j(n). \tag{4.4.6}$$

Равенство (3) вытекает из определения сумм Клостермана и соотношений (4) - (6) при $m = n$. Лемма доказана.

Лемма 4.4.4. *Имеет место следующее неравенство:*

$$K_k(\chi; n, c) \leq \tau(n)\ (н.о.д.\ (n,c))^{1/2} c^{1/2}. \tag{4.4.7}$$

Доказательство. При нечётных k суммы Клостермана сводятся к суммам Салье, и оценка (7) может получена элементарными методами (см., например, [103]). При чётных k это неравенство впервые доказал А. Вейль [165].

При $Q \in \mathbb{N}$ и $|\nu| \leq 1$ положим

$$\mathcal{K}_Q^{(\nu)}(\chi; n, x) := \sum_{Q|c,\ c\leq x} c^{-1/2} K_k(\chi; n, c) \exp(\frac{4\pi\nu i}{c}).$$

Пусть $P \in \mathbb{R}_+$ и

$$\mathcal{Q}(P) := \{pN | p \in \mathcal{P},\ P < p \leq 2P,\ (p, 2n) = (1)\}$$

Лемма 4.4.5. *Пусть* $D \in \mathbb{N},\ k = 2l+1,\ l \in \mathbb{N} \setminus \{1\},\ 8|N,\ D|N$ *и*

$$\chi \colon \mathbb{Z} \to \{0, \pm 1\},\ \chi \colon m \mapsto (\frac{D}{m}).$$

Если $n \in \mathbb{N}_{sf}$ *и* $(n, N) = (1)$, *то*

$$\sum_{Q\in\mathcal{Q}(P)} |\mathcal{K}_Q^{(\nu)}(\chi; n, x)| \ll (xP^{-1/2} + xn^{-1/2} +$$

$$(x+n)^{5/8}(x^{1/4}P^{3/8} + n^{1/8}x^{1/8}P^{1/4}))\tau(n)\log n. \tag{4.4.8}$$

Доказательство. Из условия $D|N$ следует, что

$$K_k(\chi;n,c)=\sum_{d\in(\mathbb{Z}/c\mathbb{Z})^*}(\frac{D}{d})\,\varepsilon_d^{-k}\,(\frac{c}{d})\exp(\frac{2\pi in(d+d^{-1})}{c})=$$

$$D^{-1}\sum_{d\in(\mathbb{Z}/Dc\mathbb{Z})^*}\varepsilon_d^{-k}\,(\frac{Dc}{d})\exp(\frac{2\pi inD(d+d^{-1})}{Dc})=D^{-1}K_k(1;Dn,Dc).$$

Так как, не нарушая общности, можно предположить, что D и потому Dn свободны от квадратов, оценка (8) следует из теоремы Иванца [103, теорема 3].

Лемма 4.4.6. *Пусть* $k=2l+1,\ l\in\mathbb{N}\setminus\{1\},\ 4|N$ *и* χ *- характер Дирихле по модулю* N*. Тогда найдётся ортонормированный базис*

$$\{\varphi_j|\varphi_j(z)=\sum_{n=1}^{\infty}a_j(n)e^{2\pi inz},\ 1\le j\le g(k)\}$$

пространства $S_{k/2}(N,\chi)$ *такой, что*

$$a(\varphi,m^2t)\ll_\varepsilon m^{k/2-1+\varepsilon}\,(\sum_{n=1}^{g(k)}|a_j(t)|^2)^{1/2}||\varphi|| \tag{4.4.9}$$

при $\varepsilon>0,\ \varphi\in S_{k/2}(N,\chi),\ t\in\mathbb{N}_{sf}$ *и* $(m,N)=(1),\ m\in\mathbb{N}$.

Доказательство. Рассмотрим ортонормированный базис общих собственных функций

$$\{\varphi_j|\varphi_j(z)=\sum_{n=1}^{\infty}a_j(n)e^{2\pi inz},\ 1\le j\le g(k)\}$$

семейства операторов Гекке

$$\{T_p|p\in\mathcal{P},\ (p,N)=(1)\}$$

пространства $S_{k/2}(N,\chi)$. При $t\in\mathbb{N}_{sf}$ и $1\le j\le g(k)$ положим

$$\sum_{n=1}^{\infty}A_j(t,n)n^{-s}:=L(s-l+1,\psi_t)\sum_{n=1}^{\infty}a_j(tn^2)n^{-s}$$

и

$$\Phi_j(t,z):=\sum_{n=1}^{\infty}A_j(t,n)e^{2\pi inz},$$

где

$$\psi_t(m) := \chi(m)(\frac{t}{m})(\frac{-1}{m})^l \text{ и } L(s,\psi_t) := \sum_{n=1}^{\infty} \psi_t(n) n^{-s}.$$

Как известно (см., например, [59, теорема 4.3], $\Phi_j(t,z) \in S_{2l}(N,\chi^2)$; более того [59, предложение 5.1], параболическая форма $\Phi_j(t,z)$ является общей собственной функцией семейства операторов Гекке

$$\{T_p | p \in \mathcal{P},\ (p,N) = (1)\}.$$

Поэтому из леммы 2 следует, что

$$|a_j(tm^2)| = |\sum_{d|m} \mu(d)\psi_t(d) d^{l-1} A_j(t, n/d)| \le \sum_{d|m} d^{l-1} |A_j(t,n/d)| \le$$

$$|A_j(t,1)| \tau(m) \sum_{d|m} d^{l-1} (n/d)^{l-1/2} \ll_\varepsilon n^{l-1/2+\varepsilon}$$

при $(m,N) = (1)$ и $\varepsilon > 0$. Но $A_j(t,1) = a_j(t)$; следовательно,

$$a_j(tm^2) \ll_\varepsilon |a_j(t)| m^{l-1/2+\varepsilon} \text{ при } (m,N) = (1) \text{ и } \varepsilon > 0. \tag{4.4.10}$$

Пусть

$$\varphi = \sum_{j=1}^{g(k)} \beta_j \varphi_j,$$

тогда

$$|a(\varphi, tm^2)|^2 = |\sum_{j=1}^{g(k)} \beta_j a_j(tm^2)|^2 \le \sum_{j=1}^{g(k)} |\beta_j|^2 \sum_{j=1}^{g(k)} |a_j(tm^2)|^2$$

и потому

$$|a(\varphi, tm^2)| \le ||\varphi|| (\sum_{j=1}^{g(k)} |a_j(tm^2)|^2)^{1/2}. \tag{4.4.11}$$

Оценка (9) вытекает из (10) и (11).

Следствие 4.4.3. *Пусть* $D \in \mathbb{N}$, $k = 2l+1$, $l \in \mathbb{N} \setminus \{1\}$, $4|N$, $D|N$, χ *- определённый в лемме 5 характер Дирихле,* $\varphi \in S_{k/2}(N,\chi)$, $||\varphi|| = 1$ *и* $(n,N) = (1)$. *Тогда*

$$a(\varphi, n) \ll_{k,\varepsilon} n^{k/4-2/7+\varepsilon} \text{ при } \varepsilon > 0. \tag{4.4.12}$$

Доказательство. При $n \in \mathbb{N}_{sf}$ оценка (12) выводится из леммы 5 так же, как теорема 1 работы [103] выводится из теоремы 3 этой работы (см. [103, стр. 400 - 401]). Оценка (12) для произвольного n, под условием $(n, N) = (1)$, следует из леммы 6 и этой оценки для свободных от квадратов n.

Доказательство теоремы 2. Утверждение теоремы следует из леммы 1, леммы 2 (при чётном k) и следствия 3 (при нечётном k).

При $\varphi \in S_{3/2}(N, \chi)$ и $t \in \mathbb{N}_{sf}$ положим

$$F_t(\varphi)(z) := \sum_{n=1}^{\infty} A(\varphi; t, n) e^{2\pi i n z},$$

где

$$\sum_{n=1}^{\infty} A(\varphi; t, n) n^{-s} := L(s, \psi_t) \sum_{n=1}^{\infty} a(\varphi, tn^2) n^{-s} \text{ и } \psi_t(m) := \chi(m)(\frac{t}{m}).$$

Следуя [151], положим далее

$$U^{\perp} := \{\varphi | \varphi \in S_{3/2}(N, \chi),\ (\forall\, t \in \mathbb{N}_{sf}) F_t(\varphi) \in S_2(N/2, \chi^2)\}.$$

Лемма 4.4.7. *Пусть $N \in \mathbb{N}$, $4|N$, χ - характер Дирихле по модулю N и $\varphi \in U^{\perp}$. Тогда*

$$a(\varphi, n) \ll_{\varphi, \varepsilon} n^{1/2 - 1/28 + \varepsilon} \text{ при } \varepsilon > 0 \text{ и } (n, N) = (1),\ n \in \mathbb{N}. \tag{4.4.13}$$

Доказательство. Пусть $\varphi \in U^{\perp}$, тогда [69, (2.5)] функция

$$f \colon H \to \mathbb{C},\ f \colon z \mapsto y^{3/4} \varphi(z),\ z = x + iy,\ x \in \mathbb{R},\ y \in \mathbb{R}_+^*$$

есть форма Маасса веса $3/2$ и потому [69, теорема 5] (цитируемая теорема Дьюка выводится автором методами работы Иванца [103] из обобщённой формулы Н.В. Кузнецова для суммы сумм Клостермана, полученной Н.В. Проскуриным [36]):

$$a(\varphi, n) \ll_{\varphi, \varepsilon} n^{1/2 - 1/28 + \varepsilon} \text{ при } \varepsilon > 0 \text{ и } (n, N) = (1),\ n \in \mathbb{N}_{sf}. \tag{4.4.14}$$

С другой стороны, из леммы 2 следует, что

$$|a(\varphi, tm^2)| = |\sum_{d|m} \mu(d)\psi_t(d)A(\varphi; t, m/d)| \leq \sum_{d|m} |A(\varphi; t, m/d)| \leq$$

$$|A(\varphi; t, 1)|\tau(m)\sum_{d|m}(m/d)^{1/2} \ll_\varepsilon |a(\varphi, t)|m^{1/2+\varepsilon}$$

при $t \in \mathbb{N}_{sf},\ m \in \mathbb{N},\ (m, N) = (1)$ и $\varepsilon > 0$, откуда, ввиду соотношения (14), и вытекает (13).

Доказательство теоремы 3. Утверждение теоремы следует из леммы 7 и теорем Шульце - Пиллота [151, следствия 2 и 3].

Доказательство следствия 1. Пусть $n \in \mathbb{N}$ и $n = 7$ (8). При $n = p^l n_1,\ (n_1, p) = (1),\ l \in \mathbb{N} \setminus \{1, 2\}$ положим $n_2 = p^{l-3}n_1$, тогда $n_2 = 3$ (8) и потому

$$|\{y|y \in \mathbb{Z}^3,\ y_1^2 + y_2^2 + y_3^2 = n_2\}| \gg_\varepsilon n_2^{1/2-\varepsilon} \text{при } \varepsilon > 0. \tag{4.4.15}$$

Так как каждой паре $(z, y),\ z \in \mathbb{Z}^2,\ y \in \mathbb{Z}^3$, под условием

$$z_1^2 + z_2^2 = p^3,\ y_1^2 + y_2^2 + y_3^2 = n_2$$

отвечает единственное решение уравнения $f(x) = n,\ x \in \mathbb{Z}^3$, доказываемая оценка

$$r_f(n) \gg_{\varepsilon,p} n^{1/2-\varepsilon} \tag{4.4.16}$$

следует из (15). Пусть теперь $n = p^l n_1,\ (n_1, p) = (1)$ с $l \in \{0, 1, 2\}$. Рассмотрим квадратичную форму

$$g(x) := x_1^2 + x_2^2 + p^{3-l}x_3^2;$$

из теорем 1 и 3 следует, что

$$r_g(n_1) \gg_{\varepsilon,p} n_1^{1/2-\varepsilon}. \tag{4.4.17}$$

Для того чтобы вывести (16) из (17) в этом случае, достаточно сопоставить паре решений целочисленных (z, y) уравнений

$$z_1^2 + z_2^2 = p^l,\ g(y) = n_1$$

решение уравнения $f(x) = n,\ x \in \mathbb{Z}^3$.

4. Для доказательства теоремы 4 нам потребуются равномерные по весу оценки коэффициентов Фурье параболических форм. Впервые такие оценки были получены в работах [42], [9]; наше изложение лишь по форме отличается от выводов и рассуждений этих работ.

Следствие 4.4.4. *Предположим, в обозначениях леммы* 2, *что* $k \geq 2$, $\varphi \in S_k(N, \chi)$ *и* $(n, N) = (1)$. *Тогда*

$$a(\varphi, n) \ll_{N,\varepsilon} \frac{(4\pi)^{(k-1)/2} k^{1/2}}{\Gamma(k-1)^{1/2}} n^{(k-1)/2+\varepsilon} ||\varphi|| \text{ при } \varepsilon > 0. \tag{4.4.18}$$

Доказательство. Положим для краткости $g := g(2k)$ и рассмотрим множество $\{\varphi_j | 1 \leq j \leq g\}$ общих собственных функций семейства операторов Гекке

$$\{T_p | p \in \mathcal{P},\ (p, N) = (1)\}$$

под условием:

$$< \varphi_i | \varphi_j >= 0 \text{ при } 1 \leq i < j \leq g \text{ и } a_j(n_j) = 1 \text{ при } 1 \leq j \leq g,$$

где $a_j(n) := a(\varphi_j, n)$ при $1 \leq j \leq g,\ n \in \mathbb{N}$ и

$$n_j := \min \{n | n \in \mathbb{N},\ a_j(n) \neq 0\} \text{ при } 1 \leq j \leq g.$$

Предположим, не нарушая общности, что $a_j(1) = 1$ при $1 \leq j \leq g_0$ и $a_j(1) = 0$ при $g_0 < j \leq g$; тогда (см.,например, [148, стр. 319]) $a_j(n) = 0$ при $j > g_0$ и $(n, N) = (1)$. Пусть

$$\varphi = \sum_{j=1}^{g} \beta_j \varphi_j;$$

тогда

$$|a(n)|^2 = |\sum_{j=1}^{g} \beta_j a_j(n)|^2 \leq \sum_{1\leq j\leq g_0} |\beta_j|^2 \sum_{1\leq j\leq g_0} |a_j(n)|^2 \tag{4.4.19}$$

при $(n, N) = (1)$. Так как $g_0 \leq g \ll_N k$ (см.,например, [148, теорема 4.2.1]), из леммы 2 и соотношения (19) следует, что

$$|a(n)|^2 \ll_{N,\varepsilon} kn^{k-1+\varepsilon} \sum_{1\leq j\leq g_0} |\beta_j|^2 \text{ при } (n, N) = (1) \text{ и } \varepsilon > 0. \tag{4.4.20}$$

С другой стороны, при $1 \leq j \leq g_0$ имеем

$$||\varphi_j||^2 = \int\limits_{\Gamma_0(N)\backslash H} y^{k-2}|\varphi_j(z)|^2 dxdy \geq \int_1^\infty y^{k-2}dy \int_0^1 |\varphi_j(z)|^2 dx =$$

$$\int_1^\infty y^{k-2}dy = \sum_{n=1}^{\infty} |a_j(n)|^2 e^{-4\pi y} \geq \int_1^\infty y^{k-2}e^{-4\pi y}dy \gg \Gamma(k-1)(4\pi)^{-(k-1)}$$

и потому

$$||\varphi||^2 = \sum_{j=1}^{g} |\beta_j|^2 ||\varphi_j||^2 \geq \sum_{1\leq j\leq g_0} |\beta_j|^2 ||\varphi_j||^2 \gg \Gamma(k-1)(4\pi)^{-(k-1)} \sum_{1\leq j\leq g_0} |\beta_j|^2.$$

Оценка (18) вытекает из этого неравенства и оценки (20); тем самым, следствие 4 доказано.

Лемма 4.4.8. *Пусть*

$$D \in \mathbb{N},\ k = 2l + 1,\ l \in \mathbb{N} \setminus \{1\},\ 8|N,\ D|N,$$

χ *есть определённый в лемме 5 характер Дирихле,*

$$\varphi \in S_{k/2}(N, \chi) \text{ и } (n, N) = (1).$$

Тогда

$$a(\varphi, n) \ll_{N,\varepsilon} \frac{(4\pi)^{k/4-1/2}k^{3/4}}{\Gamma(k/2-1)^{1/2}} n^{(k-1)/4-1/96+\varepsilon}||\varphi|| \text{ при } \varepsilon > 0. \tag{4.4.21}$$

Доказательство. Пусть

$$p \in \mathcal{P},\ Q = pN \text{ и } b(p) := [\Gamma_0(N) : \Gamma_0(Q)].$$

Обозначим через $(\cdot|\cdot)$ скалярное произведение в пространстве $S_{k/2}(pN,\chi)$ и через $h(p)$ размерность этого пространства; ясно, что

$$(f_1|f_2) =< f_1|f_2 > b(p) \text{ при } \{f_1,f_2\} \subseteq S_{k/2}(N,\chi).$$

Введём в рассмотрение ортонормированный базис

$$\{\varphi_j|\varphi_j(z) = \sum_{n=1}^{\infty} a_j(n)e^{2\pi inz},\ 1 \le j \le g(k)\}$$

пространства $S_{k/2}(N,\chi)$, положим $\psi_j := b(p)^{-1/2}\varphi_j$ и рассмотрим ортонормированный базис $\{\psi_j|1 \le j \le h(p)\}$ пространства $S_{k/2}(pN,\chi)$. Так как $b(p) \le p+1$ и $h(p) \le g(k)$, из тождества (3) следует, что

$$\sum_{j=1}^{g(k)} |a_j(n)|^2 \le (p+1)\sum_{j=1}^{g(k)} |a(\psi_j,n)|^2 \le$$

$$(p+1)\frac{(4\pi n)^{k/2-1}}{\Gamma(k/2-1)}(1+2\pi\sum_{c\in\mathbb{N},Q|c}|X(k;n,c)|),$$

где

$$X(k;n,c) := \frac{K_k(\chi;n,c)}{c}J_{k/2-1}(\frac{4\pi n}{c}),$$

или

$$\frac{\Gamma(k/2-1)}{(p+1)(4\pi n)^{k/2-1}}\sum_{j=1}^{g(k)}|a_j(n)|^2 \le 1+2\pi|\sum_{c\in\mathbb{N},Q|c}X(k;n,c)|.$$

Пусть $P \gg (\log n)^2$, тогда

$$\sum_{Q\in\mathcal{Q}(P)}(p+1)^{-1} \gg (\log P)^{-1},\ |\mathcal{Q}(P)| \ll P(\log P)^{-1}$$

и потому

$$\frac{\Gamma(k/2-1)}{(4\pi n)^{k/2-1}}\sum_{j=1}^{g(k)}|a_j(n)|^2 \ll P+(\log P)\sum_{Q\in\mathcal{Q}(P)}|\sum_{c\in\mathbb{N},Q|c}X(k;n,c)|. \qquad (4.4.22)$$

При

$$S_1 := \sum_{Q\in\mathcal{Q}(P)}|\sum_{c>n^{47/48},Q|c}X(k;n,c)|,\ S_2 := \sum_{Q\in\mathcal{Q}(P)}|\sum_{c\le n^{47/48},Q|c}X(k;n,c)|$$

и $P := n^{1/8}$ неравенство (22) принимает вид

$$\frac{\Gamma(k/2-1)}{(4\pi n)^{k/2-1}} \sum_{j=1}^{g(k)} |a_j(n)|^2 \ll P + (\log P)(S_1 + S_2). \tag{4.4.23}$$

Полагая

$$u := n^{47/48},\ \beta(c) := c^{-1/2} K_k(\chi; n, c) \text{ и } f(u) := u^{-1/2} J_{k/2-1}(\frac{4\pi n}{u}),$$

так что

$$X(k; n, c) = f(c)\beta(c) \ \text{ и } \ \mathcal{K}_Q^{(0)}(\chi; n, u) = \sum_{c \le u, Q|c} \beta(c),$$

и воспользовавшись тождеством

$$\sum_{c>u, Q|c} f(c)\beta(c) = -\mathcal{K}_Q^{(0)}(\chi; n, u) f(u) - \int_u^\infty f'(y) \mathcal{K}_Q^{(0)}(\chi; n, y) dy,$$

получим

$$|S_1| \le |f(u)| \sum_{Q \in \mathcal{Q}(P)} |\mathcal{K}_Q^{(0)}(\chi; n, u)| + \int_u^\infty |f'(y)| \sum_{Q \in \mathcal{Q}(P)} |\mathcal{K}_Q^{(0)}(\chi; n, y)| dy. \tag{4.4.24}$$

Из интегрального представления функций Бесселя

$$J_{\nu+l}(z),\ l \in \mathbb{Z},\ l \ge 0,\ \mathrm{Re}\ \nu > -1/2,$$

через полиномы Гегенбауэра $G_l^\nu(y)$ [116, стр. 80] и известной оценки [116, стр. 225]

$$|G_l^{3/2}(y)| \le (l+2)(l+1) \text{ при } |y| \le 1$$

следует, что

$$|f(u)| \ll n^{-11/24} \ \text{ и } \ |f'(y)| \ll n^{3/2}(1 + ny^{-1})e^{-3}. \tag{4.4.25}$$

Соотношения (24), (25) и (8) дают:

$$S_1 \ll_\varepsilon n^{1/2-1/48+\varepsilon} \text{ при } n \in \mathbb{N}_{sf},\ (n, N) = (1) \text{ и } \varepsilon > 0. \tag{4.4.26}$$

С другой стороны, из известного неравенства (см., например, [9, стр. 61])

$$J_{k/2-1}(z) \ll k^{3/2} z^{-1/2} \ \text{ при } \ z \ge 1$$

и леммы 4 следует, что

$$X(k;n,c)=\frac{K_k(\chi;n,c)}{c}J_{k/2-1}(\frac{4\pi n}{c})\ll k^{3/2}\tau(n)\ (\text{н.о.д. }(n,c))^{1/2}n^{-1/2}$$

и потому (ср. [103, (4.2)])

$$S_2\ll_{N,\varepsilon}k^{3/2}n^{1/2-1/48+\varepsilon}\ \text{ при }\ (n,N)=(1)\text{ и }\varepsilon>0. \tag{4.4.27}$$

Соотношения (23), (26) и (27) позволяют заключить, что

$$\frac{\Gamma(k/2-1)}{(4\pi n)^{k/2-1}}\sum_{j=1}^{g(k)}|a_j(n)|^2\ll_{N,\varepsilon}k^{3/2}n^{1/2-1/48+\varepsilon}$$

при $n\in\mathbb{N}_{sf},\ (n,N)=(1)$ и $\varepsilon>0$. Для завершения доказательства леммы 8 остаётся применить лемму 6.

Обозначим через Δ_l оператор Лапласа на l-мерной сфере $S_l,\ l\geq 2$. Как известно (см., например, [44, предложение 3.5 на стр. 97]),

$$L^2(S_l)=\sum_{m=0}^{\infty}\oplus\mathcal{H}_m,\ \Delta_l|\mathcal{H}_m=g_l(m)I_m,\ h_l(m):=\dim\mathcal{H}_m,$$

где I_m есть единичная матрица порядка h_m,

$$g_l(m)=m(m+l-1)\ \text{ и }\ h_l(m)=\frac{(2m+l-1)(m+l-2)!}{m!(l-1)!}$$

при $m\in\mathbb{N}\cup\{0\}$. Выберем ортонормированный базис

$$\{\sigma_{jm}|1\leq j\leq h(m)\}$$

пространства $\mathcal{H}_m$; как известно [44, (2.145) и теорема 2.9],

$$\sigma_{11}=1\text{ и }\sum_{j=1}^{h(m)}\sigma_{jm}(y_1)\overline{\sigma_{jm}(y_2)}=(2m+l-1)(l-1)^{-1}G_m^{(l-1)/2}(y_1^ty_2)$$

при $\{y_1,y_2\}\subseteq S_l,\ m\in\mathbb{N}\cup\{0\}$. Пусть $f\in L^2(S_l)$; положим

$$f=\sum_{m=0}^{\infty}H_m(f),\ H_m(f)=\sum_{j=1}^{h(m)}a(f;j,m)\sigma_{jm}(x),\ H_m(f,x):=H_m(f)(x)$$

при $x \in S_l$, где

$$a(f;j,m) = \int\limits_{S_l} H_m(f,x)\overline{\sigma_{jm}(x)}d\lambda_l(x),$$

так что

$$H_m(f,x) = \frac{2m+l-1}{l-1}\int\limits_{S_l} G_m^{(l-1)/2}(x^t y)f(y)d\lambda_l(y) \text{ при } m \in \mathbb{N}\cup\{0\} \quad (4.4.28)$$

и, в частности,

$$H_0(f,x) = \int\limits_{S_l} f(y)d\lambda_l(y).$$

Более того,

$$a(f;j,m) = (m(m+l-1))^{-\alpha}\int\limits_{S_l} H_m(f,x)\overline{\Delta_l^\alpha\sigma_{jm}(x)}d\lambda_l(x),$$

и потому из самосопряжённости оператора Δ_l следует, что

$$H_m(f,x) = \frac{2m+l-1}{(l-1)(m(m+l-1))^\alpha}\int\limits_{S_l} \Delta_l^\alpha f(y)G_m^{(l-1)/2}(x^t y)d\lambda_l(y) \quad (4.4.29)$$

при $\{m,\alpha\} \subseteq \mathbb{N}$ и $f \in L^2(S_l)\cap C^\infty(S_l)$. Обозначим через $|x-y|$ расстояние между точками $x,\ y$ пространства $\mathbb{R}^n,\ n \in \mathbb{N}$ и положим

$$|x-T| := \inf\{|x-y| \ |y \in T\} \text{ при } T \subseteq \mathbb{R}^n \text{ и } x \in \mathbb{R}^n$$

и

$$U_\delta(\omega) := \{y|y \in S_l,\ |y-\omega| \le \delta\} \text{ при } \omega \subseteq S_l \text{ и } \delta \in \mathbb{R}_+.$$

Пусть

$$f_0 : [-1,1] \to [0,1],\ f_0(x) := \exp(x^2(x^2-1)^{-1}) \text{ при } |x| \le 1$$

и

$$f(x) := \begin{cases} f_0(x) & \text{при } |x| \le 1 \\ 0 & \text{при } |x| \ge 1. \end{cases}$$

При $0 < \delta < 1/4$ и $e_1 := \begin{pmatrix} 1 \\ 0 \\ ... \\ 0 \end{pmatrix}$ положим

$$c(\delta) := (\int\limits_{U_\delta(\{e_1\})} f_0(\frac{|e_1 - y|}{\delta}) d\lambda_l(y))^{-1}.$$

Пусть $\omega \in \Omega$; введём в рассмотрение характеристические функции множеств ω и $U_\delta(\omega)$:

$$\chi^{(1)} : S_l \to \{0,1\},\ \chi^{(1)}(x) := \begin{cases} 1 & \text{при } x \in \omega \\ 0 & \text{при } x \in S_l \setminus \omega \end{cases}$$

$$\chi^{(2)} : S_l \to \{0,1\},\ \chi^{(2)}(x) := \begin{cases} 1 & \text{при } x \in U_\delta(\omega) \\ 0 & \text{при } x \in S_l \setminus U_\delta(\omega) \end{cases}$$

и определим функции

$$\chi^{(j)}_\delta : S_l \to [0,1],\ \chi^{(j)}_\delta : x \mapsto c(\delta) \int\limits_{S_l} \chi^{(j)}(y) f(\frac{|e_1 - y|}{\delta}) d\lambda_l(y),\ j \in \{1,2\}.$$

Ясно, что $\chi^{(j)}_\delta \in C^\infty(S_l)$ при $j \in \{1,2\}$; положим, для краткости,

$$H^{(j)}_m(\delta; x) := H_m(\chi^{(j)}_\delta, x).$$

Лемма 4.4.9. *При $j \in \{1,2\}$ имеют место следующие соотношения:*

$$\chi^{(j)}_\delta(S_l \setminus U_{j\delta}(\omega)) = \{0\},\ \chi^{(1)}_\delta(\omega \setminus U_\delta(\partial\omega)) = \chi^{(2)}_\delta(\omega) = \{1\} \tag{4.4.30}$$

и

$$\max\{|H^{(j)}_m(\delta; x)|\ |x \in S_l\} \ll_{\omega,\alpha} \frac{m^{(l-3)/2}}{(m\delta)^{2\alpha-1}} \ \ при\ \ \alpha \in \mathbb{N}. \tag{4.4.31}$$

Доказательство. Соотношения (30) легко следуют из определения функций $\chi^{(j)}_\delta$; докажем (31). По построению,

$$\max\{|\Delta^\alpha_l \chi^{(j)}_\delta(x)|\ |x \in S_l\} \ll_{w,\alpha} \delta^{-2\alpha} \tag{4.4.32}$$

и

$$\Delta_l^{\alpha}\chi_{\delta}^{(j)}(x) = 0 \text{ при } x \in S_l \setminus U_{j\delta}(\partial w). \tag{4.4.33}$$

Из соотношений (29), (32), (33) и известной оценки (см., например, [116, стр. 226])

$$G_m^{(l-1)/2}(\cos\varphi) \ll \varphi^{-(l-1)/2} m^{(l-3)/2} \text{ при } 0 \le \varphi \le \pi$$

следует, что

$$H_m^{(j)}(\delta; x) \ll_{w,\alpha} \frac{m^{(l-1)/2}}{(m\delta)^{2\alpha}} \int\limits_{U_{i\delta}(\partial w)} \varphi^{-(l-1)/2} d\lambda_l(y),\ \cos\varphi := x^t y. \tag{4.4.34}$$

Переходя к сферическим координатам φ, z под условием

$$y = (\cos\varphi)x + (\sin\varphi)z,\ x^t z = 0,$$

получим (см., например, [44, стр. 7 - 8])

$$d\lambda_l(y) = \pi^{-1/2}\Gamma((l+1)/2)\Gamma(l/2)^{-1}(\sin\varphi)^{(l-1)} d\varphi d\lambda_{l-1}(z),$$

так что

$$\int\limits_{U_{j\delta}(\partial w)} \varphi^{-(l-1)/2} d\lambda_l(y) \ll \int\limits_{U_{j\delta}(\partial w)} d\varphi d\lambda_{l-1}(z) \ll_w \delta,$$

и оценка (34) принимает вид:

$$H_m^{(i)}(\delta; x) \ll_{w,\alpha} \delta m^{(l-1)/2} (m\delta)^{-2\alpha}.$$

Лемма доказана.

Положим

$$I^{(j)}(\delta;\varepsilon) := \sum_{1 \le m \le \delta^{-1-\varepsilon}} \sum_{f(x)=n,\ x\in\mathbb{Z}^k} H_m^{(j)}(\delta; \pi(x)) \text{ при } j \in \{1,2\},$$

и пусть

$$I_0(\delta;\varepsilon) := |I^{(1)}(\delta;\varepsilon)| + |I^{(2)}(\delta;\varepsilon)|.$$

Следствие 4.4.5. *Пусть* $k \ge 3,\ f \in \mathcal{F}_k,\ n \in \mathbb{N}$ *и* $\varepsilon > 0$. *Тогда*

$$r_f(n,\omega) = \lambda_l(\omega) r_f(n) + O_{\omega,\varepsilon}(\delta r_f(n)) + O(I_0(\delta;\varepsilon)). \tag{4.4.35}$$

Доказательство. Из соотношений (30) следует, что

$$\sum_{f(x)=n,\ x\in\mathbb{Z}^k} \chi_\delta^{(1)}(\pi(x)) \le r_f(n,\omega) \le \sum_{f(x)=n,\ x\in\mathbb{Z}^k} \chi_\delta^{(2)}(\pi(x)). \tag{4.4.36}$$

По построению,

$$\chi_\delta^{(j)}(y) = \sum_{m=0}^{\infty} H_m^{(j)}(\delta;y) \text{ и } H_0^{(j)}(\delta;y) = \int\limits_{S_l} \chi_\delta^{(j)}(y)(y)d\lambda_l(y)$$

при $y \in S_l$ и $j \in \{1,2\}$ и, значит, ввиду (36),

$$r_f(n,\omega) = \lambda_l(\omega) r_f(n) + O_\omega(\delta r_f(n)) + O(I_0(\delta;\varepsilon)) + O(I_1(\delta;\varepsilon)), \tag{4.4.37}$$

где

$$I_1(\delta;\varepsilon) := \sum_{j\in\{1,2\}} \sum_{m>\delta^{-1-\varepsilon}} \sum_{f(x)=n,\ x\in\mathbb{Z}^k} |H_m^{(j)}(\delta;\pi(x))|.$$

Соотношение (31) даёт:

$$I_1(\delta;\varepsilon) \ll_{\omega,\alpha} r_f(n) \sum_{m>\delta^{-1-\varepsilon}} \frac{m^{(l-3)/2}}{(m\delta)^{2\alpha-1}} \ll r_f(n)\delta^{(2\alpha-(l+1)/2)\varepsilon-(l-1)/2},$$

откуда при $\alpha > (\varepsilon+1)(l+1)(4\varepsilon)^{-1}$ получаем

$$I_1(\delta;\varepsilon) \ll_{\omega,\varepsilon} \delta r_f(n). \tag{4.4.38}$$

Доказываемая оценка (35) следует из (37) и (38).

Положим

$$P_m^{(j)}(\delta;x) := f(x)^{m/2} H_m^{(j)}(\delta;\pi(x))$$

и

$$\Theta_{m,\delta}^{(j)}(z) := \sum_{x\in\mathbb{Z}^k} P_m^{(j)}(\delta;x) e^{2\pi i f(x)z} = \sum_{n=1}^{\infty} c_m^{(j)}(n) e^{2\pi i n z},$$

где

$$c_m^{(j)}(n) := n^{m/2} \sum_{x\in\mathbb{Z}^k, f(x)=n} H_m^{(j)}(\delta;\pi(x)),$$

при $j \in \{1,2\},\ m \in \mathbb{N}$ и $z \in H$.

Лемма 4.4.10. *Пусть* $k \geq 3,\ f \in \mathcal{F}_k,\ \{m, \alpha\} \subseteq \mathbb{N},\ j \in \{1, 2\},\ r := k/2$ *и* $\varepsilon > 0$. *Тогда*

$$\Theta_{m,\delta}^{(j)} \in S_{r+m}(N(f), \chi_f)$$

и

$$||\Theta_{m,\delta}^{(j)}||^2 \ll_{f,\omega,\alpha,\varepsilon} \frac{\Gamma(r+m-1)m^{r+\varepsilon}}{(4\pi)^{r+m-1}}(m^{r-2}(m\delta)^{1-2\alpha})^2.$$

Доказательство. Полином $P_m^{(j)}(\delta; x)$ является однородным сферическим полиномом от x степени m и, значит,

$$\Theta_{m,\delta}^{(j)} \in S_{r+m}(N(f), \chi_f),$$

[146], [157, предложение 2.1 на стр. 456].

Введём в рассмотрение $\Gamma_0(N)$ - фундаментальную область $\mathcal{H}(N)$ на верхней полуплоскости H, обозначим через B множество параболических вершин в $\overline{\mathcal{H}(N)}$ и рассмотрим открытое покрытие

$$\mathcal{H}(N) = \bigcup_{b \in B} V_b \ \text{ с } \ b \in \overline{V_b},\ V_b \subseteq H.$$

Ясно, что

$$||\Theta_{m,\delta}^{(j)}||^2 = \int\limits_{\mathcal{H}(N)} y^{k-2}|\Theta_{m,\delta}^{(j)}(z)|^2 dxdy \leq \sum_{b \in B} \int\limits_{V_b} y^{m+r-2}|\Theta_{m,\delta}^{(j)}(z)|^2 dxdy. \quad (4.4.39)$$

Пусть $\gamma_b \in \mathrm{SL}_2(\mathbb{Z})$ и $\gamma_b b = i\infty$, тогда

$$\gamma_b V_b \subseteq \{x + iy | \{x, y\} \subseteq \mathbb{R},\ 0 \leq x \leq 1,\ y \geq 1/2\}$$

и потому

$$\int\limits_{V_b} y^{m+r-2}|\Theta_{m,\delta}^{(j)}(z)|^2 dxdy \leq \int\limits_0^1 dx \int\limits_{1/2}^{\infty} y^{m+r-2}|\Theta_{m,\delta}^{(j)}(\gamma_b^{-1}z)|^2. \quad (4.4.40)$$

При $a \in (\mathbb{Z}/N\mathbb{Z})^k,\ N := N(f)$, положим

$$Z(a, k) := \{x | x \in \mathbb{Z}^k,\ x = a \pmod N\}$$

и

$$\Theta_{m,\delta}^{(j)}(a,z) := \sum_{x\in Z(a,k)} P_m^{(j)}(\delta;x)e^{2\pi i f(x)z} = \sum_{n=1}^{\infty} c_{m,a}^{(j)}(n)e^{2\pi i n z},$$

где

$$c_{m,a}^{(j)}(n) := n^{m/2} \sum_{x\in Z(a,k), f(x)=n} H_m^{(j)}(\delta;\pi(x)).$$

Так как $r_f(n) \ll_{f,\varepsilon} n^{r-1+\varepsilon}$, из леммы 9 следует, что

$$c_{m,a}^{(j)}(n) \ll_{f,\omega,\alpha,\varepsilon} n^{m/2+r-1+\varepsilon} m^{r-2}(m\delta)^{1-2\alpha} \text{ при } \varepsilon > 0.$$

С другой стороны, см., например, [146],

$$\Theta_{m,\delta}^{(j)}(\gamma z) = \sum_{a\in(\mathbb{Z}/N\mathbb{Z})^k} \kappa(a,\gamma)\Theta_{m,\delta}^{(j)}(a,z),\ \kappa(a,\gamma)\in\mathbb{C},$$

при $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, так что неравенства (39) и (40) дают: $||\Theta_{m,\delta}^{(j)}||^2 \le$

$$\sum_{b\in B}\int_0^1 dx \int_{1/2}^{\infty} y^{m+r-2}|\Theta_{m,\delta}^{(j)}(\gamma_b^{-1}z)|^2 \ll_f \sum_{a\in(\mathbb{Z}/N\mathbb{Z})^k}\int_0^1 dx\int_{1/2}^{\infty} y^{m+r-2}|\Theta_{m,\delta}^{(j)}(a,z)|^2$$

$$= \sum_{a\in(\mathbb{Z}/N\mathbb{Z})^k}\int_{1/2}^{\infty} y^{m+r-2}\sum_{n=1}^{\infty}|c_{m,a}^{(j)}(n)|^2 e^{-4\pi n y}dy \ll_{f,\omega,\alpha,\varepsilon} (m^{r-2}(m\delta)^{1-2\alpha})^2 S_m,$$

где

$$S_m := \sum_{n=1}^{\infty} n^{m+2(r-1)+\varepsilon}\int_{1/2}^{\infty} y^{m+r-2}e^{-4\pi n y}dy = (4\pi)^{-(m+r-1)}\sum_{n=1}^{\infty} n^{(r-1)+\varepsilon} I_n,$$

$$I_n := \int_{1/2\pi n}^{\infty} y^{m+r-2}e^{-4\pi y}dy \text{ и, тем самым, } S_m \ll \frac{\Gamma(r+m-1)m^{r+\varepsilon}}{(4\pi)^{r+m-1}}.$$

Лемма доказана.

Следствие 4.4.6. *Пусть* $k \ge 3$, $r := k/2$, $f \in \mathcal{F}_k$, $\{m,n,\alpha\} \subseteq \mathbb{N}$, $(n, 2d(f)) = (1)$ *и* $\varepsilon > 0$. *Тогда*

$$I_0(\delta;\varepsilon) \ll_{f,\omega,\varepsilon} n^{\nu_k+(r-1)/2+\varepsilon}\delta^{-\mu_k-(3r-1)/2+\varepsilon}, \tag{4.4.41}$$

где $\nu_k = \mu_k = 0$ *при чётных* k *и* $\nu_k = 23/96$, $\mu_k = 1/4$ *при нечётных* k.

Доказательство. Положим

$$\beta(k;m,n) := \begin{cases} 1 & \text{при } 2|k, \\ m^{3/4}n^{23/96} & \text{при } (2,k)=(1) \end{cases}$$

и пусть $j \in \{1,2\}$. Из следствия 4 (при чётных k) или леммы 8 (при нечётных k) и леммы 10 следует, что

$$c_m^{(j)}(n) \ll_{f,\omega,\alpha,\varepsilon} \frac{m^{3(r-1)/2+\varepsilon}}{(m\delta)^{2\alpha-1}} n^{(r+m-1)/2+\varepsilon}\beta(k;m,n). \tag{4.4.42}$$

По определению,

$$I^{(j)}(\delta;\varepsilon) := \sum_{1\le m\le \delta^{-1-\varepsilon}} n^{-m/2}c_m^{(j)}(n),$$

так что оценка (42) с $\alpha = 1$ даёт:

$$I_0(\delta;\varepsilon) \ll_{f,\omega,\varepsilon} n^{(r-1)/2+\varepsilon}\delta^{-1} \sum_{1\le m\le \delta^{-1-\varepsilon}} m^{(3r-5)/2+\varepsilon}\beta(k;m,n),$$

откуда немедленно вытекает доказываемая оценка (41).

Доказательство теоремы 4. Так как $r_f(n) \ll_{f,\varepsilon} n^{(k-2)/2+\varepsilon}$ при $\varepsilon > 0$, утверждение теоремы следует из соотношений (35) и (41) с $\delta = n^{-\alpha(k)}$.

4.5 Об одной эллиптической кривой

В этом этом параграфе с незначительными изменениями воспроизводится содержание совместной работы [67].

1. Как известно, определённые над $\mathbb{Q}$ эллиптические кривые модулярны, [168], [54]; дальнейшее развитие идей и техники цитированных работ позволило доказать модулярность ряда эллиптических кривых, определённых над вполне вещественными полями, см., например, [79] и цитированную в этой работе литературу. Значительно труднее исследовать эллиптические кривые, определённые над другими полями. В недавней работе [66] предложен алгоритм, позволяющий в принципе проверить модулярность любой конкретно

заданной эллиптической кривой над мнимым квадратичным полем, и впервые доказана модулярность трёх таких кривых без комплексного умножения. Воспользовавшись этим алгоритмом, М. Минк в своей дипломной работе [119] доказала модулярность ещё одной кривой без комплексного умножения, определённой над $\mathbb{Q}(\sqrt{-23})$. В этом параграфе подробно описывается действие предложенного в работе [66] алгоритма на примере этой кривой, ср. [67]. Не имея возможности подробно остановиться на истории вопроса, отметим только, что эллиптические кривые над мнимыми квадратичными полями и соответствующие автоморфные формы изучались в работах ряда авторов, см., например, [162, теорема 3], [112] и цитированную в недавнем обзоре [153] литературу.

Введём в рассмотрение мнимое квадратичное поля K, положим

$$\mathrm{Gal}(K|\mathbb{Q}) = \{1, \tau\}$$

и обозначим через $\mathfrak{E}(K)$ множество эллиптических кривых, определённых над полем K. Пусть $E \in \mathfrak{E}(K)$; обозначим через $\mathfrak{f}(E)$ ведущий модуль кривой E, через $\mathcal{Q}_2,\ \mathcal{Q}_1,\ \mathcal{Q}_{-1}$ и $\mathcal{Q}_0$ множества простых идеалов $\mathfrak{p}$, для которых кривая E обладает сответственно хорошей, неразложимой мультипликативной, разложимой мультипликативной и аддитивной редукцией по модулю $\mathfrak{p}$, так что

$$\mathcal{P}(K) = \bigcup_{i\in\{0,\pm1,2\}} \mathcal{Q}_i \ \text{ и } \ \mathcal{Q}_2 = \{\mathfrak{p}|\mathfrak{p} \in \mathcal{P}(K),\ \mathfrak{f}(E) \neq 0\ (\mathfrak{p})\}.$$

Положим

$$a(\mathfrak{p}) = q + 1 - |E(\mathbb{F}_q)|,\ q := N\mathfrak{p}, \ \text{ при } \ \mathfrak{p} \in \mathcal{Q}_2,$$

$$\text{и } \ a(\mathfrak{p}) = \varepsilon \ \text{ при } \ \mathfrak{p} \in \mathcal{Q}_\varepsilon,\ \varepsilon \in \{-1, 0, 1\};$$

$$l_\mathfrak{p}(E, t) := 1 - a(\mathfrak{p})t + (N\mathfrak{p})t^2 \text{ при } \mathfrak{p} \in \mathcal{Q}_2$$

$$\text{и } \ l_\mathfrak{p}(E, t) := 1 + a(\mathfrak{p})t \text{ при } \mathfrak{p}|\mathfrak{f}(E).$$

Предложение 4.5.1. *Пусть* $\{E, E'\} \subseteq \mathfrak{E}(K)$. *Если кривые* E *и* E' *изогенны, то*

$$(\forall\, \mathfrak{p} \in\ \mathcal{P}(K))\ l_{\mathfrak{p}}(E,t) = l_{\mathfrak{p}}(E',t).$$

Обратно, пусть

$$|\{\mathfrak{p} | \mathfrak{p} \in \mathcal{P}(K),\ l_{\mathfrak{p}}(E,t) \neq l_{\mathfrak{p}}(E',t)\}| < \infty,$$

тогда кривые E *и* E' *изогенны.*

Доказательство. Это теорема Фалтингса [76, следствие 2 на стр. 361].

По теореме Хассе,

$$|\ a(\mathfrak{p})| \leq 2N\mathfrak{p}^{1/2}\ \text{ при }\ \mathfrak{p} \in \mathcal{P}(K). \tag{4.5.1}$$

Положим

$$L(E,s) := \prod_{\mathfrak{p} \in\ \mathcal{P}(K)} l_{\mathfrak{p}}(E, N\mathfrak{p}^{-s})^{-1}\ \text{ при }\ s \in \mathbb{C}_{3/2}.$$

Функция $L(E,s)$ называется L - функцией Хассе - Вейля эллиптической кривой E.

Гипотеза 4.5.1. *Положим* $A(E) := (2\pi)^{-2}(N\mathfrak{f}(E))^{1/2}|\ d_K|$. *Существует целая функция* $s \mapsto \Lambda(E,s)$, *удовлетворящая функциональному уравнению*

$$\Lambda(E, 2-s) = \varepsilon\Lambda(E,s)\ \ \textit{при}\ \ s \in \mathbb{C}\ \ c\ \ \varepsilon \in \{\pm 1\} \tag{4.5.2}$$

и такая, что

$$\Lambda(E,s) = A(E)^s\Gamma(s)^2 L(E,s)\ \textit{при}\ \ s \in \mathbb{C}_{3/2}.$$

Гипотеза 1 есть классическая гипотеза Хассе - Вейля, ср. [154].

Гипотеза 4.5.2. *Знак* ε *в функциональном уравнении (2) определяется чётностью ранга* $r(E)$ *кривой* E*:*

$$\varepsilon = (-1)^{r(E)}.$$

Гипотеза 2 является частью гипотез Бёрча и Свиннертон - Дайера.

Обозначим через $\mathfrak{F}$ совокупность параболических $\mathrm{GL}_2(\mathbb{A}_K)$ - автоморфных форм f типа $(1, \mathfrak{n}(f), \mathcal{H}_\infty)$ в смысле Вейля [167, стр. 143] под условием

$$T_\mathfrak{p} f = c(\mathfrak{p}) f,\ c(\mathfrak{p}) \in \mathbb{C} \ \text{ при } \ \mathfrak{p} \in \mathcal{P}(K),\ \mathfrak{n}(f) \neq 0\ (\mathfrak{p}),$$

где $\mathbb{A}_K$ есть кольцо аделей поля K и $T_\mathfrak{p}$ суть операторы Гекке.

Пусть $f \in \mathfrak{F}$. Рассмотрим эйлерово произведение

$$L(f,s) := \prod_{\mathfrak{p} \in\, \mathcal{P}(K)} l_\mathfrak{p}(f, N\mathfrak{p}^{-s})^{-1}, \tag{4.5.3}$$

где

$$l_\mathfrak{p}(f,t) := 1 - c(\mathfrak{p})t + (N\mathfrak{p})t^2 \ \text{ при } \ \mathfrak{p} \in \mathcal{P}(K),\ \mathfrak{n}(f) \neq 0\ (\mathfrak{p})$$

и

$$l_\mathfrak{p}(f,t) := 1 + c(\mathfrak{p})t,\ c(\mathfrak{p}) \in \{0, \pm 1\} \ \text{ при } \ \mathfrak{p} \in \mathcal{P}(K),\ \mathfrak{p} | \mathfrak{n}(f).$$

Как известно, бесконечное произведение (3) абсолютно сходится при $s \in \mathbb{C}_{3/2}$ [106].

Предложение 4.5.2. *Положим* $A(f) := (2\pi)^{-2}(N\mathfrak{n}(f))^{1/2}|d_K|$ *и обозначим через* ε_0 *собственное значение оператора инволюции Фрике. Существует целая функция* $s \mapsto \Lambda(f,s)$*, удовлетворящая функциональному уравнению*

$$\Lambda(f, 2-s) = -\varepsilon_0 \Lambda(f,s) \ \ \textit{при} \ \ s \in \mathbb{C} \tag{4.5.4}$$

и такая, что

$$\Lambda(f,s) = A(f)^s \Gamma(s)^2 L(f,s) \ \ \textit{при} \ \ s \in \mathbb{C}_{3/2}.$$

Доказательство. Рассмотрим автоморфную пару $f, \tilde{f}$. Так как функция $\tilde{f}$ является собственной функцией операторов Гекке с теми же собственными значениями, что и функция f [167, стр. 45], из известной теоремы об однократности спектра [147], [106] следует, что $\tilde{f} = \lambda f$ с $\lambda \in \mathbb{C}^*$. С другой стороны, $\tilde{f} = Jf$, где J - оператор инволюции Фрике. Поэтому доказываемое утверждение следует из [167, теорема 6].

Гипотеза 4.5.3. *При* $\mathfrak{p} \in \mathcal{P}(K)$ *и* $\mathfrak{n}(f) \neq 0(\mathfrak{p})$ *имеет место следующее неравенство:*

$$|c(\mathfrak{p})| \leq 2N\mathfrak{p}^{1/2}.$$

Гипотеза 3 до сих пор не доказана. Эта гипотеза является аналогом гипотезы Рамануджана - Петерсона, доказанной Делинем [63].

Обозначения. Положим $\mathfrak{n}_1(f) := (2d_K)\mathfrak{n}(f)$ при $f \in \mathfrak{F}$;

$$\mathcal{R}(K) := \{f | f \in \mathfrak{F},\ (\forall\, \mathfrak{p} \in\ \mathcal{P}(K))\ l_{\mathfrak{p}}(f,t) \in \mathbb{Q}[t]\}$$

$$\mathcal{M}(K) := \{(E,f) | E \in \mathfrak{E}(K),\ f \in \mathfrak{F},\ (\forall\, \mathfrak{p} \in\ \mathcal{P}(K))\ l_{\mathfrak{p}}(E,t) = l_{\mathfrak{p}}(f,t)\}.$$

и

$$\mathcal{M}_1(K) := \{(E,f) | E \in \mathfrak{E}(K),\ f \in \mathfrak{F},\ \mathfrak{f}(E) = \mathfrak{n}(f),$$

$$l_{\mathfrak{p}}(E,t) = l_{\mathfrak{p}}(f,t)\ \text{ при }\ \mathfrak{p} \in \mathcal{P}(K),\ \mathfrak{p} | \mathfrak{n}_1(f)\}.$$

Определение 4.5.1. *Эллиптическая кривая* E *называется модулярной кривой, если* $(\exists f \in \mathfrak{F})\ (E,f) \in \mathcal{M}(K)$.

Следствие 4.5.1. *Пусть* $(E,f) \in \mathcal{M}(K)$. *Тогда*

$$f \in \mathcal{R}(K),\ \mathfrak{n}(f) = \mathfrak{f}(E),$$

эллиптическая кривая E *удовлетворяет гипотезе* 1 *и автоморфная форма* f *удовлетворяет гипотезе* 3.

Доказательство. Доказываемое утверждение вытекает из предложения 2 и оценки (1).

Следствие 4.5.2. *Модулярные эллиптические кривые* E *и* E' *изогенны тогда и только тогда, когда*

$$(\exists f \in \mathfrak{F})\ \{(E,f),(E',f)\} \subseteq \mathcal{M}(K).$$

Доказательство. Доказываемое утверждение вытекает из предложения 1 и сильной теоремы однократности [147], [106].

Следуя [38], рассмотрим модуль Тэйта $T_2(E)$ и двумерное диадическое представление

$$\rho_E : G_K \to \text{ Aut } V_2(E),$$

описывающее действие группы Галуа G_K на векторном пространстве

$$V_2(E) := T_2(E) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$$

над полем $\mathbb{Q}_2$. Пусть $\mathfrak{p} \in \mathcal{P}(K)$. Обозначим через $\varphi(\mathfrak{p})$ класс автоморфизма Фробениуса в группе G_K, соответствующий "точке" $\mathfrak{p}$. Если $2\mathfrak{f}(E) \neq 0\ (\mathfrak{p})$, то представление ρ_E не разветвлено в точке $\mathfrak{p}$ и характеристический полином оператора $\rho_E(\varphi(\mathfrak{p}))$ равен $l_{\mathfrak{p}}(E,t)$, т.е.

$$\text{tr } \rho_E(\varphi(\mathfrak{p})) = a(\mathfrak{p}) \ \text{ и } \ \det \rho_E(\varphi(\mathfrak{p})) = N\mathfrak{p}.$$

Более того,

$$\rho_E(G_K) \subseteq \text{Aut } T_2(E) \ \text{ и } \ \text{Aut } T_2(E) \cong \text{GL}_2(\mathbb{Z}_2);$$

в дальнейшем, не нарушая общности, мы будем предполагать, что

$$\rho_E(G_K) \subseteq \text{GL}_2(\mathbb{Z}_2). \tag{4.5.5}$$

Представления ρ_E, отвечающие эллиптическим кривым E без комплексного умножения, неприводимы. Все эти утверждения доказаны, например, в цитированной выше монографии [38].

Следствие 4.5.3. *Пусть $\{E, E'\} \subseteq \mathfrak{E}(K)$. Если кривые E и E' не имеют комплексного умножения, не изогенны и*

$$L(E,s) = L(E',s) \tag{4.5.6}$$

то изогенны кривые E' и τE.

Доказательство. Положим

$$W_1 := V_2(E),\ W_2 := V_2(\tau E),\ W_3 := V_2(E'),\ W_4 := V_2(\tau E')$$

и обозначим через ρ_i представление группы Галуа G_K на векторном пространстве $W_i,\ 1 \leq i \leq 4$. Из равенства (6) и теоремы плотности Чеботарёва следует, что

$$\mathrm{tr}\ (\rho_1 \oplus \rho_2) = \mathrm{tr}\ (\rho_3 \oplus \rho_4)$$

и потому [1, гл. VIII, §12, no.1, предложение 3]

$$\rho_1 \oplus \rho_2 \cong \rho_3 \oplus \rho_4.$$

Значит, $\rho_3 \cong \rho_1$ или $\rho_3 \cong \rho_2$; следовательно, в силу предложения 1, кривая E' изогенна одной из кривых E или τE.

Пусть $f \in \mathcal{R}(K)$. Следуя работам [162], [48], построим неприводимое представление

$$\rho_f : G_K \to\ \mathrm{GL}_2(\bar{\mathbb{Q}}_2),$$

удовлетворяющее следующим условиям:

$$\rho_f(G_K) \subseteq \mathrm{GL}_2(\mathfrak{O}_R), \tag{4.5.7}$$

где $\mathfrak{O}_R$ есть кольцо целых элементов поля R и

$$\mathbb{Q}_2 \subseteq R \subseteq \bar{\mathbb{Q}}_2,\ [R : \mathbb{Q}_2] \leq 4;$$

если $\mathfrak{p} \in \mathcal{P}(K)$ и $\mathfrak{n}_1(f) \neq 0\ (\mathfrak{p})$, то представление ρ_f не разветвлено в точке $\mathfrak{p}$ и характеристический полином оператора $\rho_f(\varphi(\mathfrak{p}))$ равен $l_{\mathfrak{p}}(E, t)$, т.е.

$$\mathrm{tr}\ \rho_f(\varphi(\mathfrak{p})) = c(\mathfrak{p})\ \text{ и }\ \det \rho_f(\varphi(\mathfrak{p})) = N\mathfrak{p}.$$

Пусть $\{\mathfrak{p}, \mathfrak{q}\} \subseteq \mathcal{P}(K),\ \mathfrak{n}_1(f) \neq 0\ (\mathfrak{p}),\ \mathfrak{n}_1(f) \neq 0\ (\mathfrak{q})$ и

$$l_{\mathfrak{p}}(f, t) = (1 - \alpha(\mathfrak{p})t)(1 - \beta(\mathfrak{p})t),\ l_{\mathfrak{q}}(f, t) = (1 - \alpha(\mathfrak{q})t)(1 - \beta(\mathfrak{q})t);$$

если $c(\mathfrak{q}) \neq 0$ и $\alpha(\mathfrak{p}) \neq \beta(\mathfrak{p})$, то поле

$$R = \mathbb{Q}_2(\alpha(\mathfrak{p}), \alpha(\mathfrak{q})). \tag{4.5.8}$$

удовлетворяет условию (7).

Следствие 4.5.4. *Имеет место следующее соотношение*

$$\mathcal{M}(K) = \{(E,f)|(E,f) \in \mathcal{M}_1(K),\ \rho_E \cong \rho_f\}.$$

Доказательство. Пусть $(E,f) \in \mathcal{M}_1(K)$, тогда $\mathfrak{f}(E) = \mathfrak{n}(f)$ и $l_\mathfrak{p}(E,t) = l_\mathfrak{p}(f,t)$ при $\mathfrak{p}|\mathfrak{n}_1(f)$; если, кроме того, $\rho_E \cong \rho_f$, то

$$a(\mathfrak{p}) = \operatorname{tr} \rho_E(\varphi(\mathfrak{p})) = \operatorname{tr} \rho_f(\varphi(\mathfrak{p})) = c(\mathfrak{p})$$

при $\mathfrak{p} \nmid \mathfrak{n}_1(f)$, так как $2\mathfrak{f}(E)|\ \mathfrak{n}_1(f)$. Отсюда следует, что

$$\mathcal{M}(K) \supseteq \{(E,f)|(E,f) \in \mathcal{M}_1(K),\ \rho_E \cong \rho_f\}.$$

Пусть $(E,f) \in \mathcal{M}(K)$, тогда

$$l_\mathfrak{p}(E,t) = l_\mathfrak{p}(f,t) \text{ при } \mathfrak{p} \in\ \mathcal{P}(K). \tag{4.5.9}$$

Из соотношения (9) следует, что $(E,f) \in \mathcal{M}_1(K)$ и

$$\operatorname{tr} \rho_E(\varphi(\mathfrak{p})) = a(\mathfrak{p}) = c(\mathfrak{p}) = \operatorname{tr} \rho_f(\varphi(\mathfrak{p})) \text{ при } \ \mathfrak{p} \nmid \mathfrak{n}_1(f),\ \mathfrak{p} \in\ \mathcal{P}(K). \tag{4.5.10}$$

Из теоремы плотности Чеботарёва и соотношения (10) следует, что множество

$$\{\sigma \mid\ \sigma \in G_K,\ \operatorname{tr} \rho_E(\sigma) = \operatorname{tr} \rho_f(\sigma)\}$$

является плотным подмножеством группы G_K. Значит, $\operatorname{tr} \rho_E = \operatorname{tr} \rho_f$; поэтому из [1, гл. VIII, §12, no.1, предложение 3] следует, что $\rho_E \cong \rho_f$, так как представления ρ_E и ρ_f неприводимы и, следовательно, полупросты. Таким образом,

$$\mathcal{M}(K) \subseteq \{(E,f)|(E,f) \in \mathcal{M}_1(K),\ \rho_E \cong \rho_f\}.$$

Тем самым следствие 4 доказано.

2. Нам потребуется несколько простых результатов из теории групп. Обозначим через $\mathcal{C}_n$ циклическую группу порядка n и через $\mathfrak{S}_n$ симметрическую группу перестановок n элементов. Как известно,

$$\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) \text{ и } \ \mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3.$$

Лемма 4.5.1. *Рассмотрим представления*

$$\rho_1, \rho_2 : \mathfrak{S}_3 \to \ \mathrm{GL}_2(\mathbb{F}_2).$$

Если

$$\mathrm{Ker}\ \rho_1 = \mathrm{Ker}\ \rho_2 = \mathcal{C}_1,$$

то представления ρ_1 и ρ_2 эквивалентны.

Доказательство. В этом нетрудно убедиться.

Лемма 4.5.2. *Пусть $\gamma \in \mathrm{GL}_2(\mathbb{F}_2)$, тогда*

$$\mathrm{tr}\ \gamma = 0 \Leftrightarrow \gamma^2 = 1.$$

Proof. В этом нетрудно убедиться.

Как известно, группа $\mathfrak{S}_3$ порождается транспозициями $\zeta := (12)$ и $\eta := (13)$, а группа $\mathfrak{S}_4$ - циклами $\omega_1 := (1324)$ и $\omega_2 := (1234)$. Определим эпиморфизмы

$$\tau_1 : \mathfrak{S}_4 \times \mathcal{C}_2 \to \ \mathfrak{S}_3 \times \mathcal{C}_2,\ \tau_1 : (\omega_1, 1) \mapsto (\zeta, 1),\ (\omega_2, 1) \mapsto (\eta, 1),\ (1, \zeta) \mapsto (1, \zeta)$$

и

$$\tau_2 : \mathfrak{S}_4 \times \mathcal{C}_2 \to \ \mathfrak{S}_4,\ \tau_2 : (\alpha, \beta) \mapsto (\alpha, 1) \text{ при } \alpha \in \mathfrak{S}_4,\ \beta \in \mathcal{C}_2.$$

Обозначим через $\mathrm{ord}\ \gamma$ порядок группового элемента γ.

Лемма 4.5.3. *Имеют место следующие соотношения:*

$$\mathrm{Ker}\ \tau_1 \cong \mathcal{C}_2^2 \ \textit{и}\ \ \mathrm{Ker}\ \tau_2 \cong \mathcal{C}_2.$$

Пусть $\gamma \in \mathfrak{S}_4 \times \mathcal{C}_2$, тогда

$$\mathrm{ord}\ \gamma = 6 \Leftrightarrow \mathrm{ord}\ \tau_1(\gamma) = 6 \ \ \textit{и}\ \ \mathrm{ord}\ \gamma = 4 \Leftrightarrow \mathrm{ord}\ \tau_2(\gamma) = 4.$$

Доказательство. В этом нетрудно убедиться.

Рассмотрим группу

$$\mathfrak{G} := \{(m, n) \mid \ m \in M_2(\mathbb{F}_2),\ n \in \mathrm{GL}_2(\mathbb{F}_2)\},$$

определив груповую операцию по формуле

$$(m_1, n_1) \cdot (m_2, n_2) := (m_1 + n_1 m_2 n_1^{-1}, n_1 n_2)$$

при $\{(m_1, n_1), (m_2, n_2)\} \subseteq \mathfrak{G}$. Положим

$$M_2^{(0)}(\mathbb{F}_2) := \{a \mid \ a \in M_2(\mathbb{F}_2),\ \mathrm{tr}\ a = 0\}$$

и рассмотрим подгруппу

$$\mathfrak{G}^{(0)} := \{(m, n) \mid \ m \in M_2^{(0)}(\mathbb{F}_2),\ n \in \mathrm{GL}_2(\mathbb{F}_2)\};$$

группы $\mathfrak{G}$. Определим отображение

$$g : \mathfrak{G} \to \ \mathbb{F}_2,\ g : (m, n) \mapsto \mathrm{tr}\ (m \cdot n) \ \text{ при } \ (m, n) \in \mathfrak{G}$$

и положим $g_0 := g \mid \mathfrak{G}^{(0)}$.

Лемма 4.5.4. *Группа $\mathfrak{G}^{(0)}$ изоморфна прямому произведению $\mathfrak{S}_4 \times \mathcal{C}_2$.*

Доказательство. Положим

$$v_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, v_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, v_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, v_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

заметим, что матрицы $\{v_0, v_1, v_2\}$ образуют базис векторного пространства $M_2^{(0)}(\mathbb{F}_2)$ над полем $\mathbb{F}_2$ и $v_3 = v_1 + v_2$, и отождествим $\mathrm{GL}_2(\mathbb{F}_2)$ с $\mathfrak{S}_3$, воспользовавшись изоморфизмом

$$\iota : \mathfrak{S}_3 \to \mathrm{GL}_2(\mathbb{F}_2),\ \iota : (12) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \iota : (13) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Легко видеть, что $\mathfrak{G}^{(0)} = H_1 \times H_2$, где

$$H_1 := \{(0, \nu), (v_i, \nu) \mid \ 1 \leq i \leq 3,\ \nu \in \mathfrak{S}_3\} \ \text{ и } \ H_2 := \{(0, (1)), (v_0, (1))\}$$

с таблицей умножения

$$(v_k, \sigma) \cdot (v_i, \tau) = (v_k + v_{\sigma(i)}, \sigma\tau),\ \{\sigma, \tau\} \subseteq \mathfrak{S}_3,\ 0 \leq i, k \leq 3, \qquad (4.5.11)$$

где $\sigma(0) = 0$ при $\sigma \in \mathfrak{S}_3$. Ясно, что $H_2 \cong \mathcal{C}_2$. Рассмотрим группу Клейна

$$\mathfrak{B}_2 := \{(1), (12)(34), (13)(24), (14)(23)\}$$

и определим мономорфизм

$$\vartheta^{(0)} : \mathfrak{B}_2 \to M_2^{(0)}(\mathbb{F}_2),\ \vartheta^{(0)} : (13)(24) \mapsto v_2,\ (14)(23) \mapsto v_1.$$

Так как

$$\mathfrak{S}_4 = \bigcup_{\sigma \in \mathfrak{S}_3} \mathfrak{B}_2 \sigma,$$

отображение

$$\vartheta : \mathfrak{S}_4 \to\ H_1,\ \vartheta : \alpha\sigma \mapsto (\vartheta^{(0)}(\alpha), \sigma),\ \alpha \in \mathfrak{B}_2,\ \sigma \in \mathfrak{S}_3,$$

есть изоморфизм. Таким образом, $\mathfrak{S}_4 \cong H_1$ и, значит, $\mathfrak{G}^{(0)} \cong \mathfrak{S}_4 \times \mathcal{C}_2$. Лемма доказана.

Обозначим через $j : \mathfrak{G}^{(0)} \to \mathfrak{S}_4 \times \mathcal{C}_2$ построенный при доказательстве леммы 4 изоморфизм.

Лемма 4.5.5. *Имеет место следующее соотношение:*

$$g_0^{-1}(\{1\}) = \{\sigma \mid\ \sigma \in \mathfrak{G}^{(0)},\ \mathrm{ord}\ \sigma \in \{4, 6\}\}. \tag{4.5.12}$$

Доказательство. Соотношение (12) вытекает из закона умножения (11) и определения отображения g_0.

Обозначим через $\mathfrak{f}(L|k)$ ведущий модуль конечного абелева расширения $L|k$ полей алгебраических чисел.

Лемма 4.5.6. *Рассмотрим конечное циклическое расширение расширение $T|k$ полей алгебраических чисел степени $l := [T : k]$. Если $l \in \mathcal{P}$, то*

$$\mathfrak{f}(T|k) = \prod_{\mathfrak{p} \in \mathcal{P}(k)} \mathfrak{p}^{\alpha(\mathfrak{p})},\ \alpha(\mathfrak{p}) \in \mathbb{Z},$$

где

$$\alpha(\mathfrak{p}) \in \{0, 1\}\ \ при\ \ \mathfrak{p} \nmid l\ \ \ и\ \ \ 2 \leq \alpha(\mathfrak{p}) \leq \frac{le(\mathfrak{p}, l)}{l-1} + 1\ \ при\ \ \mathfrak{p} | \ l.$$

Доказательство. См. [60, стр. 149-150, 487].

3. В этом разделе излагается так называемый метод Фалтингса - Серра (ср. [66], [155], [152]). Рассмотрим два непрерывных диадических представления

$$\rho_1, \rho_2 : G_K \to \mathrm{GL}_2(\mathbb{Z}_2);$$

при $i \in \{1, 2\}$, положим $\chi_i := \mathrm{tr}\ \rho_i$ и обозначим через

$$\bar{\rho}_i : G_K \to \mathrm{GL}_2(\mathbb{F}_2)$$

редукцию представления ρ_i по модулю 2. Предположим, что

$$\bar{\rho}_1 = \bar{\rho}_2,\ \bar{\rho}_1(G_K) = \mathrm{GL}_2(\mathbb{F}_2),\ \det \rho_1 = \det \rho_2$$

и представления ρ_1 и ρ_2 не разветвлены вне конечного подмножества S множества простых идеалов $\mathcal{P}(K)$ поля K. Пусть $\mathrm{Ker}\ \bar{\rho}_1 = G_L$, тогда $L|K$ есть конечное нормальное расширение и $\mathrm{Gal}(L|K) \cong \mathfrak{S}_3$. Обозначим через $\mathfrak{M}$ множество полей M таких, что $L \subseteq M \subseteq \bar{\mathbb{Q}}$ и $M|K$ является конечным нормальным расширением, не разветвлённым в точках множества $\mathcal{P}(K) \setminus S$. При $M \in \mathfrak{M},\ \mathfrak{p} \in \mathcal{P}(K),\ \mathfrak{P} \in \mathcal{P}(L),\ \mathfrak{P}|\mathfrak{p}$ определим $f_M(\mathfrak{p})$ равенством

$$N_{M/K}\mathfrak{P} = \mathfrak{p}^{f_M(\mathfrak{p})}.$$

Лемма 4.5.7. *Пусть $\chi_1 \neq \chi_2$. Тогда найдётся поле M, удовлетворяющее следующим условиям:*

(i) $M \in \mathfrak{M}$;

(ii) группа Галуа $\mathrm{Gal}(M|K)$ изоморфна подгруппе группы $\mathfrak{S}_4 \times \mathcal{C}_2$;

(ii), $f_M(\mathfrak{p}) \in \{4, 6\}$ при некотором $\mathfrak{p}$ в $\mathcal{P}(K) \setminus S$;

(iv), $f_M(\mathfrak{p}) \in \{4, 6\} \Rightarrow \chi_1(\varphi(\mathfrak{p})) \neq \chi_2(\varphi(\mathfrak{p}))$ для любого $\mathfrak{p}$ в $\mathcal{P}(K) \setminus S$.

Доказательство. Положим

$$r := \max\{s | s \in \mathbb{N},\ \chi_1 = \chi_2 \pmod{2^s}\}. \tag{4.5.13}$$

Из неравенства $\chi_1 \neq \chi_2$ следует, что $r \in \mathbb{N}$. Можно показать, что

$$\rho_1 = (1 + 2^r \mu)\rho_2$$

для некоторой функции $\mu : G_K \to M_2(\mathbb{Z}_2)$, см. [156, теорема 1] и [66, замечание 6]. Обозначим через $\bar{\mu} : G_K \to M_2(\mathbb{F}_2)$ редукцию функции μ по модулю 2. Отображение

$$h : G_K \to \mathfrak{G},\ h : \sigma \mapsto (\bar{\mu}(\sigma), \bar{\rho}_1(\sigma)) \text{ при } \sigma \in G_K$$

есть гомоморфизм и $h(G_K) \subseteq \mathfrak{G}^{(0)}$, так как

$$\det \rho_1 = \det \rho_2 \ \text{ и } \ \det (1 + 2^r \mu) = 1 + 2^r \mathrm{tr}\ \mu \pmod{2^{r+1}}$$

и потому $\mathrm{tr}\ \bar{\mu} = 0$. Пусть

$$M := \{x \mid \ x \in \bar{K}, \sigma x = x \text{ при } \sigma \in \mathrm{Ker}\ h\}.$$

Тогда $M \in \mathfrak{M},\ \mathrm{Ker}\ h = G_M,\ \mathrm{Gal}(M|K) \cong h(G_K),\ f_M(\mathfrak{p}) = \mathrm{ord}\ h(\varphi(\mathfrak{p}))$ при $\mathfrak{p} \in \mathcal{P}(K) \backslash S$ и, ввиду леммы 6, группа Галуа $\mathrm{Gal}(M|K)$ изоморфна подгруппе группы $\mathfrak{S}_4 \times \mathcal{C}_2$. Определим отображение

$$h_0 := g \circ h,\ h_0 : G_K \to \mathbb{F}_2,\ h_0 : \sigma \mapsto \mathrm{tr}\ (\bar{\mu}(\sigma)\bar{\rho}_1(\sigma)) \text{ при } \sigma \in G_K.$$

Как следует из леммы 5,

$$h_0(\sigma) = 1 \Leftrightarrow \mathrm{ord}\ h(\sigma) \in \{4, 6\}.$$

Предположим, что

$$(\forall \mathfrak{p} \in \mathcal{P}(K) \setminus S)\ f_M(\mathfrak{p}) \notin \{4, 6\}. \tag{4.5.14}$$

Тогда $\mathrm{ord}\ h(\varphi(\mathfrak{p})) \notin \{4, 6\}$ и потому

$$0 = h_0(\varphi(\mathfrak{p})) = \mathrm{tr}\ (\bar{\mu}(\varphi(\mathfrak{p}))\bar{\rho}_1(\varphi(\mathfrak{p}))) = (\chi_1(\varphi(\mathfrak{p})) - \chi_2(\varphi(\mathfrak{p})))2^{-r} \pmod 2,$$

то есть

$$|\chi_1(\varphi(\mathfrak{p})) - \chi_2(\varphi(\mathfrak{p}))|_2 \leq 2^{-r-1} \ \text{ при } \ \mathfrak{p} \in \mathcal{P}(K) \setminus S. \tag{4.5.15}$$

По теореме плотности Чеботарёва, из соотношения (15) следует, что

$$\chi_1 = \chi_2 \pmod{2^{r+1}}.$$

Так как последнее сравнение противоречит определению (13), соотношение (14) не имеет места; значит, существует простой идеал $\mathfrak{p}$ в $\mathcal{P}(K) \setminus S$, для которого $f_M(\mathfrak{p}) \in \{4, 6\}$ и потому

$$1 = h_0(\varphi(\mathfrak{p})) = \operatorname{tr}\,(\bar{\mu}(\varphi(\mathfrak{p}))\bar{\rho}_1(\varphi(\mathfrak{p}))) = (\chi_1(\varphi(\mathfrak{p})) - \chi_2(\varphi(\mathfrak{p})))2^{-r} \pmod 2,$$

откуда, в частности, следует, что $\chi_1(\varphi(\mathfrak{p})) \neq \chi_2(\varphi(\mathfrak{p}))$. Лемма доказана.

Лемма 4.5.8. *Предположим, что для любого расширения полей $M|K$ с $M \in \mathfrak{M}$ из соотношения* $\operatorname{Gal}(M|K) \cong \mathfrak{S}_3 \times \mathcal{C}_2$ *следует, что*

$$(\exists \mathfrak{p} \in \mathcal{P}(K) \setminus S)\ f_M(\mathfrak{p}) = 6 \text{ и } \chi_1(\varphi(\mathfrak{p})) = \chi_2(\varphi(\mathfrak{p})),$$

а из соотношения $\operatorname{Gal}(M|K) \cong \mathfrak{S}_4$ *следует, что*

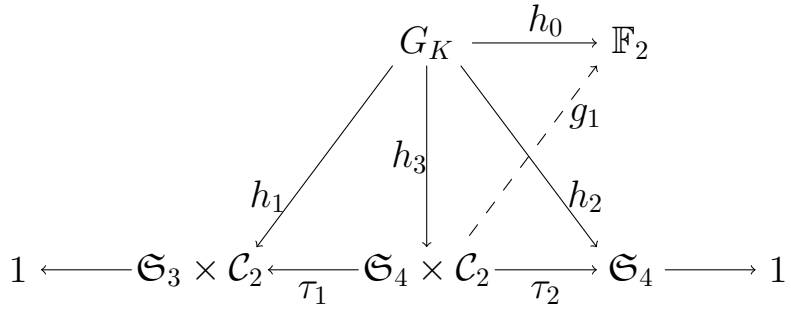
$$(\exists \mathfrak{p} \in \mathcal{P}(K) \setminus S)\ f_M(\mathfrak{p}) = 4 \text{ и } \chi_1(\varphi(\mathfrak{p})) = \chi_2(\varphi(\mathfrak{p})).$$

Тогда $\rho_1 \cong \rho_2$.

Доказательство. Предположим, что представления ρ_1 и ρ_2 не эквивалентны. Тогда, так как эти представления неприводимы, из известной и уже цитированной леммы [1, гл. VIII, §12, no. 1, предложение 3] следует, что $\chi_1 \neq \chi_2$ и, значит, по только что доказанной лемме 7, существуют поле M в $\mathfrak{M}$, гомоморфизм $h_3 : G_K \to \mathfrak{S}_4 \times \mathcal{C}_2$ под условием $h_3(G_K) \cong \operatorname{Gal}(M|K)$ и простой идеал $\mathfrak{p}$ в $\mathcal{P}(K) \setminus S$ с $f_M(\mathfrak{p}) \in \{4, 6\}$. Отображения

$$h_0,\ h_3 := j \circ h,\ h_1 := \tau_1 \circ h_3,\ h_2 := \tau_2 \circ h_3,\ g_1 := g_0 \circ j^{-1},\ \tau_1,\ \tau_2$$

образуют коммутативную диаграмму с точной нижней строкой:



Положим

$$M_i := \{x | x \in \bar{K}, \sigma x = x \text{ при } \sigma \in \operatorname{Ker} h_i\},\ i = 1, 2,$$

и заметим, что

$$\operatorname{Ker} h_3 = G_M,\ \operatorname{Ker} h_i = G_{M_i},\ \operatorname{Gal}(M_i|K) \cong h_i(G_K) \text{ и } M_i \subseteq M$$

при $i \in \{1, 2\}$. Так как $M \in \mathfrak{M}$ и $\operatorname{Gal}(L|K) \cong \mathfrak{S}_3$, существует эпиморфизм

$$j_0 : h_3(G_K) \to\ \mathfrak{S}_3;$$

пусть $h_0 := j_0 \circ h_3$, тогда $\operatorname{Ker} h_0 = G_L$. Легко видеть, что $\operatorname{Ker} h_i \subseteq \operatorname{Ker} h_0$ и потому $L \subseteq M_i$ при $i = 1, 2$. Итак, $\{M_1, M_2\} \subseteq \mathfrak{M}$. Пусть $\sigma \in \varphi(\mathfrak{p})$, тогда $\operatorname{ord} h_3(\sigma) \in \{4, 6\}$ и потому из леммы 3 следует, что $\operatorname{ord} h_1(\sigma) = 6$ или $\operatorname{ord} h_2(\sigma) = 4$. Таким образом,

$$h_1(G_K) = \mathfrak{S}_3 \times \mathcal{C}_2 \ \text{ или } \ h_2(G_K) = \mathfrak{S}_4. \tag{4.5.16}$$

По условию леммы, из дизъюнкции (16) вытекает, что существует простой идеал $\mathfrak{p}$, удовлетворяющий следующим условиям:

$$\mathfrak{p} \in \mathcal{P}(K) \setminus S,\ \chi_1(\varphi(\mathfrak{p})) = \chi_2(\varphi(\mathfrak{p}))\ \text{ и }\ (f_{M_1}(\mathfrak{p}) = 6 \text{ или } f_{M_2}(\mathfrak{p}) = 4).$$

Но существование такого идеала противоречит выбору поля M по лемме 7. Тем самым, лемма 8 доказана.

4. Положим теперь $K = \mathbb{Q}(\sqrt{-23})$ и пусть

$$\omega := \frac{1 + \sqrt{-23}}{2}.$$

Тогда $\mathfrak{o}_K = \mathbb{Z} \oplus \omega\mathbb{Z},\ d_K = -23$ и $h_K = 3$. Пусть $p \in \mathcal{P}$. Обозначим через $\mathfrak{p}_p$ один из простых идеалов кольца $\mathfrak{o}_K$ под условием $\mathfrak{p}_p \in \mathcal{P}(K),\ \mathfrak{p}_p | p$ и положим $p\mathfrak{o}_K = \mathfrak{p}_p\bar{\mathfrak{p}}_p$ при $p\mathfrak{o}_K \notin \mathcal{P}(K)$, так что, например,

$$23\mathfrak{o}_K = \mathfrak{p}_{23}^2,\ \bar{\mathfrak{p}}_{23} = \mathfrak{p}_{23},\ 3\mathfrak{o}_K = \mathfrak{p}_3\bar{\mathfrak{p}}_3,\ 5\mathfrak{o}_K = \mathfrak{p}_5.$$

Положим

$$\mathfrak{N} := \{\mathfrak{p}_2, \bar{\mathfrak{p}}_2, \mathfrak{p}_3, \bar{\mathfrak{p}}_3, \mathfrak{p}_{23}\} \text{ и } \mathfrak{m} := (2)^3(3)^2\mathfrak{p}_{23}.$$

Рассмотрим эллиптическую кривую

$$E: \ y^2 + (\omega+1)xy + y = x^3 + (\omega+1)x^2 - 7x + (5-3\omega) \tag{4.5.17}$$

и обозначим через f параболическую форму f_{44} из списка Лингхама [112, гл. 7].

Лемма 4.5.9. *Эллиптическая кривая E не имеет комплексного умножения и ранк E равен 1; $f \in \mathcal{R}(K)$ и $\Lambda(f, 2-s) = -\Lambda(f, s)$ при $s \in \mathbb{C}$;*

$$(E, f) \in \mathcal{M}_1(K), \ \mathfrak{f}(E) = \mathfrak{n}(f) = \mathfrak{p}_2\mathfrak{p}_3^3\bar{\mathfrak{p}}_3, \ \mathfrak{n}_1(f) := (46)\cdot\mathfrak{n}(f);$$

$$a(\mathfrak{p}) = c(\mathfrak{p}) \ \ \textit{при} \ \ N\mathfrak{p} < 50, \ \mathfrak{p} \in \ \mathcal{P}(K),$$

и

$$c(\mathfrak{p}_2) = c(\mathfrak{p}_5) = 1, c(\bar{\mathfrak{p}}_2) = c(\mathfrak{p}_{13}) = -2, c(\mathfrak{p}_3) = 0,$$

$$c(\bar{\mathfrak{p}}_3) = c(\bar{\mathfrak{p}}_{13}) = c(\mathfrak{p}_{23}) = -1, c(\mathfrak{p}_7) = 6, c(\mathfrak{p}_{29}) = -6,$$

$$c(\bar{\mathfrak{p}}_{29}) = -9, c(\mathfrak{p}_{31}) = c(\bar{\mathfrak{p}}_{47}) = 3, c(\bar{\mathfrak{p}}_{31}) = -10,$$

$$c(\mathfrak{p}_{41}) = -8, c(\bar{\mathfrak{p}}_{41}) = c(\mathfrak{p}_{47}) = 5.$$

Доказательство. Эти утверждения доказаны в цитированной выше диссертации Лингхама [112, гл. 7].

В этом параграфе будет доказана следующая теорема.

Теорема 4.5.1. *Автоморфная форма f и эллиптическя кривая* (17) *связаны соотношением $(E, f) \in \mathcal{M}(K)$.*

Следствие 4.5.5. *Кривая E удовлетворяет гипотезам 1 и 2, а автоморфная форма f - гипотезе 3.*

Доказательство. Это утверждение вытекает из теоремы 1, следствия 1 и леммы 9.

Теорема 4.5.2. *Диадические представления ρ_E и ρ_f эквивалентны.*

Теорема 1 вытекает из теоремы 2, следствия 4 и леммы 9. Остаётся доказать теорему 2.

Из соотношения (8) и леммы 9 следует, что поле

$$R = \mathbb{Q}_2(\alpha(\mathfrak{p}_{41}), \alpha(\bar{\mathfrak{p}}_{31})) = \mathbb{Q}_2(\sqrt{-1}, \sqrt{-6})$$

удовлетворяет соотношению (7). Не нарушая общности, положим

$$R := \mathbb{Q}_2(\sqrt{-1}, \sqrt{-6}); \tag{4.5.18}$$

обозначив через $\mathfrak{m}_R$ максимальный идеал кольца O_R, получим

$$O_R/\mathfrak{m}_R \cong \mathbb{F}_2.$$

Обозначим через

$$\bar{\rho}_E : G_K \to \mathrm{GL}_2(\mathbb{F}_2)$$

редукцию представления ρ_E по модулю (2) (ср. (5)) и через

$$\bar{\rho}_f : G_K \to \mathrm{GL}_2(\mathbb{F}_2)$$

редукцию представления ρ_f по модулю $\mathfrak{m}_R$ (ср. (7) и (18)). Пусть

$$\mathrm{Ker}\ \bar{\rho}_E = G_L \ \text{ и } \ \mathrm{Ker}\ \bar{\rho}_f = G_{L'},$$

тогда $L|K$ и $L'|K$ суть конечные нормальные расширения полей с

$$\mathrm{Gal}(L|K) \cong \bar{\rho}_E(G_K) \ \text{ и } \ \mathrm{Gal}(L'|K) \cong \bar{\rho}_f(G_K).$$

Лемма 4.5.10. *Поле L является композитом двух полей K_1 и K_2 под условием*

$$[K_1 : K] = 3,\ [K_2 : K] = 2,\ K_2 \cong \mathbb{Q}[t]/(f(t)),$$

где $f(t) := t^4 - t^3 + 8t^2 - t + 1$. Кроме того,

$$d_L = 2^{13} \cdot 3^7 \cdot 23^6, \ \ \mathrm{Gal}(L|K) \cong \mathfrak{S}_3$$

и, значит, $\bar{\rho}_E(G_K) = \mathrm{GL}_2(\mathbb{F}_2)$.

Доказательство. Приведём уравнение (17) к форме Вейерштрасса

$$E:\ y^2 = F(x),\ F(t) := t^3 + \frac{7\omega - 1}{4}\, t^2 + \frac{\omega - 13}{2}\, t + \frac{21}{4} - 3\omega = \prod_{i=1}^{3}(t - \alpha_i)$$

и положим $K_1 := K(\alpha_1)$. По построению, $L = K(\alpha_1, \alpha_2, \alpha_3)$; стандартные алгорифмы [144] приводят к сформулированным результатам.

Следствие 4.5.6. *Расширения полей $L|K$ и $L'|K$ не разветвлены в точке $\mathfrak{p}$ при $\mathfrak{p} \in \mathcal{P}(K) \setminus \mathfrak{N}$.*

Доказательство. Пусть $\mathfrak{p} \in \mathcal{P}(K) \setminus \mathfrak{N}$. Из лемм 9 и 10 следует, что $\mathfrak{n}_1(f) \neq 0 \pmod{\mathfrak{p}}$ и $d_L \neq 0 \pmod{\mathfrak{p}}$, значит, расширения $L|K$ и $L'|K$ не разветвлены в точке $\mathfrak{p}$.

Следствие 4.5.7. *Имеет место соотношение*

$$|\bar{\rho}_f(G_K)| \notin \{1, 2\}.$$

Доказательство. Это утверждение следует из леммы 2, так как $\operatorname{tr} \bar{\rho}_f(\varphi(\mathfrak{p}_5)) = 1$, по лемме 9.

Рассмотрим поле алгебраических чисел k и, при $\mathfrak{a} \in I_0(k)$, положим

$$J(\mathfrak{a}) := \{\mathfrak{A} | \mathfrak{A} = \mathfrak{B}\mathfrak{C}^{-1},\ \{\mathfrak{B},\ \mathfrak{C}\} \subseteq I_0(k),\ (\mathfrak{B}\mathfrak{C}, \mathfrak{a}) = (1)\},$$

$$Pr(\mathfrak{a}) := \{(\alpha) | \alpha \in k^*,\ \alpha = 1 \pmod{\mathfrak{a}}\},\ H(\mathfrak{a}) := J(\mathfrak{a})/Pr(\mathfrak{a});$$

обозначим через $k(\mathfrak{a})|k$ абелево расширение, соответствующее (по одной из теорем теории полей классов) группе $H(\mathfrak{a})$, и отождествим, не нарушая общности, группы $H(\mathfrak{a})$ и $\operatorname{Gal}(k(\mathfrak{a})|k)$. Обозначим через $\hat{B}$ группу характеров конечной абелевой группы B.

Лемма 4.5.11. *Группа $\bar{\rho}_f(G_K)$ не изоморфна группе $\mathcal{C}_3$.*

Доказательство. Положим $\mathcal{P}_0 := \{\mathfrak{p}_7, \mathfrak{p}_{13}\}$. Ясно, что

$$\mathcal{P}_0 \subseteq \mathcal{P}(K) \setminus \mathfrak{N}\,;$$

с другой стороны, в силу леммы 9,

$$(\forall \mathfrak{q} \in \mathcal{P}_0)\mathrm{tr}\ \bar{\rho}_f(\varphi(\mathfrak{q})) = 0. \tag{4.5.19}$$

Допустим, что $|\bar{\rho}_f(G_K)| = 3$. Тогда $L'|K$ есть циклическое расширение третьей степени, и потому, в силу леммы 6 и следствия 6,

$$K \subseteq L' \subseteq K(\mathfrak{m}).$$

Пусть $\chi \in \hat{H}(\mathfrak{m})$ и $\mathrm{Ker}\ \chi = \mathrm{Gal}(K(\mathfrak{m})|L')$, тогда $\mathrm{ord}\ \chi = 3$. С другой стороны, $\chi(\mathfrak{p}_7) \neq 1$ или $\chi(\mathfrak{p}_{13}) \neq 1$ [144] и потому существует простой идеал $\mathfrak{q}$ под условием

$$\mathrm{ord}\ \bar{\rho}_f(\varphi(\mathfrak{q})|L')) = 3 \ \text{ и } \ \mathfrak{q} \in \mathcal{P}_0.$$

Из последнего условия и леммы 2 следует, что

$$(\exists \mathfrak{p} \in \mathcal{P}_0)\mathrm{tr}\ \bar{\rho}_f(\varphi(\mathfrak{p})) = 1. \tag{4.5.20}$$

Соотношения (19) и (20) противоречат друг другу, и значит $|\bar{\rho}_f(G_K)| \neq 3$. Лемма доказана.

Следствие 4.5.8. *Имеет место следующее соотношение:*

$$\bar{\rho}_f(G_K) = \mathrm{GL}_2(\mathbb{F}_2).$$

Доказательство. Это утверждение вытекает из леммы 11 и следствия 7.

Лемма 4.5.12. *Представление $\rho_f : G_K \to \mathrm{GL}_2(\bar{\mathbb{Q}}_2)$ эквивалентно некоторому представлению $\check{\rho}_f : G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$.*

Доказательство. В силу следствия 8, представление $\bar{\rho}_f$ абсолютно неприводимо. Из теоремы плотности Чеботарёва и леммы 9 следует, что $\mathrm{tr}\ \rho_f(G_K) \subseteq \mathbb{Q}_2$. С другой стороны, $\rho_f(G_K) \subseteq \mathrm{GL}_2(O_R)$ и $O_R \cap \mathbb{Q}_2 = \mathbb{Z}_2$. Значит, $\mathrm{tr}\ \rho_f(G_K) \subseteq \mathbb{Z}_2$ и существование искомого представления $\check{\rho}_f$ следует из [156, следствие 5] (cf. [66, теорема 5.5]).

В силу леммы 10 и следствия 8,

$$\mathrm{Gal}(L|K) \cong \mathrm{Gal}(L'|K) \cong \mathfrak{S}_3$$

однозначно определены квадратичные расширения $K_2|K$ и $K_2'|K$ под условием

$$K \subseteq K_2 \subseteq L \ \text{ и } \ K \subseteq K_2' \subseteq L'.$$

Лемма 4.5.13. *Поля K_2 и K_2' совпадают: $K_2 = K_2'$.*

Доказательство. Как и при доказательстве леммы 11, из леммы 6 и следствия 6 вытекает включение

$$K \subseteq K_2 \cdot K_2' \subseteq K(\mathfrak{m}).$$

Пусть $\{\psi, \psi'\} \subseteq \hat{H}(\mathfrak{m})$, $\mathrm{Ker}\ \psi = G(K(\mathfrak{m})|K_2)$ и $\mathrm{Ker}\ \psi' = G(K(\mathfrak{m})|K_2')$. Пусть $\mathfrak{p} \in \mathcal{P}(K) \setminus \mathfrak{N}$; ясно, что простой идеал $\mathfrak{p}$ равен произведению двух различных простых идеалов в поле K_2 (соответственно в поле K_2') тогда и только тогда, когда $\psi(\mathfrak{p}) = 1$ (соответственно $\psi'(\mathfrak{p}) = 1$). Положим

$$\mathcal{P}_1 := \{\mathfrak{p}_5, \bar{\mathfrak{p}}_{13}, \bar{\mathfrak{p}}_{29}, \mathfrak{p}_{31}, \bar{\mathfrak{p}}_{41}\};$$

ясно, что $\mathcal{P}_1 \subseteq (\mathcal{P}(K) \setminus \mathfrak{N})$, и можно показать [144], что

$$H(\mathfrak{m})/H(\mathfrak{m})^2 \cong \mathcal{C}_2^6,$$

множество $\mathcal{P}_1$ порождает подгруппу группы $H(\mathfrak{m})/H(\mathfrak{m})^2$, изоморфную группе $\mathcal{C}_2^5$, и $\psi(\mathcal{P}_1) = \{1\}$. Допустим, что $\psi \neq \psi'$, тогда $\psi'(\mathfrak{p}_0) = -1$ при некотором $\mathfrak{p}_0$ в $\mathcal{P}_1$, откуда следует, что идеал $\mathfrak{p}_0$ равен произведению трёх различных простых идеалов в поле L', ибо $\mathrm{Gal}(L'|K) \cong \mathfrak{S}_3$, и потому

$$\mathrm{ord}\ \bar{\rho}_f(\varphi(\mathfrak{p}_0)) = \mathrm{ord}\ \bar{\rho}_f(\varphi(\mathfrak{p}_0)|L') = \mathrm{ord}\ (\varphi(\mathfrak{p}_0)|L') = 2. \tag{4.5.21}$$

Из леммы 2 и соотношения (21) следует, что $\mathrm{tr}\ \bar{\rho}_f(\varphi(\mathfrak{p}_0)) = 0$ и, следовательно, $\mathrm{tr}\ \rho_f(\varphi(\mathfrak{p}_0)) = c(\mathfrak{p}_0) = 0 \pmod 2$. С другой стороны, $c(\mathfrak{p}) = 1 \pmod 2$ при $\mathfrak{p} \in \mathcal{P}_1$, по лемме 9. Полученное противоречие показывает, что $\psi = \psi'$ и, значит, $K_2 = K_2'$.

Лемма 4.5.14. *Поля L и L' совпадают: $L = L'$.*

Доказательство. Положим $\mathfrak{N}_1 := \{\mathfrak{q}_2, \bar{\mathfrak{q}}_2, \mathfrak{q}_3, \bar{\mathfrak{q}}_3, \mathfrak{q}_{23}, \bar{\mathfrak{q}}_{23}\}$, $\mathfrak{N}_1 \subseteq \mathcal{P}(K_2)$, где

$$(2) = \mathfrak{q}_2\bar{\mathfrak{q}}_2^2,\ (3) = \mathfrak{q}_3^2\bar{\mathfrak{q}}_3,\ (23) = (\mathfrak{q}_{23}\bar{\mathfrak{q}}_{23})^2 \text{ в } I_0(K_2),$$

и пусть $\mathfrak{m}_1 := \mathfrak{q}_2\bar{\mathfrak{q}}_2\mathfrak{q}_3^4\bar{\mathfrak{q}}_3^2\mathfrak{q}_{23}\bar{\mathfrak{q}}_{23}$, $\mathfrak{m}_1 \in I_0(K_2)$. Из леммы 13, леммы 6 и следствия 6 следует (мы опускаем детали, ср. [119]), что

$$K_2 \subseteq L \cap L' \subseteq L \cdot L' \subseteq K_2(\mathfrak{m}_1).$$

Пусть $\{\psi, \psi'\} \subseteq \hat{H}(\mathfrak{m}_1)$, $\operatorname{Ker}\psi = G(K_2(\mathfrak{m}_1)|L)$, и $\operatorname{Ker}\psi' = G(K_2(\mathfrak{m}_1)|L')$. Пусть $\mathfrak{q} \in \mathcal{P}(K_2) \setminus \mathfrak{N}_1$; ясно, что простой идеал $\mathfrak{q}$ равен произведению трёх различных простых идеалов в поле L (соответственно в поле L') тогда и только тогда, когда $\psi(\mathfrak{q}) = 1$ (соответственно $\psi'(\mathfrak{q}) = 1$). Положим
$\mathcal{P}_2 := \{\mathfrak{q}_{13}, \mathfrak{q}_{29}, \bar{\mathfrak{q}}_{29}\}$, где

$$(13) = \mathfrak{p}_{13}\bar{\mathfrak{p}}_{13},\ (29) = \mathfrak{p}_{29}\bar{\mathfrak{p}}_{29} \text{ в } I_0(K)$$

и

$$\mathfrak{q}_{13} = \mathfrak{p}_{13}\mathfrak{o}_{K_2},\ \mathfrak{p}_{29} = \mathfrak{q}_{29}\bar{\mathfrak{q}}_{29} \text{ в } I_0(K_2);$$

ясно, что $\mathcal{P}_2 \subseteq \mathcal{P}(K_2) \setminus \mathfrak{N}_1$, и можно показать [144], что

$$H(\mathfrak{m}_1)/H(\mathfrak{m}_1)^3 \cong \mathcal{C}_3^4,$$

множество $\mathcal{P}_2$ порождает подгруппу группы $H(\mathfrak{m})/H(\mathfrak{m})^3$, изоморфную группе $\mathcal{C}_3^3$, и $\psi(\mathcal{P}_2) = \{1\}$. Допустим, что $\psi \neq \psi'$, тогда $\psi'(\{\mathfrak{q}_{29}, \bar{\mathfrak{q}}_{29}\}) \neq \{1\}$ и потому

$$\operatorname{ord}\bar{\rho}_f(\varphi(\mathfrak{p}_{29})) = \operatorname{ord}\bar{\rho}_f(\varphi(\mathfrak{p}_{29})|L')) = \operatorname{ord}(\varphi(\mathfrak{p}_{29})|L') = 3. \qquad (4.5.22)$$

Из леммы 2 и соотношения (22) следует, что $\operatorname{tr}\bar{\rho}_f(\varphi(\mathfrak{p}_{29})) = 1$ и, следовательно, $\operatorname{tr}\rho_f(\varphi(\mathfrak{p}_{29})) = c(\mathfrak{p}_{29}) = 1$ (2). С другой стороны, по лемме 9, $c(\mathfrak{p}_{29}) = -6$. Полученное противоречие показывает, что $\psi = \psi'$ и, значит, $L = L'$.

Предложение 4.5.3. *Представления $\bar{\rho}_E$ and $\bar{\rho}_f$ эквивалентны.*

Доказательство. Согласно лемме 14,

$$\operatorname{Ker} \bar{\rho}_E = \operatorname{Ker} \bar{\rho}_f = G_L.$$

Поэтому доказываемое утверждение вытекает из леммы 1, ибо

$$\bar{\rho}_f(G_K) = \bar{\rho}_E(G_K) = \mathrm{GL}_2(\mathbb{F}_2),$$

в силу леммы 10 и следсвия 8.

В силу леммы 12, не нарушая общности, можно предположить, что

$$\rho_f(G_K) \subseteq \mathrm{GL}_2(\mathbb{Z}_2).$$

Положим

$$\mathfrak{m}_2 := \mathfrak{t}_{23}\bar{\mathfrak{t}}_{23}\mathfrak{t}_{2,1}^7(\prod_{i=2}^{4}\mathfrak{t}_{2,i})^5\prod_{i=1}^{4}\mathfrak{t}_{3,i},\ \{\mathfrak{t}_{2,i},\mathfrak{t}_{3,i},\mathfrak{t}_{23},\bar{\mathfrak{t}}_{23}|1\leq i\leq 4\}\subseteq\mathcal{P}(L),$$

где

$$(2)=\mathfrak{t}_{2,1}^3(\prod_{i=2}^{4}\mathfrak{t}_{2,i})^2,\ (3)=\mathfrak{t}_{3,1}^6\prod_{i=2}^{4}\mathfrak{t}_{3,i},\ (23)=(\mathfrak{t}_{23}\bar{\mathfrak{t}}_{23})^2 \text{ в } I_0(L).$$

Обозначим через

$$X := \{\chi|\chi\in\hat{H}(\mathfrak{m}_2),\ \chi^2=1\}$$

группу вещественных характеров группы $H(\mathfrak{m}_2)$; можно показать [144], что $X\cong\mathcal{C}_2^{16}$. Учитывая, что $\sigma\mathfrak{m}_2=\mathfrak{m}_2$ при $\sigma\in\mathrm{Gal}(L|K)$, положим

$$(\sigma\chi)(g) := \chi(\sigma g) \text{ при } \chi\in\hat{H}(\mathfrak{m}_2),\ \sigma\in\mathrm{Gal}(L|K),\ g\in H(\mathfrak{m}_2).$$

Как и в no. 3, заменив S на $\mathfrak{N}$, обозначим через $\mathfrak{M}$ множество полей M таких, что $L\subseteq M\subseteq\bar{\mathbb{Q}}$ и $M|K$ является конечным нормальным расширением, не разветвлённым в точках множества $\mathcal{P}(K)\setminus\mathfrak{N}$.

Лемма 4.5.15. *Пусть $M\in\mathfrak{M}$ и предположим, что*

$$\mathrm{Gal}(M|K)\cong\mathfrak{S}_3\times\mathcal{C}_2.$$

Тогда

$$(\exists\,\mathfrak{p}\in(\mathcal{P}(K)\setminus\mathfrak{N}))\ f_M(\mathfrak{p})=6 \text{ и } \mathrm{tr}\,(\rho_E(\varphi(\mathfrak{p})))=\mathrm{tr}\,(\rho_f(\varphi(\mathfrak{p}))).$$

Доказательство. Рассмотрим введённое при доказательстве леммы 13 множество

$$\mathcal{P}_1 = \{\mathfrak{p}_5, \bar{\mathfrak{p}}_{13}, \bar{\mathfrak{p}}_{29}, \mathfrak{p}_{31}, \bar{\mathfrak{p}}_{41}\},$$

напомним, что $\mathcal{P}_1 \subseteq \mathcal{P}(K) \setminus \mathfrak{N}$, и положим

$$\mathcal{P}_3 := \{\mathfrak{t} \mid \ \mathfrak{t} \in \mathcal{P}(L),\ \mathfrak{t} | \prod_{\mathfrak{q} \in \mathcal{P}_1} \mathfrak{q}\}.$$

Из леммы 6 следует, что $M \subseteq L(\mathfrak{m}_2)$. Положим

$$X_1 := \{\chi | \chi \in X,\ \sigma\chi = \chi \text{ при } \sigma \in \mathrm{Gal}(L|K)\}.$$

Обозначим через ψ вещественный характер группы $H(\mathfrak{m}_2)$, отвечающий расширению $M|L$; из условия $\mathrm{Gal}(M|K) \cong \mathfrak{S}_3 \times \mathcal{C}_2$ следует, что $\psi \in X_1$ [66, предложение 5.7]. Можно показать [144], что $X_1 \cong \mathcal{C}_2^5$, что $f_L(\mathfrak{p}) = 3$ при $\mathfrak{p} \in \mathcal{P}_1$, что

$$(\exists\, \mathfrak{t} \in \mathcal{P}_3)\ \chi(\mathfrak{t}) = -1$$

при $\chi \in X_1 \setminus \{1\}$, и, в частности, $\psi(\mathfrak{t}_0) = -1$ для некоторого простого идеала $\mathfrak{t}_0$ в $\mathcal{P}_3$. Пусть

$$\mathfrak{P} \in \mathcal{P}(M),\ \mathfrak{p}_0 \in \mathcal{P}_1,\ \mathfrak{P}|\mathfrak{t}_0 \text{ и } \mathfrak{t}_0|\mathfrak{p}_0;$$

тогда

$$N_{M/L}\mathfrak{P} = {\mathfrak{t}_0}^2,\ N_{L/K}\mathfrak{t}_0 = {\mathfrak{p}_0}^3 \text{ и, значит } N_{M/K}\mathfrak{P} = {\mathfrak{p}_0}^6.$$

Таким образом, $f_M(\mathfrak{p}_0) = 6$ и $\mathfrak{p}_0 \in (\mathcal{P}(K) \setminus \mathfrak{N})$. С другой стороны, так как $\mathfrak{p}_0 \in \mathcal{P}_1$ и, значит, $N\mathfrak{p}_0 < 50$, из леммы 9 следует, что

$$\mathrm{tr}\ (\rho_E(\varphi(\mathfrak{p}_0))) = a(\mathfrak{p}_0) = c(\mathfrak{p}_0) = \mathrm{tr}\ (\rho_f(\varphi(\mathfrak{p}_0))).$$

Лемма доказана.

Лемма 4.5.16. *Пусть $M \in \mathfrak{M}$ и предположим, что $\mathrm{Gal}(M|K) \cong \mathfrak{S}_4$. Тогда*

$$(\exists\, \mathfrak{p} \in (\mathcal{P}(K) \setminus \mathfrak{N}))\ f_M(\mathfrak{p}) = 4 \text{ и } \mathrm{tr}\ (\rho_E(\varphi(\mathfrak{p}))) = \mathrm{tr}\ (\rho_f(\varphi(\mathfrak{p}))).$$

Доказательство. Положим

$$\mathcal{P}_4 := \{\mathfrak{p}_7, \mathfrak{p}_{13}, \bar{\mathfrak{p}}_{31}, \mathfrak{p}_{41}\},\ \mathcal{P}_5 := \{\mathfrak{t} \mid\ \mathfrak{t} \in \mathcal{P}(L),\ \mathfrak{t}|\prod_{\mathfrak{q}\in\mathcal{P}_1} \mathfrak{q}\}$$

и заметим, что $\mathcal{P}_4 \subseteq \mathcal{P}(K) \setminus \mathfrak{N}$. Легко видеть, что $\mathrm{Gal}(M|K) \cong \mathcal{C}_2^2$ и потому существуют поля L_i под условием

$$L \subseteq L_i \subseteq M,\ [L_i : L] = 2,\ 1 \leq i \leq 3.$$

Применяя лемму 6 к каждому из этих полей и учитывая, что расширение $M|K$ не разветвлено в точках множества $\mathcal{P}(K)\setminus\mathfrak{N}$, находим, что $M \subseteq L(\mathfrak{m}_2)$. Обозначим через ψ_i вещественный характер группы $H(\mathfrak{m}_2)$, отвечающий расширению $L_i|L,\ 1 \leq i \leq 3$. Можно доказать [66, лемма 5.6 и предложение 5.7], что найдутся элементы $\{\sigma,\ \tau\}$ группы $\mathrm{Gal}(L|K)$ под условием

$$\mathrm{ord}\,\tau = 2,\ \mathrm{ord}\,\sigma = 3,\ \{\psi_i \mid\ 1 \leq i \leq 3\} = \{\sigma^j\psi_1 \mid\ 0 \leq j \leq 2\} \text{ и } \tau\psi_1 = \psi_1.$$

Можно показать [119], [144], что $f_L(\mathfrak{p}) = 2$ при $\mathfrak{p} \in \mathcal{P}_4$ и $\psi_1(\mathfrak{t}) = -1$ для некоторого простого идеала $\mathfrak{t}$ из множества $\mathcal{P}_5$; пусть

$$\mathfrak{p}_0 \in \mathcal{P}_4,\ \mathfrak{t}|\mathfrak{p}_0,\ \mathfrak{P} \in \mathcal{P}(L_1) \text{ и } \mathfrak{P}|\mathfrak{t}.$$

Тогда

$$N_{L/K}\mathfrak{P} = N_{L/K}(N_{L_1/L}\mathfrak{P}) = N_{L/K}\mathfrak{t}^2 = {\mathfrak{p}_0}^4.$$

Так как $\mathrm{Gal}(M|K) \cong \mathfrak{S}_4$, отсюда следует, что $f_M(\mathfrak{p}) = 4$. С другой стороны, $N\mathfrak{p}_0 < 50$, так как $\mathfrak{p}_0 \in \mathcal{P}_4$, и потому из леммы 9 следует, что

$$\mathrm{tr}\,(\rho_E(\varphi(\mathfrak{p}_0))) = a(\mathfrak{p}_0) = c(\mathfrak{p}_0) = \mathrm{tr}\,(\rho_f(\varphi(\mathfrak{p}_0))).$$

Лемма доказана.

Доказательство теоремы 2. Из леммы 15, леммы 16, предложения 3 и следствия 8 вытекает, что представления ρ_E и ρ_f удовлетворяют условиям леммы 8 с $S = \mathfrak{N}$, и потому $\rho_E \cong \rho_f$. Теорема доказана.

4.6 О подмногообразиях особых точек в полных пересечениях

В этом параграфе излагаются результаты, полученные в работе [43] в соавторстве с А. Г. Александровым.

1. Рассмотрим алгебраически замкнутое поле k и идеал $\mathfrak{B}$ кольца $k[x]$, $x := (x_1, ..., x_n)$. Положим, как обычно,

$$Z(\mathfrak{B}) := \{\alpha | \alpha \in k^n,\ f(\alpha) = 0 \ \text{ при } \ f(x) \in \mathfrak{B}\},$$

$$\sqrt{\mathfrak{B}} := \{f(x) | f(x) \in k[x],\ (\exists l \in \mathbb{N})\ f(x)^l \in \mathfrak{B}\}$$

и заметим, что, по теореме Гильберта о нулях,

$$\sqrt{\mathfrak{B}} := \{f(x) | f(x) \in k[x],\ (\forall \alpha \in Z(\mathfrak{B}))\ f(\alpha) = 0\}. \tag{4.6.1}$$

Пусть

$$f_j(x) \in k[x],\ d_j \in \mathbb{N},\ 1 \leq j \leq r,\ n > r$$

и предположим, что $f_j(x)$ есть однородный полином степени d_j. При $\mu \in k^r$, рассмотрим аффинные схемы

$$V_\mu := \operatorname{Spec} k[x]/\mathfrak{A}_\mu,$$

где

$$\mathfrak{A}_\mu := (f_1(x) - \mu_1, ..., f_r(x) - \mu_r),$$

и якобиян

$$\partial f := (\partial_i f_j)_{1 \leq i \leq n, 1 \leq j \leq r}$$

отображения $f\colon B^n \to B^r$, определённого для любой k-алгебры B; обозначим через $\mathfrak{r}(f, x)$ ранг матрицы $\partial f(x)$. Ясно, что $0 \leq \mathfrak{r}(f, b) \leq r$ при $b \in B^n$; условие $\mathfrak{r}(f, x) < r$ определяет аффинную схему

$$W := \operatorname{Spec} k[x]/J,$$

где J есть идеал кольца $k[x]$, порождённый минорами порядка r матрицы $\partial f(x)$.

Определение. Пусть A - коммутативное кольцо, $V := \mathrm{Spec}\, A$ и I - идеал кольца A под условием

$$\{\mathfrak{p} | \mathfrak{p} \in V,\ A_{\mathfrak{p}} \text{ не есть регулярное кольцо}\} = \{\mathfrak{p} | \mathfrak{p} \in V,\ I \subseteq \mathfrak{p}\};$$

будем называть схему $\mathrm{Sing}\, V := \mathrm{Spec}\, A/I$ *подмногообразием особых точек* схемы V.

Обозначим через V^* замыкание (в топологии Зарисского) объединения

$$\bigcup_{\mu \in k^r} \mathrm{Sing}\, V_\mu$$

подмногообразий особых точек схем V_μ и положим

$$\mathfrak{D} := \bigcap_{\mu \in k^r} (J, \mathfrak{A}_\mu).$$

Лемма 4.6.1. *Имеет место соотношение:* $J \subseteq \mathfrak{D} \subseteq \sqrt{J}$.

Доказательство. Ясно, что $J \subseteq \mathfrak{D}$. Пусть $h \in \mathfrak{D}$, тогда для любого μ в k^r найдутся полиномы $p_j^{(\mu)}$ и q_μ под условием

$$h = q_\mu + \sum_{j=1}^{r} p_j^{(\mu)}(f_j(x) - \mu_j),\ q_\mu \in J,\ p_j^{(\mu)} \in k[x] \text{ при } 1 \leq j \leq r.$$

Пусть $\alpha \in Z(J)$, тогда $q_\mu(\alpha) = 0$ и, значит,

$$h(\alpha) = \sum_{j=1}^{r} p_j^{(\mu)}(\alpha)(f_j(\alpha) - \mu_j) \text{ при } \mu \in k^r.$$

Взяв $\mu_j = f_j(\alpha)$ при $1 \leq j \leq r$, получим $h(\alpha) = 0$. Таким образом, включение $\mathfrak{D} \subseteq \sqrt{J}$ следует из соотношения (1). Лемма доказана.

Теорема 4.6.1. *Пусть* $\dim V_0 = n - r$, *тогда* $V^* = \mathrm{Spec}\, k[x]/\mathfrak{D}$.

Из леммы 1 и теоремы 1 вытекает следующее утверждение.

Следствие 4.6.1. *Пусть* $\dim V_0 = n - r$, *тогда схемы* V^* *и* W *гомеоморфны; в частности,* $\dim V^* = \dim W$. *Более того,* $V^*(k) = W(k)$.

Теорема 1 и следствие 1 навеяны некоторыми замечаниями в известной работе Бёрча [49] (ср. [43, стр. 149-150]). Теорема 1 будет доказана в no. 3 средствами коммутативной алгебры. В no. 2 приводятся необходимые сведения из теории коммутативных колец; доказанное в этом разделе предложение 1, вероятно, интересно и само по себе.

2. Рассмотрим коммутативное кольцо A, конечное подмножество I этого кольца и идеал $\mathfrak{B}$ кольца A, порождённый множеством I. Обозначим i-ую группу гомологий комплекса Косуля пары (A, I) через $H_i(I, A)$ и положим $H_i(\mathfrak{B}, A) := H_i(I, A)$ при $i \in \mathbb{N}_0$. Говорят, что множество I определяет *полное пересечение*, если

$$(\forall i \in \mathbb{N})\ H_i(I, A) = 0,$$

ср. [52, §9, no. 4]. Последовательность $\{a_1, ..., a_l\}$ элементов кольца A называется *регулярной*, если элемент a_1 не является делителем нуля в кольце A и образ элемента a_{j+1} в фактор-кольце $A/(a_1, ..., a_j)$ не является делителем нуля при $1 \leq j \leq l-1$. Обозначим через $\mathfrak{R}(A)$ множество регулярных последовательностей кольца A и через $R(\alpha)$ длину последовательности α при $\alpha \in \mathfrak{R}(A)$. Пусть $\mathfrak{C} \subseteq A$; положим

$$\operatorname{dp} \mathfrak{C} := \sup\{R(\alpha) | \alpha \in \mathfrak{R}(A)\} \ \text{ и } \ \operatorname{ht} \mathfrak{C} := \min\{\operatorname{ht} \mathfrak{p} | \mathfrak{p} \in \operatorname{Spec} A,\ \mathfrak{C} \subseteq \mathfrak{p}\}$$

и заметим, что $\mathfrak{C} \neq (1) \Rightarrow \operatorname{dp} \mathfrak{C} = \operatorname{ht} \mathfrak{C}$ для любого идеала $\mathfrak{C}$ кольца Коэна-Маколея.

Лемма 4.6.2. *Пусть* $a \in A^l,\ B \in \mathrm{GL}_l(A)$ *и* $b = Ba$. *Множество*

$$\{a_1, ..., a_l\}$$

определяет полное пересечение в том и только в том случае, когда этим свойством обладает множество

$$\{b_1, ..., b_l\}.$$

Доказательство. См. [52, §9, no. 6, предложение 6, b)].

Лемма 4.6.3. *Если последовательность* $\{a_1, ..., a_l\}$ *элементов кольца* A *является регулярной, то множество* $\{a_j | 1 \leq j \leq l\}$ *определяет полное пересечение.*

Доказательство. См. [52, §9, no. 7, теорема 1].

Лемма 4.6.4. *Рассмотрим* $\mathbb{N}_0$ *- градуированное коммутативное кольцо* A *и пусть*

$$\mathfrak{m} := \{a_j | 1 \leq j \leq l\},\ \mathfrak{m} \subseteq A.$$

Если множество $\mathfrak{m}$ *определяет полное пересечение и все элементы этого множества суть однородные элементы положительной степени кольца* A*, то последовательность* $\{a_1, ..., a_l\}$ *является регулярной.*

Доказательство. См. [117, теорема 16.5 (ii)].

Лемма 4.6.5. *Предположим, что подмножество* $\{bc, a_j | 1 \leq j \leq l\}$ *коммутативного кольца* A *определяет полное пересечение. Тогда как множество* $\{b, a_j | 1 \leq j \leq l\}$*, так и множество* $\{c, a_j | 1 \leq j \leq l\}$ *определяют полное пересечение.*

Доказательство. Это утверждение следует из известной теоремы (см., например, [52, §9, no. 5, следствие 3]) о группах гомологий комплекса Косуля и определения полного пересечения.

Предложение 4.6.1. *Рассмотрим* $\mathbb{N}_0$ *- градуированное коммутативное кольцо* A*. Пусть* $\mathfrak{m} := \{a_j | 1 \leq j \leq l\}$, $\mathfrak{m} \subseteq A$ *и* $\mu \in (A^* \cup \{0\})^l$*. Если множество* $\mathfrak{m}$ *определяет полное пересечение и все элементы этого множества суть однородные элементы положительной степени кольца* A*, то и множество* $\{a_j + \mu_j | 1 \leq j \leq l\}$ *определяет полное пересечение.*

Доказательство. Предположим, что все элементы множества $\mathfrak{m}$ суть однородные элементы степени d; по условию, $d \in \mathbb{N}$. Не нарушая общности, предположим, что $\mu_l \in A^*$. Пусть $b_i \in (A^* \cup \{0\})$ и $h_i = a_i + b_i a_l$ при $1 \leq i \leq l-1$. Из леммы 2 следует, что множество $\{a_l, h_i | 1 \leq i \leq l-1\}$

определяет полное пересечение; поэтому, в силу леммы 4, последовательность $\{h_1, ..., h_{l-1}, a_l\}$ и, значит, её подпоследовательность $\{h_1, ..., h_{l-1}\}$ являются регулярными. Докажем, что элемент $h_l := a_l + \mu_l$ не есть делитель нуля в кольце $A/\mathfrak{A}$, $\mathfrak{A} := (h_1, ..., h_{l-1})$. Пусть

$$ch_l \in \mathfrak{A},\ c \in A,\ c = \sum_{j=0}^{N} c_j,\ N \in \mathbb{N},$$

степень c_j равна j при $1 \leq j \leq N$ и $c_j = 0$ при $j \in \mathbb{Z} \setminus \mathbb{N}_0$, тогда

$$(\sum_{j=0}^{N} a_l c_j + \sum_{j=0}^{N} \mu_l c_j) \in \mathfrak{A}$$

и, значит, в силу однородности идеала $\mathfrak{A}$,

$$(a_l c_{d-j} + \mu_l c_j) \in \mathfrak{A} \text{ при } 1 \leq j \leq N; \tag{4.6.2}$$

из соотношения (2) легко следует (индукция по j !), что $c \in \mathfrak{A}$. Таким образом, последовательность $\{h_1, ..., h_l\}$ регулярна и, значит, в силу леммы 3, множество $\{h_j | 1 \leq j \leq l\}$ определяет полное пересечение. Поэтому из леммы 1 следует, что и множество $\{h_l, h_j - b_j h_l | 1 \leq j \leq l-1\}$ определяет полное пересечение. При $1 \leq j \leq l-1$, положим $b_j = -\mu_j/\mu_l$, тогда $\{h_j | 1 \leq j \leq l\} = \{a_j + \mu_j | 1 \leq j \leq l\}$. Тем самым, наше утверждение доказано для множества $\mathfrak{m}$ элементов одинаковой степени.

Пусть $1 \leq j \leq l$. Обозначим через d_j степень элемента a_j множества $\mathfrak{m}$; по условию, $d_j \in \mathbb{N}$. Обозначим через d наименьшее общее кратное чисел d_j, $1 \leq j \leq l$, и положим $e_j := d/d_j$ при $1 \leq j \leq l$. Так как все элементы

$$a_j^{e_j},\ 1 \leq j \leq l,$$

суть элементы степени d, то, по доказанному выше, множество

$$\{a_j^{e_j} - (-\mu_j)^{e_j} | 1 \leq j \leq l\}$$

определяет полное пересечение. Но

$$a_j^{e_j} - (-\mu_j)^{e_j} = (a_j + \mu_j)\beta_j,\ \beta_j := \sum_{0 \leq i \leq e_j} a_j^i (-\mu_j)^{e_j - i} \text{ при } 1 \leq j \leq l,$$

и доказываемое утверждение следует из леммы 5.

Лемма 4.6.6. *Если конечно порождённое над полем кольцо A является областью целостности, то*

$$\dim A/\mathfrak{B} + \operatorname{ht} \mathfrak{B} = \dim A$$

для любого идеала $\mathfrak{B}$ кольца A.

Доказательство. См., например, [74, следствие 13.4].

Лемма 4.6.7. *Рассмотрим идеал $\mathfrak{B} := (a_1, ..., a_l)$ коммутативного нетёрова кольца A под условием $\mathfrak{B} \neq A$. Тогда*

$$\operatorname{dp} \mathfrak{B} = l - \sup\{i | i \in \mathbb{N}_0,\ H_i(\mathfrak{B}, A) \neq 0\}; \tag{4.6.3}$$

в частности, последовательность $\{a_1, ..., a_l\}$ регулярна в том и только в том случае, когда $\operatorname{dp} \mathfrak{B} = l$.

Доказательство. См., [117, теорема 16.8 и её следствие].

3. Докажем следующее утверждение.

Лемма 4.6.8. *Пусть $\dim V_0 = n - r$, тогда $(\forall \mu \in k^r)\ \mathfrak{A}_\mu \neq (1)$.*

Доказательство. Положим $\mathfrak{A}_\mu(t) := (f_1(x) - \mu_1 t^{d_1}, ..., f_r(x) - \mu_r t^{d_r})$ и заметим, что $\mathfrak{A}_\mu(1) = \mathfrak{A}_\mu$. По известной теореме (см., например, [90, гл. I, предложения 1.13 и 7.1]),

$$\dim \operatorname{Spec} k[x,t]/\mathfrak{A}_\mu(t) \geq n - r + 1. \tag{4.6.4}$$

С другой стороны, по условию леммы,

$$\dim \operatorname{Spec} k[x,t]/(\mathfrak{A}_\mu(t), t) = \dim V_0 = n - r. \tag{4.6.5}$$

Предположим, что $\mathfrak{A}_\mu = (1)$ для некоторого μ из k^r, тогда $(\mathfrak{A}_\mu(t), t-1) = (1)$, ибо

$$\operatorname{Spec} k[x,t]/(\mathfrak{A}_\mu(t), t-1) \cong \operatorname{Spec} k[x]/\mathfrak{A}_\mu,$$

и, значит,

$$(\forall \alpha \in k^*)(\mathfrak{A}_\mu(t), t-\alpha) = (1). \tag{4.6.6}$$

Положим, для краткости,

$$\mathfrak{B} := \bigcap_{\alpha \in k} (\mathfrak{A}_\mu(t), t-\alpha);$$

из соотношения (6) следует, что

$$\mathfrak{B} = (\mathfrak{A}_\mu(t), t). \tag{4.6.7}$$

Пусть $(a,b) \in Z(\mathfrak{A}_\mu(t))$ и $g(x,t) \in \mathfrak{B}$, тогда $g(x,t) = g_\alpha(x,t) + h_\alpha(x,t)(t-\alpha)$ с $g_\alpha(x,t) \in \mathfrak{A}_\mu(t)$ и $h_\alpha(x,t) \in k[x,t]$ при $\alpha \in k$; в частности,

$$(\forall \alpha \in k) g(a,b) = h_\alpha(a,b)(b-\alpha),$$

откуда (при $\alpha = b$) следует, что $g(a,b) = 0$. Таким образом,

$$\mathfrak{A}_\mu(t) \subseteq \mathfrak{B} \subseteq \sqrt{\mathfrak{A}_\mu(t)}. \tag{4.6.8}$$

Из соотношений (4), (5), (7) и (8) получаем

$$n - r + 1 \leq \dim \operatorname{Spec} k[x,t]/\mathfrak{B} = n - r;$$

полученное противоречие показывает, что $(\forall \mu \in k^r)\ \mathfrak{A}_\mu \neq (1)$. Лемма доказана.

Идеал $\mathfrak{B}$ коммутативного кольца A называется *чистым идеалом* высоты r, если $\operatorname{ht} \mathfrak{p} = r$ для любого простого идеала $\mathfrak{p}$ этого кольца под условием

$$\mathfrak{B} \subseteq \mathfrak{p} \ \text{ и } \ (\forall \mathfrak{q} \in \operatorname{Spec} A)\ \mathfrak{B} \subseteq \mathfrak{q} \Rightarrow \mathfrak{p} \subseteq \mathfrak{q}.$$

Предложение 4.6.2. *Если* $\dim V_0 = n - r$ *и* $\mu \in k^r$ *, то идеал* $\mathfrak{A}_\mu$ *кольца* $k[x]$ *есть чистый идеал высоты* r.

Доказательство. В силу леммы 6, из условия $\dim V_0 = n - r$ следует, что $\operatorname{ht} \mathfrak{A}_0 = r$, значит, $\operatorname{dp} \mathfrak{A}_0 = r$, ибо кольцо $k[x]$ является кольцом Коэна-Маколея; в силу леммы 7, отсюда следует, что последовательность $\{f_1, ..., f_r\}$ регулярна, так как $\mathfrak{A} \neq k[x]$, и, значит (лемма 3 !), множество $\{f_j | 1 \leq j \leq r\}$ определяет полное пересечение. Пусть $\mu \in k^r$; из предложения 1 следует, что множество $\{f_j - \mu_j | 1 \leq j \leq r\}$ определяет полное пересечение и потому

$$(\forall i \in \mathbb{N})\ H_i(\mathfrak{A}_\mu, A) = 0.$$

С другой стороны, $H_0(\mathfrak{A}_\mu, A) \neq 0$, ибо $H_0(\mathfrak{A}_\mu, A) \cong k[x]/\mathfrak{A}_\mu$ и $\mathfrak{A}_\mu \neq (1)$, по лемме 8. Поэтому из соотношения (3) следует, что $\operatorname{dp} \mathfrak{A}_\mu = r$ и, значит, $\operatorname{ht} \mathfrak{A}_\mu = r$. Для завершения доказательства достаточно воспользоваться теоремой о несмешиваемости идеалов [74, следствие 16.20].

Доказательство теоремы 1. Пусть $\mu \in k^r$; в силу предложения 1, многообразие V_μ удовлетворяет условиям теоремы о якобияне [74, следствие 16.20], и потому

$$\operatorname{Sing} V_\mu = \operatorname{Spec} k[x]/(J, \mathfrak{A}_\mu),$$

откуда следует, что

$$V^* = \overline{\bigcup_{\mu \in k^r} \operatorname{Sing} V_\mu} = \operatorname{Spec} k[x]/\mathfrak{D}.$$

Теорема доказана.

4.7 Универсальные полиномы и доказуемость в математике

В этом параграфе коротко описываются результаты, полученные в работе [57] в соавторстве с М. Карлом (ср. [58]).

1. Изучение множеств целых точек $V(\mathbb{Z})$ аффинных $\mathbb{Z}$ - схем V - одна из главных тем диофантовой геометрии. Несколько лет назад [56], [57], воспользовавшись развитой при решении десятой проблемы Гильберта техникой [22]

- [24], [62] (см. также [34]), нам удалось построить полином $F(t,x)$ такой, что $F(t,x) \in \mathbb{Z}[t,x],\ x := (x_1,...,x_n),\ n \in \mathbb{N}$, и, при подходящей нумерации математических утверждений, l-ое математическое утверждение доказуемо тогда и только тогда, когда

$$V_l(\mathbb{Z}) \neq \emptyset, \text{ где } V_l := \operatorname{Spec} \mathbb{Z}[x]/(F(l,x)).$$

Таким образом, любую математическую проблему можно свести к вопросу о том, непусто ли множество $V(\mathbb{Z})$ для некоторой аффинной $\mathbb{Z}$ - схемы V. Более того, легко видеть, что, в терминологии [24], массовая проблема существования целых точек на гиперповерхностях $V_l,\ l \in \mathbb{N}$, алгоритмически не разрешима; тем самым, получено ещё одно доказательство алгоритмической неразрешимости десятой проблемы Гильберта.

Идея нашего построения не нова, ср. [62, pp. 327-328], [72]: по теореме Матиясевича [22], [23], любое перечислимое множество и, в частности, множество теорем формальной математики, является диофантовым, откуда и следует существование требуемого полинома; тем не менее, нам пришлось преодолеть серьёзные технические трудности. В этом параграфе, следуя [58] и отсылая читателя за дальнейшими подробностями к цитированным выше работам [56], [57], я постараюсь коротко описать нашу конструкцию.

Рассмотрим формальную систему П, алфавит языка которй состоит из бесконечного множества предметных переменных $\mathcal{X} := \{t_i \mid i \in \mathbb{N}\}$ и шести символов

$$\neg,\ \supset,\ \forall,\ \epsilon,\ (,\ ).$$

Множество формул $\mathfrak{F}$ теории П определяется индуктивно:
(i) при $\{x,\ y\} \subseteq \mathcal{X}$ выражение $(x\ \epsilon\ y)$ есть элементарная формула;
(ii) если $\{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F}$ и $x \in \mathcal{X}$, то $\{\neg\,\mathfrak{A},\ (\mathfrak{A} \supset \mathfrak{B}),\ \forall x\,\mathfrak{A}\} \subseteq \mathfrak{F}$.
Пусть $\mathfrak{A} \in \mathfrak{F}$; $\{x,y\} \subseteq \mathcal{X}$; обозначим через $[\mathfrak{A}]_f$ множество свободных переменных формулы $\mathfrak{A}$ и через $\mathfrak{A}[x|y]$ формулу, получаемую в результате подстановки переменной y вместо каждого *свободного* вхождения переменной x в

формулу $\mathfrak{A}$. Аксиомы этой теории делятся на пять групп (ср. [118, стр. 69-70], [34, стр. 7-8]):

$$\mathcal{A}_1 := \{\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{A}) \mid \{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F}\};$$

$$\mathcal{A}_2 := \{(\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C})) \supset ((\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \mathfrak{C})) \mid \{\mathfrak{A},\ \mathfrak{B},\ \mathfrak{C}\} \subseteq \mathfrak{F}\};$$

$$\mathcal{A}_3 := \{(\neg\, \mathfrak{B} \supset \neg\, \mathfrak{A}) \supset ((\neg\, \mathfrak{B} \supset \mathfrak{A}) \supset \mathfrak{B}) \mid \{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F}\};$$

$$\mathcal{A}_4 := \{\forall x\ (\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \forall x\ \mathfrak{B}) \mid \{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F},\ x \in \mathcal{X} \setminus [\mathfrak{A}]_f\};$$

$$\mathcal{A}_5 := \{(\forall x\ \mathfrak{A}) \supset \mathfrak{A}[x|y] \mid \mathfrak{A} \in \mathfrak{F},\ \{x,\ y\} \subseteq \mathcal{X},\ \text{ни одно свободное вхождение переменной } x \text{ не лежит в области действия квантора } (\forall y)\}.$$

Множество $\mathfrak{T}$ теорем теории П определяется индуктивно:

(i) $\bigcup_{j=1}^{5} \mathcal{A}_j \subseteq \mathfrak{T}$;

(ii) если $\{\mathfrak{A}_1,\ (\mathfrak{A}_1 \supset \mathfrak{A}_2)\} \subseteq \mathfrak{T}$, то $\mathfrak{A}_2 \in \mathfrak{T}$ (*"модус поненс"*);

(iii) если $\mathfrak{A} \in \mathfrak{T}$ и $x \in \mathcal{X}$, то $\forall x\ \mathfrak{A} \in \mathfrak{T}$ (*"обобщение"*).

Как известно, аксиоматическая теория множеств Гёделя - Бернайса конечно аксиоматизируема в описанной системе П [85], [118, гл. 4]; обозначим через $\mathfrak{m}_0$ конъюнкцию теоретико-множественных аксиом этой теории (ср. [118, гл. 4], [57]). По построению, $\mathfrak{m}_0 \in \mathfrak{F}$; положим

$$\mathfrak{T}_0 := \{\mathfrak{A} \mid \mathfrak{A} \in \mathfrak{F},\ (\mathfrak{m}_0 \supset \mathfrak{A}) \in \mathfrak{T}\}.$$

Множество $\mathfrak{T}_0$ можно рассматривать как множество всех математических теорем (доказуемых в теории множеств Гёделя-Бернайса).

Замечание. Читатель, вероятно, обратил внимание на то, что, описывая нашу систему П, мы пользуемся (мета)языком обычной математики; символы $\{\subseteq,\ \in,\ \bigcup,\ \setminus\}$ являются, разумеется, буквами этого метаязыка.

2. Определим взаимно однозначные отображения

$$p\colon \mathbb{N}^2 \to \mathbb{N},\ p\colon a \mapsto p(a) \text{ при } a \in \mathbb{N}^2,$$

где

$$p(x) := \frac{(x_1 + x_2 - 2)(x_1 + x_2 - 1)}{2} + x_2,\ x := (x_1, x_2),$$

и $\mathcal{N}\colon \mathfrak{F} \to \mathbb{N}$, положив

$$\mathcal{N}(t_i\ \varepsilon\ t_j) = 4p(i,j) - 3 \ \text{ при } \ \{i,\ j\} \subseteq \mathbb{N},$$

$$\mathcal{N}(\neg\ \mathfrak{A}) = 4\mathcal{N}(\mathfrak{A}) - 2 \ \text{ при } \ \mathfrak{A} \in \mathfrak{F},$$

$$\mathcal{N}(\mathfrak{A} \supset \mathfrak{B}) = 4p(\mathcal{N}(\mathfrak{A}), \mathcal{N}(\mathfrak{B})) \ \text{ при } \ \{\mathfrak{A},\ \mathfrak{B}\} \subseteq \mathfrak{F}$$

и

$$\mathcal{N}(\forall t_i\ \mathfrak{A}) = 4p(i, \mathcal{N}(\mathfrak{A})) - 1 \ \text{ при } \ \mathfrak{A} \in \mathfrak{F} \text{ и } i \in \mathbb{N}.$$

Легко видеть [57], что

$$\mathcal{N}(\mathcal{A}_j) = \{u | u \in \mathbb{N},\ (\exists\, b \in \mathbb{N}^{l_j}) g_j(u,b) = 0\} \ \text{ при } \ j \in \{1,2,3\},$$

где

$$g_1(u,x) := u - 4p(x_1, 4p(x_2, x_1)),\ x := (x_1, x_2),\ l_1 = 2;$$

$$g_2(u,x) := u - 4p(4p(x_1, 4p(x_2, x_3)), 4p(4p(x_1, x_2), 4p(x_1, x_3))),$$

$$x := (x_1, x_2, x_3),\ l_2 = 2;$$

$$g_3(u,x) := u - 4p(4p(4x_2 - 2, 4x_1 - 2), 4p(4p(4x_2 - 2, x_1), x_2)),$$

$$x := (x_1, x_2),\ l_3 = 2.$$

Гораздо труднее построить полиномы $g_4(u,x)$ и $g_5(u,y)$ под условием

$$\mathcal{N}(\mathcal{A}_j) = \{u | u \in \mathbb{N},\ (\exists\, b \in \mathbb{N}^{l_j}) g_j(u,b) = 0\} \ \text{ при } \ j \in \{4,5\}$$

и такие, что $g_4(u,x) \in \mathbb{Z}[u,x],\ g_5(u,y) \in \mathbb{Z}[u,y],\ x := (x_1, ..., x_n)$, $y := (y_1, ..., y_m)$ с $n = l_4,\ m = l_5$. Не останавливаясь на деталях этой конструкции, заметим только, что в нашей работе [57] построены полиномы g_4 и g_5 с $l_4 = 8878$ и $l_5 = 17873$. При построении этих полиномов используется техника, развитая в работах по десятой проблеме Гильберта, см., например,

[24] и цитированную в этой монографии литературу; для краткости, будем называть эту технику *"диофантовым кодированием"* (ср. [24, гл. 3], [57]). Положим

$$G_1(u,x) := x(u_3 - 4p(u_2,u_1)),\ u := (u_1,u_2,u_3)$$

и

$$G_2(v;x) := v_1 - 4p(x,v_2) + 1,\ v := (v_1,v_2).$$

Пусть

$$\mathfrak{A}_i \in \mathfrak{F} \text{ и } a_i := \mathcal{N}(\mathfrak{A}_i) \text{ при } i \in \{1,2,3\},\ a := (a_1,a_2,a_3);$$

легко видеть, что формула $\mathfrak{A}_1$ следует из формул $\mathfrak{A}_2$ и $\mathfrak{A}_3$ по правилу "модус поненс" тогда и только тогда, когда

$$(\exists\, b \in \mathbb{N})G_1(a;b) = 0.$$

Пусть

$$\mathfrak{A}_i \in \mathfrak{F} \text{ и } a_i := \mathcal{N}(\mathfrak{A}_i) \text{ при } i \in \{1,2\},\ a := (a_1,a_2);$$

легко видеть, что формула $\mathfrak{A}_1$ следует из формулы $\mathfrak{A}_2$ по правилу "обобщение" тогда и только тогда, когда

$$(\exists\, b \in \mathbb{N})G_2(a;b) = 0.$$

Применяя технику диофантового кодирования к полиномам

$$G_1, G_2, g_1, g_2, g_3, g_4 \text{ и } g_5,$$

можно построить полином $f(t,x),\ x := (x_1,...,x_n),\ n := 14518112$, под условием

$$\mathcal{N}(\mathfrak{T}) = \{a | a \in \mathbb{N},\ (\exists\, b \in \mathbb{Z}^n) f(a,b) = 0\}$$

и такой, что $f(t,x) \in \mathbb{Z}[t,x]$; детали этой конструкции подробно описаны в наших работах [56], [57].

Как известно, множество $\mathcal{N}(\mathfrak{T})$, будучи, по построению, перечислимым, не

является разрешимым [118, следствие 3.46 на стр. 218]. Поэтому массовая проблема существования целых точек на гиперповерхностях

$$W_l : f(l,x) = 0,\ l \in \mathbb{N}$$

и, тем более, десятая проблема Гильберта алгоритмически не разрешимы.

3. Обозначим аксиоматическую теорию множеств Гёделя - Бернайса через $\mathfrak{S}$. Положим

$$m := \mathcal{N}(\mathfrak{m}_0 \supset (t_1\ \varepsilon\ t_1)),\ F_0(x) := f(m,x) \text{ и } V_0 := \operatorname{Spec} \mathbb{Z}[x]/(F_0(x)).$$

Если система $\mathfrak{S}$ непротиворечива (т.е. $\mathfrak{T}_0 \neq \mathfrak{F}$), то формула $(t_1\ \varepsilon\ t_1)$ недоказуема в $\mathfrak{S}$ (т.е. $(t_1\ \varepsilon\ t_1) \notin \mathfrak{T}_0$). Следовательно,

$$V_0(\mathbb{Z}) = \emptyset \Leftrightarrow \mathfrak{T}_0 \neq \mathfrak{F}.$$

Предположим, что система $\mathfrak{S}$ непротиворечива, тогда утверждение

$$V_0(\mathbb{Z}) = \emptyset$$

недоказуемо в $\mathfrak{S}$ без привлечения дополнительной аксиомы о существовании достаточно больших кардиналов.

Обозначим через $\mathfrak{P}$ кольцо полиномов с целыми рациональными коэффициентами и через $\mu(P),\ P \in \mathfrak{P}$, число переменных полинома P. Как известно, существует полином $U(u,v,x_1,...,x_9)$ такой, что $U \in \mathfrak{P}$ и, при подходящей нумерации полиномов $\nu\colon \mathfrak{P} \to \mathbb{N}$, имеет место соотношение

$$\{a | a \in \mathbb{N},\ (\exists\, b \in \mathbb{Z}^{\mu(P)-1}) P(a,b) = 0\} =$$

$$\{a | a \in \mathbb{N},\ (\exists\, b \in \mathbb{Z}^{9}) U(\nu(P),a,b) = 0\} \text{ при } P \in \mathfrak{P};$$

полином U называется *"универсальным полиномом"* (ср. [24, гл. 4], [34, §6]). В частности,

$$\mathcal{N}(\mathfrak{T}) = \{a | a \in \mathbb{N},\ (\exists\, b \in \mathbb{Z}^{9}) U(\nu(f),a,b) = 0\};$$

разумеется, полином $U(\nu(f),v,x_1,...,x_9)$ от 10-ти переменных не "проще" нашего полинома $f(t,x)$ от 14518113-ти переменных.

Заключение

Остановимся ещё раз на некоторых из обсуждавшихся в диссертации результатах.

Глава первая. В этой главе описывается аналитическое поведение скалярных произведений L - рядов Артина - Вейля. Вопрос о продолжимости L - функций Дракcла [68], отличных от скалярных произведений
L - рядов Гекке, в правую полуплоскость $\mathbb{C} \setminus \mathbb{C}_0$ остаётся открытым.

Глава вторая. Затронутые в этой главе вопросы заслуживают дальнейшего рассмотрения. Две открытые проблемы:

1) Дать явное описание моделей Нерона алгебраических торов, определённых над полем алгебраических чисел и не расщепимых над расширениями без высшего ветвления.

2) Описать целые модели определённого над полем алгебраических чисел аффинного торического многообразия и изучить распределение целых точек на этих моделях.

Глава третья. Доказать бесконечность множества $\mathcal{P} \cap \{n^2+1 | n \in \mathbb{N}\}$ (простейший нелинейный случай гипотезы Буняковского) в настоящее время, вероятно, невозможно. В этой ситуации представляет интерес перенесение методов этой главы на неполные норменные формы более высоких степеней (ср. [95, стр. 3]).

Глава четвёртая. В первой из коротких заметок рассматриваются классические задачи о распределенни степенных вычетов и невычетов; для этих задач получены асимптотические формулы с неулучшаемым остаточным членом. Безусловное (без предположения о справедливости гипотезы Римана) доказательство асимптотической формулы со степенным понижением для числа точек с взаимно простыми координатами в плоской "звёздообразной"области

пока не получено (ср. §1.2). Исследования числа рациональных точек ограниченной высоты на многообразиях Фано ("гипотеза Батырева - Манина") есть богатая бурно развивающаяся область диофантовой геометрии; полученная в третьей заметке асимптотическая формула - один из первых результатов в этой области. В связи с рассматриваемыми в четвёртой заметке задачами аналитической теории квадратичных форм следует заметить, что задача о распределении целых точек на двумерных гиперболоидах в общем случае пока не решена (см., однако, [17], [3], [55], [69], [70]). Рассматриваемая в пятой заметке проблема модулярности эллиптических кривых, определённых над мнимыми квадратичными полями, есть важная открытая проблема арифметической геометрии. Как уже отмечалась, наши рассмотрения в шестой заметке уточняют формулировку классической теоремы Берча [49] о разрешимости диофантовых уравнений с большим числом переменных. Описанные в седьмой заметке полиномы позволяют в принципе свести любую математическую проблему к разрешимости некоторого диофантова уравнения.

Тема этой работы лежит в предгорьях горного массива геометрии Аракелова, ставящей своей целью синтез алгебраических и аналитических методов изучения диофантовых проблем. Если читатель, побродив по предгорьям и ознакомившись, в частности, с моей работой, пойдёт наверх, в горы, как это пытаюсь сделать я, значит, мой труд не пропал даром.

Литература

1. Н. Бурбаки, *Алгебра. Часть 3. Модули, кольца, формы,* Наука, Москва, 1966.
2. Н. Бурбаки, *Коммутативная алгебра,* Москва, Мир, 1971.
3. В.А. Быковский, Формула следа для скалярного произведения рядов Гекке и её приложения, *Записки научных семинаров ЛОМИ,* 226 (1996), 144 - 153.
4. А.И. Виноградов, О продолжимости в левую полуплоскость скалярного произведения L - рядов Гекке с характерами величины, *Известия АН СССР. Серия матем.* 29:4 (1965), 485 - 492.
5. В.Е. Воскресенский, *Алгебраические торы,* Наука, Москва, 1977.
6. В.Е. Воскресенский, Б.Э. Кунявский, Б.З. Мороз, О целых моделях алгебраических торов, *Алгебра и анализ,* 14 (2002), вып. 1, 46-70.
7. Э. Гайгалас, Распределение простых идеалов в двух мнимых квадратичных полях, I, II, *Литовский математический сборник,* 19:2 (1979), 45 - 60 и 19:4 (1979), 65 -76.
8. А.О. Гельфонд, Ю.В. Линник, *Элементарные методы в аналитической теории чисел,* Физматгиз, Москва, 1962.
9. Е.П. Голубева, О.М. Фоменко, Асимтотическое распределение целых точек на двумерной сфере, *Записки научных семинаров ЛОМИ,* 160 (1987), 54 - 71.
10. Е.П. Голубева, О.М. Фоменко, Замечание об асимтотическом распределении целых точек на большой двумерной сфере, *Записки научных семинаров ЛОМИ,* 185 (1990), 22 - 28.
11. В.А. Гриценко, Частное сообщение, Июнь 2015 г.
12. Т. Клебергер, Б.З. Мороз, Группы Андре Вейля и распределение простых идеалов, *Труды МИАН,* 296(2017), 140-149.

13. И.П. Кубилюс, О некоторых задачах геометрии простых чисел, *Математический сборник,* 31(73):3 (1952), 507-542.

14. Б.Э. Кунявский, Б.З. Мороз, О целых моделях аффинных торических многообразий, *Труды СПбМО,* 7 (1999), 116-123.

15. Б.Э. Кунявский, Б.З. Мороз, О целых моделях алгебраических торов и аффинных торических многообразий, *Труды СПбМО,* 13 (2007), 97-119.

16. Ю.В. Линник, Частное сообщение, Март 1962 г.

17. Ю.В. Линник, *Эргодические свойства алгебраических полей,* Издательство Ленинградского университета, 1967.

18. Ю.В. Линник, *Избранные труды. Теория чисел. Эргодический метод и L-функции,* Наука, Ленинград, 1979.

19. А.В. Малышев, О представлении целых чисел положительными квадратичными формами, *Труды МИАН СССР,* 65 (1962).

20. А.В. Малышев, О взвешенном количестве целых точек, лежащих на поверхности второго порядка, *Записки научных семинаров ЛОМИ,* 1 (1966), 6 - 83.

21. А.В. Малышев, Дискретный эргодический метод Ю.В. Линника и его дальнейшее развитие, [18, стр. 418 - 430].

22. Ю.В. Матиясевич, Диофантовость перечислимых предикатов, *Доклады АН СССР,* 191:2 (1970), 279-282.

23. Ю.В. Матиясевич, Диофантово представление перечислимых предикатов, *Известия АН СССР. Серия математическая,* 35:1 (1971), 3-30.

24. Ю.В. Матиясевич, *Десятая проблема Гильберта,* Наука, Москва, 1993.

25. Б.З. Мороз, О распределении степенных вычетов и невычетов, *Вестник ЛГУ,* 16 (1961), no. 19, 164 - 169.

26. Б.З. Мороз, Аналитическое продолжение скалярного произведения рядов Гекке двух квадратичных полей и его применение, *ДАН СССР,* 150:4 (1963), стр. 752-754.

27. Б.З. Мороз, О продолжимости скалярного произведения рядов Гекке двух квадратичных полей, *ДАН СССР,* 155:6 (1964), стр. 1265-1267.

28. Б.З. Мороз, Аналитические задачи, связанные с абелевыми полями, Диссертация на соискание учёной степени кандидата физико-математических наук, Ленинград, 1964.

29. Б.З. Мороз, Композиция бинарных квадратичных форм и скалярное произведение рядов Гекке, *Труды МИАН СССР,* 80 (1965), 102 - 109.

30. Б.З. Мороз, О распределении пар простых дивизоров двух квадратичных полей I, II, *Вестник ЛГУ,* 19:4 (1965), 47 - 57 и 1:1 (1966), 64 - 79.

31. Б.З. Мороз, Распределение целых точек на многомерных гиперболоидах и конусах, *Записки научных семинаров ЛОМИ,* 1 (1966), 84 - 113.

32. Б.З. Мороз, О дзета-функциях полей алгебраических чисел, *Математические заметки,* 4(1968), 333-339.

33. Б.З. Мороз, О представлении простых чисел полиномами (обзор последних результатов), *Труды института математики НАН Беларуси,* 13:1 (2005), 114-119.

34. Б.З. Мороз, *Диофантовы уравнения и доказуемость в математике,* МЦНМО, Москва, 2008.

35. Б.З. Мороз, *Аналитические задачи в алгебраической теории чисел и диофантовой геометрии,* МЦНМО, Москва, 2017.

36. Н.В. Проскурин, Формулы суммирования для общих сумм Клостермана, *Записки научных семинаров ЛОМИ,* 82 (1979), 103 - 135.

37. Ж.-П. Серр, *Линейные представления конечных групп,* Мир, Москва, 1970.

38. Ж.-П. Серр, *Абелевы l-адические представления и эллиптические кривые,* Мир, Москва, 1973.

39. Е. Титчмарш, *Теория функций,* Наука, Москва, 1980.

40. Дж. Тэйт, Теоретико-числовое введение, *Автоморфные формы, представления и L-функции, стр.* 73 - 112, Мир, Москва, 1984.

41. О.М. Фоменко, Продолжимость на всю плоскость и функциональное уравнение скалярного произведения L - рядов Гекке двух квадратичных полей, *Труды МИАН СССР,* 128 (1972), 232 - 241.

42. О.М. Фоменко, О равномерном распределении целых точек на многомерных эллипсоидах, *Записки научных семинаров ЛОМИ,* 154 (1986), 144 - 153.

43. A.G. Aleksandrov, B.Z. Moroz, Complete intersections in relation to a paper of B. J. Birch, *Bulletin of the London Mathematical Society,* 34 (2002), 149-154.

44. K. Atkinson, W. Han, Spherical harmonics and approximation on the unit sphere: an introducton, *Lecture Notes in Mathematics,* 2044 (2012), Springer - Verlag.

45. A. Axer, Über einige Grenzsätze, *Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Mathematisch-Naturwissenschafte Klasse,* 120, Abt. IIa (1911), 271 - 283.

46. V.V. Batyrev, Yu.I. Manin, Sur le nombre des points rationnels de hauteur borné des variétés algébriques, *Mathematische Annalen,* 286 (1990), 27 - 43.

47. B. Blomer, Uniform bounds for Fourier coefficients of theta-series with arithmetic applications, *Acta Arithmetica,* 114 (2004), 1 - 21.

48. T. Berger, G. Harcos, l-adic representations associated to modular forms over imaginary quadratic fields, *International Math. Research Notices,* 2007, no. 23, 16 pp.

49. B.J. Birch, Forms in many variables, *Proceedings of the Royal Society, Series A,* 265 (1961/1962), 245 - 263.

50. M. Bondarko, Ideals in an extension of a number field as modules over the ring of untegers in a ground field, in: Proceedings of the Session in analytic

number theory and Diophantine equations (ed. by D.R. Heath-Brown and B.Z. Moroz), *Bonner Math. Schriften,* 360 (2003).

51. S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models,* Springer-Verlag, Berlin, 1990.
52. N. Bourbaki, *Algébra, chapitre 10, Algébra homologique,* Masson, Paris, 1980.
53. R. de la Bretèche, Sur le nombre de points de hauteur borné d'une certaine surface cubique singulière, Astérisque, 251 (1998), 51 - 77.
54. C. Breuil, C. Brian, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *Journal of the American Math. Society*, 14 (2001), 843-939.
55. V.A. Bykovskii, Uniform distribution of integral points on hyperboloids, *Аналитические методы в теории чисел,теории вероятностей и математической статистике (Тезисы докладов),* Санкт-Петербург, 2005, 12-13 .
56. M. Carl, *Formale Mathematik und diophantische Gleichungen,* Diplomarbeit, Universität Bonn, 2007.
57. M. Carl, B.Z. Moroz, On a Diophantine representation of the predicate of provability, *Записки научных семинаров ПОМИ,* 407 (2012), 77 - 104.
58. M. Carl, B.Z. Moroz, A polynomial encoding provability in pure mathematics (outline of an explicit construction), *Bulletin of the Belgian Mathematical Society,* 20 (2013), 181-187.
59. B.A. Cipra, On the Niwa-Shintani theta-kernel lifting of modular forms, *Nagoya Mathematical Journal,* 91 (1983), 49 - 117.
60. H. Cohen, *Advanced topics in Computational Number Theory,* Springer-Verlag, 2000.
61. H. Davenport, On character sums in finite fields, *Acta Mathematica,* 71 (1939), 99 - 121.

62. M. Davis, Yu. Matijasevič, Ju. Robinson, Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution, *Proceedings of Symposia in Pure Mathematics,* 28 (1976), 323-378.

63. P. Deligne, La conjecture de Weil. I. *Publications Mathématiques de l'I.H.E.S.,* 43 (1974), 273 - 307.

64. P. Deligne, J-P. Serre, Formes modulaires de poids 1. *Annales scientifiques de l'École Normale Supérieure, Sér. 4,* 7 (1974), 507 - 530.

65. L.E. Dickson, *History of the theory of numbers,* vol. 1, Chelsea Publ. Company, New York, 1952.

66. L. Dieulefait, L. Guerberoff, A. Pacetti, Proving modularity for a given elliptic curve over an imaginary quadratic field, *Mathematics of Computation,* 79 (2010), 1145-1170.

67. L.V. Dieulefait, M. Mink, B.Z. Moroz, On an elliptic curve defined over $\mathbb{Q}(\sqrt{-23})$, *Алгебра и Анализ,* 24:4 (2012), 64 - 83.

68. P.K.J. Draxl, L-Funktionen algebraischer Tori, *Journal of Number Theory,* 3 (1971), 444–467.

69. W. Duke, Hyperbolic distribution problems and half-integral weight Maass forms, *Inventiones Mathematicae,* 92 (1988), 73 - 90.

70. W. Duke, J.B. Friedlander, and H. Iwaniec, Weyl sums for quadratic roots, *International Mathematics Research Notices,* 2012, no. 11, 2493 - 2549.

71. W. Duke, R. Schulze-Pillot, Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids, *Inventiones Mathematicae,* 99 (1990), 49 - 57.

72. V.H. Dyson, J.P. Jones, J.C. Shepherdson, Some Diophantine forms of Gödel's theorem, *Archiv für Mathematische Logik und Grundlagenforschung,* 22 (1982), no. 1-2, 51-60.

73. B. Edixhoven, Néron models and tame ramification, *Compositio Mathematica,* 81 (1992), 291-306.

74. D. Eisenbud, *Commutative algebra with a view towards algebraic geometry,* Graduate texts in mathematics, no. 150, Springer-Verlag, 1995.

75. T. Estermann, On certain functions represented by Dirichlet series, *Proceedings of the London Mathematical Society,* 27 (1928), 435 - 448.

76. G. Faltings, Endlichkeitssätze für abelsche Varietätet über Zahlkörpern, *Invent. Math.,* 73 (1983), 349-366.

77. A. Felikson, P. Tumarkin, On the volume of a six-dimensional polytope, *arXiv:math/0502167v1[math.MG],* 8 Feb 2005.

78. E. Fouvry, H. Iwaniec, Gaussian primes, *Acta Arithmetica*, 79 (1997), 249-387.

79. N. Freitas, B.V. Le Hung, S. Siksek, Elliptic curves over real quadratic fields are modular, arXiv:1310.7088, 13 Nov. 2013.

80. J. Friedlander, H. Iwaniec, Using a parity-sensitive sieve to count prime values of a polynomial, *Proceedings of the National Academy of Sciences of the USA* 94 (1997), 1054-1058.

81. J. Friedlander, H. Iwaniec, The polynomial $X^2 + Y^4$ captures its primes, *Annals of Mathematics,* 148 (1998), 945-1040.

82. J. Friedlander, H. Iwaniec, Asymptotic sieve for primes, *Annals of Mathematics,* 148 (1998), 1041-1065.

83. A. Fröhlich, M. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1991.

84. W. Fulton, *Introduction to toric varieties,* Annals of Mathematics Studies, no. 131, Princeton University Press, Princeton, NJ, 1993.

85. K. Gödel, *The consistency of the axiom of choice and of the generalised continuum hypothesis with the axioms of set theory,* Princeton University Press, 1940.

86. A. Grothendieck, Technique de descente et théorèmes d'existence en géométrie algébrique. I.Généralités. Descente par morphismes fidèlement plats, *Séminaire Bourbaki, 12e année,* 1959/60, no. 190.

87. J. Hadamard, Théorème sur les séries entières, *Acta Mathematica,* 22 (1899), 55 - 63.

88. H. Halberstam, H.-E. Richert, Sieve methods, *London Mathematical Society Monographs series*, 4 (1974), Academic Press, London.

89. G. Harman, Prime-detecting sieves, *London Mathematical Society Monographs series*, 33 (2007), Princeton University Press, Princeton, New Jersey.

90. R. Hartshorne, *Algebraic geometry,* Springer-Verlag, 1977.

91. H. Hasse, Zetafunktionen und L-Funktionen zu einem arithmetischen Funktionenkörper von Fermatschen Typus, Abhandlungen Deutscher Akademie der Wissenschaften, Berlin, Kl. Mathem.-Nat., no. 4 (1954), 70 pp.

92. D.R. Heath-Brown, Ternary quadratic forms and sums of three square-full numbers, *Séminare de Théorie des Nombres, Paris 1986-87*, Birhäuser, Boston/Basel, 1988, 137 - 163.

93. D.R. Heath-Brown, A new form of the circle method, and its application to quadratic forms, *Journal für die reine und angewandte Mathematik,* 481 (1996), 149 - 206.

94. D.R. Heath-Brown, The solubility of diagonal cubic Diophantine equations, *Proceedings of the London Mathematical Society (3),* 79 (1999), 241-259.

95. D.R. Heath-Brown, Primes represented by $x^3 + 2y^3$, *Acta Mathematica,* 186 (2001), 1-84.

96. D.R. Heath-Brown, B.Z. Moroz, The density of rational points on the cubic surface $X_0^3 = X_1X_2X_3$, *Mathematical Proceedings of the Cambridge Philosophical Society,* 125 (1999), 385 - 395.

97. D.R. Heath-Brown, B.Z. Moroz, Primes represented by binary cubic forms, *Proceedings of the London Mathematical Society (3),* 84 (2002), 257-288.

98. D.R. Heath-Brown, B.Z. Moroz, On the representation of primes by cubic polynomials in two variables, *Proceedings of the London Mathematical Society (3),* 88 (2004), 289-312.

99. E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen (zweite Mitteilung), *Mathematische Zeitschrift,* 6 (1920), 11 -51.

100. M.N. Huxley, Exponential sums and lattice points II, *Proceedings of the London Mathematical Society,* 66 (1993), 279 - 301.

101. M.N. Huxley, W.G. Nowak, Primitive lattice points in convex planar domains, *Acta Arithmetica,* 76 (1996), 271 - 283.

102. H. Iwaniec, Primes represented by quadratic polynomials in two variables, *Acta Arithmetica*, 24 (1974), 435-322.

103. H. Iwaniec, Fourier coefficients of modular forms of half-integral weight, *Inventiones Mathematicae,* 87 (1987), 385 - 401.

104. H. Iwaniec *Topics in classical theory of automorphic forms,* American Mathematical Society, Providence, RI, 1997.

105. H. Iwaniec, E. Kowalski, *Analytic number theory,* American Mathematical Society, Providence, RI, 2004.

106. H. Jacquet, J.A. Shalika, On Euler products and the classification of automorphic representations, I, *American Journal of Mathematics,* 103 (1981), 499-558.

107. N. Kurokawa, On the meromorphy of Euler products, *Proceedings of the Japan Academy,* 54A (1978), 163–166.

108. N. Kurokawa, On Linnik's problem, *Proceedings of the Japan Academy,* 54A (1978), 167–169.

109. N. Kurokawa, On the meromorphy of Euler products, I, II, *Proceedings of the London Mathematical Society,* 53 (1986), 1–47 and 209-236.

110. E. Landau, A. Walfisz, Über die Nichtforsetzbarkeit einiger durch Dirichletsche Reihen definierter Funktionen, *Rendiconti di Palermo,* 44 (1920), 82–86.

111. W.-Ch. W. Li, B.Z. Moroz, On ideal classes of number fields containing integral ideals of equal norms, *Journal of Number Theory,* 21 (1985), 185-203.

112. M. Lingham, Modular forms and elliptic curves over imaginary quadratic fields, Ph.D. Thesis, University of Nottingham, 2005.

113. Q. Liu, D. Lorenzini, Special fibers of Néron models and wild ramification, *Journal für die reine und angewandte Mathematik,* 532 (2001), 179-222.

114. P. Llorente, E. Nart, Effective determination of the decomposition of the rational primes in a cubic field, *Proceedings of the American Mathematical Society*, 87 (1983), 579-585.

115. G.W. Mackey, Induced representations of locally compact groups, I *Annals of Mathematics,* 55 (1952), 101–139.

116. W. Magnus, F. Oberhettinger, R.P. Soni, *Formulas and theorems for the special functions of mathematical physics,* Springer-Verlag, 1966.

117. H. Matsumura, *Commutative ring theory,* Cambridge studies in advanced mathematics, no. 8, Cambridge University Press, 1989.

118. E. Mendelson, *Introduction to Mathematical Logic,* Chapman & Hall/CRM, 2001.

119. M. Mink, Beweis der Hasse - Weilschen Vermutung für eine elliptische Kurve über einem imaginär-quadratischen Körper, *Diplomarbeit, Rheinische Friedrich-Wilhems-Universität Bonn*, 2010.

120. T. Mitsui, Generalised prime number theorem, *Japanese Journal of Mathematics,* 26 (1956), 1-42.

121. B.Z. Moroz, On the convolution of L-functions, *Mathematika,* 27 (1980), 312 - 320.

122. B.Z. Moroz, Euler products (variation on a theme of Kurokawa's), *Astérisque,* 94 (1982), 143 - 151.

123. B. Z. Moroz, Scalar product of L-functions with Größencharacters: its meromorphic continuation and natural boundary, *Journal für die reine und angewandte Mathematik,* 332 (1982), 99 - 117.

124. B.Z. Moroz, Vistas in analytic number theory, *Bonner Mathematische Schriften,* 156 (1984), Universität Bonn.

125. B.Z. Moroz, On the distribution of integral and prime ideals with equal norm, Annales de l'Institut Fourier, 34 (1984), fasc. 4, 1-17.

126. B.Z. Moroz, On the number of primitive lattice points in plane domains, *Monatshefte für Mathematik,* 99 (1985), 37 - 42.

127. Produits eulériens sur les corps de nombres, *Comptes Rendus de l'Académie des Sciences (Paris), Série I,* 301 (1985), no. 10, 459-462.

128. B.Z. Moroz, Analytic arithmetic in algebraic number fields, *Lecture Notes in Mathematics,* 1205 (1986), Springer - Verlag.

129. B.Z. Moroz, Integral points on norm-form varieties, *Journal of Number Theory,* 24 (1986), 272-283.

130. B.Z. Moroz, On the number of integral points on a norm-form variety in a cube-like domain, *Journal of Number Theory,* 27 (1987), 106-110.

131. B.Z. Moroz, Estimates for character sums in number fields, *Israel Journal of Mathematics,* 60 (1987), 1-21.

132. B.Z. Moroz, Equidistribution of Frobenius classes and the volumes of tubes, *Acta Arithmetica,* 51 (1988), 269 - 276.

133. B.Z. Moroz, On a class of Dirichlet series associated to the ring of representations of a Weil group, *Proceedings of the London Mathematical Society,* 56 (1988), 209 - 228.

134. B.Z. Moroz, Recent progress in analytic arithmetic of positive definite quadratic forms, *MPIM Preprint,* 89-50 (1989).

135. B.Z. Moroz, On the representation of large integers by integral ternary positive definite quadratic forms *Astérisque,* 209 (1992), 275 - 278.

136. B.Z. Moroz, On the distribution of integral points on an algebraic torus defined by a system of norm-form equations, *Quarterly Journal of Mathematics,* 45 (1994), 243-253.

137. B.Z. Moroz, Exercises in analytic arithmetic on an algebraic torus, Israel Mathematical Conferences Proceedings (F. Hirzebruch Festband), 9 (1996), 347-359.

138. B.Z. Moroz, On the integer points of some toric varieties, *Quarterly Journal of Mathematics,* 48 (1997), 67-82.

139. B.Z. Moroz, On the distribution of integer points in the real locus of an affine toric variety, Lecture Notes of the London Mathematical Society, 237 (1997), 283-292.

140. B.Z. Moroz, On the integer points of an affine toric variety (general case), *Quarterly Journal of Mathematics,* 50 (1999), 37-47.

141. W.D. Neumann, D.B. Zagier, Volumes of hyperbolic three manifolds, *Topology,* 24 (1985), 307 - 332.

142. W.G. Nowak, Primitive lattice points in starlike planar sets, *Pacific Journal of Mathematics,* 179 (1997), 163 - 178.

143. T. Oda, *Lectures on torus embeddings and applications*, Tata Institute of Fundamental Research, Bombay, 1978.

144. The PARI Group (Bordeaux), *PARI/GP*, version 2.4.3.

145. E. Peyre, Hauteurs et nombres de Tamagawa sur les variétés de Fano, Duke Mathematical Journal, 79 (1995), 101 - 217.

146. W. Pfetzer, Die Wirkung der Modulsubstitutionen auf mehrfache Thetareihen zu quadratischen Formen ungerader Variablenzahl, *Archiv der Mathematik,* 4 (1953), 448 - 454.

147. I.J. Piatetski-Shapiro, Multiplicity one theorems, *Proceedings symposia in pure mathematics,* 33 (1979), Part 1, 209-212.

148. R.A. Rankin *Modular forms and functions,* Cambridge University Press, Cambridge, 1977.

149. P. Satgé, Un analogue du calcul de Heegner, *Invent. Math.,* 87 (1987), 425-439.

150. A. Schinzel, On the relation between two conjectures on polynomials, *Acta Arithmetica*, 38 (1981), 285-322.

151. R. Schulze-Pillot, Thetareihen positiv definiter quadratischer formen, *Inventiones Mathematicae,* 75 (1984), 283 - 299.

152. M. Schütt, On the modularity of Calabi-Yau threefolds with bad reduction at 11, *Canad. Math. Bull.*, 49 (2006), 296-312.

153. M.H. Sengun, Arithmetic aspects of Bianchi groups, in: *G. Böckle, G. Wiese, (eds.), Computations with modular forms,* Springer (2014), 279-315.

154. J-P. Serre, Facteurs locaux des fonctions $\hat{z}$eta des variétés algébriques (définitions et conjectures), *Séminaire Delange-Pisot-Poitou, Théoire des nombres*, t. 11, n^0 2 (1969/70), exp. n^0 19, p. 1-15.

155. J-P. Serre, Résume des cours de 1984-1985, *Annuaire du Collége de France* (1985), 85-90.

156. J-P. Serre, Représentations linéaires sur des anneaux locaux, d'apres Carayol, *Prépubl. Inst. Math. Jussieu,* no. 49 (1995).

157. G. Shimura, On modular forms of half-integral weight, *Annals of Mathematics,* 97 (1973), 440 - 481.

158. J.-M. Shyr, A generalization of Dirichlet's unit theorem, *Journal of Number Theory,* 9 (1977), 213-217.

159. C.L. Siegel, Über die analytische Theorie der quadratischen Formen, *Annals of Mathematics,* 36 (1935), 527 - 606.

160. R.P. Stanley, Linear homogeneous Diophantine equations and magic labelings of graphs, *Duke Mathematical Journal,* 40 (1973), 607-632.

161. P. Swinnerton-Dyer, The solubility of diagonal cubic surfaces, *Annales Scientifiques de l'École Normale Supérieure (4),* 34 (2001), no. 6, 891-912.

162. R. Taylor, l-adic representations associated to modular forms over imaginary quadratic fields. II, *Inventiones Mathematicae,* 116 (1994), 619-643.

163. E.C. Titchmarsh, *The theory of the Riemann zeta-function,* Oxford University Press, 1986.

164. V.E. Voskresenskii, *Algebraic groups and their birational invariants*, American Mathematical Society, Translations of mathematical monographs, 179 (1998).

165. A. Weil, On some exponential sums, *Proceedings of the National Academy of Sciences of the USA,* 34 (1948), 204 - 207.

166. A. Weil, Sur la théorie du corps de classes, *Journal of the Mathematical Society of Japan,* 3 (1951), 1 - 35.

167. A. Weil, *Dirichlet series and automorphic forms,* Lecture Notes in Mathematics, 189 (1971), Springer-Verlag.

168. A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics,* 141 (1995), 443-451.

169. Y. Yomdin, Metric properties of semialgebraic sets and mappings and their applications, *Géométrie algébrique et applcations, III (La Rábida),* Hermann, Paris, 1987, 165-183.

170. Y. Yomdin, Metric semialgebraic geometry with applications in smooth analysis, *Preprint,* 1987.

171. D.B. Zagier, On the number of Markoff numbers below a given boundary, *Mathematics of Computation,* 39 (1982), 709 - 723.